MINISTERIO
DE EMPLEO
Y SEGURIDAD SOCIAL

SUBSECRETARÍA

S.G. DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIONES

Declaración de Prácticas de Certificación del Prestador de Servicios de Certificación del Ministerio

sgtic@meyss.es
E03721106

C/ PASEO DE LA CASTELLANA 63
28071 MADRID
TEL: 91 363.11.88
FAX: 91 363.07.73

Control de versiones

Identificador	D003
Título	Declaración de Prácticas de Certificación del Prestador de Servicios de Certificación del Ministerio
Versión	02
Estado del documento	Aprobado
Fecha de aprobación	12.06.2017
Fecha de caducidad	12.06.2018
OID	1.3.6.1.4.1.27781.2.3.1

Registro de Cambios

Versión	Fecha	Comentario
1.0	05.11.2009	Versión final del documento
1.1	29.03.2010	Cambios en el número ISO/IANA del MPR e Identificador de Objeto (OID) de los certificados emitidos por el PSCMTIN
1.2	10.09.2010	Cambio encabezado eliminando DG Servicios Añadidos apartados del art. 21 LFE en el apartado 5.8
1.3	07.04.2011	Cambios en el número del Identificador de Objeto (OID) del certificado OCSP. Desaparición de la restricción del OCSP no Check
1.4	16.02.2012	Actualización de los OID
1.5	10.08.2012	Actualización estructura organizativa. Nuevo formato del documento editable. Añadido anexo C.
1.6	21.03.2014	Añadido Perfil de Certificado de Empleado Público Centralizado y Gestionado por un HSM
1.7	04.07.2014	Se suprime el Anexo B El anexo C pasa a ser anexo B con una redacción nueva para las CRL históricas Se elimina de las referencias el Esquema de Identificación y firma electrónica de las AAPP Nueva redacción de los apartados 4.9.3, 6.1.1 y 6.2.1
1.8	18.06.2015	Se añade SHA-256
1.9	18.03.2016	Actualizada la normativa aplicable
1.10	30.05.2016	Corregidos errores tipográficos menores Eliminada referencia a SHA-1
1.11	13.03.2017	Añadidas nueva CA Raíz y SubCA y URL asociadas Actualizados servicios cualificados ofrecidos
02	12.06.2017	Cambios auditoría eiDAS Añadida sección 1.7

Tabla de contenidos abreviada

Tabla de contenidos

1 Introducción

El Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, más conocido como eIDAS, contempla la posibilidad de erigirse como Prestador Cualificado de Servicios de Confianza y, junto con las normas europeas ETSI EN 319 401 (sobre Prestadores de Servicios de Confianza), ETSI EN 319 411-1 (sobre la emisión de certificados), ETSI EN 319 411-2 (sobre la emisión de certificados cualificados), recoge los requisitos necesarios para ello.

El presente documento recoge la **Declaración de las Prácticas de Certificación del Prestador de Servicios de Confianza del Ministerio de Empleo y Seguridad Social (PSCM)**, desde ahora, DPCM.

La DPCM detalla las obligaciones que el PSCM se compromete a cumplir en relación con las medidas de seguridad técnicas y organizativas; las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados electrónicos; la gestión de los datos de creación y verificación de firma electrónica y de los certificados electrónicos; los perfiles de los certificados y los mecanismos de información sobre su vigencia.

La DPCM se ha redactado conforme a las especificaciones de la [IETF RFC 3647]. Para su correcta lectura se recomienda cierto conocimiento general de los conceptos de PKI, certificado electrónico y firma electrónica.

La DPCM se encuentra publicada en la URL que aparece en el Anexo B: Enlaces (URL).

1.1 Presentación

En el ámbito de la presente DPCM y de la política específica para cada certificado, el PSCM emite, revoca y ofrece información de validación de los siguientes tipos de certificados:

Certificado Cualificado	Soporte	Nivel aseguramiento eIDAS	Propósito
Empleado Público	Tarjeta	Alto	Firma electrónica Autenticación
Empleado Público	HSM	Sustancial (medio)	Firma electrónica Autenticación
Sello Electrónico	Contenedor	Sustancial (medio)	Firma electrónica

Las especificidades relativas a cada tipo de certificado emitido por el PSCM están reguladas en la política (perfil) específica para cada certificado.

1.1.1 Relación entre la DPCM y otros documentos

La DPCM se complementa con los documentos que describen los perfiles de los certificados.

1.2 Nombre del documento e identificación

Este documento se denomina **Declaración de Prácticas de Certificación del PSCM**, con la información reflejada en el control de versiones del documento (pág. ii).

La DPCM se encuentra publicada en la URL que aparece en el Anexo B: Enlaces (URL).

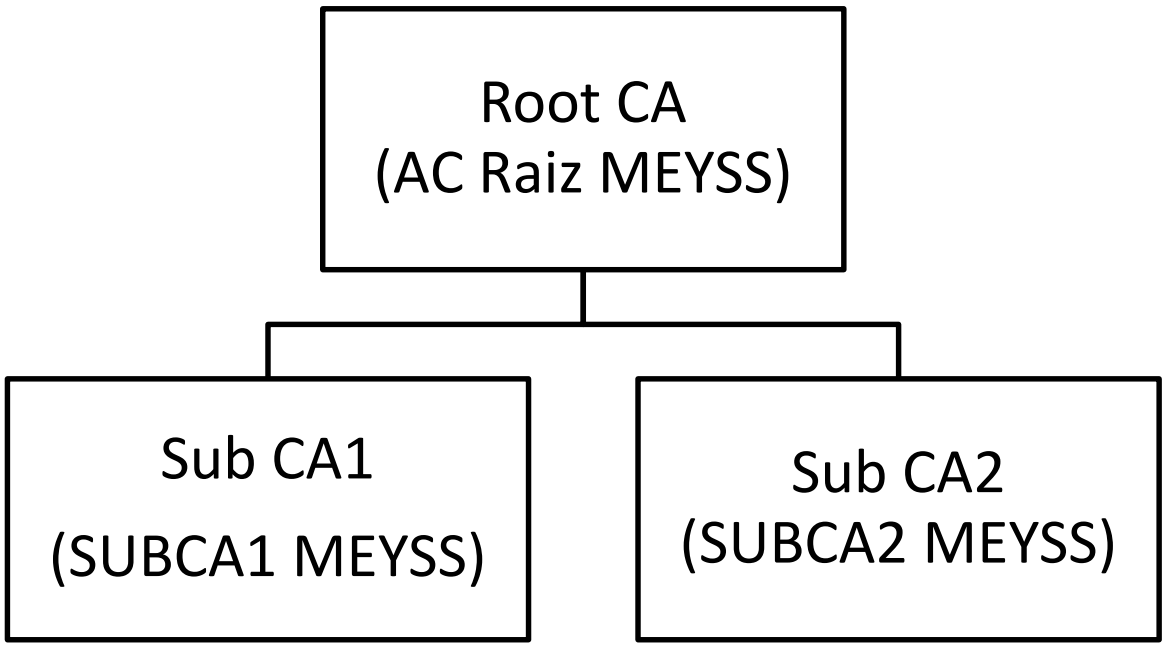
1.3 Participantes en los servicios de certificación

Los participantes en los servicios de certificación que intervienen en el Prestador de Servicios de Confianza son los siguientes:

- La Entidad de Certificación.
- Las Entidades de Registro.
- La Entidad de Validación.
- Los suscriptores (usuarios) de los certificados.

1.3.1 Entidad de Certificación

La Entidad de Certificación está compuesta de una Autoridad de Certificación Raíz y de Autoridades de Certificación Subordinadas.



Root CA = Autoridad de Certificación Raíz.

SubCA1 = Autoridad de Certificación Subordinada para la emisión de certificados de sello electrónico y de los CEPCHSM (certificados electrónicos de empleado público centralizados y gestionados por un HSM).

SubCA2 = Autoridad de Certificación Subordinada para la emisión de certificados de empleado público en tarjeta inteligente (qscd).

Los datos del certificado de la Autoridad de Certificación Raíz son los siguientes:

Emisor	CN = AC RAIZ MEYSS 2.5.4.97 = VATES-S2819001E SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS OU = S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL L = MADRID C = ES
Titular	CN = AC RAIZ MEYSS 2.5.4.97 = VATES-S2819001E SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS OU = S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL L = MADRID C = ES
Número de Serie	58 41 50 86
Periodo de Validez	viernes, 02 de diciembre de 2016 11:14:28 domingo, 02 de diciembre de 2046 11:44:28
Función resumen del certificado	sha1 28 56 1D 3F 12 2A B1 F1 16 31 DE AF A3 E0 50 BB 51 FE A4 D2

Los datos del certificado de la Autoridad de Certificación Subordinada 1 para los certificados de empleado público centralizados y gestionados por un HSM y certificados de sello electrónico son los siguientes:

Emisor	CN = AC RAIZ MEYSS 2.5.4.97 = VATES-S2819001E SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS OU = S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL L = MADRID C = ES
Titular	CN = SUBCA1 MEYSS 2.5.4.97 = VATES-S2819001E SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS OU = S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL L = MADRID C = ES
Número de Serie	58 41 50 C1
Periodo de Validez	viernes, 02 de diciembre de 2016 12:26:29 martes, 02 de diciembre de 2036 12:56:29
Función resumen del certificado	sha1 E2 CB BC 57 AD 98 42 0C 34 7D A7 C2 57 79 5D C5 FD C5 FD 27

Los datos del certificado de la Autoridad de Certificación Subordinada 2 para los certificados de empleado público en tarjeta inteligente son los siguientes:

Emisor	CN = AC RAIZ MEYSS 2.5.4.97 = VATES-S2819001E SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS OU = S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL L = MADRID C = ES
Titular	CN = SUBCA2 MEYSS 2.5.4.97 = VATES-S2819001E SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS OU = S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL L = MADRID C = ES
Número de Serie	58 41 50 C2
Periodo de Validez	viernes, 02 de diciembre de 2016 12:52:49 martes, 02 de diciembre de 2036 13:22:49
Función resumen del certificado	sha1 02 1C E9 FB 78 00 CF DD 58 31 BF 89 69 8D 82 5F 4E D2 0D 29

Por razones históricas de validación, los datos del anterior certificado raíz son los siguientes:

Versión SHA-256:

Emisor	CN = AC1 RAIZ MTIN SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN OU = SUBDIRECCION GENERAL DE PROCESO DE DATOS O = MINISTERIO DE TRABAJO E INMIGRACION L = MADRID C = ES
Titular	CN = AC1 RAIZ MTIN SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN OU = SUBDIRECCION GENERAL DE PROCESO DE DATOS O = MINISTERIO DE TRABAJO E INMIGRACION L = MADRID C = ES
Número de Serie	12 1c 2e 70 09 a0 97 a6
Periodo de Validez	jueves, 05 de noviembre de 2009 17:17:45 domingo, 03 de noviembre de 2019 17:17:45
Función resumen del certificado	sha1 0e 9e 4f 47 68 6e b0 37 49 56 a0 6c c7 b0 4d 1a 90 b3 bf 50

Versión SHA-1:

Emisor	CN = AC1 RAIZ MTIN SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN OU = SUBDIRECCION GENERAL DE PROCESO DE DATOS O = MINISTERIO DE TRABAJO E INMIGRACION L = MADRID C = ES
Titular	CN = AC1 RAIZ MTIN SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN OU = SUBDIRECCION GENERAL DE PROCESO DE DATOS O = MINISTERIO DE TRABAJO E INMIGRACION L = MADRID C = ES
Número de Serie	05 0b 41 5e 82 7b
Periodo de Validez	jueves, 05 de noviembre de 2009 17:17:45 domingo, 03 de noviembre de 2019 17:17:45
Función resumen del certificado	sha1 6a d2 3b 9d c4 8e 37 5f 85 9a d9 ca b5 85 32 5c 23 89 40 71

Cada tipo de certificado está descrito en un documento con el perfil del certificado.

1.3.2 Entidades de Registro

Las Entidades de Registro asisten al PSCM en las funciones de identificación, registro y autenticación de los suscriptores, así como en otras tareas relativas a la gestión de los certificados y correcta asignación a los solicitantes. Tienen como misión principal la de garantizar que la información contenida en la solicitud del certificado sea completa y veraz. Las tareas que desempeñan son:

- Identificación y autenticación de la identidad de las personas solicitantes y receptoras de los certificados.
- Entrega de los dispositivos seguros de creación de firma a los suscriptores o responsables de los certificados.
- Aprobación de la generación de los certificados.
- Almacenamiento de los documentos en relación con los servicios de certificación o envío de los mismos para su almacenamiento.

Las Entidades de Registro están compuestas, de manera conjunta, por los servicios telemáticos que permiten la gestión del ciclo de vida de los certificados y por los puestos de expedición presencial que operan dedicados a tal fin.

Las Entidades de Registro llevan a cabo la identificación de los solicitantes de certificados conforme a las normas de la DPCM y el acuerdo suscrito con la Entidad de Certificación. En el caso de que las Entidades de Registro pertenezcan al Ministerio, no será precisa la firma de ningún acuerdo y las relaciones entre ambas se regirán por la DPCM y las Políticas de Certificación que sean de aplicación. Las Entidades de Registro competentes para la gestión de solicitudes de certificación se encuentran definidas para cada tipo de certificado.

La Entidad de Certificación podrá valerse de una o varias Entidades de Registro elegidas libremente para la prestación del servicio de certificación.

Los servicios ofrecidos por las Entidades de Registro para los certificados de Empleado Público se encuentran disponibles a través de la red interna del Ministerio.

1.3.3 Entidad de Validación

Las Entidades de Validación son las encargadas de suministrar información sobre la vigencia de los certificados electrónicos emitidos por una Entidad de Certificación. Para proporcionar esta información, las Entidades de Validación usan los servicios de la lista de entidades de confianza (TSL), estructura que mantiene la relación de los servicios de certificación admitidos por todas las AAPP.

La Entidad de Validación del PSCM presta servicio a los usuarios de forma que se puede comprobar el estado del certificado de forma instantánea, segura y fiable.

El acceso a los servicios de validación del estado de los certificados se ofrece de forma pública. La ubicación del servicio de validación OCSP y del certificado del servicio OCSP se encuentra en el Anexo B: Enlaces (URL).

1.3.4 Usuarios finales

Los usuarios finales son las entidades o personas que disponen y utilizan los certificados electrónicos emitidos por las Entidades de Certificación del PSCM. En concreto, podemos distinguir los siguientes usuarios finales:

- Los solicitantes de certificados.
- Los suscriptores de certificados.
- Los responsables de certificados.
- Los verificadores de certificados (relying parties).

1.3.4.1 Solicitantes de los certificados

Todo certificado es solicitado por una persona en su propio nombre, en nombre de una institución o en nombre de otra persona física o jurídica.

En el caso de certificados de Empleado Público en cualquiera de sus perfiles, el solicitante debe ser empleado público del organismo.

En el caso de certificados Sello Electrónico y Sellado de Respuestas OCSP la petición deberá proceder de empleados públicos.

1.3.4.2 Suscriptores de los certificados

Los suscriptores de certificados son las AAPP y las personas, físicas o jurídicas, así identificadas en el campo *Subject* del certificado y que aseguran que utilizan su clave y su certificado de acuerdo con la DPCM.

En los certificados de Sello, dentro del campo *Subject* (concretamente en el atributo *Common Name*) también se identifica el dispositivo o servidor al que están asociados.

Con el fin de evitar cualquier conflicto de intereses, el suscriptor y la organización del PSCM deberán ser entidades diferentes.

1.3.4.3 Responsables de los certificados

Los responsables de certificados, esto es de la custodia de los certificados, son las personas físicas así identificadas en el objeto *Identidad Administrativa* dentro de la extensión *SubjectAltName*. Adicionalmente el responsable del certificado puede estar identificado en los campos *Given Name* y *Surname* del *Subject* del certificado.

En el caso de cualquier tipo de certificado de Empleado Público emitido por el PSCM, el responsable del certificado es el titular del mismo.

En el caso de certificados de Sello Electrónico el responsable será un empleado público.

En el caso del certificado de Sellado de Respuestas OCSP, el responsable del mismo será el responsable del PSCM.

1.3.4.4 Verificadores de los certificados

Los verificadores son las entidades (incluyendo personas físicas, AAPP, personas jurídicas y otras organizaciones) que, utilizando el certificado de un suscriptor emitido por una entidad de certificación que opera bajo la DPCM, verifican la integridad de un mensaje firmado electrónicamente; identifican al emisor del mensaje; o establecen un canal confidencial de comunicaciones con el propietario del certificado, basándose en la confianza de la validez de la relación entre el nombre del suscriptor y la clave pública del certificado proporcionada por la entidad de certificación. Un verificador utilizará la información contenida en el certificado para determinar la utilización del certificado para un uso en particular.

1.4 Uso de los certificados

Los certificados que se circunscriben a la DPCM deberán ser utilizados sólo para las transacciones definidas en los sistemas y aplicaciones permitidos. La expedición efectiva de los certificados soportados en la DPCM obliga al suscriptor a la aceptación y uso de los mismos en los términos expresados en la DPCM.

Se recalca que está fuera del ámbito de la DPCM garantizar la viabilidad tecnológica de las aplicaciones que harán uso de cualquiera de los perfiles de certificados definidos en la DPCM.

No se permite en modo alguno el uso de cualquiera de los certificados fuera del ámbito descrito en la DPCM, pudiendo ser causa de revocación inmediata el uso indebido de los mismos.

Cada tipo de certificado emitido por el PSCM con correspondencia en los definidos por la [Ley 40/2015] y reglamento eIDAS tendrá su uso delimitado por lo dispuesto en la ley. El resto de los certificados se atendrán a lo especificado en el mismo certificado o en sus documentos de perfil.

1.5 Administración de la DPCM

1.5.1 Organización que administra el documento

La *Subsecretaría del Ministerio* ostenta la representación ordinaria del ministerio y la dirección de sus servicios comunes, así como el ejercicio de las atribuciones a que se refiere el artículo 15, de 14 de abril, de Organización y Funcionamiento de la AGE, y, en particular,

la coordinación y gestión de los recursos humanos, financieros, tecnológicos y materiales del departamento.

De la Subsecretaría depende la *SGTIC* (antigua Subdirección General de Proceso de Datos) responsable del impulso y coordinación de la política informática del ministerio y de sus diferentes organismos, la coordinación de la administración electrónica en el departamento, la planificación y gestión de los sistemas de información necesarios para el funcionamiento de los servicios, la gestión y administración de las redes de comunicaciones de telefonía y datos de los servicios centrales, interprovinciales y del exterior, la administración de la presencia en Internet del ministerio, el asesoramiento y asistencia en tecnologías de la información y las comunicaciones, la supervisión en materia de tecnologías de la información y de las comunicaciones de los organismos autónomos adscritos a excepción del Servicio Público de Empleo Estatal y de los dependientes de la Secretaría de Estado de la Seguridad Social.

Por ello, el responsable de la SGTIC es el responsable del PSCM (incluyendo las Entidades de Certificación, Registro y Validación) y por ende es el responsable de la definición, revisión y divulgación de la DPCM. Existen dos responsables adjuntos al responsable del PSCM que asesoran y colaboran en la definición, análisis y mejora del PSCM así como lo sustituyen en caso de ausencia prolongada de este, de acuerdo con lo legalmente aplicable. Ambos adjuntos son los responsables adjuntos de la SGTIC.

1.5.2 Datos de contacto de la organización

Subdirección General de Tecnologías de la Información y las Comunicaciones
C/ Paseo de la Castellana 63
28071 – Madrid, Spain
admin_ca@mtin.es / admin_ca@meyss.es
Teléfono : 91 363 11 88/9 – Fax : 91 363 07 73

1.5.3 Procedimiento de gestión del documento

1.5.3.1 Procedimiento de Especificación de Cambios

Corresponde al responsable del PSCM la aprobación y aplicación de los cambios propuestos a la DPCM de acuerdo con el plan de calidad de la documentación del PSCM.

El responsable de seguridad del PSCM revisará la DPCM al menos una vez al año o cada vez que se produzca un cambio significativo en ese período. Los errores, actualizaciones, sugerencias o mejoras sobre este documento, deberán comunicarse a la organización cuyos datos de contacto aparecen en la sección 1.5.2. Toda comunicación deberá incluir una descripción del cambio, su justificación y la información de la persona que solicita la modificación.

Todos los cambios aprobados en la DPCM se difundirán a todas las partes interesadas según lo especificado en el apartado siguiente.

1.5.3.2 Procedimientos de Publicación

El PSCM publica toda la información que considere oportuna relativa a los servicios ofrecidos (incluyendo la DPCM) en un repositorio accesible a todos sus usuarios. La ubicación de la DPCM actualizada está publicada en:

http://ca.empleo.gob.es/meyss/DPCyPoliticas

1.5.3.3 Procedimiento de Aprobación de la DPCM y de Políticas Externas

El responsable de seguridad del PSCM solicitará la aprobación de la DPCM al responsable del PSCM que aprobará la misma (o no) de acuerdo con el plan de calidad de la documentación del PSCM.

1.6 Definiciones y acrónimos

1.6.1 Definiciones

En el ámbito de la DPCM se utilizan las siguientes definiciones:

Autenticación	Proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico.
C	Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
Certificado de Firma Electrónica	Declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona.
CN	Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
CSR	Conjunto de datos que contienen una clave pública y su firma electrónica utilizando la clave privada asociada, enviado a la Entidad de Certificación para la emisión de un certificado electrónico que contenga dicha clave pública.
Directorio	Repositorio de información que sigue el estándar X.500 de ITU-T.
DN	Identificación unívoca de una entrada dentro de la estructura de directorio X.500.
Firma electrónica	Los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.
Firmante	Una persona física que crea una firma electrónica.
Función hash	Operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la función hash.
Hash o huella digital	Resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.
HSM	Módulo de seguridad criptográfico empleado para almacenar claves y realizar operaciones criptográficas de modo seguro.

Identificación	Procedimiento de reconocimiento de la identidad de un solicitante o titular de certificados
O	Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
OCSP	Protocolo que permite comprobar en línea la vigencia de un certificado electrónico.
OTP	One Time Password, código de un solo uso que permite una autenticación pero solamente una vez.
OU	Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
PIN	Contraseña que protege el acceso a una tarjeta criptográfica.
PKCS	Estándares de PKI desarrollados por RSA Laboratories y aceptados internacionalmente.
PKIX	Grupo de trabajo dentro del IETF constituido con el objeto de desarrollar las especificaciones relacionadas con la PKI e Internet.
Prestador de servicios de confianza	Una persona física o jurídica que presta uno o más servicios de confianza.
Prestador cualificado de servicios de confianza	Prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la cualificación.
PUK	Contraseña que permite desbloquear una tarjeta criptográfica que ha sido bloqueada por introducción consecutiva de un PIN incorrecto.
RFC	Estándar emitido por la IETF.
Validación	El proceso de verificar y confirmar la validez de una firma o sello electrónicos.

1.6.2 Acrónimos

AAPP	Administraciones Públicas
AGE	Administración General del Estado
AR	Entidad de Registro, también denominada Autoridad de Registro
AV	Entidad de Validación, también denominada Autoridad de Validación
C	Country (País)
CA	Certification Authority (Entidad de Certificación)
CDP	CRL Distribution Point (Punto de Distribución de las CRL)
CEC	Código de Emisión de Certificados
CEN	Comité Européen de Normalisation
CEPCHSM	Certificado de Empleado Público Centralizado y Gestionado por un HSM
CN	Common Name (Nombre Común)
CP	Certificate Policy
CPD	Centro de Proceso de Datos
CPS	Certification Practice Statement
CRL	Certificate Revocation List, Lista de Revocación de Certificados
CSP	Cryptographic Service Provider, Proveedor de Servicios Criptográficos
CSR	Certificate Signing Request (petición de certificado)

CWA	CEN Workshop Agreement
DN	Distinguished Name (Nombre Distintivo)
DPC	Declaración de Prácticas de Certificación
DPCM	Declaración de Prácticas de Certificación del Ministerio
eIDAS	Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 , relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
ETSI	European Telecommunications Standard Institute
FIPS	Federal Information Processing Standard (Estándar USA de procesado de información)
GTP	Grupo de Trabajo Permanente
HSM	Hardware Security Module
IETF	Internet Engineering Task Force (organismo de estandarización de Internet)
LDAP	Lightweight Directory Access Protocol (protocolo de acceso a servicios de directorio)
LOPD	Ley Orgánica de Protección de Datos de Carácter Personal
MINETAD	Ministerio de Energía, Turismo y Agenda Digital
MINHAP	Ministerio de Hacienda y Administraciones Públicas
O	Organization (Organización)
OU	Organizational Unit (Unidad Organizativa)
OID	Object Identifier (Identificador de objeto único)
OCSP	On-line Certificate Status Protocol
PIN	Personal Identification Number (número de identificación personal)
PKCS	Public Key Infrastructure Standards (estándares de PKI)
PKI	Public Key Infrastructure (Infraestructura de Clave Pública)
PKIX	Grupo de trabajo dentro del IETF (Internet Engineering Task Group)
PSC	Prestador de Servicios de Certificación / Prestador de Servicios de Confianza
PSCM	Prestador Cualificado de Servicios de Confianza del Ministerio
PUK	PIN UnlocK Code (código o clave de desbloqueo del PIN)
RA	Registration Authority
RFC	Request For Comments
SGTIC	Subdirección General de Tecnologías de la Información y las Comunicaciones
TSL	Trust-service Status List (Lista de Entidades de Confianza)
TSP	Trust Service Provider
TSPM	PSCM
VA	Validation Authority (Autoridad de Validación)

1.7 Condiciones generales de los servicios del PSCM

La naturaleza jurídica del PSCM como organismo público de la Administración General del Estado, está libre de cualquier presión comercial, financiera y de otro tipo que puedan influir negativamente en la confianza en los servicios que presta. Su estructura organizativa garantiza la imparcialidad en la toma de decisiones relativas al establecimiento, el

aprovisionamiento y el mantenimiento y la suspensión de los servicios de certificación, y en particular las operaciones de generación y revocación de certificados.

El PSCM subcontrata ciertas actividades, como las del desarrollo, despliegue y monitorización de algunos de sus sistemas informáticos. Estas actividades se desarrollan según lo establecido en las políticas y prácticas de certificación del PSCM y en los contratos y acuerdos formalizados con las entidades que realizan tales actividades de acuerdo con la ley de Contratos del Sector Público [RD 3/2011].

La DPCM y Políticas de Certificación recogen las obligaciones y responsabilidades generales de las partes implicadas en los diferentes servicios de certificación para su uso dentro de los límites establecidos y del marco de aplicación correspondiente, siempre en el ámbito de competencias de cada una de dichas partes. Todo lo anterior se entiende sin perjuicio de las especialidades que pudieran existir en los contratos, convenios o acuerdos de aplicación.

El PSCM declara que todas las prácticas de sus servicios de confianza son operadas en cualquier caso bajo el principio de no discriminación.

El PSCM publica los términos y condiciones de uso de sus servicios en el sitio web http://ca.empleo.gob.es. Cualquier cambio relevante será notificado a través de este sitio web publicando un anuncio en la página inicial y las versiones antigua y nueva del documento. Después de 30 días, la versión antigua podrá ser eliminada pero será almacenada por el PSCM durante al menos 15 años pudiendo ser consultada por cualquier interesado que presente una causa justificada.

1.7.1 Política de seguridad

El PSCM define una política de seguridad que ha sido aprobada por el responsable del PSCM. Esta política de seguridad establece cómo el PSCM gestiona la seguridad de la información que maneja.

El PSCM publica y comunica su política de seguridad de la información a sus empleados a través de su Intranet.

La política de seguridad se revisa anualmente o bien si hay cualquier cambio o evento significativo que afecte al PSCM.

Cualquier cambio en la política de seguridad se comunica a los suscriptores y terceras partes (verificadores, organismos de evaluación y supervisión etc.) cuando sea aplicable.

1.7.2 Análisis de Riesgos

Tal y como se señala en la política de seguridad, el PSCM aplica una metodología de análisis de riesgos (MAGERIT) para llevar a cabo una evaluación de los riesgos que identifique, analice y evalúe los riesgos asociados a los servicios de confianza desde un punto de vista técnico y de negocio.

A partir de los resultados obtenidos, el PSCM selecciona las medidas de tratamiento del riesgo más apropiadas asegurándose de que el nivel seguridad es proporcional al nivel del riesgo. Entonces, El PSCM determina todos los requisitos de seguridad y procedimientos operacionales necesarios para implementar las medidas de tratamiento del riesgo escogidas y las documenta en sus prácticas de certificación.

El responsable del PSCM aprueba la evaluación de riesgos y acepta el riesgo residual identificado.

La evaluación de riesgos se revisa cada dos años o bien si se ha producido un cambio o evento significativo que afecte al PSCM.

2 Publicación de información y Repositorio de Certificados

2.1 Repositorio de certificados y de información

El PSCM dispone de un repositorio de información pública en la dirección http://ca.empleo.gob.es disponible durante las 24 horas, los 7 días de la semana.

En caso de fallo grave del sistema fuera del control del PSCM, este se compromete a realizar los mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 5.7.4 de este documento.

El repositorio del PSCM:

- Garantiza la disponibilidad de la información en línea. Puede proporcionarse una versión en soporte papel si es necesario.
- Facilita la utilización de un servicio rápido y seguro de consulta del Registro de certificados emitidos que está a disposición de los terceros que confían en los certificados.
- Mantiene un sistema actualizado de certificados en el que se indican los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida.
- Emite Listas de Certificados Revocados (CRL) y proporciona servicios de verificación en tiempo real de certificados, mediante Online Certificate Status Protocol (OCSP) en las URL que aparecen en el Anexo B: Enlaces (URL).
- Publica los términos y condiciones de uso de los certificados.

Dicha documentación se mantendrá publicada durante un período mínimo de quince años desde la emisión del certificado.

El servicio de revocación y validación de certificados del PSCM está disponible las 24 horas del día, los 7 días de la semana, excepto el mínimo tiempo requerido para las operaciones de mantenimiento o de resolución de incidentes graves.

2.2 Publicación de información de la Entidad de Certificación

La dirección de la DPCM se encuentra en el Anexo B: Enlaces (URL).

La dirección con los certificados de la CA raíz y de las SubCA se encuentra en el Anexo B: Enlaces (URL).

La dirección del servicio se encuentra en el Anexo B: Enlaces (URL).

La dirección de la publicación de las CRL se encuentra en el Anexo B: Enlaces (URL).

2.3 Frecuencia de publicación

La información anteriormente indicada, incluyendo perfiles y la DPCM, se publica tan pronto como se encuentre aprobada. Los cambios en la DPCM se rigen por lo establecido en la sección 1.5.3 del presente documento.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en las secciones 4.9.7 y 4.9.9 de este documento.

El PSCM notificará a sus usuarios los cambios en sus prácticas y especificaciones y en los términos y condiciones de uso de sus servicios a través de su sitio web. El PSCM pondrá un

anuncio de los cambios en la página inicial y publicará la versión antigua y moderna del documento. Tras 30 días, la versión antigua podrá ser eliminada aunque el PSCM retendrá la misma durante al menos 15 años, pudiendo ser consultada por cualquier interesado que presente una causa justificada.

2.4 Control de acceso

El PSCM solamente permite el acceso de lectura a la información publicada en su repositorio. Sin embargo, establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del repositorio de información, protegiendo igualmente la integridad y autenticidad de la información de estado de revocación.

El PSCM emplea sistemas fiables para su repositorio de información de modo tal que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3 Identificación y autenticación

3.1 Gestión 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 [ITU-T X.501] y contenido en el campo *Subject*, incluyendo un componente *Common Name*. Todos los certificados emitidos cumplen, además, con la norma [IETF RFC 6818].

3.1.2 Normalización e Identidad Administrativa

El PSCM utiliza el esquema de nombres normalizado propuesto por la AGE *Identidad Administrativa* para cada tipo y perfil de certificado emitido. De este modo se utiliza un marco común, asignando exactamente el mismo nombre a sellos, organizaciones, puestos y unidades, etc. para toda la Administración Pública Estatal.

El objeto Identidad Administrativa utiliza el número ISO/IANA *2.16.724.1.3.5.x.x* como base para identificarlo, de este modo se establece un identificador unívoco a nivel internacional. Para cada certificado su valor es:

Certificados conformes a eIDAS:

- Certificado de Sello Electrónico para la Actuación Automatizada (Nivel Medio)

  2.16.724.1.3.5.6.2
- Empleado Público (Nivel Alto)

  2.16.724.1.3.5.7.1
- Empleado Público Centralizado y Gestionado por HSM (Nivel Medio)

  2.16.724.1.3.5.7.2

Certificados previos a eIDAS:

- Certificado de Sello Electrónico para la Actuación Automatizada (Nivel Medio)

  2.16.724.1.3.5.2.2
- Empleado Público (Nivel Alto)

  2.16.724.1.3.5.3.1
- Empleado Público Centralizado y Gestionado por HSM (Nivel Medio)

  2.16.724.1.3.5.7.2

Certificado	Campos "Identidad Administrativa" fijos
SELLO ELECTRÓNICO PARA LA ACTUACIÓN AUTOMATIZADA	• Tipo de certificado • Nombre de la entidad suscriptora • NIF entidad suscriptora • Denominación de sistema o componente
EMPLEADO PÚBLICO	• Tipo de certificado • Nombre de la entidad suscriptora • NIF entidad suscriptora

	• DNI/NIE del responsable • Nombre de pila • Primer apellido • Segundo apellido
EMPLEADO PÚBLICO CENTRALIZADO Y GESTIONADO POR HSM	• Tipo de certificado • Nombre de la entidad en la presta servicios • NIF de la entidad en la que presta servicios • DNI/NIE del responsable • Nombre de pila • Primer apellido • Segundo apellido

Certificado	Campos "Identidad Administrativa" opcionales
SELLO ELECTRÓNICO PARA LA ACTUACIÓN AUTOMATIZADA	• DNI/NIE del responsable • Nombre de pila • Primer apellido • Segundo apellido • Correo electrónico
EMPLEADO PÚBLICO	• Número de identificación de personal • Correo electrónico • Unidad organizativa • Puesto o cargo
EMPLEADO PÚBLICO GESTIONADO POR HSM	• Número de identificación de personal • Correo electrónico • Unidad organizativa • Puesto o cargo

3.1.3 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:

- Se codifica el nombre tal y como aparece en la documentación acreditativa. Se podrá optar por utilizar mayúsculas únicamente para codificar los nombres.
- Se podrán eliminar las tildes, para garantizar la mayor compatibilidad técnica posible.
- Se podrán eliminar caracteres en blanco redundantes entre cadenas alfanuméricas, como los duplicados o los situados al principio o al final de cadenas alfanuméricas, siempre que no supongan dificultad en la interpretación de la información.
- Los nombres podrán ser adaptados y reducidos, al objeto de garantizar el cumplimiento de los límites de longitud aplicables a cada campo del certificado.

Y en concreto, para los certificados de empleado público, aplica lo siguiente:

- Se incluye obligatoriamente el NOMBRE, de acuerdo con lo indicado en el DNI/NIE.

- Se incluye obligatoriamente el PRIMER y SEGUNDO APELLIDO, separados únicamente por un espacio en blanco, de acuerdo con lo indicado en el DNI/NIE. En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter).
- Se incluye obligatoriamente el número de DNI/NIE, junto con la letra de control, de acuerdo con lo indicado en el DNI/NIE.
- Se incluye obligatoriamente un SÍMBOLO o CARÁCTER que separe el nombre y apellidos del número de DNI.
- Se incluye un literal (*AUTENTICACION*, *FIRMA* o *CIFRADO*) que identifica la tipología del certificado. Este identificador siempre será al final del *CN* y entre paréntesis. En el caso de un nivel de aseguramiento medio, si se agrupan varios perfiles en un único certificado, no incluirá esta opción.

3.1.4 Uso de anónimos y seudónimos

No se permiten.

3.1.5 Interpretación de formatos de nombres

Las normas de codificación de los campos siguen las recomendaciones de [IETF RFC 6818] usando UTF-8.

El PSCM proporciona el método de extracción de cada uno de los datos individualizados, que, en su conjunto, determinan de forma unívoca la identidad del titular y/o custodio del certificado electrónico. En concreto, para cada tipo de certificado emitido, los datos proporcionados serán:

- Certificado de Empleado Público[1] y Certificado de Empleado Público Centralizado y Gestionado por HSM[2]:
    - Descripción del tipo de certificado.
    - Nombre del titular.
    - Primer apellido del titular.
    - Segundo apellido del titular (opcional en caso de extranjeros).
    - Número de identificación personal (ej. DNI / NIE…).
    - Nombre de la entidad en la que está suscrito el empleado.
    - Número de Identificación de entidad en la que está adscrito el empleado (ej. NIF/CIF).
    - Unidad de destino a la que está suscrito el empleado.
    - Cargo o puesto de trabajo.
    - Dirección de correo electrónico.
- Certificado de Sello Electrónico para la Actuación Automatizada[3]:
    - Descripción del tipo de certificado.
    - Denominación de sistema o componente informático.

[1] No se admite la relación de representación en este tipo de certificados.
[2] No se admite la relación de representación en este tipo de certificados.
[3] No se admite la relación de representación en este tipo de certificados.

- Nombre de la entidad suscriptora.
- Número de Identificación de la entidad suscriptora (ej. NIF/CIF).

3.1.6 Unicidad de los nombres

Los nombres de los suscriptores de certificados son únicos para cada servicio de generación de certificados operado por una Entidad de Certificación y para cada tipo de certificado; es decir, una persona puede tener a su nombre certificados de tipos diferentes expedidos por la misma Entidad de Certificación.

También puede tener certificados a su nombre del mismo tipo expedidos por diferentes Entidades de Certificación.

No se puede volver a asignar un nombre de suscriptor que ya haya sido ocupado, a un suscriptor diferente.

3.1.7 Resolución de conflictos relativos a nombres

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el suscriptor, de derechos de terceros.

La Entidad de Certificación no determina que un solicitante de certificados tiene derecho sobre el nombre que aparece en una solicitud de certificado.

Así mismo, la Entidad de Certificación no actúa como árbitro o mediador, ni de ninguna otra manera resuelve ninguna disputa concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

La Entidad de Certificación se reserva el derecho de rehusar una solicitud de certificado por causa de conflicto de nombre.

Los conflictos de nombres de responsables de certificados que aparezcan identificados en los certificados con su nombre real se solucionarán 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

En esta sección se establecen los requisitos relativos a los procedimientos de identificación y autenticación que se emplean durante el registro de suscriptores y responsables de certificados, que se realiza con anterioridad a la emisión y entrega de los mismos.

3.2.1 Prueba de posesión de clave privada

Esta sección describe los métodos que se emplean para demostrar que se posee la clave privada correspondiente a la clave pública objeto de certificación.

El método de demostración de posesión de la clave privada es PKCS#10 o bien el procedimiento fiable de entrega y aceptación del dispositivo seguro de creación de firma y su correspondiente procedimiento de descarga de certificados u otra prueba criptográfica o procedimiento equivalente.

En el ámbito del CEPCHSM, una vez que el empleado público ha sido registrado en el sistema con nivel avanzado de garantía de registro y ha solicitado expresamente la emisión de cualquiera de sus CEPCHSM con los controles de directorio activo y otros factores de

autenticación, dicha emisión se llevará a cabo la primera vez que el empleado público acceda al procedimiento de generación.

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

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

3.2.2 Autenticación de la identidad de una organización

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

- 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.

3.2.3 Autenticación de la identidad de un solicitante

Esta sección contiene requisitos para la comprobación de la identidad de una persona física identificada en un certificado.

3.2.3.1 Elementos de identificación requeridos

El PSCM utiliza los siguientes elementos, reflejados en una declaración firmada por el usuario solicitante del certificado, para acreditar la identidad del mismo. Para la identificación personal del titular del certificado se solicitará:

- DNI, NIE o Pasaporte para acceder al nombre de pila, el primer y el segundo apellidos.
- El nombre de la entidad a la que está suscrito el empleado, en su caso.

El PSCM guarda soporte escrito o electrónico de tal identificación conteniendo al menos:

- La identidad de la persona que realiza la identificación.
- Una declaración firmada de la persona que realiza la autenticación que garantice que la identificación del suscriptor se ha realizado según lo especificado en la DPCM.
- La fecha de la verificación.

En el momento de la firma de dicha declaración, el usuario acepta las condiciones de uso de los certificados y se somete a lo estipulado en la DPCM en lo relativo a las condiciones de uso de los mismos.

3.2.3.2 Validación de los elementos de identificación

La validez de los datos de identificación presentes en la solicitud de certificados se realiza contrastando la información de la solicitud con la documentación aportada, electrónicamente o en soporte físico, por parte de la Entidad de Registro correspondiente.

3.2.3.3 Necesidad de presencia personal

Se requiere presencia física directa del solicitante de los certificados para la obtención de los siguientes tipos de certificados:

- Certificado de Empleado Público de nivel alto.
- Certificado de Empleado Público de nivel medio (CEPCHSM).

En el caso del CEPCHSM también se admite la posibilidad de usar un certificado electrónico cualificado.

Se permite la identificación sin presencia física, basada en bases de datos administrativas o en certificados vigentes para los siguientes tipos de certificados:

- Certificado de Sello Electrónico de nivel medio.

De esta forma, se emplean métodos basados en la presencia física indirecta cuando la validación de la identidad se ha producido de forma personal anteriormente y los registros de las AAPP se mantienen permanentemente actualizados.

Se garantiza, en cualquier caso, la entrega y aceptación del certificado por el suscriptor o responsable del certificado.

3.2.3.4 Vinculación de la persona física con una organización

Se identifica y autentica la vinculación de la persona física con las AAPP mediante la verificación de documentos oficiales que garantizan esta vinculación como BOE o documento de toma de posesión o equivalente.

3.2.4 Información de suscriptor no verificada

No se incluye información de suscriptor no verificada en los certificados.

3.2.5 Criterios para operar con AC externas

La DPCM no contempla el establecimiento de relaciones de confianza con Prestadores de Servicios de Certificación externos.

3.3 Identificación y autenticación de solicitudes de renovación

No se renuevan certificados que hayan sido revocados en ningún caso, debiéndose proceder a una nueva solicitud y validación de la identidad, de acuerdo con lo establecido en la sección 3.2.

3.3.1 Validación para la renovación periódica de certificados

Por defecto, el PSCM no admite la renovación periódica de certificados. En el caso del CEPCHSM, la renovación del certificado se lleva a cabo de forma que se cumplen los requisitos que la ley marca con respecto a los plazos máximos permitidos desde que el empleado público realizó el registro presencial. En caso contrario, para renovar su certificado el empleado tendrá que personarse en la oficina de registro siguiendo los procedimientos de comprobación de la identidad del empleado desarrollados a tal efecto.

3.3.2 Validación para la renovación de certificados después de la revocación

Por defecto, el PSCM no admite la renovación de certificados después de su revocación siendo de aplicación lo contemplado en el punto anterior.

3.4 Identificación y autenticación de la solicitud de revocación

El PSCM autentica las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una persona autorizada.

En general, se consideran suficientemente autenticadas las solicitudes de revocación firmadas con certificados reconocidos o medio equivalente. En el caso de solicitudes de revocación de certificados personales, se verifica que la solicitud procede de una cuenta interna del ministerio.

3.5 Autenticación de una petición de suspensión

El PSCM no admite la suspensión de certificados.

4 Requisitos de operación del ciclo de vida de los certificados

4.1 Solicitud de emisión de los certificados

4.1.1 Legitimación para solicitar la emisión

Antes de la emisión y entrega de un Certificado de Sello Electrónico o de Empleado Público existe una solicitud previa que se realiza a instancia de parte.

4.1.1.1 Especificaciones para los Certificados de Empleado Público

La solicitud de emisión del certificado debe ser firmada por el solicitante siendo necesario el que este acredite su identidad, de acuerdo con lo establecido en la sección 3.2 de este documento. Esto conlleva la entrega de un código único secreto de emisión del certificado (CEC) así como la entrega del dispositivo criptográfico de firma y claves de acceso asociadas. El CEC, junto con otros datos de autenticación, permite la generación de los pares de claves y descarga del certificado en el dispositivo criptográfico de firma.

Junto con la solicitud se entrega información con los siguientes contenidos:

- Información básica sobre el tipo y uso del certificado, incluyendo especialmente información sobre la Entidad de Certificación y la DPC aplicable, así como sus obligaciones, facultades y responsabilidades.
- Información sobre el certificado y el dispositivo criptográfico.
- Obligaciones del responsable del certificado.
- Responsabilidad del responsable del certificado.

Estos contenidos podrán comunicarse de forma indirecta indicando la URL en la que puede descargarse la DPCM.

4.1.1.2 Especificaciones para los Certificados de Empleado Público Centralizados y Gestionados por HSM

La solicitud de emisión del CEPCHSM debe ser firmada por el solicitante siendo necesario el que este acredite su identidad, de acuerdo con lo establecido en la sección 3.2 de este documento. Esto conlleva la personación para registrar los factores de autenticación que se emplearán posteriormente para generar y descargar telemáticamente los certificados.

Junto con la solicitud se entrega información con los siguientes contenidos:

- Información básica sobre el tipo y uso del certificado, incluyendo especialmente información sobre la Entidad de Certificación y la DPC aplicable, así como sus obligaciones, facultades y responsabilidades.
- Información sobre el certificado.
- Obligaciones del responsable del certificado.
- Responsabilidad del responsable del certificado.

Estos contenidos podrán comunicarse de forma indirecta indicando la URL en la que puede descargarse la DPCM.

4.1.1.3 Especificaciones para los Certificados de Sello Electrónico

La petición deberá proceder de empleados públicos. El solicitante deberá incluir sus datos y los del responsable del certificado en la solicitud de emisión del certificado, siendo imprescindible la identificación del responsable en la recogida del mismo.

El responsable de la Entidad de Certificación autorizará la emisión de los certificados de Sello Electrónico a partir de la resolución de la *Subsecretaría del Ministerio* o titular del organismo público competente, publicada en la sede electrónica correspondiente.

En los casos en que el Certificado de Sello Electrónico incorpore un órgano, deberá demostrarse su identidad a través de bases de datos administrativas u otros documentos equivalentes.

4.1.2 Procedimiento de alta: responsabilidades

La entidad que realiza el registro se asegura de que las solicitudes de certificado son completas, precisas y están debidamente autorizadas. Antes de la emisión y entrega del certificado, dicha entidad informa al suscriptor o responsable del certificado de los términos y condiciones aplicables al certificado. La citada información se comunica en soporte duradero, en papel o electrónicamente, y en lenguaje fácilmente comprensible.

La solicitud va acompañada de la documentación justificativa de la identidad y otras circunstancias del solicitante y del suscriptor, de acuerdo con lo establecido en las secciones 3.2.2 y 3.2.3 de este documento.

Las funciones de registro pueden ser ejercidas por el PSCM o un colaborador expresamente designado.

4.2 Procesamiento de la solicitud

4.2.1 Especificaciones para los Certificados de Empleado Público de nivel alto y medio

Adicionalmente a la información contenida en la solicitud, la Entidad de Certificación:

- Incluye en el certificado las informaciones establecidas en el artículo 11 de la LFE, de acuerdo con lo establecido en la sección 7 Perfiles de certificados y listas de certificados revocados de la DPCM.
- Garantiza la fecha y la hora en que se expidió un certificado.
- Utiliza sistemas y productos fiables que están protegidos contra toda alteración y que garantizan la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Asegura que el certificado se emite por sistemas que utilizan protección contra falsificación y, cuando la Entidad de Certificación genera claves privadas, garantizan el secreto de las claves durante el proceso de generación de dichas claves.

4.2.2 Especificaciones para los Certificados de Sello Electrónico

Una vez recibida la solicitud de Certificado de Sello Electrónico, la Entidad de Certificación revisa la información proporcionada con especial énfasis en la identidad del responsable del certificado y en la autorización para la emisión del mismo. Si la información no es correcta,

la Entidad de Certificación deniega la petición. En caso de que los datos sean correctos, la Entidad de Certificación procederá a la emisión del certificado.

4.3 Emisión del certificado

4.3.1 Acciones de la Entidad de Certificación durante el proceso de emisión

La Entidad de Certificación:

- Utiliza un procedimiento de descarga y generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Cuando la Entidad de Certificación genera el par de claves, utiliza un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves y garantiza, que la clave privada es entregada de forma segura al suscriptor o responsable del certificado.
- Protege la confidencialidad e integridad de los datos de registro, especialmente en el caso de que sean intercambiados con el suscriptor o responsable del certificado.
- Almacena los certificados emitidos con los permisos de acceso y controles de seguridad regulados y necesarios para ello, garantizando la seguridad de las comunicaciones.
- No almacena claves privadas asociadas a los certificados excepto en el caso del CEPCHSM en el que el sistema genera en ese momento la clave privada y la almacena en el sistema de forma protegida de forma que se garantiza su uso bajo el control exclusivo del titular del certificado.

Adicionalmente, la Entidad de Certificación:

- Incluye en el certificado las informaciones establecidas en el artículo 11.2 de la LFE.
- Indica la fecha y la hora en las que se expidió un certificado.
- Utiliza un procedimiento de gestión de dispositivos seguros de creación de firma que asegura que son entregados de forma segura al suscriptor o responsable del certificado.
- Utiliza productos protegidos contra alteraciones, garantizando la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.
- Utiliza medidas contra la falsificación de certificados y para garantizar el secreto de las claves durante el proceso de generación de las mismas.
- Cuando emite un certificado de acuerdo con una solicitud, efectúa las notificaciones establecidas en el siguiente apartado.

4.3.2 Notificación de la emisión al suscriptor

La aprobación de la solicitud de los certificados de Empleado Público se comunica mediante la entrega de forma segura del certificado.

En el ámbito del CEPCHSM a la finalización del proceso de generación del certificado se informa al empleado público de que se encuentra disponible dicho certificado para su uso, pudiendo ser utilizado a partir de ese mismo momento para los procesos de firma electrónica.

En otro caso, la Entidad de Certificación notifica al solicitante la denegación de la solicitud mediante correo electrónico, teléfono o cualquier otro medio utilizando como datos de contacto los reflejados en la solicitud.

4.4 Entrega y aceptación del certificado

4.4.1 Responsabilidades de la Entidad de Certificación

En el caso de Certificados de Empleado Público, la Entidad de Certificación proporciona al suscriptor acceso al certificado a través de la aplicación diseñada a tal efecto que permite la generación del par de claves y la descarga del certificado en el dispositivo criptográfico en su caso. Para la descarga del certificado es imprescindible la utilización del CEC.

En el ámbito del CEPCHSM la Entidad de Certificación proporciona al suscriptor acceso al certificado a través de la aplicación diseñada a tal efecto que permite la generación del par de claves. El sistema informa al empleado público de que va a emitir su certificado y en ese momento se genera su clave privada y se almacena en el sistema de forma protegida, de modo que se garantiza su uso bajo el control exclusivo de su titular. A la finalización del proceso de generación del certificado se informa al empleado público de que se encuentra disponible dicho certificado para su uso, pudiendo ser utilizado a partir de ese mismo momento para los procesos de firma electrónica.

En el caso de Certificados de Sello Electrónico, la Entidad de Certificación entrega de forma segura el certificado. Esta entrega se producirá presencialmente previa identificación del suscriptor o responsable. Junto al certificado se entrega información con los siguientes contenidos:

- Información básica sobre el tipo y uso del certificado, incluyendo especialmente información sobre la Entidad de Certificación y la DPCM, así como sus obligaciones, facultades y responsabilidades.
- Información sobre el certificado y el dispositivo criptográfico, de existir este.
- Obligaciones del responsable del certificado.
- Responsabilidad del responsable del certificado.

4.4.2 Conducta que constituye aceptación del certificado

El dispositivo criptográfico destinado a albergar certificados (si el certificado usa este soporte) se acepta mediante la firma de la hoja de entrega por parte del suscriptor o, en su caso, por parte del responsable del certificado.

En el caso de Certificados de Empleado Público se considera aceptado el certificado mediante la utilización de un mecanismo telemático de descarga del certificado. En el caso de certificados cuyo par de claves se haya generado en un dispositivo seguro de creación de firma bajo el control exclusivo del usuario, se considera que el usuario acepta el certificado mediante la acción de descargarlo en el citado dispositivo.

Adicionalmente, en el caso del CEPCHSM es necesario el registro de al menos un segundo factor de autenticación y su introducción posterior para la descarga y aceptación del certificado. El propio acto de emisión conlleva la aceptación implícita del CEPCHSM.

En el caso de Certificados de Sello Electrónico se considera aceptado el certificado mediante la firma de la hoja de entrega por parte del responsable del certificado.

4.4.3 Publicación del certificado

Los datos de identificación de los certificados se publican en el repositorio interno, en ningún caso de libre acceso, sin el consentimiento previo de los responsables de certificado.

4.4.4 Notificación de la emisión a terceros

No aplicable.

4.5 Uso del par de claves y del certificado

4.5.1 Requisitos generales de uso

Los certificados se utilizarán de acuerdo con su función propia y finalidad establecida, sin que puedan utilizarse en otras funciones y con otras finalidades. De la misma forma, los certificados tendrán que utilizarse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

La extensión *Key Usage* se utiliza para establecer límites técnicos a los usos que puede darse a una clave privada correspondiente a una clave pública listada en un certificado X.509 v3. Sin embargo, se debe tener en cuenta que la efectividad de las limitaciones basadas en extensiones de certificados depende en ocasiones de la operación de aplicaciones informáticas que no han sido fabricadas, ni pueden estar controladas, por las Entidades de Certificación del PSCM.

Los Certificados de Empleado Público de nivel alto se utilizan con un dispositivo seguro de creación de firma electrónica, que cumple los requisitos establecidos por el artículo 24 de la LFE, con la DPCM y con las correspondientes condiciones adicionales.

El CEPCHSM tiene como finalidad la autenticación y la firma electrónica avanzada de documentos electrónicos.

4.5.2 Uso por los suscriptores

Los suscriptores deberán:

- Cumplir las obligaciones que se establecen en este documento y en el artículo 23.1 de la LFE.
- Suministrar a las Entidades de Registro información exacta, completa y veraz con relación a los datos que estas les soliciten para realizar el proceso de registro.
- Conocer y aceptar las condiciones de utilización y restricciones de uso de los certificados, en particular las contenidas en la DPCM que le sean de aplicación, así como las modificaciones que se realicen sobre las mismas
- Comunicar a la Entidad Competente, a través de los mecanismos que se habilitan a tal efecto, cualquier malfuncionamiento del certificado.
- Proteger sus claves privadas en todo momento, conforme a lo establecido en este documento. En especial, los suscriptores de un certificado deben ser especialmente diligentes en la custodia de su dispositivo seguro de creación de firma, con la finalidad de evitar usos no autorizados.

- Notificar en los plazos adecuados, a la Entidad de Certificación del PSCM que haya proporcionado el certificado, la sospecha de compromiso de clave o su pérdida. Esta notificación deberá realizarse por los mecanismos previstos en la DPCM.

Si el suscriptor genera sus propias claves, deberá:

- Crear, en su caso, las claves dentro del dispositivo seguro de creación de firma utilizando un algoritmo reconocido como aceptable para la firma electrónica reconocida.
- Utilizar longitudes y algoritmos de clave reconocidos como aceptables para la firma electrónica reconocida.
- No revelar ningún factor de autenticación que permita la utilización de las claves privadas asociadas a CEPCHSM.

4.5.3 Uso por un tercero que confía en los certificados

Es obligación de aquellas terceras partes que confían en los certificados emitidos por una Entidad de Certificación del PSCM:

- Utilizar los certificados para los propósitos para los cuales fueron emitidos, tal y como se detalla en la información del certificado (por ejemplo, lo definido en la extensión *Key Usage* y *Extended Key Usage)*.
- Controlar que cada certificado que se utilice es válido según lo establecido en los estándares X.509 v3 e [IETF RFC 6818].
- Establecer la confianza en la Entidad de Certificación que ha emitido el certificado verificando la cadena de certificación de acuerdo con las recomendaciones del estándar X.509 v3 e [IETF RFC 6818].
- Utilizar los certificados correspondientes a tipos definidos en [Ley 40/2015] sólo para aquellas transacciones que estén sujetas a lo indicado en [Ley 40/2015] o la DPCM.

4.6 Renovación de certificados sin renovación de claves

De forma general, el PSCM no permite la renovación de certificados sin renovación de claves. En el caso del CEPCHSM las renovaciones de certificados realizadas en el ámbito de la DPCM se realizarán con cambio de claves.

4.7 Renovación de certificados con renovación de claves

En general, el procedimiento aplicable a la renovación del certificado con renovación de claves implica la solicitud de un nuevo certificado con nuevas claves asociadas. En el caso del CEPCHSM, todas las renovaciones, con independencia de su causa, se realizarán con cambio de claves. En este contexto se permite la renovación con cambio de claves de un certificado por la caducidad de los certificados u olvido de la contraseña establecida en la emisión del certificado.

4.8 Modificación de certificados

La modificación de certificados se refiere al caso en que los atributos del suscriptor o del responsable del certificado que no formen parte del control de unicidad previsto por la DPCM hayan variado. El PSCM no permite la modificación de certificados.

4.9 Revocación y suspensión de certificados

La revocación de un certificado es el acto por el cual se deja sin efecto la validez de un certificado antes de su fecha de caducidad. El efecto de la revocación de un certificado es la pérdida de validez del mismo, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia la revocación de un certificado inhabilita el uso legítimo del mismo por parte del titular.

El PSCM no permite la suspensión de certificados.

4.9.1 Causas de revocación de certificados

Una Entidad de Certificación del PSCM revocará un certificado por alguna de las siguientes causas:

1. Circunstancias que afectan la información contenida en el certificado:
   - Modificación de alguno de los datos contenidos en el certificado.
   - Descubrimiento de que alguno de los datos aportados en la solicitud de certificado es incorrecto, así como de la alteración o modificación de las circunstancias verificadas para la expedición del certificado.
   - Descubrimiento de que alguno de los datos contenido en el certificado es incorrecto.
2. Circunstancias que afectan a 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 la DPCM.
   - 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.
   - El compromiso de las claves privadas del empleado público por pérdida, robo, hurto, modificación, divulgación o revelación de la clave personal de acceso que permite la activación de dichas claves, incluso por cualquier otra circunstancia, incluidas las fortuitas, que indiquen el uso de las claves privadas por entidad ajena a su titular.
3. Circunstancias que afectan a 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

4. Circunstancias que afectan al 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, términos de uso y condiciones o en la DPCM.
   - El uso del certificado para actividades criminales.
   - La incapacidad sobrevenida o la muerte del suscriptor o responsable del certificado.
   - Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 3.4 de la DPCM.
5. Otras circunstancias:
   - La finalización del servicio de la Entidad de Certificación, de acuerdo con lo establecido en la sección 5.8 de la DPCM.
   - Otras causas debidamente justificadas.

El instrumento jurídico que vincula a la Entidad de Certificación con el suscriptor establece que el suscriptor debe solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias indicadas anteriormente.

4.9.2 Legitimación para solicitar la revocación

Puede solicitar la revocación de un certificado:

- El suscriptor a cuyo nombre fue emitido el certificado.
- Un representante legalmente autorizado por el suscriptor o responsable del certificado.
- La Entidad de Registro que solicitó la emisión del certificado.
- Quien tenga conocimiento de una o varias de las causas que justifican la revocación, según se indica en el punto 4.9.1.

4.9.3 Procedimientos de solicitud de revocación

Para solicitar la revocación de certificados, la Entidad de Certificación tiene en cuenta las siguientes reglas.

La revocación de un certificado debe solicitarse a la Entidad de Certificación o, en su caso, a la Entidad de Registro que aprobó la solicitud de certificación, proporcionando la siguiente información:

- Fecha de solicitud de la revocación.
- Identidad del suscriptor.

- Razón detallada para la petición de revocación.
- Nombre y título de la persona que pide la revocación.
- Información de contacto de la persona que pide la revocación.

En aquellos casos en que se requiera revocación inmediata del certificado, se enviará un correo electrónico a la Entidad de Certificación o, en su caso, a la Entidad de Registro. Los datos de contacto serán los indicados en la sección 1.5.2. Los suscriptores de CEPCHSM podrán solicitar la revocación de los mismos mediante la aplicación on line disponible 24x7. Estas solicitudes se procesarán automáticamente procediendo a la revocación de los certificados de forma inmediata.

La solicitud será autenticada, por su destinatario, de acuerdo con los requisitos establecidos antes de proceder a la revocación. La solicitud de revocación será procesada tras su recepción:

- En el caso de que el destinatario de la solicitud fuera la Entidad de Registro, una vez autenticada la petición, ésta remitirá una solicitud de revocación del certificado a la Entidad de Certificación.
- La Entidad de Certificación antes de realizar la revocación deberá comprobar la autenticidad de la petición. Queda a su criterio llevar a cabo medidas de comprobación de las razones de revocación. Si la petición de revocación es válida en forma y los motivos son suficientes, la Entidad de Certificación revocará el certificado publicando su número de serie y demás información de identificación en la CRL así como en el servicio OCSP. La Entidad de Certificación no podrá reactivar el certificado, una vez revocado.

4.9.4 Plazo temporal de solicitud de revocación

El PSCM procederá a la inmediata revocación del certificado tan pronto como verifique la identidad del solicitante.

4.9.5 Plazo máximo de procesamiento de la solicitud de revocación

La fecha y hora utilizada en los servicios de revocación está sincronizada con UTC al menos cada 24 horas.

El retraso máximo entre la recepción de una solicitud de revocación de un certificado y el cambio en la información del estado del mismo es de 24 horas.

4.9.6 Obligación de consulta de información de revocación de certificados

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

La Autoridad de Certificación del PSCM pone a disposición de los verificadores un servicio de información de estado de los certificados basados en el protocolo OCSP y, al menos, otra forma de acceso y descarga de las listas de certificados revocados (CRL).

Los servicios de verificación del estado de revocación de los certificados ofrecidos por el PSCM son gratuitos.

4.9.7 Frecuencia de emisión de listas de revocación de certificados (CRL)

En cada certificado se especifica la dirección de la CRL que le corresponda, mediante la extensión *cRLDistributionPoints*.

La lista de revocación de certificados de las entidades finales se emite al menos una vez cada 24 horas o bien cuando ocurre una revocación con un período de validez de 24 horas.

4.9.8 Periodo máximo de publicación de CRL

El cambio de estado de la vigencia de un certificado se indica en la CRL transcurridos menos de 5 minutos desde que se produjo dicho cambio. Esto implica que el retraso máximo entre la confirmación de la revocación del certificado, o su suspensión, para que sea efectivo y el cambio real en la información de su estado es de 5 minutos.

4.9.9 Disponibilidad de servicios de comprobación de estado de certificados

Los verificadores podrán consultar los certificados publicados en el Repositorio de la Entidad de Certificación, por medio de OCSP o CRL.

El PSCM asegura un nivel de servicio, garantizando la disponibilidad de todos los servicios de certificación ofrecidos y, en especial, los de información del estado de la vigencia de los certificados. El PSCM asegura la integridad y autenticidad de la información del estado de los certificados.

El servicio está disponible en línea 24 horas al día, 7 días a la semana. En caso de fallo del sistema, el PSCM lanzará el Plan de Continuidad de Negocio para solventar el incidente tan pronto como sea posible.

4.9.10 Obligación de consulta de servicios de comprobación de 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 la DPCM.

El PSCM indicará en sus certificados los mecanismos de acceso público y abierto a sus servicios de información de estado de certificados, mediante los siguientes métodos:

4.9.10.1 Emisión de Listas de Revocación de Certificados (CRL)

La emisión de CRL se realiza en la modalidad de completas (contienen la lista completa de los certificados revocados), indicándose esta circunstancia dentro de los certificados mediante el empleo de la extensión Puntos de Distribución de las CRL (*cRLDistributionPoints*) definida en la especificación técnica [IETF RFC 6818], de la siguiente forma:

- Se incluirá al menos un Punto de Distribución de las CRL, pudiéndose incluir dos Puntos de Distribución, apuntando a servidores separados.
- El citado Punto de Distribución de las CRL contendrá el nombre de localización de la CRL.

La ubicación de la lista de certificados revocados se encuentra en el Anexo B: Enlaces (URL).

4.9.10.2 Protocolo OCSP

El PSCM ofrece el servicio de verificación de estado de certificados mediante protocolo OCSP de acuerdo con la [IETF RFC 6960] indicando esta circunstancia dentro de los certificados, mediante el empleo de la extensión Información de Acceso a Autoridad (*AuthorityInfoAccess*) definida en las especificaciones técnicas [IETF RFC 6818] y [IETF RFC 6960], de la siguiente forma:

- Se incluye una Descripción de Acceso, que contiene el OID reservado para el acceso a servicios OCSP y la URL en que se encuentra el servidor OCSP.

La ubicación del servicio OCSP se encuentra en el Anexo B: Enlaces (URL).

4.9.11 Otras formas de información de revocación de certificados

El PSCM no cuenta con otras formas de información sobre revocación de certificados.

4.9.12 Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de una Entidad de Certificación del PSCM se notificará a todos los participantes a través de medios oficiales de comunicación o de difusión general.

4.10 Servicios de comprobación de estado de certificados

4.10.1 Características de operación de los servicios

Las CRL se podrán descargar desde el Repositorio de la Entidad de Certificación y serán instaladas por los verificadores. Los verificadores también podrán consultar el estado de los certificados mediante el protocolo OCSP.

4.10.2 Disponibilidad de los servicios

Los servicios de información del estado de la vigencia de los certificados se ofrecen 24 horas al día, 7 días por semana.

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de la Autoridad de Certificación, ésta intentará que este servicio se mantenga inactivo el menor tiempo posible.

4.10.3 Otras características

No estipulado.

4.11 Finalización de la validez de los certificados

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

- Revocación anticipada del certificado por cualquiera de las causas recogidas en el presente documento en el apartado 4.9.1.
- Expiración de la vigencia del certificado.

Si no se solicita la renovación del certificado, la extinción de su validez supondrá la extinción de la relación entre el suscriptor y la Entidad de Certificación.

4.12 Custodia y recuperación de claves

En el ámbito del CEPCHSM, la clave privada generada y asociada a este certificado quedará custodiada por la Entidad de Certificación del PSCM, teniendo en cuenta que el acceso a esta clave será realizada por medios que garantizan, con un alto nivel de confianza, el control exclusivo por parte del empleado público.

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

De acuerdo con el eIDAS, el PSCM (como prestador de servicios de certificación que expide certificados reconocidos) al gestionar los datos de creación de firma electrónica en nombre del firmante, podrá duplicar los datos de creación de firma únicamente con objeto de efectuar una copia de seguridad de los citados datos siempre que se cumplan los siguientes requisitos:

- la seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales;
- el número de conjuntos de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio.

El PSCM no podrá duplicar los datos de creación de firma para ninguna otra finalidad.

5 Controles de seguridad física, de gestión y de operaciones

5.1 Controles de seguridad física

El PSCM dispone de instalaciones que protegen físicamente la prestación de los servicios de generación de certificados y de gestión de revocación del compromiso causado por accesos no autorizados a los sistemas o a los datos. Los módulos criptográficos están protegidos contra la pérdida y el uso no autorizado.

El PSCM posee controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los equipamientos empleados para la prestación de los servicios indicados. La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios indicados.

La política de seguridad física y ambiental aplicable a la prestación de los servicios indicados establece prescripciones para las siguientes contingencias, que se documentan sucintamente en la DPCM:

- Allanamiento y entrada no autorizada.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.
- Incendios e inundaciones y otros desastres naturales.
- Derrumbamiento de la estructura.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.).

5.1.1 Localización y construcción de las instalaciones

La localización de las instalaciones permite la presencia de fuerzas de seguridad en un plazo de tiempo razonablemente inmediato desde que se notifica una incidencia a los mismos. El PSCM tiene a su disposición el personal de seguridad del Ministerio en las instalaciones.

La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intentos de intrusiones por la fuerza.

5.1.2 Acceso físico

La DPCM delega los controles de acceso físico en el Área de Seguridad del Ministerio y en la SGTIC.

El PSCM establece varios niveles de restricción de acceso a los diferentes perímetros y barreras físicas definidas.

Para el acceso a las dependencias del PSCM donde se llevan a cabo procesos relacionados con el ciclo de vida del certificado, es necesaria la autorización previa, identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

La identificación, ante el sistema de control de accesos, se realiza mediante reconocimiento de algún parámetro biométrico del individuo, excepto en caso de visitas escoltadas.

La generación de claves criptográficas de la Entidad de Certificación, así como su almacenamiento, se realizó en dependencias específicas para estos fines y requiere de acceso y permanencia duales (al menos dos personas simultáneamente).

En cualquier caso, las máquinas y plataformas indicadas en la DPCM y que corresponden a los sistemas de certificación se encuentran etiquetadas convenientemente para su correcta identificación y ubicadas en el CPD bajo los criterios de seguridad de aplicación por la unidad citada anteriormente.

La posesión y custodia de las llaves de acceso a los armarios que albergan las plataformas de los sistemas es exclusivo del personal de la SGTIC.

El sistema completo de la Entidad de Certificación Raíz está bajo la responsabilidad de la SGTIC ubicándose en sus instalaciones de seguridad.

Todas las operaciones críticas con los certificados se realizan en recintos físicamente seguros, con niveles de seguridad específicos para los elementos más críticos y con vigilancia durante las 24 horas al día, los 7 días de la semana. Estos sistemas están aislados de otros, de forma que sólo el personal autorizado pueda acceder a ellos.

5.1.3 Electricidad y aire acondicionado

Los equipos informáticos del PSCM están convenientemente protegidos ante fluctuaciones o cortes del suministro eléctrico, que pudieran dañarlos o interrumpir el servicio.

Las instalaciones cuentan con un sistema de estabilización de la corriente, así como con un sistema de generación propio con autonomía suficiente para mantener el suministro durante el tiempo que requiera el cierre ordenado y completo de todos los sistemas informáticos.

Los equipos informáticos están ubicados en un entorno donde se garantiza una climatización (temperatura y humedad) adecuada para unas condiciones óptimas de trabajo.

5.1.4 Exposición al agua

El PSCM dispone de sistemas de detección de inundaciones adecuados para proteger los equipos y activos ante tal eventualidad.

5.1.5 Advertencia y protección de incendios

Todas las instalaciones y activos del PSCM cuentan con sistemas automáticos de detección y extinción de incendios.

En concreto, los dispositivos criptográficos, y soportes que almacenan claves del PSCM, cuentan con un sistema específico y adicional al resto de la instalación, para la protección frente al fuego.

5.1.6 Almacenamiento de soportes

El almacenamiento de soportes de información se realiza de forma que se garantiza tanto su integridad como su confidencialidad, de acuerdo con la clasificación de la información establecida. Los soportes están protegidos contra daños, robo, deterioro y obsolescencia.

El acceso a estos soportes, incluso para su eliminación, está restringido a personas específicamente autorizadas.

5.1.7 Tratamiento de residuos

La eliminación de soportes, tanto en papel como magnéticos, se realiza mediante mecanismos que garantizan la imposibilidad de recuperación de la información. En el caso de soportes magnéticos, se procede al formateo o borrado permanente. En otro caso, se procede a la destrucción física del soporte. En el caso de documentación en papel, éste se somete a un tratamiento físico de destrucción.

5.1.8 Backup fuera de las instalaciones

El PSCM almacena copias de respaldo de la su información esencial en un entorno seguro protegido contra accidente y a una distancia suficiente para prevenir cualquier daño en caso de incidente, desastre o fallo del soporte.

El servicio de backup se prueba regularmente para asegurar que satisface los requisitos del Plan de Continuidad de Negocio.

5.2 Controles de procedimientos

El personal al servicio del PSCM realiza los procedimientos administrativos y de gestión de acuerdo con lo establecido en la DPCM y con la política y procedimientos de seguridad establecidos.

5.2.1 Roles fiables

Un rol fiable es un rol definido con responsabilidades que pueden conducir a problemas de seguridad si no se realizan de forma satisfactoria, bien accidental o maliciosamente.

El responsable de seguridad del PSCM define y documenta los roles fiables que deben ser aprobados por el responsable del PSCM.

El responsable del PSCM nombra y asigna los roles fiables al personal del PSCM bajo el principio del "menor privilegio" y teniendo en cuenta su formación, experiencia y los controles de seguridad descritos en este documento. Si es necesario, el PSCM proporcionará formación técnica y en seguridad adecuada para el personal nombrado.

Los roles fiables principales son responsable de Seguridad, Administrador de Sistemas, Operadores de Aplicaciones, Auditor de Sistemas y Oficial de Registro.

5.2.2 Número de personas por tarea

Para reforzar la seguridad del sistema, más de una persona está asignada a cada rol, con la excepción del rol de Responsable de Seguridad.

5.2.3 Identificación y autenticación para cada función

Todos los roles fiables requieren la verificación de la identidad por medios seguros: todos los roles fiables están asignados a individuos. El PSCM guarda documentación específica con los detalles de cada rol fiable.

5.2.4 Roles que requieren separación de tareas

El PSCM sigue los requisitos de seguridad generales del estándar [CWA 14167] para definir la separación de tareas por roles. El responsable del PSCM documenta y aprueba esta separación de tareas a petición del responsable de seguridad.

5.3 Controles de personal

5.3.1 Requisitos de historial, calificaciones, experiencia y autorización

El PSCM emplea personal cualificado y con la experiencia necesaria, para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados. Este requisito se aplica al personal de gestión del PSCM, especialmente en relación con los procedimientos de seguridad. La cualificación y experiencia se complementan mediante una formación y entrenamiento apropiados.

El personal en puestos fiables se encuentra libre de intereses personales que entren en conflicto con el desarrollo de la función que tenga encomendada.

El PSCM no asignará a ningún puesto fiable o de gestión a una persona que no sea idónea para el puesto, especialmente por haber sido condenada por delito o falta que afecte a su idoneidad para el puesto.

5.3.2 Procedimientos de verificación de historial

El PSCM contrastará o solicitará los elementos pertinentes que demuestren la veracidad de la información reflejada en el historial de las personas contratadas a las que se refiere el punto anterior.

5.3.3 Requisitos de formación

El PSCM formará al personal en puestos fiables y de gestión, hasta que alcancen la cualificación necesaria, de acuerdo con lo establecido en la sección 5.3.1 de la DPCM.

La formación debe incluir los siguientes contenidos:

- Principios y mecanismos de seguridad de la Autoridad de Certificación, así como el entorno de usuario de la persona a formar.
- Versiones de maquinaria y aplicaciones en uso.
- Tareas que debe realizar la persona.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.

5.3.4 Requisitos y frecuencia de actualización formativa

El PSCM realizará una actualización en la formación del personal al menos cada 12 meses centrada en nuevas amenazas y en las prácticas de seguridad establecidas.

5.3.5 Secuencia y frecuencia de rotación laboral

El PSCM podrá establecer métodos de rotación laboral para la prestación del servicio en turnos, con el objeto de cubrir las necesidades de 24x7 del servicio.

5.3.6 Sanciones por acciones no autorizadas

El PSCM dispone de un sistema sancionador [RD 3/2011] y [RD 5/2015], para depurar las responsabilidades derivadas de acciones no autorizadas, que se encuentra adecuado a la legislación laboral aplicable y, en especial, coordinado con el sistema sancionador del convenio colectivo u otra normativa que resulte de aplicación al personal. Las acciones

disciplinarias incluyen la suspensión o el despido de la persona responsable de la acción dañina.

5.3.7 Requisitos de contratación de profesionales externos

El PSCM podrá contratar puntualmente profesionales externos para cualquier función, incluso para un rol fiable, en cuyo caso deberán someterse a los mismos controles que los restantes empleados. Estas contrataciones se hacen conforme a [RD 3/2011].

En el caso de que el profesional no deba someterse a tales controles, estará constantemente acompañado por personal autorizado, cuando se encuentre en las instalaciones del PSCM.

5.3.8 Suministro de documentación al personal

El PSCM suministra la documentación que estrictamente precise su personal en cada momento, al objeto de que sea suficientemente competente.

5.4 Procedimientos de auditoría de seguridad

5.4.1 Tipos de eventos registrados

El PSCM guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado de los sistemas.
- Inicio y terminación de la aplicación de la autoridad de certificación o de la autoridad de registro central.
- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema.
- Generación y cambios en las claves del PSCM.
- Cambios en las políticas de emisión de certificados.
- Intentos de entrada y salida del sistema.
- Intentos no autorizados de entrada en la red del PSCM.
- Intentos no autorizados de acceso a los ficheros del sistema.
- Escrituras e intentos fallidos de escritura en el Repositorio de certificados.
- Eventos relacionados con el ciclo de vida del certificado, como solicitud, emisión, revocación y renovación de un certificado.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación del mismo.
- Otros eventos recogidos por sistemas de Log de la autoridad de certificación o de la autoridad de registro, incluyendo las labores de administración del sistema.
- Otros eventos recogidos por sistemas de Log de la Base de Datos.
- Otros eventos recogidos por sistemas de Log de los módulos criptográficos.

El PSCM almacena, de forma manual o electrónica, la siguiente información:

- La ceremonia de generación de claves.
- Los registros de acceso físico.

- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de incidencias de seguridad.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal.
- Posesión de datos de activación, para operaciones con la clave privada del PSCM.

5.4.2 Frecuencia de tratamiento de registros de auditoría

Los registros de auditoría se examinan por lo menos una vez a la semana en busca de actividad sospechosa o no habitual.

El procesamiento de los registros de auditoría se realiza mediante una revisión de los registros, verificando que estos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros.

Las acciones llevadas a cabo a partir de la revisión de auditoría también son documentadas.

5.4.3 Periodo de conservación de registros de auditoría

Los registros de auditoría se almacenan en el recinto durante por lo menos dos meses después de ser procesados y a partir de ese momento se archivan de acuerdo con la sección 5.5.2 de la DPCM.

5.4.4 Protección de los registros de auditoría

Los ficheros de registros, tanto manuales como electrónicos, están protegidos de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada usando controles de acceso lógico y físico.

La entidad que lleva a cabo el proceso de los registros de auditoría no posee capacidad de modificación de los registros. Existen procedimientos que aseguran que no se puedan eliminar o destruir los registros de eventos antes de que haya expirado su periodo de almacenamiento.

5.4.5 Procedimientos de copia de respaldo

Se generan, al menos, copias incrementales de respaldo de registros de auditoría diariamente y copias completas semanalmente.

5.4.6 Sistema de acumulación de registros de auditoría

El sistema de acumulación de registros de auditoría está compuesto por los registros de la aplicación, por los registros de red y por los registros del sistema operativo, además de por los datos manualmente generados, que son almacenados por el personal debidamente autorizado.

5.4.7 Notificación del acontecimiento de auditoría al causante del evento

Cuando el sistema de acumulación de registros de auditoría registra un evento, no es preciso enviar una notificación al que causó el evento. Se comunica si el resultado de su acción ha tenido éxito o no, pero no que se ha auditado la acción.

5.4.8 Análisis de vulnerabilidades

El PSCM controla cualquier intento de violación de la integridad del sistema de gestión de certificados, incluyendo los equipos soportes, las localizaciones físicas y el personal asignado a su operativa.

Los análisis de vulnerabilidad son ejecutados, repasados y revisados a través de un examen de esos eventos monitorizados. Estos análisis son ejecutados diariamente, mensualmente y anualmente de acuerdo con el Plan de Auditoría o documento que lo sustituya del PSCM.

5.5 Archivo de informaciones

El PSCM garantiza que toda la información relativa a los certificados se guarda durante un período de tiempo apropiado, según lo establecido en la sección 5.5.2 de la DPCM.

5.5.1 Tipos de eventos registrados

El PSCM almacena todos los eventos que tienen lugar durante el ciclo de vida de un certificado y registra las operaciones realizadas por los sistemas en el proceso de estos eventos.

5.5.2 Periodo de conservación de registros

El PSCM archiva los registros especificados en la sección anterior de este documento sin pérdida durante un periodo de 15 años como mínimo.

5.5.3 Protección del archivo

El PSCM mantiene la integridad y la confidencialidad del archivo que contiene los datos incluidos en los certificados emitidos y archiva los datos anteriormente citados de forma completa.

5.5.4 Procedimientos de copia de respaldo

El PSCM realiza copias de respaldo incrementales diarias de sus documentos electrónicos. Además, realiza copias de respaldo completas semanalmente.

Adicionalmente, se guardan los documentos en papel en un lugar fuera de las instalaciones del propio prestador para casos de recuperación de datos de acuerdo con la sección 5.7 de la DPCM.

5.5.5 Requisitos de sellado de tiempo

El PSCM emite los certificados y las CRL con información fiable de fecha y hora. Esta información de fecha y hora no está firmada electrónicamente.

Los servidores que emiten certificados y las CRL se sincronizan cada hora con un servidor externo NTP que mantiene la hora y fecha oficial (UTC) en España.

Los eventos significativos del PSCM se guardan con la hora exacta, estando esta sincronizada con UTC al menos una vez al día tal y como se requiere en los logs de auditoría.

5.5.6 Localización del sistema de archivo

El PSCM dispone de un sistema de mantenimiento de datos de archivo fuera de sus propias instalaciones.

5.5.7 Procedimientos de obtención y verificación de información de archivo

Sólo el personal autorizado tiene acceso a los datos de archivo, ya sea en las mismas instalaciones del PSCM o en su ubicación externa. En particular, se registrará cualquier acceso o intento de acceso a los datos de auditoría.

5.6 Renovación de claves de una Entidad de Certificación

No aplica.

5.7 Compromiso de claves y recuperación de desastre

El PSCM cuenta con procedimientos para la respuesta rápida a incidentes y notificar cualquier brecha de seguridad a las partes interesadas dentro de las 24 horas a partir de su identificación. Si se produce cualquier pérdida de integridad que afecte a un empleado público, la notificación se realizará en el momento de acuerdo con el Plan de Contingencias. Cualquier informe de incidente y procedimiento de respuestas se desarrollan bajo el principio de minimización de daños y fallos de funcionamiento ante incidentes de seguridad.

El PSCM resolverá cualquier vulnerabilidad crítica dentro de las 48 horas posteriores a su descubrimiento.

5.7.1 Corrupción de recursos, aplicaciones o datos

Cuando tenga lugar un evento de corrupción de recursos, aplicaciones o datos se iniciarán las gestiones necesarias, de acuerdo con el Plan de Contingencias, para hacer que el sistema vuelva a su estado normal de funcionamiento.

5.7.2 Revocación de la clave pública de la Entidad de Certificación

En el caso de que el PSCM revoque su Entidad de Certificación por cualquiera de los motivos expresados en la DPCM, llevará a cabo lo siguiente:

- Informará del hecho publicando una CRL.
- Realizará todos los esfuerzos necesarios para informar de la revocación a todos los suscriptores así como a los terceros que confían en esos certificados.
- En su caso, notificará este hecho al órgano competente de la AGE.

5.7.3 Compromiso de la clave privada de la Entidad de Certificación

El Plan de Continuidad de Negocio del PSCM considera el compromiso o la sospecha de compromiso de su clave privada como un desastre. En caso de compromiso, se realizarán como mínimo las siguientes acciones:

- Realizará todos los esfuerzos necesarios para informar del compromiso a todos los suscriptores y verificadores.
- Indicará que los certificados y la información del estado de revocación que han sido entregados usando la clave del PSCM ya no son válidos. Para ello, se ejecutarán los siguientes pasos:
    - Revocación del certificado del PSCM.
    - Publicación de la CRL correspondiente.
    - Revocación masiva de certificados generados por la Entidad de Certificación, procediendo a la eliminación de los mismos por los mecanismos implementados en el sistema a tal fin.

5.7.4 Desastre sobre las instalaciones

El conjunto de sistemas que conforman la Entidad de Certificación está implementado en condiciones de alta disponibilidad y redundancia en todos y cada uno de los componentes que lo conforman. De esta manera se garantiza la continuidad de los servicios frente a la caída de cualquiera de sus componentes.

De manera añadida, el PSCM cuenta con un centro de respaldo o de recuperación de desastres, que da continuidad a dichos servicios frente a catástrofe o mantenimiento de las instalaciones que albergan el sistema primario. El centro de respaldo dispone de las protecciones físicas de seguridad detalladas en el Plan de Seguridad correspondiente.

El PSCM desarrolla, mantiene, prueba y, si es necesario, ejecutará su Plan de Continuidad de Negocio. Este plan expone cómo restaurar los servicios de los sistemas de información para el caso de que ocurra un desastre sobre las instalaciones.

El PSCM es capaz de restaurar la operación normal de los servicios de revocación en las 24 horas siguientes al desastre, pudiendo, como mínimo, ejecutarse las siguientes acciones:

- En su caso, revocación de certificados.
- Publicación de información de revocación.

La base de datos de respaldo utilizada está sincronizada con la base de datos de producción, dentro de los límites temporales especificados en el Plan de Continuidad de Negocio del PSCM.

Tras cualquier tipo de desastre, el PSCM tomará todas las medidas posibles para evitar la repetición del mismo.

5.8 Finalización del servicio

El PSCM cuenta con un Plan de Finalización de sus servicios que especifica el procedimiento a seguir en el caso de que ocurra tal suceso. Este plan minimiza los problemas que puedan sufrir suscriptores y terceras partes como resultado de la finalización de los servicios ofrecidos por el PSCM.

El PSCM comunicará al suscriptor por cualquier medio que garantice el envío y la recepción de la notificación, con un plazo mínimo de antelación de 2 meses a su fecha de su extinción, su intención de cesar como PSC.

La responsabilidad de esta notificación corresponde al responsable del PSCM, quien decidirá el mecanismo más adecuado.

El responsable del PSCM decidirá cómo publicar la última CRL para hacer disponible la información sobre el estado de revocación de los certificados más allá del período de validez de los mismos.

En el supuesto de que el PSCM decidiera transferir la actividad a otro PSC, comunicará al MINETAD y al suscriptor de sus certificados los acuerdos de transferencia. A tal efecto el PSCM enviará el documento explicativo de las condiciones de transferencia así como de las condiciones de utilización que regularán las relaciones entre el suscriptor y el PSC al cual se transfieren los certificados. Esta comunicación se realizará por cualquier medio que garantice el envío y la recepción de la notificación, con una antelación mínima de 2 meses al cese de su actividad.

El suscriptor deberá consentir de forma expresa la transferencia de los certificados, aceptando las condiciones del PSC al que se transfieren. Transcurrido el plazo de dos meses, sin que exista acuerdo de transferencia o sin que el suscriptor acepte expresamente la misma, los certificados serán revocados.

En el supuesto de que no existieran acuerdos con otros PSC, finalizado el plazo de los 2 meses de antelación en la comunicación, todos los certificados serán revocados de manera automática.

Se dará por finalizado cualquier autorización de terceros con los que el PSCM mantenga un contrato de prestación de servicios (identificación, emisión, albergue, etc.).

Cualquier clave privada, incluyendo las copias de respaldo, será destruida o retirada de su uso de tal forma que de ningún modo estas claves puedan ser recuperadas.

Una vez la Autoridad de Registro cese en el ejercicio de las funciones que asuma transferirá los registros con obligación legal de resguardar que mantenga al PSCM, siendo cualquier otra información cancelada y destruida.

El coste necesario para cumplir con estos requisitos descansa sobre la responsabilidad patrimonial de la Administración General del Estado.

6 Controles de seguridad técnica

El PSCM emplea sistemas y productos fiables que están protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

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

Los pares de claves de la Entidad de Certificación Raíz se generaron en un módulo criptográfico con certificación FIPS 140-2 nivel 3 y acreditación [CCEAL4+]. Los pares de claves de las Entidades de Validación y Entidades de Registro se generaron en servidores seguros.

Antes de la caducidad del certificado raíz de la Autoridad de Certificación del PSCM utilizado para la firma de las claves de los suscriptores, la Autoridad de Certificación del PSCM generará un nuevo certificado y aplicará todas las acciones posibles que eviten la suspensión de las operaciones de cualquier entidad que confíe en el certificado de la CA. El nuevo certificado de la CA será generado y distribuido de acuerdo con esta política.

Los pares de claves del resto de certificados se generan de acuerdo a la siguiente tabla:

CERTIFICADO	NIVEL	MÉTODO DE GENERACIÓN
EMPLEADO PÚBLICO	Alto	Generación de claves por el usuario en tarjeta criptográfica.
EMPLEADO PÚBLICO CENTRALIZADO Y GESTIONADO POR HSM	Medio	Generación de claves por el usuario centralizadas y gestionadas por HSM. Generados en el dispositivo criptográfico centralizado en conformidad con los requisitos de certificación FIPS 140-2 y acreditación [CCEAL4+].
SELLO ELECTRÓNICO PARA LA ACTUACIÓN AUTOMATIZADA	Medio	Emisión con generación de claves por el prestador y entrega en formato PKCS#12 (soporte software). • Generación de claves en software. Implica que el usuario emplea estas claves en su contenedor software seguro. Emisión con generación de claves por el solicitante y solicitud en formato PKCS#10 (soporte software). Entrega del certificado en formato PKCS#7. • Generación de claves por el usuario en software.

Los dispositivos seguros pueden ser tarjetas criptográficas, tokens USB criptográficos, o cualquier otro tipo de dispositivo, en especial módulos criptográficos (HSM), que cumplan

con los requisitos de seguridad establecidos por la normativa vigente para los dispositivos seguros.

El PSCM guarda un documento que refleja que la ceremonia se desarrolló de acuerdo con el procedimiento establecido y que garantizó la integridad y confidencialidad del par de claves. Este documento fue firmado de acuerdo con [ETSI EN 319 411-1].

6.1.2 Entrega de la clave privada al suscriptor

En el caso de Certificados de Empleado Público de nivel alto la clave privada se genera directamente en el dispositivo criptográfico que cumple lo establecido en [CWA 14169].

En el caso del CEPCHSM la clave privada se genera y gestiona por el HSM no entregándose en ningún caso al suscriptor puesto que sólo se permite el acceso a la utilización de la misma.

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

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

En el caso de certificados de sello electrónico la clave privada del certificado es generada por la Entidad de Certificación y se entrega debidamente protegida a través de un PKCS#12.

6.1.3 Entrega de la clave pública al emisor del certificado

Las claves públicas de los Certificados de Empleado Público las genera el propio emisor de certificados, momento en que obtiene una copia de las mismas.

El método de remisión de la clave pública al PSCM se hace mediante el formato estándar PKCS#10, otra prueba criptográfica equivalente o cualquier otro método aprobado por la AGE.

6.1.4 Distribución de la clave pública del Prestador de Servicios de Certificación

Los datos de verificación de firma del PSCM se distribuyen en un formato (autofirmado) conforme a los estándares del mercado mediante su publicación en el repositorio del PSCM.

Para la comprobación de la autenticidad de cualquier "certificado autofirmado", elemento último de cualquier Cadena de Certificación, se puede verificar la huella digital correspondiente con la publicada en la sección 1.3.1 de este documento.

6.1.5 Tamaños de claves

La DPCM utiliza el escenario de seguridad definido por la AGE que determina el criterio de robustez y viabilidad aplicable para cada perfil de certificado de acuerdo con [CCN-STIC-405].

Las especificaciones que se incluyen a continuación siguen la especificación técnica [ETSI TS 102 176-1]. Se distinguen requisitos criptográficos para las autoridades emisoras y para entidades o certificados finales. Se distingue su aplicación en un nivel de aseguramiento alto y medio.

- Autoridad Raíz:

Nivel Aseguramiento	Entidad	Algoritmo y longitud mínima
Alto	CA Raíz	RSA-4096
Alto	CA Subordinada	RSA-4096
Medio	CA Raíz	RSA-4096
Medio	CA Subordinada	RSA-4096

- Entidades finales:

Nivel Aseguramiento	Entidad	Algoritmo y longitud mínima
Alto	Certificados finales	RSA-2048
Medio	Certificados finales	RSA-2048

6.1.6 Generación de 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, es decir, el 4º número de Fermat ([4]).

La clave pública del CEPCHSM está codificada de acuerdo con [IETF RFC 6818] y PKCS#1. El algoritmo de generación de claves es el RSA.

6.1.7 Comprobación de calidad de parámetros de clave pública

La calidad de los parámetros es garantizada para el caso de las claves de la Entidad de Certificación Raíz en el módulo criptográfico por la acreditación [FIPS 140-2] Nivel 2 y 3, acreditación [CC EAL4+].

6.1.8 Generación de claves en aplicaciones informáticas o en bienes de equipo

Los números aleatorios necesarios para la generación de claves asociadas a certificados de nivel alto se generan en dispositivos criptográficos, ya sean módulos HSM o tarjetas criptográficas. Las claves asociadas a los certificados del PSCM se generan en hardware criptográfico que cumple los niveles de certificación de seguridad acordados.

Las claves asociadas a los Certificados de Empleado Público se generan en dispositivos criptográficos que cumplen los niveles de certificación de seguridad acordados.

La generación de claves para los restantes tipos de certificados se realiza mediante aplicaciones informáticas.

[4] El n-ésimo número de Fermat es F = (2)^(2^n)+1.

6.1.9 Propósitos de uso de claves

Las extensiones *KeyUsage* y *Extended KeyUsage* de los certificados indican los usos permitidos de las correspondientes claves privadas y de los certificados asociados.

Los niveles de aseguramiento bajo los que se emite un certificado condicionan el uso permitido para las claves como sigue:

CERTIFICADO	KEYUSAGE	EXTENDED KEYUSAGE
EMPLEADO PÚBLICO (Autenticación Nivel Alto)	Digital Signature	Email Protection Client Authentication SmartCard Logon
EMPLEADO PÚBLICO (Firma Nivel Alto)	Content Commitment	No Usado
EMPLEADO PÚBLICO HSM (Autenticación Nivel Medio)	Digital Signature	Client Authentication
EMPLEADO PÚBLICO HSM (Firma Nivel Medio)	Content Commitment	No Usado
SELLO ELECTRÓNICO PARA LA ACTUACIÓN AUTOMATIZADA	Digital Signature, Content Commitment, Key Encipherment, Data Encipherment	Email Protection Client Authentication

6.2 Protección de la clave privada y módulos criptográficos

El PSCM guarda registro de los eventos relativos a la preparación y gestión de sus módulos criptográficos.

6.2.1 Estándares de módulos criptográficos

El módulo en uso para la generación de las claves privadas de la CA Raíz y firma de los certificados, está acreditado [FIPS 140-2] y acreditación [CCEAL4+].

La puesta en marcha de cada una de las Entidades de Certificación, teniendo en cuenta que se utilizan módulos criptográficos de seguridad (HSM), conlleva las siguientes tareas:

- Inicialización del estado del módulo HSM.
- Creación de las tarjetas de administración y de operador.
- Generación de las claves de la Entidad de Certificación.

El módulo criptográfico que protege las claves privadas asociadas al CEPCHSM dispone igualmente de las acreditaciones [FIPS 140-2] y acreditación [CCEAL4+] así como la [CWA 14167].

Para las tarjetas criptográficas se aplica la homologación [CCEAL4+], cumpliendo los requisitos del artículo 24 de LFE como dispositivo seguro de creación de firma.

Todos los componentes mencionados anteriormente soportan el estándar PKCS#11 y, en el caso de las tarjetas criptográficas, el CSP de Microsoft.

El PSCM garantiza que los módulos criptográficos no fueron alterados durante su transporte ni durante su almacenamiento. El PSCM garantiza que dichos módulos funcionan correctamente.

6.2.2 Control por más de una persona sobre la clave privada

El acceso a la operativa de la clave privada de la Entidad de Certificación está sujeto a un proceso de autenticación seguro estando adicionalmente custodiada ésta por dispositivos criptográficos seguros (HSM).

La clave privada de la Entidad de Certificación Raíz del PSCM se encuentra bajo control multipersonal. Ésta se activa mediante la inicialización del software de la Entidad de Certificación por medio de la combinación mínima de operadores de la AC correspondiente. Éste es el único método de activación de dicha clave privada. Son necesarios dos operadores, de un total de cinco, para activar y usar la clave privada de la Entidad de Certificación Raíz.

La custodia de las claves privadas del resto de certificados la realizan los propios titulares de las mismas. El acceso a las claves privadas está protegido al menos mediante un PIN solo conocido por su titular. En este caso el acceso se realizará por una única persona: el responsable del certificado.

La clave privada asociada al CEPCHSM se encuentra, con un alto nivel de confianza, bajo el exclusivo control del responsable del certificado (el empleado público) y protegida por dos factores de autenticación.

6.2.3 Introducción de la clave privada en el módulo criptográfico

Las claves privadas de la Entidad de Certificación Raíz del PSCM se generaron directamente en los módulos criptográficos durante la ceremonia de generación de claves quedando almacenadas en ficheros cifrados con claves fragmentadas y en tarjetas inteligentes de las que no pueden ser extraídas. Dichas tarjetas fueron las empleadas para introducir la clave privada en el módulo criptográfico.

En el caso de Certificados de Empleado Público, las claves son generadas directamente de manera local por y en el dispositivo criptográfico.

6.2.4 Método de activación de la clave privada

La activación de la clave privada de la Entidad de Certificación requiere:

- El PED del HSM.
- El Administrador del Sistema con la llave negra (protegida por PIN) junto con la clave de la partición.
- El Operador del Sistema.

La clave privada de cada suscriptor se activa mediante la introducción del PIN en el dispositivo criptográfico o aplicación de firma.

Para la activación de la clave privada asociada al CEPCHSM se requiere que el empleado público esté autenticado con su usuario y contraseña, haya introducido su segundo factor de autenticación y la contraseña de protección de su certificado tan sólo conocida por el empleado público y no almacenada en los sistemas.

6.2.5 Método de desactivación de la clave privada

La desactivación de la clave privada del certificado raíz del PSCM se produce al desactivar la partición y apagar el sistema hasta la nueva operación que requiera una activación.

La desactivación de la clave privada de la SubCA se produce al desactivar la partición lo cual requiere:

- El PED del HSM.
- El Administrador del Sistema con la llave negra (protegida por PIN) junto con la clave de la partición.
- El Operador del Sistema.

Para certificados en tarjeta con la consideración de dispositivo seguro de creación de firma, cuando la misma se retira del dispositivo lector, o la aplicación que la utilice finaliza la sesión, es necesaria nuevamente la introducción del PIN.

Para el CEPCHSM, la desactivación de la clave privada se produce al cerrar la sesión de la aplicación que se utiliza para la firma.

6.2.6 Método de destrucción de la clave privada

Para los módulos criptográficos (HSM), las claves serán borradas de acuerdo con el Manual de Administración del HSM, sección Borrado/Destrucción para una Eliminación Segura.

En el caso de las tarjetas criptográficas se eliminan limpiando el dispositivo a través de las aplicaciones de gestión de los dispositivos.

La clave privada asociada al CEPCHSM se destruye de forma segura en cualquier proceso de renovación y revocación así como las copias realizadas para garantizar la continuidad del servicio. El conjunto completo de claves privadas se destruye de acuerdo con el Manual de Administración del HSM, sección Borrado/Destrucción para una Eliminación Segura.

6.3 Custodia, copia y recuperación de claves

6.3.1 Política y prácticas de custodia, copia y recuperación de claves

Las claves privadas de la Entidad de Certificación del PSCM se almacenan en espacios ignífugos y protegidos por controles de acceso físico dual. La custodia del conjunto de claves privadas de la Entidad de Certificación Raíz, generadas y contenidas en el módulo criptográfico tiene lugar en la SGTIC a nivel físico y lógico. El acceso requiere un proceso de autenticación múltiple basado en tarjeta criptográfica.

La custodia del conjunto de claves privadas de otros componentes como el sellado de tiempo o validación tiene lugar en la SGTIC a nivel físico y lógico. El acceso requiere un proceso de autenticación.

La custodia de la clave privada para el resto de certificados, independientemente del soporte, es responsabilidad del suscriptor, accediendo a la misma mediante PIN o contraseña segura.

La clave privada de la Entidad de Certificación Raíz del PSCM cuenta con una copia de respaldo almacenada en una dependencia independiente de aquélla donde se encuentra habitualmente debiendo ser recuperada en su caso, por personal sujeto a la política de confianza del personal. Este personal estará expresamente autorizado para estos fines. En todo momento existe una copia de seguridad en soporte físico de las claves de la Entidad de Certificación Raíz, procediéndose a su revisión cada año. Cuando las claves se almacenan en un módulo hardware de proceso dedicado, se proveen los controles oportunos para que éstas nunca puedan abandonar el dispositivo.

Los controles de seguridad a aplicar a las copias de respaldo del PSCM son de igual o superior nivel a los que se aplican a las claves habitualmente en uso.

En el caso del resto de certificados, bajo ningún concepto las claves privadas utilizadas para los servicios de no-repudio son guardadas por terceras partes: sólo los suscriptores custodiarán la única copia de esta clave en su módulo criptográfico o equivalente. Sólo en los supuestos en los que haya que dar servicio de recuperación de claves privadas para propósitos distintos del no-repudio, se podrán almacenar estas claves privadas.

En el caso del CEPCHSM es de aplicación lo detallado en la sección 4.12 de la DPCM.

6.3.2 Archivo de la clave privada

Las claves privadas de la CA del PSCM se archivan al final de su periodo de operación, de forma permanente.

6.4 Otros aspectos de gestión del par de claves

6.4.1 Archivo de la clave pública

El PSCM archiva sus claves públicas, de acuerdo con lo establecido en la sección 5.5 de la DPCM.

6.4.2 Periodos de utilización de las claves pública y privada

Los periodos de utilización de las claves son los determinados por la duración del certificado, transcurrido el cual no pueden continuar utilizándose.

6.5 Datos de activación

6.5.1 Generación e instalación de los datos de activación

Para la instauración de una Entidad de Certificación se deben crear las tarjetas criptográficas que se utilizan para las actividades de recuperación y funcionamiento. La Entidad de Certificación del PSCM opera con dos tipos de roles, cada uno con sus correspondientes tarjetas criptográficas:

- El conjunto de tarjetas de administrador. Estas tarjetas serán necesarias para recuperar el estado del HSM si ocurre algún desastre o si se desea trasladar las claves a otro módulo.
- El conjunto de tarjetas de operador. Estas tarjetas se utilizan para realizar cualquier tipo de operación con la Entidad de Certificación por lo que el operador debe introducir el PIN asociado a cada tarjeta.

Si una o más tarjetas se pierden o dañan, o uno de los administradores olvida su PIN o dejan de ser utilizables por alguna razón, deberá volverse a generar todo el conjunto de tarjetas tan pronto como sea posible.

Cuando el PSCM facilita al suscriptor un dispositivo seguro de creación de firma, los datos de activación del dispositivo (PIN), son generados de forma segura.

La activación de la clave privada asociada al CEPCHSM requiere que el empleado público esté autenticado con su usuario y contraseña y haya introducido su segundo factor de autenticación.

6.5.2 Protección de datos de activación

Sólo el personal autorizado, en este caso los Operadores y Administradores de la Entidad de Certificación posee las tarjetas criptográficas con capacidad de activación de las Entidades de Certificación y conocen los PIN y contraseñas para acceder a los datos de activación.

Cuando el PSCM facilita al suscriptor el dispositivo seguro de creación de firma, el suscriptor es el único responsable de crear los datos de activación del mismo. Ningún suscriptor deberá difundir por motivo alguno, ni almacenar en soporte alguno el PIN de activación ni de su tarjeta criptográfica personal o equivalente.

En el caso de la clave asociada al CEPCHSM, el empleado público es el único que conoce la contraseña personal del directorio activo y dispone de su segundo factor de autenticación, siendo por tanto el único responsable de la protección de los datos de activación de su clave privada.

6.6 Controles de seguridad informática

6.6.1 Requisitos técnicos específicos de seguridad informática

Existen una serie de controles en el emplazamiento de los diferentes elementos de los sistemas del PSCM.

Controles operacionales:

- Todos los procedimientos de operación están debidamente documentados en los correspondientes manuales de operación. El PSCM mantiene un Plan de Contingencias (Plan de Continuidad de Negocio).
- Están implantadas herramientas de protección contra virus y software malicioso o no autorizado.
- El PSCM aplica un procedimiento de actualización y aplicación de parches de seguridad en un tiempo razonable tras su publicación. El responsable del PSCM debe aprobar la no aplicación de estos parches y las razones para ello (cuando las desventajas sean mayores que las ventajas) deberán documentarse.
- Se lleva a cabo un mantenimiento continuado del equipamiento, con el fin de asegurar su disponibilidad e integridad continuadas.
- Existe un procedimiento de salvado, borrado y eliminación segura de soportes de información, medios removibles y equipamiento obsoleto.
- El servicio de revocación de certificados está disponible 24x7.
- Cuando se utilizan proveedores de servicios de registro externos, los intercambios de datos de registro se intercambian de forma segura y sólo con aquellos proveedores correctamente autenticados.

Control de accesos.

- Se utilizan cuentas de usuario únicos, de forma que los usuarios son relacionados con las acciones que realizan y se les puede responsabilizar de sus acciones.
- La asignación de derechos se lleva a cabo siguiendo el principio de concesión mínima de privilegios.
- Se produce una eliminación inmediata de los derechos de acceso de los usuarios que cambian de puesto de trabajo o abandonan la organización.

- La asignación de privilegios especiales se realiza "caso a caso" y se suprimen una vez terminada la causa que motivó su asignación.
- Existen directrices de calidad en las contraseñas

6.6.2 Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas por el PSCM son fiables, debiendo acreditarse dicha condición, por ejemplo, mediante una certificación de producto contra un perfil de protección adecuado, conforme a [ISO 15408], o equivalente.

6.7 Controles técnicos del ciclo de vida

6.7.1 Controles de desarrollo de sistemas

Se prestará especial atención a los requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente empleado en las aplicaciones de Entidad de Certificación y de Registro, para garantizar que los sistemas son seguros.

Se emplean procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.

6.7.2 Controles de gestión de seguridad

El PSCM mantiene un inventario de todos los activos de información y realiza una clasificación de los mismos, de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

La configuración de los sistemas se audita de forma periódica, de acuerdo con lo establecido en la sección 8.2 de la DPCM.

Se realiza un seguimiento de las necesidades de capacidad, y se planifican procedimientos para garantizar la disponibilidad y los medios de almacenamiento para los activos de información.

6.7.3 Evaluación del nivel de seguridad del ciclo de vida

La AGE podrá exigir que el PSCM se someta a evaluaciones independientes, auditorías y, en su caso, certificaciones de seguridad del ciclo de vida de los productos del prestador.

6.8 Controles de seguridad de red

El PSCM protege su red y sistemas ante cualquier tipo de ataque.

El PSCM segmenta sus sistemas en redes o zonas de acuerdo con su evaluación de riesgos y las relaciones entre sistemas y servicios fiables. El PSCM aplica los mismos controles de seguridad a todos los sistemas localizados en la misma zona.

El PSCM restringe el acceso y las comunicaciones entre zonas al estrictamente necesario para la operación de sus servicios. Las conexiones y servicios no necesarios están explícitamente prohibidos o desactivados. El conjunto de reglas establecido se revisa periódicamente.

El PSCM alberga sus sistemas críticos en una o más zonas protegidas.

Los sistemas de producción del PSCM están separados de los sistemas usados para desarrollo y pruebas.

El PSCM subcontrata o desarrolla tests de penetración y análisis de vulnerabilidad en las IP seleccionadas de sus redes públicas y privadas periódicamente de forma anual.

El PSCM configura todos los sistemas de la CA eliminando o deshabilitando todas las cuentas, aplicaciones, servicios, protocolos y puertos no usados en operaciones de la CA.

El PSCM mantiene su CA raíz desconectada.

El PSCM mantiene sus SubCA en una zona de alta seguridad.

El acceso a las diferentes redes del PSCM está limitado a individuos debidamente autorizados. En particular:

- Existen controles para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos se configuran de forma que se impidan accesos y protocolos que no sean necesarios para la operación del PSCM.
- Los datos sensibles se protegen cuando se intercambian a través de redes no seguras (incluyendo como tales los datos de registro del suscriptor).
- Los componentes locales de red se encuentran ubicados en entornos seguros y se realiza la auditoría periódica de sus configuraciones.

6.9 Sellado de tiempo

No aplicable.

7 Perfiles de certificados y listas de certificados revocados

7.1 Perfil de certificado

Los perfiles de certificados, así como las extensiones soportadas, se ajustan a lo definido por la AGE y el reglamento eIDAS.

7.1.1 Número de versión

Solo se permiten y operan con certificados basados en la versión 3 de la recomendación X.509 del ITU-T (International Telecommunications Union-Telecommunication).

7.1.2 Periodo de Validez de los certificados

La duración de los certificados emitidos se muestra a continuación:

CERTIFICADO	NIVEL	DURACIÓN
EMPLEADO PÚBLICO	Alto / Medio	Cinco años
SELLO ELECTRÓNICO PARA LA ACTUACIÓN AUTOMATIZADA	Medio	Cinco años

7.1.3 Campos y Extensiones del certificado

Todos los OID empleados para identificar los diferentes campos de los certificados son únicos a nivel internacional.

El PSCM no emite certificados que contengan extensiones propietarias marcadas como críticas. En cualquier caso, la AGE podrá ignorar el contenido de las extensiones propietarias que no estén marcadas como críticas.

El PSCM establece la sintaxis y el tratamiento semántico de los campos o extensiones contenidos en los certificados:

- No se emplea un mismo campo o extensión para establecer definiciones semánticas diferentes en un mismo tipo de certificado.
- Se proporcionará el método de extracción de cada uno de los datos individualizados, que, en su conjunto, determinan de forma unívoca el contenido de todos los campos y extensiones del certificado.
- El método de extracción y la interpretación semántica de la información no dependerá del contenido de ningún otro campo.

Los certificados cualificados emitidos bajo la DPCM incluyen la indicación expresa de que se expiden como tales (con la expresión *certificado cualificado*) dentro de la extensión *CertificatePolicies* del certificado o mediante el uso de extensiones específicas (OID 1.3.6.1.5.5.7.1.3).

A continuación se presentan los campos y extensiones de certificado de uso en la DPCM para las tipologías de certificados emitidos.

CERTIFICADO	CAMPOS OBLIGATORIOS
SELLO ELECTRÓNICO PARA LA ACTUACIÓN AUTOMATIZADA	• *Version* • *Serial Number* • *Issuer Distinguished Name (Country (C), Organization (O), Organizational Unit (OU), Common Name (CN))* • *Validity (Not Before, Not After)* • *Subject (Country (C), Organization (O), Organizational Unit (OU), OI, Common Name (CN))* • *Subject Public Key Info* • *Signature Algorithm*
EMPLEADO PÚBLICO[5]	• *Version* • *Serial Number* • *Issuer Distinguished Name (Country (C), Organization (O), Organizational Unit (OU), Common Name (CN))* • *Validity (Not Before, Not After)* • *Subject (Country (C), Organization (O), Organizational Unit (OU), Serial Number, Surname, Given Name, Common Name (CN))* • *Subject Public Key Info* • *Signature Algorithm*

CERTIFICADO	CAMPOS RECOMENDABLES
SELLO ELECTRÓNICO PARA LA ACTUACIÓN AUTOMATIZADA	• *Issuer Distinguished Name (Locality, Serial Number, Organization Identifier)* • *Subject (Surname, Given Name, Organization Identifier)*
EMPLEADO PÚBLICO[6]	• *Issuer Distinguished Name (Locality, Serial Number)* • *Subject (Organizational Unit (OU), Organizational Unit (OU), Organization Identifier, Title)*

CERTIFICADO	EXTENSIONES OBLIGATORIAS
SELLO ELECTRÓNICO PARA LA ACTUACIÓN AUTOMATIZADA	• *Authority Key Identifier* • *Subject Key Identifier* • *Key Usage* • *CRLDistributionPoint (distributionPoint)* • *Authority Info Access (Access Method, Access Location del OCSP y del calssuer)* • *Qualified Certificate Statements* • *Certificate Policies (Policy Identifier, Policy Qualifier ID [CPS Pointer, User Notice], EU qualified certificate policy Identifier (sólo si ALTO FIRMA o MEDIO / SUSTANCIAL)* • *Subject Alternative Names (Directory Name)*
EMPLEADO PÚBLICO[7]	• *Authority Key Identifier* • *Subject Key Identifier* • *CRLDistributionPoint (distributionPoint)* • *Authority Info Access (Access Method, Access Location del OCSP y de calssuer)* • *Key Usage* • *Subject Alternative Names (Directory Name= Identidad Administrativa)*

[5] Incluye los gestionados por HSM
[6] Incluye los gestionados por HSM
[7] Incluye los gestionados por HSM

CERTIFICADO	EXTENSIONES RECOMENDABLES
SELLO ELECTRÓNICO PARA LA ACTUACIÓN AUTOMATIZADA	• *Issuer Alternative Name* • *Subject Alternative Names*
EMPLEADO PÚBLICO[8]	• *Issuer Alternative Name* • *Subject Alternative Names*

7.1.4 Identificadores de objeto (OID) de los algoritmos

La DPCM utiliza el escenario de seguridad de la AGE, que determina el criterio de robustez y viabilidad aplicable para cada perfil de certificado de acuerdo con la guía [CCN-STIC-405].

Las especificaciones que se incluyen a continuación siguen la especificación técnica [ETSI TS 102 176-1]. Se distinguen requisitos criptográficos para las autoridades emisoras y para entidades o certificados finales. Se distingue su aplicación en un nivel de aseguramiento alto y medio:

- Autoridad Raíz y Subordinadas:

Nivel Aseguramiento	Entidad	Longitud
Alto y Medio	CA Raíz y subraíz	RSA-4096

- Entidades finales:

Nivel Aseguramiento	Entidad	Longitud
Alto	Certificados finales	RSA-2048
Medio	Certificados finales	RSA-2048

Las firmas de los certificados emitidos bajo la DPCM se identifican con los siguientes OID:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Así mismo, los certificados contendrán los siguientes OID para identificar los algoritmos de las claves públicas emitidas:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

El PSCM sólo certificará las claves públicas asociadas con los algoritmos criptográficos identificados anteriormente y sólo utilizará los algoritmos criptográficos de firma descritos

[8] Incluye los gestionados por HSM

anteriormente para firmar certificados, listas de certificados revocados y cualquier otro elemento de la Entidad de Certificación.

7.1.5 Formatos de nombres

La composición de nombres para los certificados de usuario cuya tipología se define en la DPCM es aquella descrita en los apartados 3.1.2 y 3.1.3. Para ello, se hará un uso de los campos *Subject Name* y *SubjectAlternativeName* según el esquema normalizado propuesto por la AGE (sección 7.1.3) y descrito en los documentos de perfiles.

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

Cada tipo de certificado recibe su propio OID unívoco (ver documentos de perfiles) y no empleado para identificar diferentes tipos, políticas o versiones de los certificados emitidos.

7.1.7 Uso de la extensión *Policy Constraints*

En todos los certificados emitidos por el PSCM, no se requiere la extensión *PolicyConstraints*, pudiendo ser una secuencia vacía.

7.1.8 Sintaxis y semántica de los calificadores de política

Contendrán el URI de la DPCM.

7.2 Perfil de la lista de certificados revocados

El perfil de la lista de certificados revocados es conforme con las normas indicadas en las correspondientes condiciones adicionales.

7.2.1 Número de versión

El PSCM únicamente utiliza las CRL conforme a lo previsto en [ITU-T X.509], así como por el perfil previsto en la especificación técnica [IETF RFC 6818].

7.2.2 CRL y extensiones

Las CRL incluirán la siguiente información:

- El campo de versión, asignado al código de versión 2.
- El campo indicativo de la próxima actualización de la CRL completa, conteniendo la fecha programada de la siguiente emisión de la CRL.

8 Auditorías de cumplimiento y otros controles

8.1 Auditorías de cumplimiento

El PSCM realiza periódicamente una auditoría interna de cumplimiento para probar que cumple los requisitos de seguridad y de operación necesarios para satisfacer la política de los servicios de certificación de la AGE.

8.2 Frecuencia de la auditoría de cumplimiento

De acuerdo con el eIDAS, el PSCM será auditado al menos cada 24 meses por un organismo de evaluación de la conformidad, además de las auditorías internas que pueda llevar a cabo bajo su propio criterio o en cualquier momento, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de claves.

8.3 Identificación y calificación del auditor

La auditoría de cumplimiento se llevará a cabo por un organismo de evaluación de la conformidad tal y como dicta el eIDAS y otra legislación aplicable.

8.4 Relación del auditor con la entidad auditada

El auditor no pertenecerá en ningún caso al personal a cargo de la operación de la Entidad de Certificación. Así mismo el auditor, en caso de ser externo, no pertenecerá a los equipos de trabajo que han participado en la implantación de la arquitectura del PSCM.

Las auditorías de cumplimiento ejecutadas por terceros serán llevadas a cabo por una entidad independiente del PSCM, la cual no deberá tener ningún conflicto de intereses que menoscabe su capacidad de llevar a cabo servicios de auditoría.

El auditor demandará el acceso al sistema con el rol específico de auditor. En las labores de inspección que quiera llevar a cabo el auditor en relación a los módulos criptográficos, estos serán siempre operados por el personal de la SGTIC, proporcionando al mismo la información requerida.

El auditor no estará nunca en ningún caso autorizado a la manipulación física de los mismos, ni se le suministrará acceso a las máquinas que soportan la plataforma. En caso de realizar auditoría de los niveles de seguridad física, estará siempre acompañado por personal de la SGTIC.

8.5 Listado de elementos objeto de auditoría

Los elementos objeto de auditoría son los siguientes:

- Procedimientos de certificación.
- Sistemas de información.
- Protección del centro de proceso de datos.
- Documentación del servicio.
- Existencia de las autorizaciones pertinentes que habilitan a los operadores de los componentes que conforman la Entidad de Certificación, siguiendo lo estipulado en

la DPCM. La verificación del no cumplimiento de esta circunstancia supone una falta muy grave.

- Medidas efectivas de seguridad en el acceso a la administración y roles de los distintos componentes que conforman la Entidad de Certificación.
- Segregación efectiva de los roles establecidos en la DPCM.
- Control y seguimiento de las versiones de software y correcta actualización del mismo, debiendo proceder a la estricta comprobación del software en explotación y las versiones oficiales soportadas por la plataforma.
- Procedimientos de contingencia.
- Capacidades de espacio de las máquinas que conforman la Entidad de Certificación de cara a prevenir desbordamientos de espacio.
- Copias físicas de respaldo del contenido de los HSM.
- Estado de las bases de datos de los sistemas.
- Adecuación de la DPCM a los requisitos eIDAS.
- Correspondencia de los procedimientos y controles técnicos presentes en la DPCM con las medidas efectivas y reales.

De manera genérica, conjuntamente con los aspectos críticos señalados anteriormente se procederá a auditar conforme a las buenas prácticas definidas en [ISO 27001] o equivalente.

8.6 Acciones a emprender como resultado de una falta de conformidad

Cuando un auditor encuentre una deficiencia en la operativa de la Entidad de Certificación o los procedimientos estipulados en la DPCM, se llevarán a cabo las siguientes acciones:

- El auditor realizará un informe con los resultados de su auditoría.
- El auditor notificará la deficiencia a las partes implicadas.
- Una vez recibido el informe de la auditoría de cumplimiento llevada a cabo, el PSCM analizará con la entidad que ha ejecutado la auditoría las deficiencias encontradas y desarrollará y ejecutará un plan correctivo que solvente dichas deficiencias.
- Una vez que las deficiencias sean subsanadas, el auditor verificará la implantación y la efectividad de las soluciones adoptadas.

Si el PSCM es incapaz de desarrollar y/o ejecutar el mencionado plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema se realizará una de las siguientes acciones:

- Revocar la clave del PSCM, tal y como se describe en la sección 5.7.2 de este documento.
- Terminar el servicio del PSCM, tal y como se describe en la sección 5.8 de este documento.

8.7 Tratamiento de los informes de auditoría

El PSCM entregará los informes de resultados de auditoría al MINETAD o a la entidad perteneciente a la AGE a la que corresponda, en un plazo máximo de 15 días tras la ejecución de la auditoría.

9 Requisitos legales

9.1 Confidencialidad

9.1.1 Tipo de información que debe protegerse

El PSCM considera como *sensible* la siguiente información y, por tanto, cuenta con las medidas de protección necesarias en cuanto a 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 o almacenadas por el PSCM.
- 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 PSCM 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 mediante los medios físicos presentes en la SGTIC la información criptográfica que conforma el acceso a la Entidad de Certificación del PSCM.

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 las 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.

9.1.2 Información no sensible

La siguiente información es considerada *no sensible*, y de esta forma es reconocida por los afectados:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del titular a un certificado emitido por el PSCM.
- El nombre y los apellidos del titular del certificado, así como cualquier otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- La dirección de correo electrónico del titular del certificado o la dirección de correo electrónico que corresponda.
- Los usos reseñados en el certificado.

- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (las CRL), así como las restantes informaciones de estado de revocación.
- La información contenida en los repositorios de certificados.
- Toda otra información que no esté indicada en la sección anterior de este documento.

9.1.3 Divulgación de información de suspensión y revocación

Véase la sección anterior.

9.1.4 Divulgación legal de información

El PSCM únicamente divulgará la información identificada como *sensible* en los casos legalmente previstos para ello. En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado serán divulgados en caso de ser requeridos para ofrecer evidencia de la correcta emisión y gestión del ciclo de vida del certificado en caso de un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

El PSCM indica estas circunstancias en la política de intimidad prevista en la sección 9.2 de este documento.

9.1.5 Divulgación de información por petición de su titular

El PSCM incluye, en la política de intimidad prevista en la sección 9.2 de este documento, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, del responsable del certificado, directamente a los mismos o a terceros.

9.2 Protección de datos personales

Para la prestación del servicio, el PSCM 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 permite recabar la información, sin consentimiento del afectado. El PSCM informa al suscriptor de sus derechos de protección de datos en el proceso de registro.

De acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y normativa de desarrollo, se informa al titular de la existencia de un fichero automatizado del que es responsable la Subsecretaría del Ministerio de Empleo y Seguridad Social, con domicilio en la calle Paseo de la Castellana 63, Madrid 28071, con correo electrónico sgtic@meyss.es y sitio web http://ca.empleo.gob.es cuya finalidad es la prestación de servicios de certificación siendo los destinatarios de la información las entidades del prestador de servicios de certificación. El titular puede ejercer sus derechos de acceso, rectificación, cancelación y oposición ante el Responsable del fichero en la dirección arriba indicada.

El PSCM desarrolla una política de intimidad, de acuerdo con la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), y documenta en la DPCM los aspectos y procedimientos de seguridad correspondientes al documento de seguridad previsto en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD. La DPCM tiene la consideración de Documento de Seguridad.

El PSCM recaba los datos exclusivamente necesarios para la expedición y la gestión del ciclo de vida del certificado.

El PSCM no divulgará ni cederá datos personales, excepto en los casos previstos en la sección 9.1 y en la sección 5.8, en caso de terminación de la Entidad de Certificación.

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 1720/2007.

9.3 Derechos de propiedad intelectual

9.3.1 Propiedad de los certificados e información de revocación

El PSCM es la única entidad que goza de los derechos de propiedad intelectual sobre los certificados que emite.

El PSCM concede licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas electrónicas y/o sistemas de cifrado dentro del ámbito de aplicación de la DPCM, según se define en la sección 1.4.

Las mismas reglas resultan de aplicación al uso de información de revocación de certificados.

9.3.2 Propiedad de la política de certificación y Declaración de Prácticas de Certificación

La AGE es la única entidad que goza de los derechos de propiedad intelectual sobre las políticas de certificación de la AGE.

La DPCM es propiedad en exclusiva del PSCM.

9.3.3 Propiedad de la información relativa a nombres

El suscriptor conserva cualquier derecho, de existir éste, relativo a la marca, producto o nombre comercial contenido en el certificado.

El suscriptor es el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 3.1 de la DPCM.

9.3.4 Propiedad de claves

Los pares de claves son propiedad de los suscriptores de los certificados. Cuando una clave se encuentra fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

9.4 Obligaciones y responsabilidad civil

9.4.1 Modelo de obligaciones del prestador de servicios de certificación

El PSCM garantiza, bajo su plena responsabilidad, que cumple con todos los requisitos establecidos para cada tipo de certificado que emite.

El PSCM es la única entidad responsable del cumplimiento de los procedimientos descritos en la DPCM, incluso cuando una parte o la totalidad de las operaciones sean subcontratadas externamente.

El PSCM presta sus servicios de certificación conforme con la DPCM, en la que se detallan funciones, procedimientos de operación y medidas de seguridad.

Antes de la emisión y entrega del certificado al suscriptor, el PSCM le informa de los términos, condiciones y limitaciones relativos al uso del certificado, de su precio – caso de tenerlo – y de sus limitaciones de uso.

Este requisito se cumple mediante un texto con los Términos y Condiciones de Uso del certificado, que puede ser transmitido electrónicamente, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

Cualquier cambio de estos términos se publica en el repositorio de información del PSCM y a través de medios internos (mensajes en el arranque de los equipos etc.).

El PSCM informa al suscriptor o custodio de la caducidad de su certificado de manera previa o simultánea a que su certificado caduque, especificando los motivos y la fecha en la que el certificado dejará de ser válido.

El PSCM comunicará a los firmantes el cese de sus actividades de prestación de servicios de certificación con dos meses de antelación e informará, en su caso, sobre las características del prestador al que se propone la transferencia de la gestión de los certificados. Las comunicaciones a los firmantes se efectuarán conforme a lo previsto en el presente documento.

El PSCM dispone de un plan de finalización del cese de su actividad en el que se especifican las condiciones en las que se realizaría.

Toda esta información pública relativa a los certificados está recogida en el Repositorio del PSCM. El PSCM vincula a suscriptores y terceros que confían en los certificados mediante instrumentos jurídicos apropiados.

9.4.2 Garantías ofrecidas a suscriptores y terceros que confían en los certificados

El PSCM, establece y rechaza garantías, y establece las limitaciones de responsabilidad aplicables. El PSCM garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por el PSCM y, en su caso, por el registrador.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de diligencia en la gestión de la solicitud de certificado o en la creación del mismo.

- Que los certificados cumplen con todos los requisitos materiales establecidos en la DPCM.
- Que los servicios de revocación y el empleo del Repositorio cumplen con todos los requisitos materiales establecidos en la DPCM.

El PSCM garantiza al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- En caso de certificados publicados en el Repositorio, que el certificado ha sido emitido al suscriptor identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con la sección 4.4 de la DPCM.
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la DPCM.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y de Repositorio.

Adicionalmente, cuando emita un certificado de firma electrónica, el PSCM garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado reconocido, de acuerdo con eIDAS y normativa relacionada.
- Que, en el caso de que genere las claves privadas del suscriptor se mantiene su confidencialidad durante el proceso.

9.4.3 Rechazo de otras garantías

El PSCM rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 9.4.2.

9.4.4 Limitación de responsabilidades

El PSCM limita su responsabilidad a la emisión y gestión de certificados y, en su caso, de pares de claves de suscriptores y de dispositivos criptográficos suministrados por el PSCM (de autenticación, de firma y verificación de firma).

El PSCM puede limitar su responsabilidad mediante la inclusión de límites de uso del certificado y límites de valor de las transacciones para las que puede emplearse el certificado.

9.4.5 Cláusulas de exención de responsabilidades

9.4.5.1 Cláusula de exención de responsabilidades con el suscriptor

El PSCM incluye, en el documento que le vincula con el suscriptor, una cláusula por la cual el suscriptor se compromete a mantener indemne al PSCM de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Falsedad o manifestación errónea realizada por el usuario del certificado.

- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión medió dolo o negligencia con respecto al PSCM, la entidad de registro o cualquier persona que confía en el certificado.
- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de dominio), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

9.4.5.2 Cláusula de exención de responsabilidades con tercero que confía en el certificado

El tercero que confía en el certificado se compromete a mantener indemne al PSCM de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.

9.4.6 Caso fortuito y fuerza mayor

El PSCM estará exento de toda responsabilidad ante los efectos que pudieran producirse por causas fortuitas o de fuerza mayor.

9.4.7 Ley aplicable

La ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la ley española, en especial:

- La Ley 59/2003, de 19 de diciembre, de Firma Electrónica (LFE).
- El Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo de 23 de Julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (eIDAS).
- La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (entrada en vigor: 2 de Octubre de 2016).
- La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (entrada en vigor: 2 de Octubre de 2016).La Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la AGE.
- La Ley Orgánica 15/1999, de 13 de diciembre, de protección de los datos de carácter personal.

- El 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.
- La Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- El Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de propiedad intelectual.
- La Política de Firma Electrónica y de Certificados de la AGE.
- La descripción de los perfiles de certificados de la Ley 11/2007, de 22 de junio asociados a la política de firma: Perfiles de certificados en su última versión disponible.
- La Resolución de la Secretaria de Estado de Función Pública del 19 de julio de 2011 por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración.
- La decisión de la Comisión Europea 130/2011, de 25 de febrero, que establece unos requisitos mínimos para el tratamiento transfronterizo de documentos firmados electrónicamente por las autoridades competentes bajo la Directiva 123/2006 relativa a los servicios en el mercado interior.

9.4.8 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

El PSCM establece, en las condiciones generales de emisión y uso de certificados, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afecta al resto de la DPCM.
- En virtud de la cláusula de supervivencia, ciertas reglas continúan vigentes tras la finalización de la prestación de servicios por el PSCM. A este efecto, se vela porque, al menos los requisitos contenidos en las secciones 8, 9.1 y 9.4 continúen vigentes tras la terminación de los servicios.
- En virtud de la cláusula de acuerdo íntegro se entiende que la DPCM contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación, en la DPCM se establece el procedimiento por el cual las partes se notifican hechos mutuamente.

9.4.9 Cláusula de jurisdicción competente

El PSCM establece que la competencia judicial internacional corresponde a los jueces españoles.

La competencia territorial y funcional se determina en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

9.4.10 Resolución de conflictos

El PSCM resolverá cualquier disputa que se derive sobre la interpretación o aplicabilidad de la DPCM a la Política de Certificación de la AGE.

Las situaciones de discrepancia que se deriven de la utilización del empleo de los certificados emitidos por el PSCM, se resolverán aplicando los mismos criterios de competencia que en los casos de los documentos firmados de forma manuscrita.

En los supuestos de controversia producidos como consecuencia de la gestión de los certificados entre las diferentes entidades de los prestadores de servicios de certificación acreditados u homologados, se estará a lo establecido en la DPCM.

Anexo A: Referencias

CCEAL4+	Common Criteria Evaluation Assurance Level (EAL) 4+.
CCN-STIC-405	Guía de seguridad de las TIC. Algoritmos y parámetros para firma electrónica segura.
CWA 14167	CEN-CWA 14167: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signature, que establece requisitos para los sistemas software y hardware que gestionan el ciclo de vida de los certificados.
CWA 14169	CEN-CWA 14169: Secure Signature-Creation Devices "EAL 4+", establece un perfil de protección dispositivos seguros de creación de firma
ETSI EN 319 403	ETSI European Standard 319 403 v2.2.2. Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing Trust Service Providers.
ETSI EN 319 411-2	ETSI European Standard 319 411-2. Policy requirements for certification authorities issuing qualified certificate
ETSI EN 319 411-3	ETSI European Standard 319 411-3. Policy requirements for Certification Authorities issuing public key certificates. Nota: Excluye los certificados de sitios web basados en los requisitos del CAB Forum.
ETSI EN 319 412-5	ETSI European Standard 319 412-5. Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile.
ETSI EN 319 421	ETSI European Standard 319 421. Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps.
ETSI TS 102 042	ETSI Technical Specification 102 042. Policy requirements for Certification Authorities issuing public key certificates. Nota: Incluye los certificados de sitio web basados en los requisitos del CAB Forum.
ETSI TS 102 158	ETSI Technical Specification 102 042. Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates
ETSI TS 102 176-1	ETSI Technical Specification 102 176-1. Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
ETSI TS 102 176-2	ETSI Technical Specification 102 176-2. Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices.
ETSI TS 119 412-2	ETSI Technical Specification 119 412-2. Profiles for Trust Service Providers issuing certificates; Part 2: Certificate Profile for certificates issued to natural persons.
FIPS 140-2	Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules.
IETF RFC 3647	Internet X509 Public Key Infrastructure Certificate Policy and Certification Practice Framework.
IETF RFC 4055	Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

IETF RFC 4491	Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
IETF RFC 6818	Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
IETF RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.
ISO 3166-1	Codes for the representation of names of countries and their subdivisions - Part 1: Country codes. Alpha-2 country codes.
ISO 9594-8	Information Technology – Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Frameworks.
ISO 15048	Common Criteria for Information Technology Security Evaluation (CC/ISO 15408).
ISO 27001	ISO/IEC 27001 (Information technology – Security techniques – Information security management systems – Requirements).
ITU-T X.501	ITU-T Recommendation X.501 TC2 (08/1997) | ISO/IEC 9594-2:1998.
ITU-T X.509	ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework.
Ley 40/2015	Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
RD 3/2011	Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público.
RD 5/2015	Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
UTF-8	8-bit Unicode Transformation Format.

Anexo B: Enlaces (URL)

Datos de contacto por correo electrónico de la organización:

admin_ca@meyss.es

Ubicación de la DPCM, perfiles de certificados, Declaración Informativa (PDS) y Términos y Condiciones:

http://ca.empleo.gob.es/meyss/DPCyPoliticas

Certificado raíz de la CA, de las SubCA y certificado OCSP

http://ca.empleo.gob.es/meyss/certificados

Servicio de validación de OCSP:

http://ca.empleo.gob.es/meyss/ocsp

CRL Raíz - AC RAIZ MEYSS:

http://ca.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz

http://ca2.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz

CRL- SUBCA1 MEYSS:

http://ca.empleo.gob.es/meyss/crl/MEYSSSubCA1

http://ca2.empleo.gob.es/meyss/crl/MEYSSSubCA1

CRL - SUBCA2 MEYSS:

http://ca.empleo.gob.es/meyss/crl/MEYSSSubCA2

http://ca2.empleo.gob.es/meyss/crl/MEYSSSubCA2

Para los servicios de certificación ofrecidos anteriores a la aplicación del reglamento eIDAS, las URL son las siguientes:

Ubicación de la DPCM y perfiles de certificados:

http://ca.mtin.es/mtin/DPCyPoliticas

Servicio de validación OCSP:

http://ca.mtin.es/mtin/ocsp

Certificado raíz, certificado del servicio OCSP y certificado de sellado de tiempo:

http://ca.mtin.es/mtin/certificados

Publicación de las CRL:

http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz

http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz

CRL históricas:

Solicitar al buzón admin_ca@meyss.es indicando la fecha de publicación y/o número de serie.