MINISTERIO
DE EMPLEO
Y SEGURIDAD SOCIAL

SUBSECRETARÍA

S.G. DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIONES

Perfil de Certificado de Empleado Público Centralizado y Gestionado por un HSM del Prestador de Servicios de Confianza del Ministerio de Empleo y Seguridad Social

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	D306
Título	Perfil de Certificado de Empleado Público Centralizado y Gestionado por un HSM del Prestador de Servicios de Confianza del Ministerio de Empleo y Seguridad Social
Versión	06
Estado del documento	Aprobado
Fecha de aprobación	07.07.2017
Fecha de caducidad	07.07.2018

Registro de Cambios

Versión	Fecha	Comentario
0.9	10.02.2014	Versión inicial
1.0	21.03.2014	Documento final
1.1	14.05.2014	Actualización apartado 3.1
1.2	18.06.2015	Se añade SHA-256
1.3	18.03.2016	Uso de la dicción centralizado Actualización de la normativa aplicable Revisión de los requisitos operativos
2.0	20.07.2016	Ajuste perfil Reglamento eIDAS (OID 1.3.6.1.4.1.27781.2.5.4.7.1)
2.1	24.01.2017	Aclaración del procedimiento Actualización de referencias
03	03.04.2017	Ajuste al formato de documentación
04	10.04.2017	Código DIR3 corregido Corregido errores detectados en apartado 2.1
05	31.05.2017	Actualización de la sección 1.4 Añadida la sección 1.6, administración del perfil Añadida la sección 1.8, condiciones generales de los servicios de certificación del CEPCHSM Añadida la sección 2, responsabilidades del repositorio de información y publicación Actualización de la sección 4.4 Añadida la sección 5, otros aspectos legales y de actividad Actualización de acuerdo a la preauditoría eIDAS
06	07.07.2017	Actualización Anexo B: - Cambio protocolo http por https en URL: https://ca.empleo.gob.es/meyss/DPCyPoliticas https://ca.empleo.gob.es/meyss/certificados - Nueva URL: https://ca.empleo.gob.es/meyss/DPCyPoliticas-en Cambios extensión Qualified Certificate Statements: Se añade QcType Se añade id-qcs-pkixQCSyntax-v2

Tabla de contenidos

1 Introducción

1.1 Presentación

El presente documento recoge el **Perfil del Certificado de Empleado Público Centralizado y Gestionado por un HSM, del Prestador de Servicios de Confianza del Ministerio de Empleo y Seguridad Social (PSCM).**

Este documento matiza y complementa la Declaración de Prácticas de Certificación del Prestador de Servicios de Confianza del Ministerio (DPCM) en lo referente a los Certificados de Empleado Público Centralizados y Gestionados por un HSM.

1.2 Descripción

El Certificado de Empleado Público Centralizado y Gestionado por un HSM (CEPCHSM) expedido por el PSCM es un **Certificado Electrónico Cualificado** al cumplir los requisitos del anexo I del Reglamento 910/2014 del Parlamento Europeo y del Consejo [eIDAS], QCP-n[1] de acuerdo con [ETSI EN 319 411-2].

Este certificado se expide en un soporte de HSM y según los niveles de seguridad determinados en el Reglamento de Ejecución (UE) 2015/1502 [Reg 2015/1502] con arreglo a lo dispuesto en el artículo 8, apartado 3, del [eIDAS], correspondiendo al nivel de aseguramiento Medio o Sustancial. El PSCM monitoriza el estatus de la certificación del HSM hasta el fin de su validez y reemplazará este una vez su certificación haya finalizado, de acuerdo con los procedimientos establecidos.

El CEPCHSM es un certificado de los previstos en la [Ley 39/2015] y en el artículo 43 de la [Ley 40/2015] para el personal al servicio de la Administración. Se emplea para la identificación de un empleado público en cualquiera de sus categorías: funcionario, laboral fijo, etc., e incluye los datos tanto del titular como de la entidad pública en la que presta servicios el empleado.

1.3 Nombre del documento e identificación

1.3.1 Identificación de este documento

Este documento se denomina **Perfil de Certificados de Empleado Público Centralizados y Gestionados por un HSM del Prestador de Servicios de Confianza del Ministerio de Empleo y Seguridad Social**, con la información reflejada en el control de versiones del documento (pág. ii).

La ubicación de la publicación de este documento se encuentra en el Anexo B.

1.3.2 Identificación de los tipos de certificado

Cada tipo de certificado emitido por el PSCM recibe su propio *OID* incluido dentro del certificado en el campo *PolicyIdentifier*. Cada *OID* es unívoco y no se emplea para identificar diferentes tipos, políticas y versiones de los certificados emitidos. El PSCM ha asignado al CEPCHSM el siguiente identificador de objeto (OID):

- CEPCHSM: *[1.3.6.1.4.1.27781.2.5.4.7.1]*

1.4 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:

a. Los solicitantes de certificados.
b. Los suscriptores de certificados.

[1] QCP-n-remote en algunas ocasiones resaltando que la clave privada es gestionada por un QSCD remoto

c. Los responsables de certificados.

d. Los verificadores de certificados.

Los solicitantes del CEPCHSM son los empleados públicos de la Administración que una vez reciben los certificados se convierten en titulares y responsables de los mismos.

Los suscriptores del CEPCHSM son los empleados públicos (personas físicas) así identificadas en el campo *Subject* del certificado y que se comprometen a utilizar su clave y su certificado de acuerdo con la DPCM.

Los responsables del CEPCHSM son los empleados públicos (personas físicas) así identificadas en el objeto *Identidad Administrativa* dentro de la extensión *SubjectAltName*. El responsable de un CEPCHSM es el titular del mismo.

Los verificadores son las entidades (incluyendo personas físicas, AAPP, personas jurídicas y otras organizaciones) que 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 el PSCM. El verificador utilizará la información contenida en el CEPCHSM para determinar la utilización del certificado para un uso en particular.

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

1.5 Uso del certificado

El CEPCHSM tiene como propósito que el empleado público pueda firmar trámites o documentos proporcionando las siguientes garantías:

- No repudio de origen.
- Integridad.

Asimismo el CEPCHSM también tiene como propósito la autenticación del empleado público en sistemas y aplicaciones informáticas.

El CEPCHSM circunscrito a este documento y a la DPCM deberá ser utilizado sólo para las transacciones definidas en los sistemas y aplicaciones permitidos. La expedición efectiva de dicho certificado obliga al suscriptor a la aceptación y uso del mismo en los términos expresados en este documento, en la DPCM y en la legislación aplicable.

Queda fuera del ámbito de este documento y de la DPCM garantizar la viabilidad tecnológica de las aplicaciones que harán uso del CEPCHSM.

No está permitido el uso del CEPCSHM fuera del ámbito descrito en la DPCM, pudiendo ser causa de revocación inmediata su uso indebido.

El PSCM, como proveedor de servicios de confianza (PSC/TSP) no se responsabiliza del contenido de los documentos firmados con un CEPCHSM ni de ningún otro uso de los certificados, como procesos de cifrado de información o comunicaciones.

El PSCM garantiza que las claves privadas permanecen, con un alto nivel de confianza, bajo el exclusivo control del empleado público titular del CEPCHSM. El titular deberá poner el cuidado y medios necesarios para garantizar la custodia de las claves de acceso a los certificados, evitando su pérdida, divulgación, modificación o uso no autorizado.

1.6 Administración del perfil

1.6.1 Organización que administra el documento

El responsable del PSCM es el responsable de la definición, revisión y divulgación de este perfil. 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 (Subdirección General de Tecnologías de la Información y las Comunicaciones).

1.6.2 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: +34 91 363 11 88/9 - Fax: +34 91 363 07 73

1.6.3 Procedimientos de gestión del documento

1.6.3.1 Procedimiento de Especificación de Cambios

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

El responsable de seguridad del PSCM revisará este perfil al menos una vez al año o cada vez que en este período se produzca cualquier cambio significativo. Los errores, actualizaciones, sugerencias o mejoras sobre este documento, deberán comunicarse a la organización cuyos datos de contacto aparecen en la sección 1.6.2. 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 este perfil se difundirán a todas las partes interesadas según lo especificado en el apartado siguiente.

1.6.3.2 Procedimiento de Publicación

El PSCM publica toda la información que considere oportuna relativa a los servicios ofrecidos (incluyendo este perfil) en un repositorio público accesible a todos sus usuarios. La ubicación de la última versión de este perfil está en:

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

1.6.3.3 Procedimiento de Aprobación

El responsable de seguridad del PSCM solicitará la aprobación de este perfil al responsable del PSCM quien debería aprobar (o no) la misma de acuerdo con el plan de calidad de la documentación del PSCM.

Cualquier nueva versión tendrá una fecha de caducidad de un año sobre la fecha en la que el perfil haya sido aprobado.

1.7 Definiciones y acrónimos

1.7.1 Definiciones

En el ámbito de este documento se utilizan las siguientes definiciones:

C	Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
CN	Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
DN	Identificación unívoca de una entrada dentro de la estructura de directorio X.500.
O	Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

OCSP	Este protocolo permite comprobar en línea la vigencia de un certificado electrónico.
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.
RFC	Estándar emitido por la IETF.

1.7.2 Acrónimos

AAPP	Administraciones Públicas.
AC	Entidad de Certificación, también denominada Autoridad de Certificación.
C	Country (País).
CA	Certification Authority, Entidad de Certificación.
CEPCHSM	Certificado de Empleado Público Centralizado y Gestionado por un HSM.
CN	Common Name (Nombre Común).
CRL	Certificate Revocation List, Lista de Revocación de Certificados.
DN	Distinguished Name (Nombre Distintivo).
DPC	Declaración de Prácticas de Certificación.
DPCM	Declaración de Prácticas de Certificación del Prestador de Servicios de Confianza del Ministerio.
HSM	Hardware Security Module, Dispositivo Seguro Hardware.
MEYSS	Ministerio de Empleo y Seguridad Social.
O	Organization.
OU	Organizational Unit (Unidad Organizativa).
OID	Object IDentifier (Identificador de objeto único).
OCSP	On-line Certificate Status Protocol.
PDS	PKI Disclosure Statement.
PSC	Prestador de Servicios de Confianza.
PSCM	Prestador de Servicios de Confianza del Ministerio.
RFC	Request For Comments.
SGTIC	Subdirección General de Tecnologías de la Información y las Comunicaciones.

1.8 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.

1.8.1 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.

1.8.2 Análisis de Riesgos

Tal y como se señala en la política de seguridad, el PSCM aplica una metodología de análisis de riesgos 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 y repositorios

2.1 Repositorios

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

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:
- publica los términos y condiciones de uso de los certificados.

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 los certificados

La dirección de la DPCM se halla en el Anexo B:

La dirección con los certificados de la CA Raíz y de las SubCA se halla en el Anexo B:

La dirección del servicio OCSP se halla en el Anexo B:

La dirección de la publicación de la CRL se halla en el Anexo B:

2.3 Frecuencia de publicación

Este documento de perfil se publica en el momento de su aprobación.

La información sobre el estado de los certificados se publica de acuerdo con lo establecido en los apartados 4.9.7 y 4.9.9 de la DPCM.

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 al repositorio

El PSCM solamente permite el acceso de lectura a la información publicada en su repositorio.

3 Identificación

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 5280].

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.

El objeto Identidad Administrativa utiliza el número ISO/IANA *2.16.724.1.3.5.X.X* proporcionado por la AGE como base para identificarlo, de este modo se establece un identificador unívoco a nivel internacional.

El número de Identidad Administrativa del certificado es:

- CEPCHSM (Nivel Medio): *2.16.724.1.3.5.7.2*

En los CEPCHSM emitidos por el PSCM se incluyen los siguientes campos de la Identidad Administrativa:

Certificado	Campos "Identidad Administrativa" fijos
CEPCHSM	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 Correo electrónico Unidad organizativa Puesto o cargo

Certificado	Campos "Identidad Administrativa" opcionales
CEPCHSM	Número de identificación de personal

El resto de aspectos relativos a las gestión de nombres (significado de los nombres, uso de anónimos y seudónimos, interpretación de formatos de nombre, unicidad de los nombres y resolución de conflictos relativos a nombres) se especifican en la DPCM.

4 Requisitos operativos

4.1 Solicitud de los certificados

El solicitante debe personarse ante la Entidad de Registro para identificarse ante la misma y obtener el código de activación. En este momento, el empleado público rellena y firma un formulario con la solicitud de emisión del CEPCHSM expedido por el PSCM. Este formulario recoge un resumen de los términos y condiciones aplicables al certificado presentes en la DPCM y documentos de perfiles.

El formulario cumplimentado y firmado es entregado a la Entidad de Registro correspondiente, la cual autentica la identidad del solicitante y se asegura de que la solicitud es completa y precisa. Las unidades que operarán como Entidades de Registro son la *Subdirección General de Recursos Humanos*.

El PSCM comprueba en los registros correspondientes, por sí mismo o por medio de las Entidades de Registro, la identidad y cualesquiera otras circunstancias personales del suscriptor del CEPCHSM, relevantes para el fin propio de éste.

La autenticación de la identidad del solicitante se realiza de acuerdo con los requisitos especificados en la DPCM. Una vez verificada la identidad del solicitante, la Entidad de Registro facilitará un Código de Activación al solicitante que permitirá, en conjunción con otros factores adicionales, la emisión del CEPCHSM.

De forma equivalente, el solicitante puede utilizar un certificado electrónico cualificado para confirmar los datos del formulario de solicitud de emisión y aceptar la los términos y condiciones de la misma.

Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, ya que ésta implica la emisión de nuevos certificados.

4.2 Emisión del CEPCHSM

El solicitante puede proceder a la emisión de forma telemática de su CEPCHSM utilizando el código de activación recibido, su DNI , su fecha de nacimiento y un código de único uso (OTP) recibido por correo electrónico que se utiliza como segundo factor de autenticación. . De forma equivalente, para la emisión del CEPCHSM el solicitante puede utilizar un certificado electrónico cualificado una vez aceptada y aprobada la solicitud del CEPCHSM.

El sistema informa al solicitante (el empleado público) de que se le va a emitir su CEPCHSM. Entonces, le solicita a este que introduzca una contraseña de protección del certificado y genera en ese momento su clave privada y la almacena en el sistema. La contraseña permite proteger el uso del CEPCHSM y asegurar que la clave privada se encuentra bajo el control exclusivo de su titular.

El par de claves para los CEPCHSM se generan en el dispositivo criptográfico centralizado en conformidad con los requisitos Common Criteria EAL 4+ ALC_FLR.1, AVA_VAN.5, así como con FIPS 140-2 Nivel 3 o equivalente.

La generación del CEPCHSM se realiza acorde con los requisitos que la ley marca con respecto a los plazos máximos permitidos desde que el solicitante realizó el registro presencial.

El PSCM utiliza un procedimiento de generación de certificados que vincula de forma segura los certificados con la información sobre el empleado público, incluyendo la clave pública certificada. También se indican la fecha y la hora en las que se expidieron los certificados y se utilizan medidas contra la falsificación de certificados y para garantizar el secreto de las claves durante el proceso de generación de las mismas.

Los certificados emitidos se almacenan en un repositorio sin el consentimiento previo de los responsables de los mismos.

La aprobación de la solicitud del CEPCHSM es implícita a la emisión de forma segura del certificado. En otro caso, la Autoridad 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.

A la finalización del proceso de generación del CEPCHSM se informa al suscriptor (el empleado público) de que se encuentra disponible dicho certificado para su uso, pudiendo ser usado a partir de ese mismo momento para los procesos de autenticación y de firma electrónica.

Para la activación de la clave privada del CEPCHSM se requiere que el empleado público introduzca la contraseña de protección de su CEPCHSM, bajo su exclusivo control, así como el segundo factor de autenticación.

Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, ya que ésta implica la emisión de nuevos certificados.

4.3 Renovación de los certificados

La renovación del CEPCHSM supone la emisión de un nuevo certificado, debiéndose proceder a una nueva solicitud y su posterior emisión como se indica en los apartados anteriores.

Se podrán habilitar mecanismos que permitan la renovación de los certificados de forma telemática (sin presencia física), siempre antes de su expiración, y cuando el período de tiempo transcurrido desde la anterior identificación con presencia física sea menor de cinco años.

4.4 Revocación de los certificados

La revocación se realiza de forma automática cuando hay una modificación en los datos del suscriptor o éste causa baja en el ministerio.

En otro caso, el suscriptor procederá a revocar manualmente el CEPCHSM a través del sitio web de autoservicio.

La hora y fecha utilizadas para la emisión de los servicios de revocación están sincronizadas con UTC al menos cada 24 horas.

El retraso máximo entre la recepción de una solicitud de revocación y la decisión de cambiar su estado es de 24 horas.

El cambio de estado de la validez de un certificado se indicará en la CRL en menos de 5 minutos desde que ocurra el cambio. Esto implica que el retraso máximo entre la confirmación de la revocación de un certificado, o su suspensión, para que esta sea efectiva y el cambio real en el status del certificado es de 5 minutos.

5 Otros aspectos legales y de actividad

5.1 Protección de datos de carácter personal

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 a los suscriptores sobre 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 PSCM. 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 el caso de terminación de la Autoridad 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.

6 Perfil del CEPCHSM

6.1 Certificado de Empleado Público Centralizado y Gestionado por un HSM para autenticación y firma

Los campos son los siguientes:

Campo	Descripción	Contenido
1. X.509v1 Field		
1.1. Version	Describe la versión del certificado	2 (= v3)
1.2. Serial Number	Número identificativo único del certificado	7c 88 54 93 b6 c9 (ejemplo)
1.3. Issuer Distinguished Name		
1.3.1. Country (C)	País	C = ES
1.3.2. Locality (L)	Localidad del prestador de servicios de confianza	L = MADRID
1.3.3. Organization (O)	Denominación (nombre "oficial" de la organización) del prestador de servicios de confianza (emisor del certificado)	O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
1.3.4. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado	OU = S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES
1.3.5. Organizational Unit (OU)	Unidad funcional dentro del prestador de servicios, responsable de la emisión del certificado	OU = PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS
1.3.6. Serial Number	NIF del Ministerio	SERIALNUMBER = S2819001E
1.3.7. OrganizationIdentifier	Identificador de organización o persona jurídica normalizado según la norma técnica ETSI EN 319 412-1	VATES-S2819001E
1.3.8. Common Name (CN)	Nombre común de la organización prestadora de servicios de certificación (emisor del certificado)	CN = SUBCA1 MEYSS
1.4. Validity	5 años	
1.4.1. Not Before	Fecha de inicio de validez	Fecha de inicio de validez, formato: UTCTime YYMMDDHHMMSSZ
1.4.2. Not After	Fecha de fin de validez	Fecha fin de validez, formato: UTCTime YYMMDDHHMMSSZ
1.5. Subject		
1.5.1. Country (C)	País	C = ES

Campo	Descripción	Contenido
1.5.2. Organization (O)	Denominación de la Administración, organismo o entidad de derecho público, a la que se encuentra vinculada el empleado	O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL (ejemplo)
1.5.3. Organizational Unit (OU)	Descripción del tipo de certificado	OU = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
1.5.4. Organizational Unit (OU)	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado	OU = SUBDIRECCION GENERAL DE ADMINISTRACION FINANCIERA (ejemplo)
1.5.5. Title	Puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público.	T = JEFE SECCION APOYO GESTION (ejemplo)
1.5.6. Serial Number	DNI/NIE/pasaporte del empleado público. Se utilizará la semántica propuesta por la norma ETSI EN 319 412-1	SERIALNUMBER = IDCES-00000000G (ejemplo)
1.5.7. Surname	Primer y segundo apellido, de acuerdo con documento de identidad (DNI/Pasaporte).	SN = DE LA CAMARA ESPAÑOL (ejemplo)
1.5.8. Given name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte).	G = JUAN ANTONIO (ejemplo)
1.5.6.Common Name (CN)	Nombre y dos apellidos de acuerdo con documento de identidad (DNI/NIE/Pasaporte), así como DNI, NIE o pasaporte separado por un guion.	CN = JUAN ANTONIO DE LA CAMARA ESPAÑOL - 00000000G (ejemplo)
1.6. Subject Public Key Info	Clave pública de la persona, codificada de acuerdo con el algoritmo criptográfico	
1.7. Signature Algorithm	Algoritmo de firma	SHA-256 con RSA Signature y longitud de clave de 2048 bits

Y las extensiones son las siguientes, teniendo en cuenta que **el único campo crítico es el campo *KeyUsage***:

Campo	Descripción	Contenido
2. X.509v3 Extensions		
2.1. Authority Key Identifier	Medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado, por ejemplo en los casos en que el emisor tiene múltiples claves de firma	
2.1.1. Key Identifier	Identificador de la clave pública del emisor	

Campo	Descripción	Contenido
2.2. Subject Key Identifier	Identificador de la clave pública del suscriptor o poseedor de claves (derivada de utilizar la función de hash SHA-256 sobre la clave pública del sujeto)	
2.3. cRLDistributionPoint	Indica cómo se obtiene la información de la CRL	
2.3.1. distributionPoint	Web donde resida la CRL (punto de distribución 1)	URL punto de distribución 1 CRL (ver anexo B)
2.3.2. distributionPoint	Web donde resida la CRL (punto de distribución 2)	URL punto de distribución 2 CRL (ver anexo B)
2.4. Authority Info Access		
2.4.1. Access Method	Id-ad-ocsp	OID 1.3.6.1.5.5.7.48.1
2.4.2. Access Location	(dirección web)	URL servicio de validación OCSP (ver anexo B)
2.4.3. Access Method	Id-ad-calssuers	OID 1.3.6.1.5.5.7.48.2
2.4.4. Access Location	URL de localización del certificado de la CA. Especifica el emplazamiento de la información.	URL del certificado de la CA (ver anexo B)
2.5. Issuer Alternative Name	Nombre alternativo de la persona de contacto de la Entidad de Certificación emisora	
2.5.1. rfc822Name	Correo electrónico de contacto de la Entidad de Certificación emisora	admin_ca@meyss.es
2.6. Key Usage	**Campo crítico** para determinar el uso	
2.6.1. Digital Signature	Se utiliza cuando se realiza la función de firma electrónica	Seleccionado “1”
2.6.2. Content Commitment	Se refiere a la cualidad de un tipo de certificado que indica al software en el que se usa que debe permitir que el usuario conozca lo que firma	Seleccionado “1”
2.6.3. Key Encipherment	Se utiliza para gestión y transporte de claves	Seleccionado “1”
2.6.4. Data Encipherment	Se utiliza para cifrar datos que no sean claves criptográficas	No seleccionado “0”
2.6.5. Key Agreement	Se usa en el proceso de acuerdo de claves	No seleccionado “0”
2.6.6. Key Certificate Signature	Se usa para firmar certificados. Se utiliza en los certificados de autoridades de certificación	No seleccionado “0”
2.6.7. CRL Signature	Se usa para firmar listas de revocación de certificados	No seleccionado “0”
2.7. Extended Key Usage		

Campo	Descripción	Contenido
2.7.1. Email Protection	Protección de correo	OID 1.3.6.1.5.5.7.3.4
2.7.2. Client Authentication	Autenticación de cliente	OID 1.3.6.1.5.5.7.3.2
2.8. Qualified Certificate Statements		
2.8.1. OcCompliance	Indicación de certificado reconocido	OID 0.4.0.1862.1.1
2.8.2. OcEuRetentionPeriod	Periodo de conservación de informaciones (15 años)	OID 0.4.0.1862.1.3
2.8.3. QcType	Tipo de certificado cualificado	OID 0.4.0.1862.1.6
2.8.3.1. QcType- esign	Certificado de firma	OID 0.4.0.1862.1.6.1
2.8.4. QcPDS	Lugar donde se encuentra la declaración PDS	OID 0.4.0.1862.1.5 URL de la PDS en inglés y en español (ver anexo B)
2.8.5. id-qcs-pkixQCSyntax-v2		OID 1.3.6.1.5.5.7.11.2
2.8.5.1. SemanticsId-Natural	Para indicar semántica de persona física definida por la EN 319 412-1	OID 0.4.0.194121.1.1
2.9. Certificate Policies		
2.9.1. Policy Identifier	OID asociado a la DPC	OID 1.3.6.1.4.1.27781.2.5.4.7.1
2.9.1.1. Policy Qualifier ID	Especificación de la DPC	
2.9.1.1.1. CPS Pointer	URL de la DPC	URL ubicación DPCM (ver anexo B)
2.9.1.1.2. User Notice	Campo explicitText	"Certificado cualificado centralizado de firma electrónica de empleado público, nivel medio. Consulte las condiciones de uso en <URL ubicación DPCM (ver anexo B)>“
2.9.2. Policy Identifier	OID asociado certificado de empleado público de nivel medio	2.16.724.1.3.5.7.2
2.9.3. Policy Identifier	QCP-n	Certificado cualificado de firma acorde al Reglamento UE 910/2014 OID 0.4.0.194112.1.0
2.10. Subject Alternate Names		
2.10.1. rfc822Name	Correo electrónico de la persona responsable del certificado	juanantonio.delacamara@meyss.es (ejemplo)
2.10.2. Directory Name	Identidad administrativa	

Campo	Descripción	Contenido
2.10.2.1. Tipo de certificado	Indica la naturaleza del certificado	2.16.724.1.3.5.7.2.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO DE NIVEL MEDIO
2.10.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	2.16.724.1.3.5.7.2.2= MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL (ejemplo)
2.10.2.3. NIF entidad suscriptora	NIF entidad suscriptora	2.16.724.1.3.5.7.2.3= S2819001E (ejemplo)
2.10.2.4. DNI/NIE del responsable	DNI o NIE del responsable del certificado	2.16.724.1.3.5.7.2.4 = 00000000G (ejemplo)
2.10.2.5. Nombre de pila	Nombre de pila del responsable del certificado	2.16.724.1.3.5.7.2.6 = “JUAN ANTONIO” (ejemplo)
2.10.2.6. Primer apellido	Primer apellido del responsable del certificado	2.16.724.1.3.5.7.2.7= “DE LA CAMARA” (ejemplo)
2.10.2.7. Segundo apellido	Segundo apellido del responsable del certificado	2.16.724.1.3.5.7.2.8 = “ESPAÑOL” (ejemplo)
2.10.2.8. Correo electrónico	Correo electrónico de la persona responsable del certificado	2.16.724.1.3.5.7.2.9= juanantonio.delacamara@meyss.es (ejemplo)
2.10.2.9. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluida el responsable del certificado	2.16.724.1.3.5.7.2.10= SUBDIRECCION GENERAL DE ADMINISTRACION FINANCIERA (ejemplo)
2.10.2.10. Puesto o cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración	2.16.724.1.3.5.7.2.11= JEFE SECCION APOYO GESTION (ejemplo)

Anexo A: Referencias

CCN-STIC-405	Guía de seguridad de las TIC. Algoritmos y parámetros para firma electrónica segura.
eIDAS	Reglamento (UE) 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.
ETSI EN 319 411-1	ETSI European Standard 319 411-1. Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
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.
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 TS 102 158	ETSI Technical Specification 102 158. 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.
ITU-T X.501	ITU-T Recommendation X.501 TC2 (08/1997) | ISO/IEC 9594-2:1998.
IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
Ley 39/2015	Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
Ley 40/2015	Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
Reg 2015/1502	Reglamento de Ejecución (UE) 2015/1502 de la Comisión de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

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:

Español**:** https://ca.empleo.gob.es/meyss/DPCyPoliticas

Inglés: https://ca.empleo.gob.es/meyss/DPCyPoliticas-en

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

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

Servicio de validación 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