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
E04929701

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	03
Estado del documento	Aprobado
Fecha de aprobación	03.04.2017
Fecha de caducidad	03.04.2018

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

Tabla de contenidos

- página en blanco -

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 mediante un HSM (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.

El 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].

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.

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):

- Certificado de Empleado Público Centralizado y Gestionado por un HSM cualificado: *[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.
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.

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 PSCM no se responsabiliza del contenido de los documentos firmados con un CEPCHSM ni recomienda el uso del CEPCHSM y sus claves asociadas para cifrar ningún tipo de información.

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, pudiendo ser causa de revocación inmediata su uso indebido. Queda fuera del ámbito de este documento y de la DPCM garantizar la viabilidad tecnológica de las aplicaciones que harán uso del CEPCHSM.

Ningún CEPCHSM debe utilizarse para actuar como Autoridad de Registro ni como Autoridad de Certificación (firmando certificados de clave pública de cualquier tipo o Listas de Certificados Revocados (CRL)).

Se garantiza que las claves privadas permanecen, con un alto nivel de confianza, bajo el 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 Definiciones y acrónimos

1.6.1 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.

1.6.2 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.

2 Identificación

2.1 Gestión de nombres

2.1.1 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 3280].

El PSCM asegura la unicidad de los *DN* (*Distinguished Names*) de los Certificados de Sello Electrónico.

2.1.2 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:

- Sello Electrónico para la Actuación Automatizada (Nivel Medio): *2.16.724.1.3.5.6.2*

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

Certificado	Campos "Identidad Administrativa" opcionales
SELLO ELECTRÓNICO PARA LA ACTUACIÓN AUTOMATIZADA	DNI/NIE del responsable Nombre de pila Primer apellido Segundo apellido Correo electrónico

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 3280].

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*

Certificado	Campos "Identidad Administrativa" fijos
EMPLEADO PÚBLICO	• 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
EMPLEADO PÚBLICO	• Número de identificación de personal • Correo electrónico • Unidad organizativa • Puesto o cargo

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 rellenar y firmar 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, la Subdirección General de Apoyo a la Gestión de la Inspección de Trabajo y Seguridad Social, las Inspecciones Provinciales, las Secretarías Generales de las Consejerías de Trabajo, la Subdirección General de Tecnologías de la Información y las Comunicaciones, la Subdirección General de Gestión de Recursos y Organización del SEPE y las Direcciones Provinciales del SEPE.

El PSCM comprueba en los registros correspondientes, por si 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 Acceso/Activación al solicitante que permitirá, en conjunción con otros factores adicionales, la emisión del mismo.

De forma equivalente, el solicitante puede utilizar un certificado electrónico cualificado para confirmar los datos del formulario de solicitud de emisión y aceptar 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 de los certificados

El solicitante puede proceder a la emisión de forma telemática de su CEPCHSM utilizando el código de acceso recibido y otros factores adicionales.

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 empleado público de que se le va a emitir su CEPCHSM, 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 de forma protegida utilizando la contraseña de protección del certificado de modo que garantice su uso bajo el control exclusivo de su titular.

Las 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 ciudadano 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 entrega de forma segura del certificado. 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.

En la finalización del proceso de generación del CEPCHSM se informa al empleado público 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 que tan sólo conoce él y no se halla almacenada en los sistemas y se requiere que el empleado público introduzca 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

El PSCM autentica las peticiones e informes relativos a la revocación de los CEPCHSM comprobando que provienen de una persona autorizada.

Las personas autorizadas para solicitar revocaciones de los CEPCHSM son: los propios empleados públicos responsables de los mismos, la Subdirección General de Recursos Humanos y el responsable del PSCM.

Los mecanismos de revocación permitidos son a través de cuentas internas de correo electrónico debidamente validadas o mediante un escrito firmado por el solicitante de la revocación.

5 Perfil del CEPCHSM

5.1 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
1.5.2.Organization (O)	Denominación de la Administración, organismo o	O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

Campo	Descripción	Contenido
	entidad de derecho público, a la que se encuentra vinculada el empleado	
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 = SUBDIRECCIÓN GENERAL DE ADMINISTRACIÓN 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:

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	
2.2. Subject Key Identifier	Identificador de la clave pública del suscriptor o poseedor de claves (derivada de utilizar la función de Hash	

Campo	Descripción	Contenido
	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	No seleccionado “1”
2.6.3.Key Encipherment	Se utiliza para gestión y transporte de claves	No 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		
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

Campo	Descripción	Contenido
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- 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 (ver anexo B)
2.8.5.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	Políticas de certificación/DPC	
2.9.1.Policy Identifier	OID asociado a la DPC o PC	OID 1.3.6.1.4.1.27781.2.5.4.7.1
2.9.2.Policy Qualifier ID	Especificación de la DPC	
2.9.2.1. CPS Pointer	URL de la DPC	URL ubicación DPCM (ver anexo B)
2.9.2.2. 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)>“
2.9.3.Policy Identifier	OID asociado certificado de empleado público de nivel medio	2.16.724.1.3.5.7.2
2.9.4.Policy Identifier	QCP-n	Certificado cualificado de firma acorde al Reglamento UE 910/2014 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	
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)

Campo	Descripción	Contenido
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 319 411-2	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)

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

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

Ubicación de Certificados:

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

Servicio de validación OCSP:

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

Publicación de las CRL de AC RAIZ MEYSS:

- Punto de distribución 1:

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

- Punto de distribución 2:

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

Publicación de las CRL de SUBCA1 MEYSS:

- Punto de distribución 1:

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

- Punto de distribución 2:

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

Publicación de las CRL de SUBCA2 MEYSS:

- Punto de distribución 1:

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

- Punto de distribución 2:

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

Publicación de las CRL de SUBCA COMPONENTES MEYSS:

- Punto de distribución 1:

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

- Punto de distribución 2:

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