



MINISTERIO
DE EMPLEO
Y SEGURIDAD SOCIAL

SUBSECRETARÍA

S.G. DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIONES

Perfil de Certificado de Empleado Público del Prestador de Servicios de Certificación del Ministerio de Empleo y Seguridad Social



Control de versiones

Identificador	D301
Título	Perfil de Certificado de Empleado Público 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
1.0	03.12.2009	Documento final
1.1	30.03.2010	Cambios en el número ISO/IANA del MPR e Identificador de Objeto (OID) del Certificado de Empleado Público emitido por el PSCM. Longitud de clave pasa de 1024 a 2048.
1.2	10.09.2010	Eliminado del encabezado la DG de Servicios
1.3	10.09.2011	Cambio SGPD por SGTIC
1.4	17.11.2011	Cambios en el OID. Desaparecen campos GivenName y Surname del Subject. Se ha eliminado propósito "key Encipherment" de los usos de la clave.
1.5	30.06.2012	Actualización de la estructura organizativa y nuevo formato
1.6	10.02.2014	Corrección de errores en extensión Subject Alternate Names
1.7	18.06.2015	Se añade SHA-256
2.0	20.07.2016	Ajuste perfil Reglamento eIDAS (OID 1.3.6.1.4.1.27781.2.5.4.1.1 y 1.3.6.1.4.1.27781.2.5.4.2.1)
03	03.04.2017	Ajuste al formato de documentación



Tabla de contenidos

1	Introducción	1
1.1	Presentación	1
1.2	Descripción	1
1.3	Nombre del documento e identificación	1
1.3.1	Identificación de este documento	1
1.3.2	Identificación de los tipos de certificado	1
1.4	Usuarios finales	1
1.5	Uso del certificado	2
1.6	Definiciones y acrónimos	2
1.6.1	Definiciones	2
1.6.2	Acrónimos	3
2	Identificación	4
2.1	Gestión de nombres	4
2.1.1	Tipos de nombres	4
2.1.2	Normalización e Identidad Administrativa	4
3	Requisitos operativos	5
3.1	Solicitud de certificados	5
3.2	Emisión de certificados	5
3.3	Renovación de certificados	6
3.4	Revocación de certificados	6
4	Perfil del Certificado de Empleado Público	7
4.1	Certificado de Empleado Público para autenticación	7
4.2	Certificado de Empleado Público para firma	11
Anexo A:	Referencias	16
Anexo B:	Enlaces (URL)	17



- página en blanco -



1 Introducción

1.1 Presentación

El presente documento recoge el **Perfil del Certificado de Empleado Público 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.

1.2 Descripción

El Certificado de Empleado Público 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.

Los certificados están soportados en dispositivos cualificados de creación de firma según el anexo II del Reglamento 910/2014 del Parlamento Europeo y del Consejo [eIDAS].

El PSCM emite dos tipos de certificados de Empleado Público para su personal según sus usos:

- Certificado de Empleado Público para firma.
- Certificado de Empleado Público para autenticación.

Por ajustarse estos certificados al nivel alto de aseguramiento se tratan como dos perfiles independientes.

El Certificado de Empleado Público de firma, 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], y permite realizar firma electrónica cualificada definida en el artículo 3 (12) de dicho reglamento.

1.3 Nombre del documento e identificación

1.3.1 Identificación de este documento

Este documento se denomina **Perfil de Certificados de Empleado Público 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 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. Los Certificados de Empleado Público emitido por el PSCM tienen asignados los siguientes identificadores de objeto (OID):

- Certificado de Empleado Público de firma (nivel alto): [1.3.6.1.4.1.27781.2.5.4.1.1]
- Certificado de Empleado Público de autenticación (nivel alto): [1.3.6.1.4.1.27781.2.5.4.2.1]

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 de certificados de Empleado Público son los propios empleados públicos del organismo que una vez reciben los certificados se convierten en titulares y responsables de los mismos.

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

Los responsables de certificados de Empleado Público son las personas físicas así identificadas en el objeto Identidad Administrativa dentro de la extensión *SubjectAltName*. El responsable de un certificado de Empleado Público es el titular del mismo.

Los verificadores son las entidades (incluyendo personas físicas, AAPP, personas jurídicas y otras organizaciones) que, utilizando el certificado de Empleado Público 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.

1.5 Uso del certificado

El Certificado de Empleado Público de firma tiene como propósito que el empleado público pueda firmar trámites o documentos proporcionando las siguientes garantías:

- No repudio de origen.
- Integridad.

El Certificado de Empleado Público de autenticación tiene como propósito la autenticación del empleado público en sistemas y aplicaciones informáticas.

Los certificados de Empleado Público 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 de Empleado Público 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 los certificados de Empleado Público fuera del ámbito descrito en la DPCM, pudiendo ser causa de revocación inmediata de los certificados por el uso indebido de los mismos.

El PSCM, en tanto que Prestador de Servicios de Confianza (PSC), no se responsabiliza del contenido de los documentos firmados con los certificados de Empleado Público, ni de cualquier otro uso de los certificados, como pueden ser procesos de cifrado de mensajes o de comunicaciones.

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.
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	Control de Emisión de Certificados, Código de Emisión de Certificados.
CN	Common Name (Nombre Común).
CP	Certificate Policy.
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 Prestador de Servicios de Confianza del Ministerio.
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.
RA	Registration Authority.
RFC	Request For Comments.
SGPD	Subdirección General de Proceso de Datos.
SGTIC	Subdirección General de Tecnologías de la Información y las Comunicaciones.
VA	Validation Authority. Entidad o Autoridad de Validación.



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].

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:

- Certificado de Firma de Empleado Público (Nivel Alto): 2.16.724.1.3.5.7.1
- Certificado de Autenticación de Empleado Público (Nivel Alto): 2.16.724.1.3.5.7.1

En los Certificados de Empleado Público emitidos por el PSCM se incluyen los siguientes campos de la Identidad Administrativa:

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 • Correo electrónico • Unidad organizativa • Puesto o cargo

Certificado	Campos "Identidad Administrativa" opcionales
EMPLEADO PÚBLICO	• 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.



3 Requisitos operativos

3.1 Solicitud de certificados

Para realizar la descarga de los certificados de Empleado Público, el solicitante debe contar con una tarjeta criptográfica, que albergará de forma segura los certificados, y con los códigos de activación, que recibirá por correo electrónico y que le permitirán la descarga y aceptación telemática de los certificados electrónicos en dispositivo criptográfico.

El procedimiento de gestión las tarjetas criptográficas utilizado por el PSCM garantiza que son entregadas de forma segura al empleado público responsable del certificado verificando su identidad.

El solicitante debe personarse e identificarse en la Entidad de Registro para que se le haga entrega de la tarjeta. En este mismo acto rellena y firma un formulario para la solicitud de emisión de los certificados de Empleado Público emitidos 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 Gestión de Recursos y Organización del SEPE y las Direcciones Provinciales del SEPE.

La autenticación de la identidad del solicitante se realiza acorde a los requisitos especificados en la DPCM. Una vez verificada la identidad del solicitante, se le entrega una copia del formulario relleno. En el caso de que se deniegue la solicitud, se notifica al solicitante la denegación 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.

3.2 Emisión de certificados

La emisión de los certificados de Empleado Público (autenticación y firma) se realiza de forma electrónica utilizando para ello los códigos de activación enviados al empleado público por correo electrónico. El lugar de descarga de los certificados se detalla en el formulario relleno. También se pone a disposición del empleado público en el lugar de descarga un manual de usuario para facilitar el uso de la aplicación de descarga electrónica de los certificados.

La aprobación de la solicitud de los Certificados de Empleado Público es implícita a la entrega de forma segura de los certificados. 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.

Se consideran aceptados los certificados mediante la utilización del mecanismo telemático de descarga de los mismos en la tarjeta criptográfica entregada al usuario.

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. En ningún caso se almacena la clave privada asociada a los mismos.

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



3.3 Renovación de certificados

La renovación de certificados de Empleado Público supone la emisión de nuevos certificados, 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.

3.4 Revocación de certificados

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

Las personas autorizadas para solicitar revocaciones de certificados de Empleado Público son: los propios empleados públicos responsables de los mismos, la Subdirección General de Recursos Humanos o un superior del empleado público (con cargo de nivel 30 o rango superior).

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.



4 Perfil del Certificado de Empleado Público

4.1 Certificado de Empleado Público para autenticación

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 organizativa 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 de Trabajo e Inmigración	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 = SUBCA2 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 entidad de derecho público, a la que se encuentra vinculada el empleado	O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL (ejemplo)



Campo	Descripción	Contenido
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), así como su DNI (Ver Criterios de Composición del campo CN para un empleado público).	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 guión	CN = JUAN ANTONIO DE LA CAMARA ESPAÑOL - 00000000G (AUTENTICACION) (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 sobre la clave pública del sujeto)	
2.3. cRLDistributionPoint	Indica cómo se obtiene la información de la CRL	



Campo	Descripción	Contenido
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-caIssuers	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 "0"
2.6.3. Key Encipherment	Se utiliza para gestión y transporte de claves	No seleccionado "0"
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
2.7.3. SmartCard Logon	Inicio de sesión con tarjeta inteligente	OID 1.3.6.1.4.1.311.20.2.2



Campo	Descripción	Contenido
2.8. Certificate Policies	Políticas de certificación/DPC	
2.8.1. Policy Identifier	OID asociado a la DPC o PC	OID 1.3.6.1.4.1.27781.2.5.4.2.1
2.8.2. Policy Qualifier ID	Especificación de la DPC	
2.8.2.1. CPS Pointer	URL de la DPC	URL ubicación DPCM (ver anexo B)
2.8.2.2. User Notice	Campo explicitText	"Certificado de personal, nivel alto, autenticación. Consulte las condiciones de uso en<URL ubicación DPCM (ver anexo B)>"
2.8.3. Policy Identifier	OID asociado certificado de empleado público de nivel alto	2.16.724.1.3.5.7.1
2.8.4. Policy Identifier	NCP+	0.4.0.2042.1.2
2.9. Subject Alternate Names		
2.9.1. rfc822Name	Correo electrónico de la persona responsable del certificado	juanantonio.delacamara@meyss.es (ejemplo)
2.9.2. User Principal Name (UPN)	UPN para smart card logon	00000000G@meyss.es (ejemplo)
2.9.3. Directory Name	Identidad administrativa	
2.9.3.1. Tipo de certificado	Indica la naturaleza del certificado	2.16.724.1.3.5.7.1.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO DE NIVEL ALTO DE AUTENTICACION
2.9.3.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	2.16.724.1.3.5.7.1.2= MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL (ejemplo)
2.9.3.3. NIF entidad suscriptora	NIF de la entidad suscriptora	2.16.724.1.3.5.7.1.3= S2819001E (ejemplo)
2.9.3.4. DNI/NIE del responsable	DNI o NIE del responsable del certificado	2.16.724.1.3.5.7.1.4 = 00000000G (ejemplo)
2.9.3.5. Nombre de pila	Nombre de pila del responsable del certificado	2.16.724.1.3.5.7.1.6 = "JUAN ANTONIO" (ejemplo)
2.9.3.6. Primer apellido	Primer apellido del responsable del certificado	2.16.724.1.3.5.7.1.7= "DE LA CAMARA" (ejemplo)
2.9.3.7. Segundo apellido	Segundo apellido del responsable del certificado	2.16.724.1.3.5.7.1.8 = "ESPAÑOL" (ejemplo)
2.9.3.8. Correo electrónico	Correo electrónico de la persona responsable del certificado	2.16.724.1.3.5.7.1.9= juanantonio.delacamara@meyss.es



Campo	Descripción	Contenido
		(ejemplo)
2.9.3.9. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluida el responsable del certificado	2.16.724.1.3.5.7.1.10= SUBDIRECCION GENERAL DE ADMINISTRACION FINANCIERA (ejemplo)
2.9.3.10. Puesto o cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración	2.16.724.1.3.5.7.1.11= JEFE SECCION APOYO GESTION (ejemplo)

4.2 Certificado de Empleado Público para 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 organizativa 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 = SUBCA2 MEYSS
1.4. Validity	5 años	
1.4.1. Not Before	Fecha de inicio de validez	Fecha de inicio de validez, formato: UTCTime YYMMDDHHMMSSZ



Campo	Descripción	Contenido
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 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 = 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), así como su DNI (Ver Criterios de Composición del campo CN para un empleado público).	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)
1.5.9. Common Name (CN)	Nombre y dos apellidos de acuerdo con documento de identidad (DNI/NIE/Pasaporte), así como DNI, NIE o pasaporte separado por una barra vertical ()	CN = JUAN ANTONIO DE LA CAMARA ESPAÑOL - 00000000G (FIRMA) (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	



Campo	Descripción	Contenido
	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 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-caIssuers	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	No seleccionado "0"
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	No seleccionado "0"
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"



Campo	Descripción	Contenido
2.6.7. CRL Signature	Se usa para firmar listas de revocación de certificados	No seleccionado "0"
2.7. Qualified Certificate Statements		
2.7.1. OcCompliance	Indicación de certificado cualificado	OID 0.4.0.1862.1.1
2.7.2. OcEuRetentionPeriod	Periodo de conservación de informaciones (15 años)	OID 0.4.0.1862.1.3
2.7.3. OcSSCD	Uso de dispositivo seguro de firma	OID 0.4.0.1862.1.4
2.7.4. QcType- esign	Certificado de firma	OID 0.4.0.1862.1.6.1
2.7.5. QcPDS	Lugar donde se encuentra la declaración PDS	OID 0.4.0.1862.1.5 URL de la PDS (ver anexo B)
2.7.6. SemnaticId-Natural	Para indicar semántica de persona física definida por la EN 319 412-1	OID 0.4.0.194121.1.1
2.8. Certificate Policies	Políticas de certificación/DPC	
2.8.1. Policy Identifier	OID asociado a la DPC o PC	OID 1.3.6.1.4.1.27781.2.5.4.1.1
2.8.2. Policy Qualifier ID	Especificación de la DPC	
2.8.2.1. CPS Pointer	URL de la DPC	URL ubicación DPCM (ver anexo B)
2.8.2.2. User Notice	Campo explicitText	"Certificado cualificado de firma electrónica de empleado público, nivel alto. Consulte las condiciones de uso en <URL ubicación DPCM (ver anexo B)>"
2.8.3. Policy Identifier	OID asociado a certificado de empleado público de nivel alto	2.16.724.1.3.5.7.1
2.8.4. Policy Identifier	QCP-n-qscd	Certificado cualificado de firma, almacenado en dispositivo cualificado acorde al Reglamento UE 910/2014 0.4.0.194112.1.2
2.9. Subject Alternate Names		
2.9.1. Directory Name	Identidad administrativa	
2.9.1.1. Tipo de certificado	Indica la naturaleza del certificado	2.16.724.1.3.5.7.1.1 = CERTIFICADO CUALIFICADO DE FIRMA DE EMPLEADO PUBLICO DE NIVEL ALTO
2.9.1.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	2.16.724.1.3.5.7.1.2 = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL (ejemplo)



Campo	Descripción	Contenido
2.9.1.3. NIF entidad suscriptora	NIF de la entidad suscriptora	2.16.724.1.3.5.7.1.3 = S2819001E (ejemplo)
2.9.1.4. DNI/NIE del responsable	DNI o NIE del responsable del certificado	2.16.724.1.3.5.7.1.4 = 00000000G (ejemplo)
2.9.1.5. Nombre de pila	Nombre de pila del responsable del certificado	2.16.724.1.3.5.7.1.6 = "JUAN ANTONIO" (ejemplo)
2.9.1.6. Primer apellido	Primer apellido del responsable del certificado	2.16.724.1.3.5.7.1.7 = "DE LA CAMARA" (ejemplo)
2.9.1.7. Segundo apellido	Segundo apellido del responsable del certificado	2.16.724.1.3.5.7.1.8 = "ESPAÑOL" (ejemplo)
2.9.1.8. Correo electrónico	Correo electrónico de la persona responsable del certificado	2.16.724.1.3.5.7.1.9 = juanantonio.delacamara@meyss.es (ejemplo)
2.9.1.9. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluida el responsable del certificado	2.16.724.1.3.5.7.1.10 = SUBDIRECCION GENERAL DE ADMINISTRACION FINANCIERA (ejemplo)
2.9.1.10. Puesto o cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración	2.16.724.1.3.5.7.1.11 = 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/DPCyPolíticas>

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>