MINISTERIO DE TRABAJO,
MIGRACIONES
Y SEGURIDAD SOCIAL

SUBSECRETARÍA

S.G. DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIONES

Perfil de Certificado de Empleado Público del Prestador de Servicios de Confianza del Ministerio

sgtic@meyss.es
EA0021880

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

Control de versiones

Identificador	D301
Título	Perfil de Certificado de Empleado Público del Prestador de Servicios de Confianza del Ministerio
Versión	08
Estado del documento	Aprobado
Fecha de aprobación	20190724

Registro de cambios

Versión	Fecha	Comentario
1.0	20091203	Documento final
1.1	20100330	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	201009110	Eliminado del encabezado la DG de Servicios
1.3	20110910	Cambio SGPD por SGTIC
1.4	20111117	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	20120630	Actualización de la estructura organizativa y nuevo formato
1.6	20140210	Corrección de errores en extensión Subject Alternate Names
1.7	20150618	Se añade SHA-256
2.0	20160720	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	20170403	Ajuste al formato de documentación
04	20170531	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 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
05	20170706	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
06	20180718	Cambio de nombre del ministerio Formato de fechas adaptado a ISO 8601: YYYYMMDD Añadido RGPD en referencias Actualizado el apartado de protección de datos

		Actualizadas las referencias a la ley de Contratos del Sector Público
07	20190613	Actualizado el DIR3 Se elimina la caducidad del documento Precisado cómo se lleva a cabo la aceptación implícita Actualización de las referencias con la LOPDGDD
08	20190724	Cambio del valor del campo caIssuers de la extensión Authority Information Access Modificación Anexo B: URL certificado SubCA

Tabla de contenidos

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 Trabajo, Migraciones 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 emitidos en una tarjeta inteligente, un dispositivo cualificado 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 electrónica (no repudio).
- 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], con el fin de realizar firma electrónica cualificada definida en el artículo 3 (12) de dicho reglamento, política QCP-n-qscd de acuerdo a [ETSI EN 319 411-2].

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 de aseguramiento): *[1.3.6.1.4.1.27781.2.5.4.1.1]*
- Certificado de Empleado Público de autenticación (nivel alto de aseguramiento): *[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 (partes confiables, en inglés relying parties).

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.

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 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 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.

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.
CN	Common Name (Nombre Común).
CRL	Certificate Revocation List, Lista de Revocación de Certificados.
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.
LOPDGDD	Ley Orgánica de Protección de Datos y garantía de los derechos digitales
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.
RGPD	Reglamento General de Protección de Datos.
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.

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 [Ley 9/2017].

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:

- 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.

4 Requisitos operativos

4.1 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 los códigos de activación, que le permitirán la descarga y aceptación telemática de los certificados electrónicos en su dispositivo criptográfico.

El procedimiento de gestión de 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 inteligente. 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 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 operan como Entidades de Registro son: la *Subdirección General de Recursos Humanos* y la *Subdirección General de Apoyo a la Gestión de la Inspección de Trabajo y Seguridad Social*.

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.

4.2 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. La URL de descarga de los certificados se detalla en la copia del formulario cumplimentado recibida por el solicitante. 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 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.

Se consideran aceptados los certificados mediante la autenticación en el portal y mediante la utilización del mecanismo telemático de descarga y generación 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 las claves privadas asociadas 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.

4.3 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.

De utilizar certificados para una renovación, por defecto, todo empleado deberá autenticarse utilizando el certificado de autenticación centralizado y gestionado por un HSM, sin poder utilizar otra método.

4.4 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.

La hora y fecha utilizadas para la emisión de los servicios de revocación está sincronizado 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 el art. 14 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (Reglamento General de Protección de Datos Personales, RGPD) le comunicamos que la Subsecretaría del Ministerio de Trabajo, Migraciones y Seguridad Social (MITRAMISS) es responsable de todos los tratamientos de datos de carácter personal que se realicen para la prestación de servicios de confianza, esto es, para la gestión de certificados de empleado público y sello electrónico que emite el Ministerio.

La Subsecretaría, a través del Prestador de Servicios de Confianza constituido, realiza estos tratamientos de acuerdo con la normativa vigente en materia de protección de los datos personales, de seguridad de la información y la propia normativa específica que regula su actividad y que recoge todos los aspectos relativos a las condiciones en las que se pueden realizar tratamientos de datos de los interesados, principalmente el Estatuto Básico de Empleado Público, la ley 39/2015 y la ley 40/2015 que regulan el funcionamiento de la Administración General del Estado y sus Empleados Públicos.

En este sentido, se han adoptado las medidas técnicas y organizativas necesarias para evitar la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales. Las medidas adoptadas tienen en cuenta el estado de la tecnología, la naturaleza de los datos y los riesgos a los que están expuestos y se revisan periódicamente para garantizar su adaptación a nuevas situaciones o escenarios de riesgo.

La Subsecretaría, como responsable de todos los tratamientos de los datos de carácter personal de los interesados y de acuerdo con los requisitos de información al mismo recogidos en el artículo 14 del Reglamento (UE) 2016/679, indica a continuación la información básica relativa a estos tratamientos:

Responsable	Subsecretaría del Ministerio de Trabajo, Migraciones y Seguridad Social Paseo de la Castellana 63 Madrid 28071 España Correo electrónico: sgtic@meyss.es
DPD	Delegado de Protección de Datos Ministerio de Trabajo, Migraciones y Seguridad Social Paseo de la Castellana 63 Madrid 28071 España Correo electrónico: dpd@meyss.es
Finalidad	Gestión de la prestación de servicios de confianza incluyendo la gestión de los certificados electrónicos de empleado público y certificados electrónico de sello electrónico de acuerdo con el Estatuto Básico de Empleado Público y leyes 39 y 40/2015
Categoría de datos	Datos identificativos: NIF/DNI, nombre y apellidos, fecha de nacimiento, correo electrónico, puesto de trabajo, unidad a la que pertenece. Datos de características personales: claves pública y privada, número de serie del certificado, código de solicitud del certificado.
Origen de datos	Fichero de Empleados Públicos que desempeñan sus servicios en el Ministerio SG de Recursos Humanos Ministerio de Trabajo, Migraciones y Seguridad Social
Comunicaciones de datos	Comunicaciones a las fuerzas y cuerpos de seguridad del estado y órganos judiciales. Datos públicos del certificado.
Transferencias internacionales de datos	No se realizan transferencias fuera de la UE
Plazo de conservación	15 años de acuerdo con la normativa vigente
Tratamientos automatizados	No se realiza ninguna elaboración de perfiles con los datos de carácter personal

Derechos del interesado: los interesados podrán ejercer los derechos de acceso, rectificación, supresión (olvido), limitación de tratamiento, oposición y portabilidad de los datos, conforme a lo establecido en los artículos 15 a 22 del RGPD.

Cómo ejercer sus derechos: dirigiéndose al responsable del tratamiento por vía electrónica, o a través de cualquier Oficina de Atención en Materia de Registros tal y como dicta la ley 39/2015.

También podrá ponerse en contacto con el Delegado de Protección de Datos en lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos (art 38.4 RGPD).

Derecho a reclamar ante la Autoridad de Control: contacte con la Agencia Española de Protección de Datos: C/ Jorge Juan, 6. 28001. Madrid. España. (http://www.aepd.es).

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.

6 Perfil del Certificado de Empleado Público

6.1 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	Período de validez (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 TRABAJO, MIGRACIONES 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 = 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), 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, 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	
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)	

Campo	Descripción	Contenido
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	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

Campo	Descripción	Contenido
2.7.3. SmartCard Logon	Inicio de sesión con tarjeta inteligente	OID 1.3.6.1.4.1.311.20.2.2
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
2.8.1.1. Policy Qualifier ID	Especificación de la DPC	
2.8.1.1.1. CPS Pointer	URL de la DPC	URL ubicación DPCM (ver anexo B)
2.8.1.1.2. User Notice	Campo explicitText	"Certificado de personal, nivel alto, autenticación. Consulte las condiciones de uso en<URL ubicación DPCM (ver anexo B)>“
2.8.2. Policy Identifier	OID asociado certificado de empleado público de nivel alto	2.16.724.1.3.5.7.1
2.8.3. 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 TRABAJO, MIGRACIONES 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)

Campo	Descripción	Contenido
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 (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)

6.2 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	Período de validez (5 años)	

Campo	Descripción	Contenido
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 TRABAJO, MIGRACIONES 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), 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, 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	
2.2. Subject Key Identifier	Identificador de la clave pública del suscriptor o poseedor de claves (derivada de utilizar la función de Hash SHA-1 / 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-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”

Campo	Descripción	Contenido
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. 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	Tipo de certificado cualificado	OID 0.4.0.1862.1.6
2.7.4.1. 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 en inglés y en español (ver anexo B)
2.7.6. id-qcs-pkixQCSyntax-v2		OID 1.3.6.1.5.5.7.11.2
2.7.6.1. SemanticsId-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
2.8.1.1. Policy Qualifier ID	Especificación de la DPC	
2.8.1.1.1. CPS Pointer	URL de la DPC	URL ubicación DPCM (ver anexo B)
2.8.1.1.2. 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)>“
2.8.2. Policy Identifier	OID asociado a certificado de empleado público de nivel alto	2.16.724.1.3.5.7.1
2.8.3. 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		

Campo	Descripción	Contenido
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 TRABAJO, MIGRACIONES Y SEGURIDAD SOCIAL (ejemplo)
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 319 411-1	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 9/2017	Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
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.
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
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.
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

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

Certificado SUBCA1

http://ca.empleo.gob.es/meyss/documentos/subca1.cer

Certificado SUBCA2

http://ca.empleo.gob.es/meyss/documentos/subca2.cer

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