@dministración electrónica

PERFILES DE CERTIFICADOS ELECTRÓNICOS

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

TÍTULO: Perfiles de certificados electrónicos

Elaboración y coordinación de contenidos:
Dirección de Tecnologías de la Información y las Comunicaciones (DTIC)

Responsable edición digital: Subdirección General de Información, Documentación y Publicaciones

1ª edición electrónica: abril de 2016

Disponible esta publicación en el Portal de Administración Electrónica (PAe):
http://administracionelectronica.gob.es/

Edita:

© Ministerio de Hacienda y Administraciones Públicas
Secretaría General Técnica
Subdirección General de Información,
Documentación y Publicaciones
Centro de Publicaciones

Colección: administración electrónica

NIPO: 630-16-298-6

GOBIERNO DE ESPAÑA · MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS · CENTRO DE PUBLICACIONES

Perfiles de certificados electrónicos

ÍNDICE

1 Consideraciones generales

1.1 Objeto

El presente documento describe los perfiles de certificados derivados del Real Decreto 1671/2009 y está adaptado a las disposiciones de la Ley 39/2015 de 1 de Octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, la Ley40/2015 de 1 de Octubre, de Régimen Jurídico del Sector Publico (LRJ) y al Reglamento (UE) 910/2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS). Dichos certificados son: certificado de sede electrónica, certificado de sello electrónico, y certificado de empleado público. Asimismo, se incluye una definición para el certificado de la subCA emisora.

También se incluyen en el anexo al final del documento, con carácter informativo, unas recomendaciones sobre los perfiles básicos para garantizar la interoperabilidad de los certificados de personas físicas, de las personas físicas representantes de personas jurídicas y de entidades sin personalidad jurídica y otros tipos de certificados, que facilitará la extracción de los datos asociados a dichos certificados y facilitará la interoperabilidad de los mismos para su uso en las relaciones con las Administraciones.

En todo caso, para que estos certificados sean cualificados, deberán ser acordes al Reglamento UE 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, y su normativa de desarrollo.

Se expone un modelo de campos mínimo, basado en los estándares vigentes e influenciados por las “mejores prácticas” que actualmente rigen los sistemas de PKI. Existen dos clasificaciones para los distintos campos: “recomendables o no” y “fijos u opcionales”, dependiendo de su importancia o necesidad, los cuales se describen en el punto 2 como perfiles de certificados. Asimismo, los certificados están distribuidos entre nivel alto o nivel medio/sustancial dependiendo del caso uso, y en consecuencia, del riesgo asociado que conlleve la aplicación del certificado.

1.2 Alcance

Se trata del documento de referencia para los certificados derivados de la LRJ (Ley de Régimen Jurídico), de acuerdo con las diversas configuraciones acordadas, atendiendo a los diferentes niveles de aseguramiento.

Según el artículo 24.1 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, la política de firma electrónica y certificados en el ámbito de la Administración General del Estado y de sus organismos públicos está constituida por

las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación.

De acuerdo al artículo 18.1 del Real Decreto 4/2010, de 8 enero por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica, la Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para la autenticación y el reconocimiento mutuo de firmas electrónicas basadas en certificados de documentos administrativos en las Administraciones Publicas. No obstante, dicha política podrá ser utilizada como referencia por otras Administraciones públicas para definir las políticas de certificados y firmas a reconocer dentro de sus ámbitos competenciales.

Según el artículo 18.4, los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de manera que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones sin ningún tipo de restricción técnica, semántica u organizativa. Dichos certificados serán los definidos en la *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y el* RD 1671/2009.

Estos perfiles habrán de conjugarse con las Políticas de certificación y Declaración de Prácticas de Certificación para completar el marco de servicios en torno a los certificados.

Estos perfiles aplican a los mecanismos de identificación y firma electrónica *previstos en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público* ; y por tanto, no afectan al hecho de que la Administración admitirá para los procedimientos administrativos electrónicos cualquier certificado cualificado emitido en el ámbito europeo de aplicación del Reglamento *(UE) No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014,* relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior , y en consonancia con las obligaciones derivadas de dicho Reglamento, de la Ley 59/ 2003 y las que puedan derivar de futuras regulaciones en la materia.

En consonancia con ello se admitirán los certificados cualificados indicados en las listas de confianza TSL de todos los países identificados a partir de la TSL europea:

- https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf
- https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

Se tendrá en consideración a este respecto lo indicado en la Decisión de Ejecución (UE) 2015/1505 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el artículo 22, apartado 5, 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.

Cuando se hace referencia estándares o normativa técnica, se entiende referenciada a la última versión disponible en el momento de emisión del certificado.

2 Caracterización de los perfiles de certificados de sede, sello, empleado público y empleado público con seudónimo

En este apartado se describen los campos que componen los diferentes perfiles de los certificados de sede, sello, empleado público y empleado público con seudónimo. Antes se debe tener en cuenta una serie de cuestiones descritas a continuación, que se tratarán como recomendaciones, las cuales deben estar en línea con lo dictado en la política concreta de certificación.

2.1 Niveles de aseguramiento

Con los niveles de aseguramiento, se determina un esquema de garantía para las aplicaciones y servicios electrónicos que deseen establecer los medios de identificación y autenticación electrónicos. Se establecerá el nivel de riesgo asociados al caso de uso concreto, y en consecuencia, se determinarán los mecanismos de identificación y autenticación admitidos.

Cada uno de los diferentes niveles conllevará un grado de “confianza”, debido en gran medida a los requisitos técnicos y de seguridad que lleve asociados cada servicio público electrónico.

Además, acorde al Esquema Nacional de Seguridad, es necesario tipificar el nivel de aseguramiento requerido por la aplicación para determinar el nivel de las credenciales (en este caso los certificados) requeridos.

Se definen dos niveles de aseguramiento:

- Nivel medio/sustancial:
  - Este nivel corresponde a una configuración de mecanismos de seguridad apropiada para la mayoría de aplicaciones.
  - El riesgo previsto por este nivel es apropiado para acceder a aplicaciones clasificadas según el ENS en los niveles de Integridad y Autenticidad como de riesgo bajo o medio.
  - Asimismo, el riesgo previsto por este nivel corresponde a los niveles de seguridad bajo y sustancial de los sistemas de identificación electrónica del reglamento UE 910/2014. Los niveles de seguridad del reglamento eIDAS aplican únicamente a los sistemas de identificación electrónica.

- Los mecanismos de seguridad mínimos aceptables incluyen los certificados X.509 en software. En los casos de certificados emitidos a personas, se corresponde con el de un "certificado cualificado", como se define en el reglamento UE 910/2014 para firma electrónica avanzada, sin dispositivo cualificado de creación de firma. En los casos de certificados emitidos a personas jurídicas, se corresponde con el de un "certificado de sello cualificado", como se define en el reglamento UE 910/2014 para sello electrónico avanzado, sin dispositivo cualificado de creación de sello. El uso de dispositivos hardware de firma (dispositivo cualificado de creación de firma o HSM) también está permitido.

- Nivel alto:

  - Este nivel corresponde a una configuración de mecanismos de seguridad apropiada para las aplicaciones que precisan medidas adicionales, en atención al análisis de riesgo realizado.

  - El riesgo previsto por este nivel es apropiado para acceder a aplicaciones clasificadas según el ENS en los niveles de Integridad y Autenticidad como de riesgo alto.

  - Asimismo, el riesgo previsto por este nivel corresponde al nivel seguridad alto de los sistemas de identificación electrónica del reglamento UE 910/2014.Los niveles de seguridad del reglamento eIDAS aplican únicamente a los sistemas de identificación electrónica.

  - Los mecanismos de seguridad aceptables incluyen los certificados X.509 en hardware. En los casos de certificados emitidos a personas, se corresponde con el de un "certificado cualificado", para "firma electrónica cualificada", como se define en el reglamento UE 910/2014. En los casos de certificados emitidos a personas jurídicas, se corresponde con el de un "sello cualificado", como se define en el reglamento UE 910/2014.

La siguiente tabla sintetiza las posibilidades de descomposición de los diferentes certificados contemplados y sus usos:

Certificados y perfiles	Nivel medio/sustancial	Nivel alto
Sello para la actuación automatizada	• Perfil de firma, autenticación y cifrado independiente o agregado según las necesidades del organismo. • Las posibilidades de uso del sello se especifican en la sección 5.1. • Sw y Hw	• Perfil de firma, autenticación y cifrado independiente o agregado según las necesidades del organismo. • Las posibilidades de uso del sello se especifican en la sección 5.1. • ispositivo Cualificado de creación de firma/HSM si se usa para autenticación de servidores según el considerando 65 del eIDAS
Sede electrónica administrativa	• Perfil único autenticación y cifrado. • Sw y Hw	• Perfil único de autenticación y cifrado. • Dispositivo hardware.
Empleado público	• Perfil de firma, autenticación y cifrado independiente o agregado según las necesidades del organismo[1]. • Sw y Hw	• Perfil independiente para firma, autenticación y cifrado. Nivel de seguridad alto definido en el punto 5.7.4 del ENS (*)
Empleado público con seudónimo	• Perfil de firma, autenticación y cifrado independiente o agregado según las necesidades del organismo[2]. Sw y Hw	• Perfil independiente para firma, autenticación y cifrado. • Nivel de seguridad alto definido en el punto 5.7.4 del ENS (*)

(*) Nivel de seguridad definido de acuerdo al Anexo II *punto 5.7.4 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.*

[1] El certificado de cifrado es opcional.
[2] El certificado de cifrado es opcional.

Los certificados de sello y empleado público incluirán implícitamente, para cada perfil definido, el nivel de aseguramiento que le corresponde mediante un identificador único: el identificador del objeto Identidad Administrativa.

2.2 Clasificación de campos/taxonomía

Hay un conjunto de campos dentro de los certificados digitales (como Subject, Key Usage...), que según están definidos en los diferentes estándares, se encuentran incluidos en extensiones opcionales. En el uso real de los certificados, estos campos se emplean casi de forma habitual ya que sin ellos el uso de los certificados no sería completo/correcto.

De todos los campos y extensiones posibles para los certificados digitales X509 v3 indicados en la RFC5280 [4] se consideran **obligatorios** (pero no marcados como críticos) todos aquellos utilizados en este documento para describir los diferentes perfiles de certificados. Adicionalmente, existen campos y extensiones que se consideran **obligatorios** para una correcta/completa adecuación del certificado a los perfiles derivados de la LAECSP, y se marcarán en la columna R ("recomendado") con un "**Sí**". Es decir, dentro del certificado no deberán marcarse como críticos aquellos campos y extensiones que se indique en la familia de normas ETSI EN 319 412 [1] que no deben serlo, pero serán de inclusión obligatoria en los perfiles según este documento, aquellos marcados con R = 'SI'.

No se podrán añadir ni modificar los usos de las claves definidos en los perfiles de este documento, correspondientes la extensión Key Usage. Para el certificado de sede no se podrán establecer en la extensión Extended Key Usage, usos que impliquen la realización de firma electrónica (no repudio).

No obstante, cada prestador podrá añadir campos y extensiones adicionales (diversas instancias del atributo OU en el SubjectName, límites de uso cuantitativos y cualitativos de los certificados -por autorización legal expresa en la Ley 59/2003-, extensiones complementarias…) para facilitar el uso de los diferentes perfiles de certificados en las aplicaciones y sistemas de las diferentes Administraciones.

En cuanto a los campos incluidos en el nuevo objeto Identidad Administrativa definido en el presente documento, existen campos fijos que deben estar obligatoria y debidamente cumplimentados en el certificado. En los perfiles de certificados que se detallan más adelante en este documento, dentro la columna R ("recomendado") se marcan con "Si", aquellos considerados como obligatorios, y con una "O" los considerados como OPCIONALES para cada perfil de certificado.

A continuación se detallan dichos campos para los diferentes certificados:

Los campos singulares acordados para identificar al certificado de sello electrónico son:

- Fijos:
  - Descripción del tipo de certificado
  - Nombre de la entidad suscriptora

- Número de Identificación Fiscal de entidad suscriptora

- Opcionales:
  - Denominación de sistema o componente informático
  - Dirección de correo electrónico
  - Datos de identificación personal del titular del órgano administrativo:
    - Nombre de pila
    - Primer apellido
    - Segundo apellido
    - DNI o NIE

Los campos singulares acordados para identificar al certificado de empleado público son:

- Fijos:
  - Descripción del tipo de certificado
  - Datos de identificación personal de titular del certificado
    - Nombre de pila
    - Primer apellido
    - Segundo apellido
    - DNI o NIE
  - Nombre de la entidad en la que está suscrito el empleado
  - NIF de la entidad

- Opcionales:
  - Unidad a la que está adscrito el cargo o puesto que desempeña el empleado público
  - Cargo o puesto de trabajo.
  - Número de identificación de personal (NIP, NRP,…)
  - Dirección de correo electrónico

Los campos singulares acordados para identificar al certificado de empleado público con seudónimo son:

- Fijos:
  - Descripción del tipo de certificado
  - Datos de identificación (seudónimo) de titular del certificado
    - Seudónimo
  - Nombre de la entidad en la que está suscrito el empleado
  - NIF de la entidad

- Opcionales:
  - Unidad a la que está adscrito el cargo o puesto que desempeña el empleado público
  - Cargo o puesto de trabajo.
  - Número de identificación de personal (NIP,…)
  - Dirección de correo electrónico

3 Identificador de objetos

Como parte de la estandarización, los campos, principalmente alineados a la RFC 5280 (X509 v3), las normas europeas (EN 319 412) y las Guías del CAB Forum, tienen OIDs (object identifiers, secuencia de números para identificar un campo) los cuales son unívocos internacionalmente.

Los prestadores de servicios de certificación deberán identificar cada tipo de certificado (Sede, sello, empleado público) con un OID específico, que deberá ser unívoco y que no podrá emplearse para identificar tipos diferentes, políticas o versiones de certificados, emitidos por dicho prestador.

Dentro de los certificados existirán campos comunes a los ya vigentes o estandarizados, ej: commonName (cuyo OID es 2.5.4.3) o serialNumber (cuyo OID es 2.5.4.5). También disponen de un conjunto de campos nuevos o "propietarios" llamados Identidad Administrativa, la cual identifica al Suscriptor del certificado de forma unívoca y completa.

Para el objeto Identidad Administrativa, al tratarse de un conjunto de campos completamente nuevos, se ha optado por la siguiente opción para asignarles los OID:

Se utilizará el número ISO/IANA del MPR 2.16.724.1.3.5.X.X como base para identificarlo, de este modo se establecería un identificador unívoco a nivel internacional, haciendo que cualquier prestador pueda utilizarlo:

OID anteriores al reglamento eIDAS. Se utilizarán únicamente durante el periodo de transición a los nuevos formatos, según se establece en el apartado 12.

2.16.724.1.3.5.1.1=*SEDE ELECTRONICA (Nivel Alto)*
2.16.724.1.3.5.1.2=*SEDE ELECTRONICA (Nivel Medio/Sustancial)*
2.16.724.1.3.5.2.1=*SELLO ELECTRONICO PARA LA ACTUACION AUTOMATIZADA (Nivel Alto)*
2.16.724.1.3.5.2.2=*SELLO ELECTRONICO PARA LA ACTUACION AUTOMATIZADA (Nivel Medio/Sustancial))*
2.16.724.1.3.5.3.1= *CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (Nivel Alto)*
2.16.724.1.3.5.3.2= *CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (Nivel Medio/Sustancial))*

Adicionalmente se definen los siguientes OID, que permiten diferenciar los certificados ya emitidos, de aquellos que se emiten conforme al reglamento UE 910/2014:

2.16.724.1.3.5.4.1= CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (Nivel Alto)
2.16.724.1.3.5.4.2= CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (Nivel Medio/Sustancial))
2.16.724.1.3.5.5.1=SEDE ELECTRONICA (Nivel Alto)
2.16.724.1.3.5.5.2=SEDE ELECTRONICA (Nivel Medio/Sustancial))

2.16.724.1.3.5.6.1=SELLO ELECTRONICO PARA LA ACTUACION AUTOMATIZADA (Nivel Alto)
2.16.724.1.3.5.6.2=SELLO ELECTRONICO PARA LA ACTUACION AUTOMATIZADA (Nivel Medio/Sustancial))
2.16.724.1.3.5.7.1CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (Nivel Alto)
2.16.724.1.3.5.7.2= CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (Nivel Medio/Sustancial))

Esto no aplica a los certificados de Sede, ya que para ajustarse a las directivas del CAB Forum no contienen el objeto Identidad Administrativa, aunque si utilizarán los mencionados OIDs para identificar el tipo de certificado en la extensión Certifícate Policies.

4 Identidad administrativa

La Identidad Administrativa, se trata de un esquema de nombres incluido en los certificados, el cual facilitará la utilización de los certificados e identificación del suscriptor del certificado debido principalmente a tres motivos:

a) Eficiencia: en un único campo (SubjectAlternativeName) se almacenará toda la información referente al custodio/poseedor (Subject) del certificado, de forma que accediendo a determinados OIDs de ese campo (previamente definidos) se encontrarán los datos más usados.
En el caso de los certificados de Sede, el campo SubjectAlternativeName se ajustará a lo indicado en las Guías del CAB Forum.

Nota: dicha información es redundante puesto que se encuentra distribuida en otros campos del certificado.

b) Semántica: el uso que actualmente se le está dando al campo CommonName, es un poco arbitrario, para evitar esta situación se separa claramente la información en varios OIDs (uno para nombre, otro para primer apellido, segundo apellido… etc.)

c) Definición: La situación de certificación actual, corresponde a un modelo relativamente maduro de certificación, los prestadores dan usos diferentes al mismo campo, lo que dificulta su utilización. Al usar este modelo unificado, se puede saber exactamente (con su significado particular), lo que está almacenado en cada campo.

Los campos “normalizados” en esta opción son el Subject name y el SubjectAlternativeName puesto que se trata de una estrategia de mínimos. Dicha estrategia, consiste en exigir la existencia de ciertos campos y la obligatoriedad de rellenarlos así como la opción de cumplimentar opcionalmente otros campos.

Deben cumplir con la normativa RFC 5280 (x.509 Public Key Infraestructure. Certificate and Certificate Revocation List CRL Profile)

En los certificados de sede se tendrán en cuenta las recomendaciones del sector, recogidas en las Guías de CAB/Forum.

4.1 Subject Name

El campo Subject Name representa la identidad de la persona o entidad que recibe el certificado.

4.1.1 Composición del nombre

El nombre contenido en el Subject Name adopta la forma de un Nombre Distinguido, de acuerdo con la Recomendación ITU-T X.501, formado por un conjunto de atributos, cuya semántica definen las especificaciones técnicas correspondientes.

El nombre del suscriptor para cualquier prestador de servicios de certificación dado. Dicho prestador podrá emitir más de un certificado al mismo suscriptor con el mismo nombre (por ejemplo, en el periodo de renovación del certificado).

Las especificaciones aplicables son las siguientes:

- IETF RFC 5280: Incorpora los atributos X.520 más habituales, para cualquier tipo de nombre dentro del certificado.
- IETF RFC 3739: Perfila el empleo de los atributos X.520 más habituales, para su uso en los nombres dentro de certificados cualificados.

Esta composición resulta el mínimo exigible, pudiendo el prestador incluir atributos adicionales en el nombre distinguido, siempre que no resulten contradictorios con los contenidos de los atributos de mínimos.

4.2 Subject Alternative Name

En la extensión Subject Alternative Name se suelen incluir identidades alternativas de la misma persona que aparece como suscriptora del certificado.

La especificación IETF RFC 5280 prevé el posible empleo de los siguientes tipos de datos:

- Identidad basada en correo electrónico.
- Identidad basada en nombre diferenciado (DN), que se suele emplear para construir un nombre alternativo basado en atributos propietarios, que no resultan ambiguos en ningún caso (por ejemplo, FNMT-RCM, IZENPE, ACCV, CATCert u otros).
- Identidad basada en nombre de dominio de Internet (DNS).
- Identidad basada en dirección IP.
- Identidad basada en identificador de recurso universal (URI).

De todos ellos se puede contener más de una instancia (por ejemplo, diversas direcciones de correo electrónico).

Todos estos nombres deben ser verificados por el prestador de servicios de certificación, cuando se incluyan en los certificados.

Como opción a valorar, se aporta una propuesta de DN para identificación inequívoca de personas físicas y suscriptores de certificados, para facilitar su procesamiento eficiente por aplicaciones automáticas, aun resultando redundante con la información ya contenida en otros campos.

Esta identidad, que denominamos "identidad administrativa ", la puede construir el prestador, de forma que se disponga de toda la información de forma homogénea dentro del certificado, especialmente debido a que algunos componentes de los nombres tienen semántica diferente, en función del tipo de certificado.

El contenido de parte de los campos descritos a continuación se normalizará en la medida de lo posible. A continuación se propone un modelo de normalización de los campos variables de los certificados.

En los certificados de sede se tendrán en cuenta las recomendaciones del sector, recogidas en las Guías de CAB/Forum.

5 Guía de cumplimentación de campos de los certificados.

La finalidad de esta propuesta es la de emplear los mismos nombres para todos los certificados, de forma que exista un marco común. De este modo, se asignará exactamente el mismo nombre a sellos, sedes, organizaciones, puestos y unidades, etc. para toda la Administración General del Estado.

En cuanto a las normas de codificación de los campos, en general no hay reglas complejas de nomenclatura. Se recomienda seguir la RFC 5280, que usa UTF-8[3] string, puesto que codifica grupos de caracteres internacionales incluyendo caracteres del alfabeto latino con diacríticos (“Ñ”, “ñ”, “Ç”, “ç”, “Ü”, “ü “, etc.). Por ejemplo, el carácter eñe (ñ), que se representa en unicode como 0x00F1. Las recomendaciones que se deben seguir en todo momento vienen descritas en la columna Formato/Observaciones dentro de cada perfil descrito en el documento, donde se incluye: el tipo de campo, su longitud y un breve ejemplo.

Junto con las recomendaciones particulares en cada perfil, se habrían de seguir los siguientes consejos para todos los literales variables:

- Todos los literales se introducen en mayúsculas, con las excepciones del nombre de dominio/subdominio y el correo electrónico que estarán en minúsculas.
- No incluir tildes en los literales alfabéticos
- No incluir más de un espacio entre cadenas alfanuméricas.
- No incluir caracteres en blanco al principio ni final de cadenas alfanuméricas.
- Se admite la inclusión de abreviaturas en base a una simplificación, siempre que no supongan dificultad en la interpretación de la información.

[3] Para más información ver RFC 2279 mejorada en 3629 (UTF-8, a transformation format of ISO 10646)

A continuación se detallan una serie listas y recomendaciones para rellenar dichos campos junto con unas propuestas para su gestión que complementan convenientemente el perfil de los certificados. Se comienza con una aproximación a campos genéricos que se aplican en la mayoría de los certificados.

- Campos entidad suscriptora y unidades

Se incluyen dentro de este grupo todas aquellos Departamentos ministeriales, órganos u organismos públicos, como Agencias, Entidades públicas u organismos autónomos correspondientes a la AGE.

Estos campos se implementan en el Subject name y Subject alternative name de los certificados y para completarlo debe tenerse en cuenta siempre el formato requerido (String UTF8 [RFC 5280] Size 128) siguiendo en la medida de lo posible las normas que se describen posteriormente.

Se seguirá la distribución establecida DIR3, siendo este directorio el que contiene la relación de órganos administrativos a que hace referencia el Artículo 9 del Esquema Nacional de Interoperabilidad (Real Decreto 4/2010). Dicho artículo establece que "Las Administraciones públicas… mantendrán una relación actualizada de sus órganos administrativos y oficinas de registro y atención al ciudadano, y sus relaciones entre ellos. Dichos órganos y oficinas se codificarán de forma unívoca y esta codificación se difundirá entre las Administraciones públicas. "

La relación actualizada de órganos administrativos y sus códigos se encuentra disponible en el portal de Administración Electrónica en el siguiente enlace:

- http://administracionelectronica.gob.es/ctt/dir3

En cuanto a las Unidades, el campo incluido tanto en Subject como en Subject alternative name identifica la unidad organizativa, en la que está incluido el suscriptor del certificado.

Para rellenarlo se debe tener en cuenta el formato requerido (string UTF8 [RFC 5280] size 128) siguiendo en la medida de lo posible la nomenclatura de DIR3

- Cargo o puesto de trabajo

Este campo incluido tanto en Subject como en Subject alternative name identifica el puesto o cargo de la persona física que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado. Para rellenarlo se debe tener en cuenta el formato requerido (string UTF8 [RFC 5280] size 128), siguiendo, en la medida de lo posible, la nomenclatura descrita en el Registro Central de Personal, sujeta a variación. Dichas descripciones están en texto libre, excepto para personal laboral de convenio único.

Es importante resaltar que, en el momento de la realización de la versión actual del documento, no se encuentran en el Registro Central de Personal los denominados altos cargos de la Administración, a nivel de denominación de cargo o puesto.

A continuación se describe una pequeña muestra:

- JEFE DE SECCIÓN
- CONSEJERO
- SECRETARIO GENERAL
- JEFE DE SERVICIO
- ABOGADO DEL ESTADO
- DIRECTOR DE PROGRAMA
- VOCAL ASESOR
- ANALISTA DE SISTEMAS
- ANALISTA PROGRAMADOR
- OPERARIO
- ADMINISTRATIVO
- AUXILIAR ADMINISTRATIVO
- ORDENANZA
- ASESOR
- JEFE DE ÁREA

5.1 Sello electrónico para la actuación automatizada

Los certificados de sello electrónico para la actuación automatizada serán considerados como certificados de sello conforme al reglamento eIDAS, por lo que deberán cumplir los requisitos impuestos a estos.

En cuanto a la aplicación del certificado de sello se requiere, además de la determinación de una taxonomía determinada, la caracterización del uso interno y del dominio semántico de los sellos emitidos.

Campos variables	Ejemplos
○ Descripción del tipo de certificado	*"SELLO ELECTRONICO"*
○ Denominación de sistema o componente informático (se incluyen varios ejemplos)	○ *"SELLO ELECTRONICO DEL MINISTERIO DE LA PRESIDENCIA"* ○ *"REGISTRO ELECTRONICO"* ○ *"SISTEMA DE VERIFICACION DE DATOS DE IDENTIDAD"* ○ *"PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA"*
○ Nombre de la entidad suscriptora	*"MINISTERIO DE LA PRESIDENCIA"*
○ Número de Identificación Fiscal de entidad suscriptora	*"S2833002"*
○ Dirección de correo electrónico	*"juanantonio.delacamara.espanol@mpr.es"*

Campos variables	Ejemplos
○ Datos de identificación personal del titular del órgano administrativo • Nombre de pila • Primer apellido • Segundo apellido • DNI o NIE	 *"JUAN ANTONIO"* *"DE LA CAMARA"* *"ESPAÑOL"* *"00000000G"*

El certificado de sello, acorde al reglamento eIDAS, puede tener tres usos: (1) "sellado de documentos", (2) "sellado de código" y (3) "certificado de autenticación de activo de la persona jurídica" (actuando como certificado de componente por ejemplo para autenticación en servidores de aplicaciones). Nunca se utilizará en exclusiva para cifrado, ni como certificado de autenticación de servidor web.

En conclusión, sólo podrá haber los siguientes perfiles:

(1) Sello de documentos: key usage tendrá el bit "ContentComitment"

(2) Sello de código: keyusage tendrá el bit "digitalSignature" combinado con el extendedkeyusage ("codeSigning")

(3) Autenticación: keyusage tendrá el bit "digitalSignature" combinado con el keyEncipherment (o KeyAgreement) y con extendedkeyusage ("serverAuth", "clientAuth"…)

Se exponen a continuación tres ejemplos concretos de situaciones relacionadas con el certificado de sello y las recomendaciones para su definición:

Caso I: uso de certificado de sello general para el organismo:

Este caso de uso consiste en la emisión de un sello de aplicación general para todos los sistemas y servicios de un organismo, como por ejemplo podría suceder en un sello de Ministerio. Este uso ha de acompañarse de procedimientos de seguridad complementarios que solventen la vulnerabilidad existente al replicar las claves e instalarlas en diferentes servidores de aplicaciones, y que ofrezcan las mayores garantías a los ciudadanos y administraciones receptores de las firmas electrónicas realizadas con dicho certificado.

En relación con esta situación, deben realizarse las siguientes recomendaciones:

1. En general, debe realizarse un análisis de riesgos y del entorno, del que se derive la posibilidad de empleo de un sello para todos los usos.

2. En estos casos, es necesario realizar la designación conveniente el nombre del sistema o componente informático, dado que habría de ser generalista para englobar el uso global previsto para la entidad suscriptora.

Ejemplo del campo “Denominación de sistema o componente informático“: “Sello electrónico del Ministerio…”.

3. Como excepción a lo indicado, se puede recomendar el empleo de un sello general para un organismo en los escenarios de intercambio de documentos electrónicos a través de la red SARA, dado que se trata de un uso muy específico que tiende a una cierta centralización en plataformas específicas de catalogación e intercambio interadministrativo de datos y documentos, de forma interoperable.

Caso II: uso de certificado de sello de unidad orgánica

Este caso se basa en la emisión de un sello a una unidad orgánica dentro de una organización como un Departamento ministerial. El certificado de sello identificaría y autenticaría a dicha unidad de forma unívoca. El NIF correspondiente se asociaría al organismo o Departamento ministerial del que dependiera, que sería el considerado el creador del sello.

Ejemplo del campo: “Denominación de sistema o componente informático“: “Sello electrónico de la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica”, y como nombre de la entidad suscriptora: “Ministerio de Hacienda y Administraciones Públicas”.

En relación con esta situación, deben realizarse las siguientes recomendaciones:

1. En general, se recomienda el empleo de esta posibilidad de forma ordinaria, sin embargo, no es conveniente llegar a un grado muy alto de desagregación en las unidades orgánicas dada la complejidad en la administración del ciclo de vida.

2. Dado que los sistemas que apliquen sistemas de identificación y autenticación basados en certificados de sello electrónico suelen estar administrados por unidades de tecnología, es una práctica conveniente asociar como denominación del sistema o componente a dicha unidad de tecnología.
   Ejemplo: “Denominación de sistema o componente informático“: “Sello electrónico de la Subdirección General de Tecnología de la Información y de las Comunicaciones”.

3. Se recomienda emitir certificados a la unidad orgánica para su uso general, por todas las aplicaciones, si bien resulta también aceptable emitir sellos específicos para aplicaciones diferentes, cuando se acredite esta necesidad.

Caso III. Uso de certificado de sello asociado a un sistema de información

Otra variante consiste en designar el sello con el nombre del sistema o plataforma que sustenta el procedimiento administrativo que requiere del sello o identificación. En estos casos es también necesario incluir el nombre del creador del sello, es decir, la persona jurídica de quien depende el sistema de información.
Ejemplo: “Denominación de sistema o componente informático“: “Registro electrónico”.

5.2 Sede electrónica administrativa

Se va a producir una gran heterogeneidad en la configuración de los escenarios técnicos que determinan una sede electrónica. Así habrá sedes electrónicas hospedadas en servidores individuales, en granjas de servidores, en sistemas clusterizados que atienden a direcciones virtuales, etc.

Se dan a continuación unas recomendaciones para la aplicación del certificado de sede a partir de diferentes configuraciones, y se revisará una propuesta semántica de los certificados.

Para la designación de sedes electrónicas dentro de una organización, se seguirán criterios claros y sin ambigüedad de la sede. No se prescribe un número o criterio concreto para determinar el número de sedes existentes en un organismo público o Departamento ministerial.

Ejemplos de designación de sedes electrónicas serían ("Nombre descriptivo de la sede electrónica"):

- "Centro de Transferencia de Tecnologías de las Administraciones Públicas"
- "Punto de Acceso General
- "Portal oficial del Ministerio de la Presidencia"

En todo caso, los certificados de sede serán considerados como certificados cualificados de autenticación web conforme al reglamento eIDAS, por lo que deberán cumplir los requisitos impuestos a estos. También se tendrán en cuenta las recomendaciones del sector, recogidas en las Guías de CAB/Forum, en especial aquellas para los certificados denominados de 'Extended Validation'.

Campos variables	Ejemplos
○ Descripción del tipo de certificado	*"SEDE ELECTRONICA"*
○ Nombre descriptivo de la sede electrónica (se incluyen varios ejemplos)	○ *"CENTRO DE TRANSFERENCIA DE TECNOLOGIAS DE LAS ADMINISTRACIONES PUBLICAS"* ○ *"PUNTO DE ACCESO GENERAL"* ○ *"PORTAL DEL HACIENDA Y ADMINISTRACIONES PÚBLICAS"*
○ Denominación de Nombre del dominio (se incluyen varios ejemplos)	○ *"ctt.mpr.es"* ○ *"administración.gob.es"* ○ *"minhap.es"*
○ Nombre de la entidad suscriptora	*"MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS"*
○ Número de Identificación Fiscal de entidad suscriptora	*"S2833002"*

A continuación se exponen tres ejemplos concretos de usos relacionadas con el certificado de sede electrónica en diferentes escenarios tecnológicos y las recomendaciones para resolver los nombres de dominio/subdominio y externalización de servicios:

Caso I: uso de certificados de sede electrónica en granjas de servidores

Este caso de uso consiste en el empleo de certificados de sede electrónica en granjas de servidores de páginas HTTPs. Dependiendo de los requisitos de disponibilidad de una sede electrónica, puede resultar frecuente que se precise más de un servidor de páginas, de forma que resulta necesario organizar una colección de servidores físicos que sirven páginas correspondientes a una misma sede lógica.

Los modelos de implementación de las granjas resultan variables, dependiendo de la tecnología que se emplee en cada caso. Uno de estos modelos de implementación asigna a cada servidor de páginas un nombre de máquina diferente, y reparte la carga de trabajo o los procesos en las diferentes máquinas, de forma que el usuario visualiza la conexión a diferentes servidores (por ejemplo, http://www1.servidor.es, http://www2.servidor.es).

Cuando en este modelo se desea asegurar la comunicación mediante el empleo de certificados, existen dos opciones:

1. La primera opción consiste en emitir un certificado para cada servidor, de forma que se deben producir tantos certificados como máquinas físicas existen.
2. La segunda opción consiste en emitir un único certificado, en cuyo campo “Denominación de nombre del dominio” se incluye un comodín (en el ejemplo, "http://*.servidor.es"), lo que permite copiar la misma clave privada en diversos servidores, e instalar el mismo certificado.
   Hay que tener en cuenta que los certificados de sede, si se desea que cumplan los criterios de Extended Validation (EV) del CAB Forum, no pueden contener un dominio wildcard.

Con todo, siendo la primera opción la más recomendable, existen otros modelos, que resultan más correctos, como por ejemplo crear una sede electrónica lógica, con independencia del número de servidores que existan físicamente, mediante balanceadores de carga.

En este caso, puede existir un único certificado de sede electrónica, pero como asume todo el trabajo de establecimiento y gestión del canal seguro, se recomienda el empleo de bienes de equipo criptográficos de alta capacidad de trabajo dedicados de forma específica.

Caso II: uso de certificados de sede en casos de hosting externo

Este caso de uso consiste en la obtención e instalación de un certificado de sede electrónica en una máquina en régimen de hospedaje en un prestador de servicios informáticos (hosting externo), dado que en este caso el operador de la sede electrónica puede no ser la propia Administración, sino dicha empresa.

Esta situación puede generar riesgos específicos relativos a la integridad y disponibilidad de la clave privada del certificado de la sede, y en su consecuencia se hace preciso establecer algunas medidas adicionales de seguridad.

1. Se recomienda generar las claves de los certificados de sede electrónica en soporte hardware, bajo el control de la Administración, mediante la realización de una ceremonia de claves, de forma previa a la instalación del hardware criptográfico en el centro de datos del prestador del servicio de hosting, o de forma posterior, con las debidas medidas de seguridad.

2. Una vez se haya realizado la generación segura de las claves, se pueden solicitar los certificados correspondientes, instalarlos e inicializar la plataforma, todo ello con controles apropiados.

3. Se recomienda, asimismo, implementar sistemas de administración remota de dicho equipo criptográfico, de forma que el control de las claves siempre se encuentre en manos de la Administración.

Caso III: uso de certificados de sede en casos de outsourcing de servicios

Este caso de uso consiste en el empleo de certificados de sede electrónica en situaciones en que la prestación completa de un servicio público se encuentra externalizada.

Se hace preciso diferenciar dos situaciones:

1. Una primera situación se refiere a la externalización completa del servicio mediante una fórmula de gestión indirecta de servicios, en que, de acuerdo con la normativa legal vigente, se presta el servicio mediante una entidad de derecho público o una empresa pública. En este primer caso, el certificado deberá identificar a dicha entidad de derecho público o a la empresa pública.

2. La segunda situación resulta análoga a la del caso de hosting de servicios, pero con la particularidad de que la Administración cede también la gestión de claves y de certificados a la empresa prestadora del servicio.

La segunda de las situaciones presentadas exige medidas adicionales de control, específicamente orientadas a reducir diversos riesgos:

1. Se recomienda regular minuciosamente en el contrato de outsourcing la autorización y régimen de uso de los certificados de sede electrónica, así como las consecuencias para los casos de infracción.

2. En algunos casos puede darse la situación de que el prestador de servicios de certificación que debe emitir el certificado no acepte una solicitud tramitada por el prestador del servicio de outsourcing, de modo que resulta recomendable establecer un procedimiento para que dicha solicitud sea realizada por la Administración para su posterior tratamiento por el outsourcer.

3. En aquellos casos en que sea preciso utilizar servicios de hosting externos que no permitan la instalación de los certificados de sede definidos en este documento, ya sea por razones técnicas o por política interna del prestador de servicios, se podrán utilizar certificados que, aun no cumpliendo los perfiles especificados en este documento, identifiquen claramente la Administración responsable, según lo recogido en el artículo 18.1 del Real Decreto 1671/2009 En estos casos, los organismos públicos de la AGE velarán porque se implanten las medidas de seguridad adecuadas para garantizar la identificación y autenticación de la Sede y la integridad y disponibilidad del certificado utilizado. Esta circunstancia se hará constar en la misma Sede electrónica y se comunicará a los departamentos responsables de la gestión de certificados admitidos en la AGE, para su constancia.

5.3 Empleado público

Los certificados de empleado público son un subtipo de los certificados de cualificados de persona física del reglamento eIDAS, por lo que deberán cumplir los requisitos impuestos a estos.

En el caso de los certificados del personal al servicio de la AGE designado como empleado público, la casuística en la asignación de información a los certificados es aún mayor que en el caso de sede y sello electrónico. A ello se suma el amplio volumen de certificados a emitir previstos y la diversidad de Prestadores que se prevé que emitan dichos certificados.

Veamos ejemplos de campos variables de empleados públicos:

Campos variables	Ejemplos
○ Descripción del tipo de certificado	*"CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO"*
○ Datos de identificación personal del titular del órgano administrativo - Nombre de pila - Primer apellido - Segundo apellido - DNI o NIE	 *"JUAN ANTONIO"* *"DE LA CAMARA"* *"ESPAÑOL"* *"00000000G"*
○ Nombre de la entidad suscriptora	*"MINISTERIO DE FOMENTO"*
○ Número de Identificación Fiscal de entidad suscriptora	*"S2833002"*
○ Dirección de correo electrónico	*"juanantonio.delacamara.espanol@mfom.es"*
○ Unidad a la que está adscrito el cargo o puesto que desempeña el empleado público	○ *"DIVISIÓN DE PROSPECTIVA Y TECNOLOGÍA DEL TRANSPORTE"* ○ *"SUBDIRECCION GENERAL DE PROCESO DE DATOS"*
○ Cargo o puesto de trabajo	*"ANALISTA PROGRAMADOR"*
○ Número de identificación de personal (NIP, NRP,…)	*"A02APE1056"*

A continuación se exponen tres ejemplos concretos de usos relacionadas con el certificado de empleado público y las recomendaciones para resolverlos:

Caso I: uso de certificados por empleados públicos vinculados a varios órganos

Este caso de uso consiste en determinadas personas, que por razón de su cargo o puesto de trabajo ostentan otros cargos en otros organismos dependientes o vinculados al organismo principal, como por ejemplo sucede con el Director General de un Ministerio que es presidente de un Ente Público dependiente del mismo.

En relación con esta situación, se pueden realizar las siguientes recomendaciones:

1. En general, se deberían diseñar las aplicaciones de forma que estas personas no tengan que disponer de un certificado para cada organismo, sino que puedan emplear el certificado del organismo principal para sus actuaciones como firmante de los restantes organismos.

2. La recomendación anterior debe entenderse sin perjuicio de los casos en que un organismo suministra una tarjeta de empleado público con funcionalidades adicionales a la firma electrónica y, en particular, cuando dicha tarjeta se emplea como instrumento para el acceso físico a las instalaciones, o para el acceso lógico a sistemas operativos y redes. En estos casos, las personas citadas dispondrán de tantas tarjetas como organismos en los que actúen.

Caso II: uso de certificados por empleados públicos de múltiples órganos/organismos

Este caso de uso consiste en determinas personas que, por razón de su rol o función, se encuentran habilitados para actuar en diferentes órganos u organismos, y, de forma bastante particular, se refiere a los empleados con habilitación nacional, como sucede con los secretarios, interventores y tesoreros de administración, que pueden actuar en diversos organismos diferentes, en función de las necesidades.

Este caso de uso resulta similar al anteriormente presentado, con la diferencia de que, en este caso, por tratarse de funciones transversales a diversos departamentos y, en algunos caso, a diversas administraciones, resulta recomendable centralizar la emisión y gestión posterior de los certificados en algún organismo, como por ejemplo, el colegio correspondiente o en la unidad administrativa oportuna, de acuerdo con la normativa vigente.

En estos casos, no se deberá posteriormente emitir certificados a estos roles, en cada uno de los órganos u organismos en que estén temporalmente adscritos, aunque ello podrá suceder cuando se acredite la necesidad, como también se ha presentado anteriormente (tarjetas de acceso físico o lógico, por ejemplo).

Caso III: uso de certificados por personas con necesidad de cifrado

Este caso de uso contempla las necesidades de gestión y uso de los certificados cuando se necesita cifrado, dado que no es obligatorio que el sistema lo ofrezca.

Se pueden realizar las siguientes recomendaciones:

En general, se recomienda emplear certificados específicos de cifrado, con segregación de claves, e implantar procedimientos de recuperación de claves de cifrado que deberán documentarse en las guías y procedimientos de seguridad.

Cuando el prestador que suministra los certificados de firma no ofrezca certificados de cifrado (como por ejemplo en el caso del DNI electrónico, cuando es utilizado por empleados público), o cuando el prestador no ofrezca servicios de recuperación de claves, deberán implantarse métodos de cifrado mediante claves simétricas bajo el control y responsabilidad de cada Administración Pública.

Números de identificación fiscal (NIF) y personal (NIP, NRP,…)
El número de identificación fiscal, será acorde a la normativa vigente. Ejemplos:

- Entidades: incluir la letra y los números. Ej: "S2833002"
- Personas: incluir los números y la letra al final, sin separación de guión. Ej: "00000000G"

El Número de Identificación Personal (NIP) en el Registro Central de Personal está compuesto por ocho posiciones numéricas y una posición de control alfanumérica. El NIP es la clave que identifica a las personas en el Sistema de Información de Registro Central de Personal.

El NIP se construye dependiendo:

1. Del tipo de documento que aportó la persona en su primera relación con la Administración General del Estado (AGE).
2. De la fecha de incorporación en su primera relación con la AGE.

<table>
<tr><th colspan="2">NIP</th><th colspan="2" rowspan="2">Documento presentado en la primera Relación de Servicios con la AGE</th><th rowspan="2">Ejemplos</th></tr>
<tr><th>Número
(8 posiciones)</th><th>Control
(1 posición)</th></tr>
<tr><td>DNI sin letra</td><td>Blanco, 1, 2</td><td colspan="2">DNI</td><td>00001234
00001234-1
00001234-2</td></tr>
<tr><td>Secuencial generado por el sistema</td><td>N</td><td>Desde 01/01/2003</td><td rowspan="2">Otro documento</td><td>0001234-N</td></tr>
<tr><td>Construido partiendo del documento presentado</td><td>3, 4, 5, 6, 7, 8, 9</td><td>Antes de 01/01/2003</td><td>0001234-3</td></tr>
</table>

5.4 Empleado público con seudónimo

En el caso de los certificados con seudónimo, hay que tener en cuenta los usos establecidos en el Real Decreto 668/2015, de 17 de julio, por el que se modifica el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos: 'aquellas actuaciones que realizadas por medios electrónicos afecten a información clasificada, a la seguridad pública o a la defensa nacional o a otras actuaciones, en las que esté legalmente justificado el anonimato para su realización'

Veamos ejemplos de campos variables de empleados públicos con seudónimo:

Campos variables	Ejemplos
○ Descripción del tipo de certificado	*"certificado electrónico de empleado público con seudónimo"*
○ Datos de identificación personal - seudónimo	*"123456789"*
○ Nombre de la entidad suscriptora	*"MINISTERIO DEL INTERIOR"*
○ Número de Identificación Fiscal de entidad suscriptora	*"S2816015H"*
○ Dirección de correo electrónico	*"policía_judicial@dgp.es"*
○ Unidad a la que está adscrito el cargo o puesto que desempeña el empleado público	○ *"DIRECCION GENERAL DE LA POLICIA"* ○ *"AGENCIA TRIBUTARIA: INSPECCION ADUANAS"*
○ Cargo o puesto de trabajo	*"SUBINSPECTOR"*
○ Número de identificación de personal (NIP siempre que no derive del DNI o de algún dato que permita deducir los datos de identificación del empleado público.…)	*"123456789"*

Con el fin de facilitar la identificación a que hace referencia el artículo 22.4 del Real decreto 1671/2003 ," Los órganos judiciales y otros órganos y personas legitimadas podrán solicitar que se les revele la identidad de los firmantes con certificado electrónico de empleado público con seudónimo," la unidad a la que está adscrito el puesto se consignará con el nivel de detalle suficiente para que, consultando al organismo, sea posible determinar el empleado público a que hace referencia el seudónimo.

Caso I: uso de certificados con puesto de trabajo o cargo y número de identificación profesional

Este caso de uso consiste en incluir como seudónimo el número de identificación profesional interno del organismo, siempre que dicho número de identificación no esté relacionado con datos personales como el número de DNI. De esta manera la identificación del empleado podría realizarse consultando los registros del organismo al que pertenece el empleado, datos que también se incluyen en el certificado.

Como ejemplo:
El seudónimo podría consistir en el Número de Identificación Profesional. Ej: NIP 11111111.

Como en el certificado se consigna también el organismo y la unidad (Ej: DIRECCION GENERAL DE LA POLICIA, *BRIGADA CENTRAL DE ESTUPEFACIENTES)*

En este caso el CN del certificado seria:
CN= SUBINSPECTOR – NIP 11111111 – DIRECCION GENERAL DE POLICIA

Caso II: uso de certificados con seudónimo

Alternativamente, si el número de identificación profesional está relacionado con el número del Documento Nacional de Identidad, el seudónimo podrá consistir en un número arbitrario, debiendo en este caso consignarse expresamente que se trata de un seudónimo.

Como ejemplo:
El seudónimo podría consistir en un número aleatorio: 123456789

En este caso el CN del certificado seria:
CN= SEUDONIMO – 123456789 – DIRECCION GENERAL DE POLICIA

En ambos casos, el Prestador de Servicios de Certificación deberá almacenar la información relevante, de conformidad con lo previsto en la Ley 59/2003, de 19 de diciembre.

6 Algoritmos

A continuación se muestran una serie de requisitos en el campo de los algoritmos, los cuales pueden resultar interesantes para crear un marco común entre los prestadores.
Es importante particularizar el empleo de algoritmos y sus longitudes de clave en los diferentes perfiles propuestos para los cuatro certificados nuevos.

Se establece un escenario de seguridad básico denominado “entorno de seguridad genérico de la AGE”, que determinará el criterio de robustez y viabilidad aplicable para cada perfil de certificado. Los dos niveles de aseguramiento recogidos en apartado 2 del presente documento se considerarán dentro de dicho escenario.

Adicionalmente y al amparo del artículo 4.4 de la Ley 59/2003, de 19 de diciembre, de firma electrónica (uso de la firma electrónica en entornos sensibles para la seguridad pública, la defensa nacional, el manejo de información clasificada) podría establecerse un entorno de alta seguridad para los prestadores o Administraciones que así lo requieran. Dicho entorno estaría fuera del alcance de este documento y debería seguir las recomendaciones de la guía CCN-STIC 405, que alinea los algoritmos y longitudes de clave frente a las amenazas de las que hay que proteger hoy día la información clasificada nacional o internacional (OTAN, UE, etc.).

A) Escenario de seguridad genérico de la Administración

Para el escenario de seguridad genérico de la Administración, se plasman a continuación la caracterización de algoritmos y longitudes de clave. Para determinar los requisitos que se incluyen a continuación se ha tenido en cuenta la especificación técnica ETSI ETSI TS 119 312 V1.1.1 (2014-11)[4] y las guías de CA Browser Forum. Se distinguen requerimientos criptográficos para las autoridades emisoras de los Prestadores de Servicios y para entidades o certificados finales:

Actualmente, en dichas guías se recomienda utilizar como mínimo, el algoritmo de firma SHA2withRSA tanto en los certificados de las raíces y subraíces como en los certificados de entidades finales. Se prohíbe el uso de SHA-1, recomendando SHA256 o SHA512 para todos los certificados. Es obligatorio el uso de al menos SHA256 para los certificados de sitios web finales emitidos con posterioridad al 1 de Enero de 2016 y para todos los certificados de sitio web a partir del 1 de Enero de 2017. En cuanto al uso de longitudes de clave RSA, la mencionada norma establece la posibilidad de utilizar RSA a 2048 para entidades finales y 4096 para raíces y subraíces.

Por lo tanto, se ofrecen las siguientes opciones, que han sido debidamente recogidas en los casos de uso de los perfiles reflejados en el presente documento. Se distingue su aplicación en un nivel de aseguramiento alto y medio/sustancial.

Debido a la constante evolución de la tecnología, estos requisitos se revisarán y podrán establecerse nuevas actualizaciones.

- Raíces y subraíces de PKIs de Prestadores de Servicios de Certificación:

Nivel Aseguramiento	**Entidad**	**Algoritmo y longitud mínima**		**Observaciones**
Todos	AC raíz y subraíz	SHA-256	RSA-4096	○ AC raíz anteriores a 2016 podrán seguir utilizando RSA-2048 durante un periodo de adaptación

- Entidades finales:

Nivel Aseguramiento	**Entidad**	**Algoritmo y longitud mínima**		**Observaciones**
Alto	Certificados finales	SHA-256	RSA-2048	○ Las claves se encuentran en un QSCD (en los certificados de empleado público y sello) o en un HSM certificado (en los certificados de sede o de sello de autenticación)
Medio/sustancial	Certificados finales	SHA-256	RSA-1024	○ Se recomienda usar longitudes de clave RSA 2048 o superior.

[4] Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

A continuación se describen los campos que componen los cuatro certificados derivados de la LAECSP (certificado de sede electrónica, certificado de sello electrónico, certificado de empleado público y certificado de empleado público con seudónimo), dividiendo cada uno de ellos entre los niveles de aseguramiento en el que nos encontremos (medio/sustancial o alto). Dentro de cada perfil se ha dividido a su vez entre campos propios del certificado y sus extensiones.

También se propone, a modo de orientativo, un certificado de CA sub raíz tipo para poder ser utilizado por prestadores y Administraciones que deseen comenzar la emisión de los nuevos perfiles de certificados.

La actualización de estos algoritmos y longitudes mínimas estarán dictados por las directrices de seguridad del CCN y de la regulación europea sobre firma electrónica. Estas directrices contemplarán los periodos de migración y de transición.

7 Certificado de SubCA

A continuación se presentan los campos mínimos que deben estar recogidos en el certificado emisor de los certificados de Administración Pública. Esto no implica la necesidad de tener una única subCA para todos los tipos de certificados finales. La estructura de la PKI es decisión del PSC, siempre que el certificado de la subCA tenga la información necesaria para su correcta identificación y su localización en la TSL.

Campo	Contenido	R	Formato/Observaciones
1. X.509v1 Field			-
1.1. Version	2 (= v3)	Sí	Integer:=2 ([RFC5280] describe la versión del certificado al usar extensiones es decir v3 su valor debe ser 2)
1.2. Serial Number	Número identificativo único del certificado.	Sí	Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280] integer positivo, no mayor 20 octetos (1-2^{159}) Se recomienda un mínimo de 20 bits de entropía Se utilizará para identificar de manera unívoca el certificado
1.3. Signature Algorithm	SHA-2 con RSA Signature, longitud de clave de 4096 bits o superior.	Sí	String UTF8 (40). Identificando el tipo de algoritmo. Al tratarse de un certificado subraíz las restricciones son mayores que las de los demás certificados. P. ej: OID 2.16.840.1.101.3.4.2

Campo	Contenido	R	Formato/Observaciones
1.4. Issuer Distinguished Name	Información relativa al prestador	Sí	Todos los campos destinados a identificar/describir el prestador de servicios serán codificados en formato UTF8
1.4.1. Country (C)	País donde el prestador de servicios expide los certificados	Sí	C = p. ej: ES (PrintableString) Size [RFC 5280] 3
1.4.2. Organization (O)	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado).	R	O = p. ej: MINISTERIO DE LA PRESIDENCIA (String UTF8) Size [RFC 5280] 128
1.4.3. Locality (L)	Localidad/dirección del prestador de servicios de certificación		L = p. ej: MADRID (String UTF8) Size [RFC 5280] 128 Si bien el campo está estipulado para introducir la localidad, se contempla la posibilidad de incluir la dirección completa
1.4.4. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.	R	OU = p. ej: AUTORIDAD DE CERTIFICACION CERTICA (String UTF8) Size [RFC 5280] 128 Se contempla el nombre de la entidad que ha emitido el certificado
1.4.5. Serial Number	Número único de identificación de la entidad de certificación, aplicable de acuerdo con el país. En España, NIF.	*	NIF = NIF entidad de certificación, p. ej: S2833002 (Printable String) Size = 9
1.4.6. organizationIdentifier	Identificador de organización o persona jurídica normalizado	*	Identificador de la organización Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
1.4.7. Common Name (CN)	Nombre común de la organización prestadora de servicios de certificación (emisor del certificado)	R	CN = p. ej: CERTICA Root CA (String UTF8) Size 80 Size [RFC 5280] 80
1.5. Validity	12 años mínimo (recomendado)	Sí	Los datos de validez creados antes del 2050 se codificarán utilizando UTCTime. A partir del 2050 se utilizará la codificación GeneralizedTime en la cual se utilizan dos dígitos más para especificar el año (4 en lugar de 2)

Campo	Contenido	R	Formato/Observaciones
1.5.1. Not Before	Fecha de inicio de validez	Sí	Fecha de inicio de validez, formato: UTCTime YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de fin de validez	Sí	Fecha fin de validez, formato: UTCTime YYMMDDHHMMSSZ
1.6. Subject	Información relativa a la SubCA	Sí	Según la RFC5280 esta parte se ha de rellenar con carácter obligatorio Según la ETSI-QC se debe reflejar obligatoriamente el campo Country Ver RFC3739 / ETSI 101862
1.6.1. Country (C)	Estado cuya ley rige el CN del Subject	Sí	C = p. ej: ES (PrintableString) Size [RFC 5280] 3
1.6.2. Organization (O)	Denominación (nombre “oficial” de la organización) del prestador de servicios de certificación (emisor de los certificados finales).	Sí	O = p. ej: AUTORIDAD DE CERTIFICACION CERTICA (String UTF8) Size [RFC 5280] 128 Se contempla el nombre de la entidad que ha emitido el certificado
1.6.3. Locality (L)	Localidad/dirección del prestador de servicios de certificación (emisor de los certificados finales).		L = p. ej: MADRID (String UTF8) Size [RFC 5280] 128 Si bien el campo está estipulado para introducir la localidad, se contempla la posibilidad de incluir la dirección completa
1.6.4. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.	Sí	OU = p. ej: MINISTERIO DE LA PRESIDENCIA (String UTF8) Size [RFC 5280] 128
1.6.5. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF.	*	NIF = NIF entidad suscriptora p. ej: S2833002 (Printable String) Size = 9
1.6.6. Organization Identifier	Identificador de la organización Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)	*	OrganizationIdentifier p. ej: VATES-S2833002.
1.6.7. Common Name (CN)	Nombre común de la organización prestadora de servicios de certificación (suscriptor del certificado).	Sí	CN = p. ej: CERTICA Root subCA (String UTF8) Size 80 Size [RFC 5280] 80

Campo	Contenido	R	Formato/Observaciones
1.7. Subject Public Key Info	Clave pública del prestador, codificada de acuerdo con el algoritmo criptográfico.	Sí	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. (String UTF8)

(*) Se deberá incluir al menos uno de los campos SerialNumber u OrganizationIdentifier

NOTA: Se recomienda incluir todos los campos marcados como 'R' (recomendado).
Es obligatorio incluir al menos uno de los campos indicados con 'R'.

7.1.1 Extensiones del certificado

Campo	Contenido	R	Formato/Observaciones
2. X.509v3 Extensions			-
2.1. Authority Key Identifier	Presente, de acuerdo con RFC 5280.	Sí	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	Path de identificación de certificación		Identificador de la clave pública del emisor (String UTF8)
2.1.2. AuthorityCertIssuer			Nombre de la CA a la que corresponde la clave identificada en keyIdentifier (String UTF8) Size 80
2.1.3. AuthorityCertSerial Number			Número de serie del certificado de CA SerialNumber = p. ej: 11112222 (Integer)
2.2. Subject Key Identifier	Presente, de acuerdo con RFC 5280.	Sí	Identificador de la clave pública del suscriptor o poseedor de claves (derivada de utilizar la función de Hash sobre la clave pública del sujeto). Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.
2.3. Key Usage		Sí	Campo crítico para determinar el uso (dependiente del certificado)
2.3.1. Digital Signature	No seleccionado "0"/"1"		En general =0. Solo =1 en caso de que se use para firmar las respuestas OCSP
2.3.2. Content Commitment	No seleccionado "0"		Se utiliza para realizar firma electrónica

Campo	Contenido	R	Formato/Observaciones
2.3.3. Key Encipherment	No seleccionado “0”		Se utiliza para gestión y transporte de claves
2.3.4. Data Encipherment	No seleccionado “0”		Se utiliza para cifrar datos que no sean claves criptográficas
2.3.5. Key Agreement	No seleccionado “0”		Se usa en el proceso de acuerdo de claves
2.3.6. Key Certificate Signature	Seleccionado “1”	Sí	Se usa para firmar certificados. Se utiliza en los certificados de autoridades de certificación
2.3.7. CRL Signature	Seleccionado “1”	Sí	Se usa para firmar listas de revocación de certificados
2.4. Certificate Policies	Políticas de certificación/DPC	Sí	
2.4.1. Policy Identifier	OID asociado a la DPC o PC	Sí	Ej: OID Private enterprise: 1.3.6.1.4.1.<num prest>.1.3.1, u OID Country assignment (2.16...) / Any Policy
2.4.2. Policy Qualifier ID	Especificación de la DPC	Sí	
2.4.2.1. CPS Pointer	URL de la DPC o, en su caso, documento legal de tercero.	Sí	URL de las condiciones de uso, p. ej: www.mpr.es/certica/emision/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).
2.4.2.2. User Notice	Ej: "Certificado raíz. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero		Campo explicitText. Se recomienda que siempre se referencie a través de un link. Se recomienda longitud no superior a 200 caracteres.
2.5. Subject Alternate Names	Nombre alternativo de la persona de contacto de la entidad suscriptora		
2.5.1. rfc822Name	Correo electrónico de contacto de la entidad suscriptora		Correo electrónico de contacto en la entidad suscriptora, p. ej: soporte.certica@mpr.es (String) Size [RFC 5280] 255

Campo	Contenido	R	Formato/Observaciones
2.6. Issuer Alternative Name	Nombre alternativo de la persona de contacto de la entidad de Certificación emisora		
2.6.1.rfc822Name	Correo electrónico de contacto de la entidad de certificación emisora.		Correo electrónico de contacto en la entidad de certificación emisora, p. ej: soporte.certica@mrp.es (String) Size [RFC 5280] 255
2.7. cRLDistributionPoint		Sí	Indica cómo se obtiene la información de CRL.
2.7.1.distributionPoint	Punto de distribución de la CRL, número 1	Sí	Web donde resida la CRL (punto de distribución 1-http/https o LDAP con servidor autenticado). (String UTF8)
2.7.2.distributionPoint	Punto de distribución de la CRL, número 2		Web donde resida la CRL (punto de distribución 2- http/https o LDAP con servidor autenticado). (String UTF8)
2.8. Authority Info Access		Sí	
2.8.1.Access Method	Id-ad-ocsp	Sí	ID de On-line Certificate Status Protocol
2.8.2.Access Location	(dirección web)	Sí	URL de On-line Certificate Status Protocol. Especifica el emplazamiento de la información (String UTF8)
2.8.3.Access Method	Id-ad-caIssuers	Sí	ID de localización del certificado de la CA
2.8.4.Access Location	(dirección web)	Sí	URL de localización del certificado de la CA. Especifica el emplazamiento de la información (String UTF8)
2.9. Basic Constraints			
2.9.1.Subject type	CA	Sí	Indicador para reconocer que se trata de un certificado raíz
2.9.2.Path Length Constraints	Ninguno		[RFC 5280] Puede especificarse un número máximo de niveles,
2.9.3.			

8 Certificado de sede electrónica administrativa

El prestador deberá asegurar la unicidad de los DN (Distinguished Names) de los certificados de sede electrónica administrativa.
Los certificados de sede electrónica deberán ser acordes a la normativa europea, en concreto al Anexo IV del Reglamento UE 910/2014 que especifica los requisitos para los certificados cualificados de autenticación de sitios web, y su normativa de desarrollo.

Se recomienda que el Prestador de Servicios de Certificación asigne Policy Identifier con OIDs diferentes para cada tipo de certificado.

Se deberán tener en cuenta las recomendaciones de la industria, en concreto las guías publicadas por el CA/Browser Forum, en especial para los certificados de validación extendida (EV).

8.1 Campos comunes a los dos niveles

Campo	Contenido	R	Formato/Observaciones
1. X.509v1 Field			-
1.1. Version	2 (= v3)	Sí	Integer:=2 ([RFC5280] describe la versión del certificado al usar extensiones es decir v3 su valor debe ser 2)
1.2. Serial Number	Número identificativo único del certificado.	Sí	Integer. SerialNumber = p. ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280] integer positivo, no mayor 20 octetos ($1- 2^{159}$) Se recomienda que tenga al menos 20 bits de entropía Se utilizará para identificar de manera unívoca el certificado
1.3. Issuer Distinguished Name	Información relativa al prestador	Sí	Todos los campos destinados a identificar/describir el prestador de servicios serán codificados en formato UTF8
1.3.1. Country (C)	País donde el prestador de servicios expide los certificados	Sí	C = p. ej: ES (PrintableString) Size [RFC 5280] 3
1.3.2. Organization (O)	Denominación (nombre “oficial” de la organización) del prestador de servicios de	Sí	O = p. ej: MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD (String UTF8) Size [RFC 5280] 128

Campo	Contenido	R	Formato/Observaciones
	certificación (emisor del certificado).		
1.3.3. Locality (L)	Localidad/dirección del prestador de servicios de certificación		L = p. ej: MADRID (String UTF8) Size [RFC 5202] 128 Si bien el campo está estipulado para introducir la localidad, se contempla la posibilidad de incluir la dirección completa
1.3.4. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.	Sí	OU = p. ej: AUTORIDAD DE CERTIFICACION CERTICA (String UTF8) Size [RFC 5280] 128 Se contempla el nombre de la entidad que ha emitido el certificado
1.3.5. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF.	*	NIF = NIF entidad suscriptora, p. ej: S2833002 (Printable String) Size = 9
1.3.6. Organization Identifier	Identificador de la organización Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)	*	OrganizationIdentifier p. ej: VATES-S2833002.
1.3.7. Common Name (CN)	Nombre común de la organización prestadora de servicios de certificación (emisor del certificado)	Sí	CN = p. ej: CERTICA Root subCA (String UTF8) Size 80 Size [RFC 5280] 80
1.4. Validity	27 meses (recomendado) Para estar acordes a las guías CAB Forum para validación extendida (9.4. Maximum Validity Period For EV Certificate)	Sí	Los datos de validez creados antes del 2050 se codificarán utilizando UTCTime. A partir del 2050 se utilizará la codificación GeneralizedTime en la cual se utilizan dos dígitos más para especificar el año (4 en lugar de 2)
1.4.1. Not Before	Fecha de inicio de validez	Sí	Fecha de inicio de validez, formato: UTCTime YYMMDDHHMMSSZ
1.4.2. Not After	Fecha de fin de validez	Sí	Fecha fin de validez, formato: UTCTime YYMMDDHHMMSSZ
1.5. Subject	Todos los campos serán codificados utilizando	Sí	Según la RFC5280 esta parte se ha de

Campo	Contenido	R	Formato/Observaciones
	UTF-8		rellenar con carácter obligatorio Según la ETSI-QC se debe reflejar obligatoriamente el campo Country Ver RFC3739 / ETSI 101862
1.5.1. Country (C)	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas.	Sí	C = p. ej: ES (PrintableString) Se codificará de acuerdo a “ISO 3166-1-alpha-2 code elements” Size [RFC 5280] 3
1.5.2. Locality	Ciudad	Si	L = p. ej : MURCIA (String UTF8) Size [RFC 5280] 128
1.5.3. Organization (O)	Denominación (nombre “oficial” de la organización) del suscriptor de servicios de certificación (custodio del certificado)	Sí	O = p. ej: MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD (String UTF8) Size [RFC 5280] 128
1.5.4. Organizational Unit (OU)	Descripción del tipo de certificado	Sí	OU= “SEDE ELECTRONICA” (String UTF8) Size [RFC 5280] 128
1.5.5. Organizational Unit (OU)	El nombre descriptivo de la sede.	Sí	OU= p. ej: PUNTO DE ACCESO GENERAL
1.5.6. Serial Number	El NIF de la entidad responsable.	Si	SerialNumber = p. ej: S2833002. Número secuencial único asignado por el prestador (Printable String)) Size [RFC 5280] 64
1.5.7. OrganizationIdentifier	Identificador de la organización Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)	Si	OrganizationIdentifier p. ej: VATES-S2833002.
1.5.8. businessCategory	Categoría de organización (requerido para certificados EV)		businessCategory = “Government Entity”
1.5.9. jurisdictionCountryName	Jurisdicción (requerido para certificados EV)		jurisdictionCountryName= “ES”
1.5.10. Common Name (CN)	Denominación de nombre de dominio (DNS) donde residirá el certificado.		CN= p. ej: administracion.gob.es . Denominación de nombre de dominio

Campo	Contenido	R	Formato/Observaciones
	Debe coincidir con el que se encuentra en la extensión Subject Alternative Names		o IP. Conforme al estándar X.500, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades. (String UTF8)) Size [RFC 5280] 80
1.6. Subject Public Key Info	Clave pública de la sede, codificada de acuerdo con el algoritmo criptográfico.	Sí	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. (String UTF8)

(*) Se deberá incluir al menos uno de los campos SerialNumber u OrganizationIdentifier

8.1.1 Extensiones del certificado

Campo	Contenido	R	Formato/Observaciones
2. X.509v3 Extensions			-
2.1. Authority Key Identifier	Presente, de acuerdo con RFC 5280.	Sí	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	Path de identificación de certificación		Identificador de la clave pública del emisor (String UTF8)
2.1.2. AuthorityCertIssuer			Nombre de la CA a la que corresponde la clave identificada en keyIdentifier (String UTF8) Size 80
2.1.3. AuthorityCertSerialNumber			Número de serie del certificado de CA (Integer)
2.2. Subject Key Identifier	Presente, de acuerdo con RFC 5280.	Sí	Identificador de la clave pública del suscriptor o poseedor de claves (derivada de utilizar la función de Hash sobre la clave pública del sujeto). Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.
2.3. Key Usage		Sí	Campo crítico para determinar el uso (dependiente del certificado)
2.3.1. Digital Signature	Seleccionado “1”	Sí	Se utiliza cuando se realiza la función de autenticación
2.3.2. Content Commitment	No seleccionado “0”		Se utiliza cuando se realiza la función de firma electrónica

Campo	Contenido	R	Formato/Observaciones
2.3.3. Key Encipherment	Seleccionado “1”	Sí	Se utiliza para gestión y transporte de claves
2.3.4. Data Encipherment	No seleccionado “0”		Se utiliza para cifrar datos que no sean claves criptográficas
2.3.5. Key Agreement	No seleccionado “0”		Se usa en el proceso de acuerdo de claves
2.3.6. Key Certificate Signature	No seleccionado “0”		Se usa para firmar certificados. Se utiliza en los certificados de autoridades de certificación
2.3.7. CRL Signature	No seleccionado “0”		Se usa para firmar listas de revocación de certificados
2.4. Issuer Alternative Name	Nombre alternativo de la persona de contacto de la Entidad de Certificación emisora		
2.4.1. rfc822Name	Correo electrónico de contacto de la Entidad de Certificación emisora		Correo electrónico de la persona de contacto de la entidad de certificación emisora. P. ej: soporte.certica@mpr.es (String) Size [RFC 5280] 255
2.5. cRLDistributionPoint		Sí	Indica cómo se obtiene la información de CRL.
2.5.1. distributionPoint	Punto de distribución de la CRL, número 1	Sí	Web donde resida la CRL (punto de distribución 1- http. (String UTF8)
2.5.2. distributionPoint	Punto de distribución de la CRL, número 2		Web donde resida la CRL (punto de distribución 2-http/https o LDAP con servidor autenticado). (String UTF8)
2.6. Authority Info Access		Sí	
2.6.1. Access Method	Id-ad-ocsp	Sí	ID de On-line Certificate Status Protocol
2.6.2. Access Location	(dirección web)	Sí	URL de On-line Certificate Status Protocol. Especifica el emplazamiento de la información (String UTF8)
2.6.3. Access Method	Id-ad-caIssuers	Sí	ID de localización del certificado de la subCA

Campo	Contenido	R	Formato/Observaciones
2.6.4. Access Location	(dirección web)	Sí	URL de localización del certificado de la CA. Especifica el emplazamiento de la información (String UTF8)

A continuación se describen los campos diferenciados para los niveles alto y medio/sustancial debido a su contenido o sus OIDs de “Identidad administrativa”:

8.2 Nivel Alto

8.2.1 Certificado:

Campo	Contenido	R	Formato/Observaciones
1. X.509v1 Field			-
1.1. Signature Algorithm	SHA-2 con RSA Signature y longitud de clave de 2048 bits	Sí	String UTF8 (40). Identificando el tipo de algoritmo, (más laxo que el del certificado raíz), y longitud de 2048 por tratarse de un certificado de nivel alto. OID 2.16.840.1.101.3.4.2.1

8.2.2 Extensiones del certificado

Campo	Contenido	R	Formato/Observaciones
2.1. Extended Key Usage		Sí	Uso extendido del certificado
2.1.1. Server Authentication	Autenticación TSL web Server	Sí	
2.2. Qualified Certificate Statements		Sí	
2.2.1. QcCompliance	Indicación de certificado cualificado	Sí	OID 0.4.0.1862.1.1
2.2.2. QcEuRetention Period	15 años	Sí	Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
2.2.3. semanticsId-Legal	Para indicar semántica de persona jurídica definida por la EN 319 412-1		0.4.0.194121.1.2

Campo	Contenido	R	Formato/Observaciones
2.2.4. QcType- web	Certificado de autenticación de web	Si	OID 0.4.0.1862.1.6.3
2.2.5. QcPDS	Lugar donde se encuentra la declaración PDS	SI	OID 0.4.0.1862.1.5
2.3. Certificate Policies	Políticas de certificación/DPC	Sí	
2.3.1. Policy Identifier	OID asociado a los certificados de sede de nivel alto	Sí	2.16.724.1.3.5.5.1
2.3.2. Policy Identifier	QCP-w		Certificado cualificado de sitio web acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web (4)
2.3.3. Policy Identifier	OID de SSL EV		0.4.0.2042.1.4
2.3.4. Policy Identifier	OID asociado a la DPC o PC	Sí	OID Private enterprise: p. ej: 1.3.6.1.4.1.<num prest>.1.3.2.1, u OID Country assignment (2.16…)
2.3.5. Policy Qualifier ID	Especificación de la DPC	Sí	
2.3.5.1. CPS Pointer	URL de la DPC o, en su caso, documento legal de tercero.	Sí	URL de las condiciones de uso, p. ej: www.minhap.es/certi41/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).
2.3.5.2. User Notice	P. ej: "Certificado cualificado de sede electrónica, nivel alto. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero	Sí	Campo explicitText. Se recomienda que siempre se referencie a través de un link. Se recomienda longitud no superior a 200 caracteres.
2.4. Subject Alternative Names	Nombre alternativo de la sede electrónica	Sí	
2.4.1. dnsName	Nombre de Dominio DNS de la Sede		Nombre Dominio DNS de la Sede, p. ej: “ administracion.gob.es” (String UTF8) Size = 128 Puede contener varios dominios.

8.3 Nivel Medio / Sustancial

8.3.1 Certificado:

Campo	Contenido	R	Formato/Observaciones
1. X.509v1 Field			-
1.1. Signature Algorithm	SHA-2 con RSA Signature y longitud de clave de al menos 2048 bits	Sí	String UTF8 (40). Identificando el tipo de algoritmo, (más laxo que el del certificado de nivel alto), y longitud de al menos 2048 bits. OID 2.16.840.1.101.3.4.2.1

8.3.2 Extensiones del certificado

Campo	Contenido	R	Observaciones
2.1. Extended Key Usage		Sí	Uso extendido del certificado
2.1.1. Server Authentication	Autenticación TSL web Server	Sí	
2.2. Qualified Certificate Statements		Sí	
2.2.1. QcCompliance	Indicación de certificado cualificado	Sí	OID 0.4.0.1862.1.1
2.2.2. semnaticsId-Legal	Para indicar semántica de persona jurídica definida por la EN 319 412-1		0.4.0.194121.1.2
2.2.3. QcEuRetentionPeriod	15 años	Sí	Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
2.2.4. QcType- web	Certificado de autenticación de web	Si	OID 0.4.0.1862.1.6.3
2.2.5. QcPDS	Lugar donde se encuentra la declaración PDS	SI	OID 0.4.0.1862.1.5

Campo	Contenido	R	Observaciones
2.3. Certificate Policies	Políticas de certificación/DPC	Sí	
2.3.1. Policy Identifier	OID asociado a los certificados de sede de nivel medio/sustancial	Sí	2.16.724.1.3.5.5.2
2.3.2. Policy Identifier	QCP-w	Si	Certificado cualificado de sitio web acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web (4)
2.3.3. Policy Identifier	OID asociado a la DPC o PC	Sí	OID Private enterprise: p. ej: 1.3.6.1.4.1.<num prest>.1.3.2.2, u OID Country assignment (2.16...)
2.3.4. Policy Qualifier ID	Especificación de la DPC	Sí	
2.3.4.1. CPS Pointer	URL de la DPC o, en su caso, documento legal de tercero.	Sí	URL de las condiciones de uso, p. ej: www.minhap.es/certica/emision/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).
2.3.4.2. User Notice	Ej: "Certificado cualificado de sede electrónica, nivel medio/sustancial. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero	Sí	Campo explicitText. Se recomienda que siempre se referencie a través de un link. Se recomienda longitud no superior a 200 caracteres.
2.4. Subject Alternate Names		Sí	Lugar donde se contemplarán los valores establecidos para la Identidad Administrativa
2.4.1. dnsName	Nombre de Dominio DNS de la Sede		Nombre Dominio DNS de la Sede, p. ej: “ administracion.gob.es” (String UTF8) Size = 128 Puede contener varios dominios. Puede contener un wildcard (*.administracino.gob.es) si no es EV

9 Certificado de sello electrónico

El prestador deberá asegurar la unicidad de los DN (Distinguished Names) de los certificados de sello electrónico para la actuación automatizada.

Indicar que, por motivos de compatibilidad, es posible la inclusión en el Common Name del Subject ciertos atributos que pudieran ser necesarios para el tratamiento, como es el caso del nombre de la entidad suscriptora o responsable del sello, y su NIF.

Los certificados de sello electrónico deberán ser acordes a la normativa europea, en concreto al Anexo III del Reglamento UE 910/2014 que especifica los requisitos para los certificados cualificados de sello electrónico, y su normativa de desarrollo.

Se recomienda que el Prestador de Servicios de Certificación asigne Policy Identifier con OIDs diferentes para cada tipo de certificado.

9.1 Campos comunes a los dos niveles

Campo	Contenido	R	Observaciones
1. X.509v1 Field			-
1.1. Version	2 (= v3)	Sí	Integer:=2 ([RFC5280] describe la versión del certificado al usar extensiones es decir v3 su valor debe ser 2)
1.2. Serial Number	Número identificativo único del certificado.	Sí	Integer. SerialNumber = p. ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280] integer positivo, no mayor 20 octetos ($1- 2^{159}$) Se utilizará para identificar de manera unívoca el certificado
1.3. Issuer Distinguished Name		Sí	Todos los campos destinados a identificar/describir el prestador de servicios serán codificados en formato UTF8
1.3.1. Country (C)	ES	Sí	C = p. ej: ES (PrintableString) Size [RFC 5280] 3
1.3.2. Organization (O)	Denominación (nombre “oficial” de la organización) del prestador de servicios de certificación (emisor del certificado).	Sí	O = p. ej: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS (String UTF8) Size [RFC 5280] 128

Campo	Contenido	R	Observaciones
1.3.3. Locality (L)	Localidad/dirección del prestador de servicios de certificación		L = p. ej: MADRID (String UTF8) Size [RFC 5280] 128 Si bien el campo está estipulado para introducir la localidad, se contempla la posibilidad de incluir la dirección completa
1.3.4. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.	Sí	OU = p. ej: AUTORIDAD DE CERTIFICACION CERTICA (String UTF8) Size [RFC 5280] 128 Se contempla el nombre de la entidad que ha emitido el certificado
1.3.5. Organization Identifier	Identificador de la organización Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)	*	OrganizationIdentifier p. ej: VATES-S2833002.
1.3.6. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF.	*	NIF = NIF entidad ej: S2833002 (Printable String) Size = 9
1.3.7. Common Name (CN)	Nombre común de la organización prestadora de servicios de certificación (emisor del certificado)	Sí	CN = p. ej: CERTICA Root subCA (String UTF8) Size 80 Size [RFC 5280] 80
1.4. Validity	5 años (recomendado)	Sí	Los datos de validez creados antes del 2050 se codificarán utilizando UTCTime. A partir del 2050 se utilizará la codificación GeneralizedTime en la cual se utilizan dos dígitos más para especificar el año (4 en lugar de 2)
1.4.1. Not Before	Fecha de inicio de validez	Sí	Fecha de inicio de validez, formato: UTCTime YYMMDDHHMMSSZ
1.4.2. Not After	Fecha de fin de validez	Sí	Fecha fin de validez, formato: UTCTime YYMMDDHHMMSSZ
1.5. Subject	Todos los campos destinados a identificar/describir el creador del sello serán codificados utilizando UTF-8	Sí	Según la RFC5280 esta parte se ha de rellenar con carácter obligatorio Según la ETSI-QC se debe reflejar obligatoriamente el campo Country Ver RFC3739 / ETSI 101862

Campo	Contenido	R	Observaciones
1.5.1. Country (C)	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas.	Sí	C = p. ej: ES (PrintableString) Size [RFC 5280] 3
1.5.2. Organization (O)	Denominación (nombre “oficial” de la organización) del creador del sello.	Sí	O = p. ej: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS (String UTF8) Size [RFC 5280] 128
1.5.3. Organizational Unit (OU)	Indica la naturaleza del certificado	Sí	OU = SELLO ELECTRONICO (String UTF8) Size [RFC 5280] 128
1.5.4. Organizational Unit (OU)	Denominación oficial de la unidad		OU = p. ej: SUBDIRECCION DE EXPLOTACION
1.5.5. Organizational Unit (OU)	Código DIR3 de la unidad		OU = p. ej: E04976701
1.5.6. Organization Identifier	Identificador de la organización distinto del nombre Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)	Si	OrganizationIdentifier p. ej: VATES-S2833002.
1.5.7. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con la legislación del país. En España, NIF.		SerialNumber = p. ej: S2833002. Número secuencial único asignado por el prestador (Printable String)) Size [RFC 5280] 64
1.5.8. 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).		Primer apellido, espacio en blanco, segundo apellido del responsable del certificado (titular del órgano) de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 80 p. ej: “DE LA CAMARA ESPAÑOL - DNI 00000000G”
1.5.9. Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)		Nombre de pila del responsable del certificado (titular del órgano) de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 p. ej: “JUAN ANTONIO”

Campo	Contenido	R	Observaciones
1.5.10. Common Name (CN)	Denominación de sistema o aplicación de proceso automático.		CN= p. ej: “PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA. Nombre descriptivo del sistema automático. Asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades. (String UTF8)) Size [RFC 5280] 80
1.6. Subject Public Key Info	Clave pública del sello, codificada de acuerdo con el algoritmo criptográfico.	Sí	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. (String UTF8)

(*) Se deberá incluir al menos uno de los campos SerialNumber u OrganizationIdentifier

9.1.1 Extensiones del certificado

Campo	Contenido	R	Observaciones
2. X.509v3 Extensions			-
2.1. Authority Key Identifier	Presente, de acuerdo con RFC 5280.	Sí	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		(String UTF8)
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier		(String UTF8) Size 80
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA		Número de serie del certificado de CA (Integer)
2.2. Subject Key Identifier	Presente, de acuerdo con RFC 5280.	Sí	Identificador de la clave pública del suscriptor o poseedor de claves (derivada de utilizar la función de Hash sobre la clave pública del sujeto). Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.
2.3. Key Usage		Sí	Campo crítico para determinar el uso (dependiente del certificado)

Campo	Contenido	R	Observaciones
2.3.1. Digital Signature	Seleccionado “1”	Sí	Se utiliza cuando se realiza la función de autenticación de activo digital de la persona jurídica
2.3.2. Content Commitment	Seleccionado “1”	Sí	Se utiliza cuando se realiza la función de sello electrónico de documento expedido por persona jurídica
2.3.3. Key Encipherment	Seleccionado “1”	Sí	Se utiliza para gestión y transporte de claves
2.3.4. Data Encipherment	No seleccionado ”0”		Se utiliza para cifrar datos que no sean claves criptográficas
2.3.5. Key Agreement	Seleccionado “1”/No seleccionado “0”	Si	Se usa en el proceso de acuerdo de claves
2.3.6. Key Certificate Signature	No seleccionado “0”		Se usa para firmar certificados. Se utiliza en los certificados de autoridades de certificación
2.3.7. CRL Signature	No seleccionado “0”		Se usa para firmar listas de revocación de certificados
2.4. Extended Key Usage			Uso extendido del certificado
2.4.1. Email Protection	Seleccionado		Protección de mail
2.4.2. Client Authentication	Seleccionado		Autenticación cliente
2.4.3. Server Authentication	Seleccionado		Autenticación de servidor
2.4.4. codeSigning	Seleccionado		Firma de código
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		Correo electrónico de contacto de la entidad de certificación emisora p. ej: soporte.certica@minhap.es (String) Size [RFC 5280] 255
2.6. cRLDistributionPoint		Sí	Indica cómo se obtiene la información de CRL.

Campo	Contenido	R	Observaciones
2.6.1. distributionPoint	Punto de distribución de la CRL, número 1	Sí	Web donde resida la CRL (punto de distribución 1 – http. (String UTF8)
2.6.2. distributionPoint	Punto de distribución de la CRL, número 2		Web donde resida la CRL (punto de distribución 2 – http/https o LDAP con servidor autenticado). (String UTF8)
2.7. Authority Info Access		Sí	
2.7.1. Access Method	Id-ad-ocsp	Sí	ID de On-line Certificate Status Protocol
2.7.2. Access Location	(dirección web)	Sí	URL de On-line Certificate Status Protocol. Especifica el emplazamiento de la información (String UTF8)
2.7.3. Access Method	Id-ad-caIssuers	Sí	ID de localización del certificado de la CA
2.7.4. Access Location	(dirección web)	Sí	URL de localización del certificado de la CA. Especifica el emplazamiento de la información (String UTF8)

A continuación se describen los campos diferenciados para los niveles alto y medio/sustancial debido a su contenido o sus OIDs de “Identidad administrativa”:

9.2 Nivel Alto

9.2.1 Certificado

Campo	Contenido	R	Observaciones
1. X.509v1 Field			-
1.1. Signature Algorithm	SHA-2 con RSA Signature y longitud de clave de 2048 bits	Sí	String UTF8 (40). Identificando el tipo de algoritmo, (más laxo que el del certificado raíz), y longitud de 2048 por tratarse de un certificado de nivel alto. OID 2.16.840.1.101.3.4.2.1

9.2.2 Extensiones del certificado

Campo	Contenido	R	Observaciones
2.1. Qualified Certificate Statements		Sí	
2.1.1. QcCompliance	Indicación de certificado cualificado	Sí	OID 0.4.0.1862.1.1
2.1.2. QcEuRetentionPeriod	15 años	Sí	Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
2.1.3. QcSSCD	Uso de dispositivo seguro de firma	Si	OID 0.4.0.1862.1.4
2.1.4. QcType- eseal	Certificado de sello	Si	OID 0.4.0.1862.1.6.2
2.1.5. QcPDS	Lugar donde se encuentra la declaración PDS	SI	OID 0.4.0.1862.1.5
2.1.6. semnaticsId-Legal	Para indicar semántica de persona jurídica definida por la EN 319 412-1		0.4.0.194121.1.2
2.2. Certificate Policies	Políticas de certificación/DPC	Sí	
2.2.1. Policy Identifier	Certificado de sello de nivel alto	Sí	2.16.724.1.3.5.6.1
2.2.2. Policy Identifier	QCP-l-qscd	Si	Certificado cualificado de sello, almacenado en dispositivo seguro acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3)
2.2.3. Policy Identifier	OID asociado a la DPC o PC	Sí	OID Private enterprise: ej: 1.3.6.1.4.1.<num prest>.1.3.3.1, u OID Country assignment (2.16...)
2.2.4. Policy Qualifier ID	Especificación de la DPC	Sí	

Campo	Contenido	R	Observaciones
2.2.4.1. CPS Pointer	URL de la DPC o, en su caso, documento legal de tercero.	Sí	URL de las condiciones de uso ej: www.minhap.es/certica/emision/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).
2.2.4.2. User Notice	Ej: "Certificado cualificado de sello electrónico de Administración, órgano o entidad de derecho público, nivel alto. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero	Sí	Campo explicitText. Se recomienda que siempre se referencie a través de un link. Se recomienda longitud no superior a 200 caracteres.
2.3. Subject Alternate Names		Sí	Lugar donde se contemplarán los valores establecidos para la Identidad Administrativa
2.3.1. rfc822Name	Correo electrónico de contacto de la entidad suscriptora del sello electrónico		Correo electrónico de contacto de la entidad suscriptora del sello. P. ej: soporte.afirma5@minhap.es (String) Size [RFC 5280] 255
2.3.2. Directory Name	Identidad administrativa	Sí	Campos específicos definidos por la Administración para los certificados RD 1671/2009. (Sequence)
2.3.2.1. Tipo de certificado	Indica la naturaleza del certificado	Sí	Tipo= SELLO ELECTRONICO DE NIVEL ALTO (String UTF8) Size = 31 2.16.724.1.3.5.6.1.*1*
2.3.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	Sí	Entidad Suscriptora = p. ej: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS (String UTF8) Size = 80 OID: 2.16.724.1.3.5.6.1.*2*
2.3.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	Sí	NIF suscriptora = NIF entidad suscriptora, p. ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.6.1.3
2.3.2.4. DNI/NIE del responsable (titular del órgano)	DNI o NIE del responsable del Sello	O	DNI/NIE responsable= p. ej: 00000000G (String UTF8) Size = 9 OID: 2.16.724.1.3.5.6.1.4

Campo	Contenido	R	Observaciones
2.3.2.5. Denominación de sistema o componente	Breve descripción de la componente que posee el certificado de sello	O	Nombre descriptivo del sistema de sellado automático, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades. Denominación sistema = p. ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA". (String UTF8) Size = 128 OID: 2.16.724.1.3.5.6.1.5
2.3.2.6. Nombre de pila (titular del órgano)	Nombre de pila del responsable del certificado	O	N = Nombre de pila del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.6.1.6 Ej: "JUAN ANTONIO"
2.3.2.7. Primer apellido (titular del órgano)	Primer apellido del responsable del certificado	O	SN1 = Primer apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.6.1.7 Ej: "DE LA CAMARA"
2.3.2.8. Segundo apellido (titular del órgano)	Segundo apellido del responsable del certificado	O	SN2 = Segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter). OID: 2.16.724.1.3.5.6.1.8 Ej: "ESPAÑOL"
2.3.2.9. Correo electrónico	Correo electrónico de la persona responsable del sello	O	Correo electrónico de la persona responsable del sello, p. ej: juanantonio.delacamara.espanol@mpr.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.6.1.9

9.3 Nivel Medio/Sustancial

9.3.1 Certificado

Campo	Contenido	R	Observaciones
2. X.509v1 Field			-
2.1. Signature Algorithm	SHA-2 con RSA Signature y longitud de clave de al menos 2048 bits	Sí	String UTF8 (40). Identificando el tipo de algoritmo, (más laxo que el del certificado de nivel alto), y longitud de al menos 2048 bits. OID 2.16.840.1.101.3.4.2.1

9.3.2 Extensiones del certificado

Campo	Contenido	R	Observaciones
2.1. Qualified Certificate Statements		Sí	
2.1.1. QcCompliance	Indicación de certificado cualificado	Sí	OID 0.4.0.1862.1.1
2.1.2. QcEuRetention Period	15 años	Sí	Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
2.1.3. QcType- eseal	Certificado de sello	Si	OID 0.4.0.1862.1.6.2
2.1.4. QcPDS	Lugar donde se encuentra la declaración PDS	SI	OID 0.4.0.1862.1.5
2.1.5. semnaticsId-Legal	Para indicar semántica de persona jurídica definida por la EN 319 412-1		0.4.0.194121.1.2
2.2. Certificate Policies	Políticas de certificación/DPC	Sí	
2.2.1. Policy Identifier	OID asociado a la DPC o PC	Sí	OID Private enterprise: p. ej: 1.3.6.1.4.1.<num prest>.1.4.3.1 u OID Country assignment (2.16...)
2.2.2. Policy Qualifier ID	Especificación de la DPC	Sí	

Campo	Contenido	R	Observaciones
2.2.2.1. CPS Pointer	URL de la DPC o, en su caso, documento legal de tercero.	Sí	URL de las condiciones de uso, p. ej: www.minhap.es/certica/emision/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).
2.2.2.2. User Notice	Ej: "Certificado cualificado de sello electrónico de Administración, órgano o entidad de derecho público, nivel Medio/Sustancial. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero	Sí	Campo explicitText. Se recomienda que siempre se referencie a través de un link. Se recomienda longitud no superior a 200 caracteres.
2.2.3. Policy Identifier	QCP-l	Si	Certificado cualificado de sello, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal (1)
2.2.4. Policy Identifier	OID asociado a certificado de sello de nivel medio	Sí	2.16.724.1.3.5.6.2
2.3. Subject Alternate Names		Sí	Lugar donde se contemplarán los valores establecidos para la Identidad Administrativa
2.3.1. rfc822Name	Correo electrónico de contacto de la entidad suscriptora del sello electrónico		Correo electrónico de contacto de la entidad suscriptora del sello, p. ej: soporte.afirma5@minhap.es (String) Size [RFC 5280] 255
2.3.2. Directory Name	Identidad administrativa	Sí	Campos específicos definidos por la Administración para los certificados Ley 11/2007. (Sequence)
2.3.2.1. Tipo de certificado	Indica la naturaleza del certificado	Sí	Tipo= SELLO ELECTRONICO DE NIVEL MEDIO (String UTF8) Size = 31 OID: 2.16.724.1.3.5.6.2.1
2.3.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	Sí	Entidad Suscriptora = p. ej: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS (String UTF8) Size = 80 OID: 2.16.724.1.3.5.6.2.2

Campo	Contenido	R	Observaciones
2.3.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	Sí	NIF suscriptora = NIF entidad suscriptora, p. ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.6.2.3
2.3.2.4. DNI/NIE del responsable (opcional)	DNI o NIE del responsable (titular del órgano) del Sello	O	DNI/NIE responsable= p. ej: 00000000G (String UTF8) Size = 9 OID: 2.16.724.1.3.5.6.2.4
2.3.2.5. Denominación de sistema o componente	Breve descripción de la componente que posee el certificado de sello	O	Nombre descriptivo del sistema de sellado automático, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades. Denominación sistema = p. ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA". (String UTF8) Size = 128 OID: 2.16.724.1.3.5.6.2.5
2.3.2.6. Nombre de pila	Nombre de pila del responsable (titular del órgano) del certificado	O	N = Nombre de pila del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.6.2.6 Ej: "JUAN ANTONIO"
2.3.2.7. Primer apellido	Primer apellido del responsable (titular del órgano) del certificado	O	SN1 = Primer apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.6.2.7 Ej: "DE LA CAMARA"
2.3.2.8. Segundo apellido	Segundo apellido del responsable (titular del órgano) del certificado	O	SN2 = Segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter). OID: 2.16.724.1.3.5.6.2.8 Ej: "ESPAÑOL"
2.3.2.9. Correo electrónico	Correo electrónico de la persona responsable (titular del órgano) del sello	O	Correo electrónico de la persona responsable del sello, p. ej: juanantonio.delacamara.espanol@minhap.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.6.2.9

10 Certificado de empleado público

Los certificados de firma electrónica y autenticación deberán ser acordes a la normativa europea, en concreto al Anexo I del Reglamento UE 910/2014 que especifica los requisitos para los certificados cualificados de persona física, y su normativa de desarrollo. Los dispositivos calificados de creación de firma deberán alinearse con el Anexo II del citado Reglamento.

El Prestador de Servicios de Certificación deberá asignar Policy Identifier con OIDs diferentes para cada tipo de certificado. Especialmente deberá asignar OID distintos para los certificados de firma, identificación y cifrado.

10.1 Criterios de composición del campo CN para un certificado de empleado público

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

Ejemplos:

JUAN ANTONIO DE LA CAMARA ESPAÑOL - DNI 00000000G (AUTENTICACION)
JUAN ANTONIO DE LA CAMARA ESPAÑOL - DNI 00000000G (FIRMA)
JUAN ANTONIO DE LA CAMARA ESPAÑOL - DNI 00000000G (CIFRADO)
JUAN ANTONIO DE LA CAMARA ESPAÑOL - DNI 00000000G
DE LA CAMARA ESPAÑOL JUAN ANTONIO |00000000G (AUTENTICACION)
DE LA CAMARA ESPAÑOL JUAN ANTONIO |00000000G (FIRMA)
DE LA CAMARA ESPAÑOL JUAN ANTONIO |00000000G (CIFRADO)
DE LA CAMARA ESPAÑOL JUAN ANTONIO |00000000G

10.2 Campos comunes a los dos niveles

Campo	Contenido	R	Observaciones
1. X.509v1 Field			-
1.1. Version	2 (= v3)	Sí	Integer:=2 ([RFC5280] describe la versión del certificado al usar extensiones es decir v3 su valor debe ser 2)
1.2. Serial Number	Número identificativo único del certificado.	Sí	Integer. SerialNumber = p. ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280] integer positivo, no mayor 20 octetos ($1- 2^{159}$) Se utilizará para identificar de manera unívoca el certificado
1.3. Issuer Distinguished Name		Sí	Todos los campos destinados a identificar/describir el prestador de servicios serán codificados en formato UTF8
1.3.1. Country (C)	ES	Sí	C = p. ej: ES (PrintableString) Se codificará de acuerdo a “ISO 3166-1-alpha-2 code elements” Size [RFC 5280] 3
1.3.2. Organization (O)	Denominación (nombre “oficial” de la organización) del prestador de servicios de certificación (emisor del certificado).	Sí	O = p. ej: MINISTERIO DE FOMENTO (String UTF8) Size [RFC 5280] 128
1.3.3. Locality (L)	Localidad/dirección del prestador de servicios de certificación		L = p. ej: MADRID (String UTF8) Size [RFC 5280] 128 Si bien el campo está estipulado para introducir la localidad, se contempla la posibilidad de incluir la dirección completa
1.3.4. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.	Sí	OU = p. ej: AUTORIDAD DE CERTIFICACION CERTICA (String UTF8) Size [RFC 5280] 128 Se contempla el nombre de la entidad que ha emitido el certificado
1.3.5. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF.	*	NIF = NIF entidad suscriptora, p. ej: S2833002 (Printable String) Size = 9

Campo	Contenido	R	Observaciones
1.3.6. Organization Identifier	Identificador de la organización Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)	*	OrganizationIdentifier p. ej: VATES-S2833002.
1.3.7. Common Name (CN)	Nombre común de la organización prestadora de servicios de certificación (emisor del certificado)	Sí	CN = p. ej: CERTICA Root subCA (String UTF8) Size 80 Size [RFC 5280] 80
1.4. Validity	5 años (recomendado)	Sí	Los datos de validez creados antes del 2050 se codificarán utilizando UTCTime. A partir del 2050 se utilizará la codificación GeneralizedTime en la cual se utilizan dos dígitos más para especificar el año (4 en lugar de 2)
1.4.1. Not Before	Fecha de inicio de validez	Sí	Fecha de inicio de validez, formato: UTCTime YYMMDDHHMMSSZ
1.4.2. Not After	Fecha de fin de validez	Sí	Fecha fin de validez, formato: UTCTime YYMMDDHHMMSSZ
1.5. Subject	Todos los campos destinados a identificar/describir al custodio/responsable del certificado o firmante serán codificados utilizando UTF-8	Sí	Según la RFC5280 esta parte se ha de rellenar con carácter obligatorio Según la ETSI-QC se debe reflejar obligatoriamente el campo Country Ver RFC3739 / ETSI 101862
1.5.1. Country (C)	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas.	Sí	C = p. ej: ES (PrintableString) Se codificará de acuerdo a “ISO 3166-1-alpha-2 code elements” Size [RFC 5280] 3
1.5.2. Organization (O)	Denominación (nombre “oficial”) de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado.	Sí	O = p. ej: MINISTERIO DE FOMENTO (String UTF8) Size [RFC 5280] 128
1.5.3. Organizational Unit (OU)	Descripción del tipo de certificado	Sí	OU = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (String UTF8) Size [RFC 5280] 128

Campo	Contenido	R	Observaciones
1.5.4. Organizational Unit (OU)	Unidad, dentro de la Administración, en la que está incluida el empleado público responsable del certificado		Unidad = p. ej: SUBDIRECCION GENERAL DE PROCESO DE DATOS (String) Size [RFC 5280] 128
1.5.5. Organizational Unit (OU)	Código DIR3 de la unidad		OU = p. ej: E04976701
1.5.6. Organizational Unit (OU)	Número de identificación del empleado público responsable del certificado (supuestamente unívoco). Se corresponde con el NRP o NIP		Número identificativo = p. ej: A02APE1056 (String UTF8) Size = 10
1.5.7. Title	Debe incluir el puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado.		Title = p. ej: ANALISTA PROGRAMADOR. Nombre descriptivo del puesto o cargo que ostenta el responsable del certificado (String UTF8) Size [RFC 5280] 128
1.5.8. Serial Number	Se recomienda usar el DNI/NIE del empleado público. Preferiblemente se utilizará la semántica propuesta por la norma ETSI EN 319 412-1	Sí	SerialNumber = p. ej: 00000000G. Número secuencial único asignado por el prestador (Printable String)) Size [RFC 5280] 64 SerialNumber = p. ej: IDCES-00000000G. 3 caracteres para indicar el número de documento (IDC= documento nacional de identidad) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64
1.5.9. 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). Obligatorio según ETSI EN 319 412-2	Si	Primer apellido, espacio en blanco, segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 80 p. ej: “DE LA CAMARA ESPAÑOL - DNI 00000000G”
1.5.10. Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte) Obligatorio según ETSI EN 319 412-2	Sí	Nombre de pila del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 p. ej: “JUAN ANTONIO”

Campo	Contenido	R	Observaciones
1.5.11. Common Name (CN)	Se deben introducir el nombre y dos apellidos de acuerdo con documento de identidad (DNI/Pasaporte), así como DNI (Ver Criterios de Composición del campo CN para un empleado público).	Sí	ej: JUAN ANTONIO DE LA CAMARA ESPAÑOL - DNI 00000000G (String UTF8)) Size [RFC 5280] 132
1.6. Subject Public Key Info	Clave pública de la persona, codificada de acuerdo con el algoritmo criptográfico.	Sí	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. (String UTF8)

(*) Se deberá incluir al menos uno de los campos SerialNumber u OrganizationIdentifier

10.2.1 Extensiones del certificado

Campo	Contenido	R	Observaciones
2. X.509v3 Extensions			-
2.1. Authority Key Identifier	Presente, de acuerdo con RFC 5280.	Sí	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	Presente, de acuerdo con RFC 5280.		Identificador de la clave pública del emisor (String UTF8)
2.1.2. AuthorityCertIssuer	Path de identificación de certificación		Nombre de la CA a la que corresponde la clave identificada en keyIdentifier (String UTF8) Size 128
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA		(Integer)
2.2. Subject Key Identifier	Presente, de acuerdo con RFC 5280.	Sí	Identificador de la clave pública del suscriptor o poseedor de claves (derivada de utilizar la función de Hash sobre la clave pública del sujeto). Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.
2.3. cRLDistributionPoint		Sí	Indica cómo se obtiene la información de CRL.

Campo	Contenido	R	Observaciones
2.3.1. distributionPoint	Punto de distribución de la CRL, número 1	Sí	Web donde resida la CRL (punto de distribución 1 -http. (String UTF8)
2.3.2. distributionPoint	Punto de distribución de la CRL, número 2		Web donde resida la CRL (punto de distribución 2 – http/https o con servidor autenticado). (String UTF8)
2.4. Authority Info Access		Sí	
2.4.1. Access Method	Id-ad-ocsp	Sí	ID de On-line Certificate Status Protocol
2.4.2. Access Location	(dirección web)	Sí	URL de On-line Certificate Status Protocol. Especifica el emplazamiento de la información (String UTF8)
2.4.3. Access Method	Id-ad-caIssuers	Sí	ID de localización del certificado de la CA
2.4.4. Access Location	(dirección web)	Sí	URL de localización del certificado de la CA. Especifica el emplazamiento de la información (String UTF8)
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		Correo electrónico de contacto de la entidad de certificación emisora, p. ej: soporte.certica@mfom.es (String) Size [RFC 5280] 255

10.3 Nivel Alto, funciones segregadas en tres perfiles de certificado

10.3.1 Certificado de firma electrónica

10.3.1.1 Certificado

Campo	Contenido	R	Observaciones
1. X.509v1 Field			-
1.1. Signature Algorithm	SHA-2 con RSA Signature y longitud de clave de 2048 bits	Sí	String UTF8 (40). Identificando el tipo de algoritmo, (más laxo que el del certificado raíz), y longitud de 2048 por tratarse de un certificado de nivel alto. OID 2.16.840.1.101.3.4.2.1

10.3.1.2 Extensiones del certificado

Campo	Contenido	R	Observaciones
2.1. Key Usage		Sí	Campo crítico para determinar el uso (dependiente del certificado)
2.1.1. Digital Signature	No seleccionado “0”		Se utiliza cuando se realiza la función de autenticación
2.1.2. Content Commitment	Seleccionado “1”	Sí	Se utiliza cuando se realiza la función de firma electrónica
2.1.3. Key Encipherment	No seleccionado “0”		Se utiliza para gestión y transporte de claves
2.1.4. Data Encipherment	No seleccionado “0”		Se utiliza para cifrar datos que no sean claves criptográficas
2.1.5. Key Agreement	No seleccionado “0”		Se usa en el proceso de acuerdo de claves
2.1.6. Key Certificate Signature	No seleccionado “0”		Se usa para firmar certificados. Se utiliza en los certificados de autoridades de certificación
2.1.7. CRL Signature	No seleccionado “0”		Se usa para firmar listas de revocación de certificados
2.2. Qualified Certificate Statements		Sí	
2.2.1. QcCompliance	Indicación de certificado cualificado	Sí	OID 0.4.0.1862.1.1
2.2.2. QcEuRetentionPeriod	15 años	Sí	Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
2.2.3. QcSSCD	Uso de dispositivo seguro de firma	Sí	OID 0.4.0.1862.1.4
2.2.4. QcType- esign	Certificado de firma	Si	OID 0.4.0.1862.1.6.1
2.2.5. QcPDS	Lugar donde se encuentra la declaración PDS	SI	OID 0.4.0.1862.1.5

Campo	Contenido	R	Observaciones
2.2.6. semnaticsId-Natural	Para indicar semántica de persona fisica definida por la EN 319 412-1		0.4.0.194121.1.1
2.3. Certificate Policies	Políticas de certificación/DPC	Sí	
2.3.1. Policy Identifier	OID asociado a certificado de empleado público de nivel alto	Sí	2.16.724.1.3.5.7.1
2.3.2. Policy Identifier	QCP-n-qscd	Si	Certificado cualificado de firma, almacenado en dispositivo cualificado acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)
2.3.3. Policy Identifier	OID asociado a la DPC o PC	Sí	OID Private enterprise: p. ej: 1.3.6.1.4.1.<num prest>.1.3.4.1 u OID Country assignment (2.16...)
2.3.4. Policy Qualifier ID	Especificación de la DPC	Sí	
2.3.4.1. CPS Pointer	URL de la DPC o, en su caso, documento legal de tercero.	Sí	URL de las condiciones de uso, p. ej: www.mfom.es/certica/emision/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).
2.3.4.2. User Notice	P. ej: " Certificado cualificado de firma electrónica de empleado público, nivel alto. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero	Sí	Campo explicitText. Se recomienda que siempre se referencie a través de un link. Se recomienda longitud no superior a 200 caracteres.
2.4. Subject Alternate Names		Sí	Lugar donde se contemplarán los valores establecidos para la Identidad Administrativa
2.4.1. rfc822Name	Correo electrónico del firmante[5]		Correo electrónico de la persona responsable del certificado, p. ej: juanantonio.delacamara.espanol@mfom.es (String) Size [RFC 5280] 255

[5] Extensión generalmente utilizada por productos S/MIME

Campo	Contenido	R	Observaciones
2.4.2. Directory Name	Identidad administrativa	Sí	Campos específicos definidos por la Administración para los certificados RD 1671/2009. (Sequence)
2.4.2.1. Tipo de certificado	Indica la naturaleza del certificado	Sí	Tipo= CERTIFICADO CUALIFICADO DE FIRMA DE EMPLEADO PUBLICO DE NIVEL ALTO(String UTF8) Size = 80 OID: 2.16.724.1.3.5.7.1.*1*
2.4.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	Sí	Entidad Suscriptora = p. ej: MINISTERIO DE FOMENTO (String UTF8) Size = 80 OID: 2.16.724.1.3.5.7.1.2
2.4.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	Sí	NIF suscriptora = NIF entidad suscriptora, p. ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.7.1.3
2.4.2.4. DNI/NIE del firmante	DNI o NIE del responsable	Sí	DNI/NIE responsable= p. ej: 00000000G (String UTF8) Size = 10 OID: 2.16.724.1.3.5.7.1.4
2.4.2.5. Número de identificación de personal	Número de identificación del firmante (supuestamente unívoco). Se corresponde con el NRP o NIP	O	Número identificativo = p. ej: A02APE1056 (String UTF8) Size = 10 OID: 2.16.724.1.3.5.7.1.5
2.4.2.6. Nombre de pila	Nombre de pila del firmante	Sí	N = Nombre de pila del firmante de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.7.1.6 Ej: “JUAN ANTONIO”
2.4.2.7. Primer apellido	Primer apellido del firmante	Sí	SN1 = Primer apellido del firmante de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.7.1.7 Ej: “DE LA CAMARA”
2.4.2.8. Segundo apellido	Segundo apellido del firmante	Sí	SN2 = Segundo apellido del firmante de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 En caso de no existir el segundo

Campo	Contenido	R	Observaciones
			apellido, se dejará en blanco (sin ningún carácter). OID: 2.16.724.1.3.5.7.1.8 Ej: “ESPAÑOL”
2.4.2.9. Correo electrónico	Correo electrónico del firmante	O	Correo electrónico del firmante. P. ej: juanantonio.delacamara.espanol@mfom.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.7.1.9
2.4.2.10. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluida el firmante	O	Unidad = p. ej: SUBDIRECCION GENERAL DE PROCESO DE DATOS (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.7.1.10
2.4.2.11. Puesto o cargo	Puesto desempeñado por el firmante dentro de la administración.	O	Puesto = p. ej: ANALISTA PROGRAMADOR (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.7.1.11

10.3.2 Certificado de autenticación

10.3.2.1 Certificado

Campo	Contenido	R	Observaciones
1. X.509v1 Field			-
1.1. Signature Algorithm	SHA-2 con RSA Signature y longitud de clave de 2048 bits	Sí	String UTF8 (40). Identificando el tipo de algoritmo, (más laxo que el del certificado raíz), y longitud de 2048 por tratarse de un certificado de nivel alto. OID 2.16.840.1.101.3.4.2.1

10.3.2.2 Extensiones del certificado

Campo	Contenido	R	Observaciones
2.1. Key Usage		Sí	Campo crítico para determinar el uso (dependiente del certificado)

Campo	Contenido	R	Observaciones
2.1.1. Digital Signature	Seleccionado “1”	Sí	Se utiliza cuando se realiza la función de autenticación
2.1.2. Content Commitment	No seleccionado “0”		Se utiliza cuando se realiza la función de firma electrónica
2.1.3. Key Encipherment	No seleccionado “0/1”		Se utiliza para gestión y transporte de claves
2.1.4. Data Encipherment	No seleccionado “0”		Se utiliza para cifrar datos que no sean claves criptográficas
2.1.5. Key Agreement	No seleccionado “0/1”		Se usa en el proceso de acuerdo de claves
2.1.6. Key Certificate Signature	No seleccionado “0”		Se usa para firmar certificados. Se utiliza en los certificados de autoridades de certificación
2.1.7. CRL Signature	No seleccionado “0”		Se usa para firmar listas de revocación de certificados
2.2. Extended Key Usage		Sí	Uso extendidos del certificado
2.2.1. Email Protection	Seleccionado	Sí	Protección de mail
2.2.2. Client Authentication	Seleccionado	Sí	Autenticación cliente
2.3. Certificate Policies	Políticas de certificación/DPC	Sí	
2.3.1. Policy Identifier	OID asociado a la DPC o PC	Sí	OID Private enterprise: p. ej: 1.3.6.1.4.1.<num prest>.1.3.4.2 u OID Country assignment (2.16...)
2.3.2. Policy Qualifier ID	Especificación de la DPC	Sí	
2.3.2.1. CPS Pointer	URL de la DPC o, en su caso, documento legal de tercero.	Sí	URL de las condiciones de uso, p. ej: www.mfom.es/certica/emision/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).
2.3.2.2. User Notice	Ej: "Certificado de personal, nivel alto, autenticación. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero	Sí	Campo explicitText. Se recomienda que siempre se referencie a través de un link. Se recomienda longitud no superior a 200 caracteres.

Campo	Contenido	R	Observaciones
2.3.3. Policy Identifier	NCP+		Certificado acorde a una política normalizada,en dispositivo seguro acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)
2.3.4. Policy Identifier	OID asociado certificado de empleado público de nivel alto	Sí	2.16.724.1.3.5.7.1
2.4. Subject Alternate Names		Sí	Lugar donde se contemplarán los valores establecidos para la Identidad Administrativa
2.4.1. rfc822Name	Correo electrónico de la persona responsable del certificado[6]		Correo electrónico de la persona responsable del certificado, p. ej: juanantonio.delacamara.espanol@mfom.es (String) Size [RFC 5280] 255
2.4.2. Directory Name	Identidad administrativa	Sí	Campos específicos definidos por la Administración para los certificados RD 1671/2009. (Sequence)
2.4.2.1. Tipo de certificado	Indica la naturaleza del certificado	Sí	Tipo= certificado electrónico de empleado público de nivel alto de autenticación CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO DE NIVEL ALTO DE AUTENTICACION (String UTF8) Size = 80 OID2.16.724.1.3.5.7.1.*1*
2.4.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	Sí	Entidad Suscriptora = p. ej: MINISTERIO DE FOMENTO (String UTF8) Size = 80 OID: 2.16.724.1.3.5.7.1.2
2.4.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	Sí	NIF suscriptora = NIF entidad suscriptora, p. ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.7.1.3
2.4.2.4. DNI/NIE del responsable	DNI o NIE del responsable del certificado	Sí	DNI/NIE responsable= p. ej: 00000000G (String UTF8) Size = 10 OID: 2.16.724.1.3.5.7.1.4

[6] Extensión generalmente utilizada por productos S/MIME

Campo	Contenido	R	Observaciones
2.4.2.5. Número de identificación de personal	Número de identificación del responsable del certificado (supuestamente unívoco)	O	Número identificativo = p. ej: A02APE1056 (String UTF8) Size = 10 OID: 2.16.724.1.3.5.7.1.5
2.4.2.6. Nombre de pila	Nombre de pila del responsable del certificado	Sí	N = Nombre de pila del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.7.1.6 Ej: "JUAN ANTONIO"
2.4.2.7. Primer apellido	Primer apellido del responsable del certificado	Sí	SN1 = Primer apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.7.1.7 Ej: "DE LA CAMARA"
2.4.2.8. Segundo apellido	Segundo apellido del responsable del certificado	Sí	SN2 = Segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter). OID: 2.16.724.1.3.5.7.1.8 Ej: "ESPAÑOL"
2.4.2.9. Correo electrónico	Correo electrónico de la persona responsable del certificado	O	Correo electrónico de la persona responsable del certificado, p. ej: juanantonio.delacamara.espanol@mfom.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.7.1.9
2.4.2.10. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluida el responsable del certificado	O	Unidad = p. ej: SUBDIRECCION GENERAL DE PROCESO DE DATOS (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.7.1.10
2.4.2.11. Puesto o cargo	Puesto desempeñado por el responsable del certificado dentro de la administración.	O	Puesto = p. ej: ANALISTA PROGRAMADOR (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.7.1.11
2.4.2.12. User Principal Name (UPN)	UPN para smart card logon	O	Campo destinado a incluir el smart card logon del sistema en que trabaje el responsable del certificado.

10.3.3 Certificado de cifrado

10.3.3.1 Certificado

Campo	Contenido	R	Observaciones
1. X.509v1 Field			-
1.1. Signature Algorithm	SHA-2 con RSA Signature y longitud de clave de 2048 bits	Sí	String UTF8 (40). Identificando el tipo de algoritmo, (más laxo que el del certificado raíz), y longitud de 2048 por tratarse de un certificado de nivel alto. OID 2.16.840.1.101.3.4.2.1

10.3.3.2 Extensiones del certificado

Campo	Contenido	R	Observaciones
2.1. Key Usage		Sí	Campo crítico para determinar el uso (dependiente del certificado)
2.1.1. Digital Signature	No seleccionado “0”		No usado
2.1.2. Content Commitment	No seleccionado “0”		No usado
2.1.3. Key Encipherment	Seleccionado “1”	Sí	Se utiliza para gestión y transporte de claves
2.1.4. Data Encipherment	Seleccionado “1”	Sí	Por tratarse de un certificado de cifrado
2.1.5. Key Agreement	No seleccionado “0”		No usado
2.1.6. Key Certificate Signature	No seleccionado “0”		No usado
2.1.7. CRL Signature	No seleccionado “0”		No usado
2.2. Extended Key Usage		Sí	Uso extendidos del certificado
2.2.1. Email Protection	Seleccionado	Sí	Protección de mail
2.2.2. Client Authentication	Seleccionado	Sí	Autenticación cliente
2.3. Certificate Policies	Políticas de certificación/DPC	Sí	
2.3.1. Policy Identifier	OID asociado a la DPC o PC	Sí	OID Private enterprise: p. ej: 1.3.6.1.4.1.<num prest>.1.3.4.3, u OID Country assignment (2.16...)

Campo	Contenido	R	Observaciones
2.3.2. Policy Qualifier ID	Especificación de la DPC	Sí	
2.3.2.1. CPS Pointer	URL de la DPC o, en su caso, documento legal de tercero.	Sí	URL de las condiciones de uso, p. ej: www.mfom.es/certica/emision/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).
2.3.2.2. User Notice	Ej: "Certificado de personal, nivel alto, cifrado. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero	Sí	Campo explicitText. Se recomienda que siempre se referencie a través de un link. Se recomienda longitud no superior a 200 caracteres.
2.3.3. Policy Identifier	OID asociado a empleado público de nivel alto	Sí	2.16.724.1.3.5.7.1
2.4. Subject Alternate Names		Sí	Lugar donde se contemplarán los valores establecidos para la Identidad Administrativa
2.4.1. rfc822Name	Correo electrónico de la persona responsable del certificado[7]		Correo electrónico de la persona responsable del certificado, p. ej: juanantonio.delacamara.espanol@mfom.es (String) Size [RFC 5280] 255
2.4.2. Directory Name	Identidad administrativa	Sí	Campos específicos definidos por la Administración para los certificados RD 1671/2009. (Sequence)
2.4.2.1. Tipo de certificado	Indica la naturaleza del certificado	Sí	Tipo= CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO DE NIVEL ALTO PARA CIFRADO (String UTF8) Size = 80 OID2.16.724.1.3.5.7.1.*1*
2.4.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	Sí	Entidad Suscriptora = p. ej: MINISTERIO DE FOMENTO (String UTF8) Size = 80 OID: 2.16.724.1.3.5.7.1.2
2.4.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	Sí	NIF suscriptora = NIF entidad suscriptora, p. ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.7.1.3
2.4.2.4. DNI/NIE del responsable	DNI o NIE del responsable del certificado	Sí	DNI/NIE responsable = p. ej: 00000000G (String UTF8) Size = 10 OID: 2.16.724.1.3.5.7.1.4

[7] Extensión generalmente utilizada por productos S/MIME

Campo	Contenido	R	Observaciones
2.4.2.5. Número de identificación de personal	Número de identificación del responsable del certificado (supuestamente unívoco)	O	Número identificativo = p. ej: A02APE1056 (String UTF8) Size = 10 OID: 2.16.724.1.3.5.7.1.5
2.4.2.6. Nombre de pila	Nombre de pila del responsable del certificado	Sí	N = Nombre de pila del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.7.1.6 Ej: "JUAN ANTONIO"
2.4.2.7. Primer apellido	Primer apellido del responsable del certificado	Sí	SN1 = Primer apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.7.1.7 Ej: "DE LA CAMARA"
2.4.2.8. Segundo apellido	Segundo apellido del responsable del certificado	Sí	SN2 = Segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter). OID: 2.16.724.1.3.5.7.1.8 Ej: "ESPAÑOL"
2.4.2.9. Correo electrónico	Correo electrónico de la persona responsable del certificado	O	Correo electrónico de la persona responsable del certificado, p. ej: juanantonio.delacamara.espanol@mfom.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.7.1.9
2.4.2.10. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluida el responsable del certificado	O	Unidad = p. ej: SUBDIRECCION GENERAL DE PROCESO DE DATOS (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.7.1.10
2.4.2.11. Puesto o cargo	Puesto desempeñado por el responsable del certificado dentro de la administración.	O	Puesto = p. ej: ANALISTA PROGRAMADOR (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.7.1.11

10.4 Nivel Medio/Sustancial

En este nivel de aseguramiento la configuración es libre en el sentido del número de certificados a incluir (1, 2 ó 3), derivado de este factor los usos que tengan cada uno de ellos reflejado en el Key Usage son diferentes, a continuación se presenta la opción de un único certificado.

En el ejemplo propuesto se usa un solo certificado para autenticación y firma. No se permite el uso de cifrado, para seguir las normas ETSI EN 319 412-2.

10.4.1 Certificado

Campo	Contenido	R	Observaciones
1. X.509v1 Field			-
1.1. Signature Algorithm	SHA-2 con RSA Signature y longitud de clave de 2048 bits	Sí	String UTF8 (40). Identificando el tipo de algoritmo, (más laxo que el del certificado raíz), y longitud de 2048 por tratarse de un certificado de nivel medio/sustancial. OID 2.16.840.1.101.3.4.2.1

10.4.2 Extensiones del certificado

Campo	Contenido	R	Observaciones
2.1. Key Usage		Sí	Campo crítico para determinar el uso (dependiente del certificado)
2.1.1. Digital Signature	Seleccionado “1”	Sí	Para tener uso de autenticación
2.1.2. Content Commitment	Seleccionado “1”	Sí	Necesario uso de firma
2.1.3. Key Encipherment	Seleccionado “1”	Sí	Se utiliza para gestión y transporte de claves
2.1.4. Data Encipherment	Seleccionado “0		No se permite el uso de cifrado en los certificados de empleado de nivel medio/sustancial, para seguir las normas ETSI EN 319 412-2, ya que es un único perfil
2.1.5. Key Agreement	No seleccionado “0”		No usado
2.1.6. Key Certificate Signature	No seleccionado “0”		No usado

Campo	Contenido	R	Observaciones
2.1.7. CRL Signature	No seleccionado “0”		No usado
2.2. Extended Key Usage		Sí	Uso extendidos del certificado
2.2.1. Email Protection	Seleccionado	Sí	Protección de mail
2.2.2. Client Authentication	Seleccionado	Sí	Autenticación cliente
2.3. Qualified Certificate Statements		Sí	
2.3.1. QcCompliance	Indicación de certificado cualificado	Sí	OID 0.4.0.1862.1.1
2.3.2. QcEuRetentionPeriod	15 años	Sí	Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
2.3.3. QcType- esign	Certificado de firma	Si	OID 0.4.0.1862.1.6.1
2.3.4. QcPDS	Lugar donde se encuentra la declaración PDS	SI	OID 0.4.0.1862.1.5
2.3.5. semnaticsId-Natural	Para indicar semántica de persona fisica definida por la EN 319 412-1		0.4.0.194121.1.1
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	OID asociado a la DPC o PC	Sí	OID Private enterprise: p. ej: 1.3.6.1.4.1.<num prest>.1.3.4.4 u OID Country assignment (2.16...)
2.4.2. Policy Qualifier ID	Especificación de la DPC	Sí	
2.4.2.1. CPS Pointer	URL de la DPC o, en su caso, documento legal de tercero.	Sí	URL de las condiciones de uso, p. ej: www.mfom.es/certica/emision/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).
2.4.2.2. User Notice	Ej: " Certificado cualificado de firma electrónica de empleado público, nivel medio. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero	Sí	URL de las condiciones de uso. Se recomienda que siempre se referencie a través de un link. (String UTF8)). Se recomienda longitud no superior a 200 caracteres.

Campo	Contenido	R	Observaciones
2.4.3. Policy Identifier	QCP-n	Si	Certificado cualificado de firma, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural (0)
2.4.4. Policy Identifier	OID que indica certificado de empleado público de nivel medio	Si	2.16.724.1.3.5.7.2
2.5. Subject Alternate Names		Sí	Lugar donde se contemplarán los valores establecidos para la Identidad Administrativa
2.5.1. rfc822Name	Correo electrónico de la persona responsable del certificado[8]		Correo electrónico de la persona responsable del certificado, p. ej: juanantonio.delacamara.espanol@mfom.es (String) Size [RFC 5280] 255
2.5.2. Directory Name	Identidad administrativa	Sí	Campos específicos definidos por la Administración para los certificados RD 1671/2009. (Sequence)
2.5.2.1. Tipo de certificado	Indica la naturaleza del certificado	Sí	Tipo= CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (de nivel medio) (String UTF8) Size = 80 OID: 2.16.724.1.3.5.7.2.1
2.5.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	Sí	Entidad Suscriptora = p. ej: MINISTERIO DE FOMENTO (String UTF8) Size = 80 OID: 2.16.724.1.3.5.7.2.2
2.5.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	Sí	NIF suscriptora = NIF entidad suscriptora, p. ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.7.2.3
2.5.2.4. DNI/NIE del responsable	DNI o NIE del firmante	Sí	DNI/NIE firmante = p. ej: 00000000G (String UTF8) Size = 10 OID: 2.16.724.1.3.5.7.2.4
2.5.2.5. Número de identificación de personal	Número de identificación del firmante (supuestamente unívoco)	O	Número identificativo = p. ej: A02APE1056 (String UTF8) Size = 10 OID: 2.16.724.1.3.5.7.2.5

[8] Extensión generalmente utilizada por productos S/MIME

Campo	Contenido	R	Observaciones
2.5.2.6. Nombre de pila	Nombre de pila del firmante	Sí	N = Nombre de pila del firmante de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.7.2.6 Ej: "JUAN ANTONIO"
2.5.2.7. Primer apellido	Primer apellido del firmante	Sí	SN1 = Primer apellido del firmante de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.7.2.7 Ej: "DE LA CAMARA"
2.5.2.8. Segundo apellido	Segundo apellido del firmante	Sí	SN2 = Segundo apellido del firmante de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter). OID: 2.16.724.1.3.5.7.2.8 Ej: "ESPAÑOL"
2.5.2.9. Correo electrónico	Correo electrónico del firmante	O	Correo electrónico del firmante. P. ej: juanantonio.delacamara.espanol@mpr.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.7.2.9
2.5.2.10. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluida el firmante	O	Unidad = p. ej: SUBDIRECCION GENERAL DE PROCESO DE DATOS (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.7.2.10
2.5.2.11. Puesto o cargo	Puesto desempeñado por el firmante dentro de la administración.	O	Puesto = p. ej: ANALISTA PROGRAMADOR (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.7.2.11
2.5.3. User Principal Name (UPN)	UPN para smart card logon	O	Campo destinado a incluir el smart card logon de Windows para el firmante.

11 CERTIFICADO DE EMPLEADO PÚBLICO CON SEUDÓNIMO

Los certificados de firma electrónica y autenticación deberán ser acordes a la normativa europea, en concreto al Anexo I del Reglamento UE 910/2014 que especifica los requisitos para los certificados cualificados de persona física, y su normativa de desarrollo. Los dispositivos calificados de creación de firma deberán alinearse con el Anexo II del citado Reglamento.

El Prestador de Servicios de Certificación deberá asignar Policy Identifier con OIDs diferentes para cada tipo de certificado. Especialmente deberá asignar OID distintos para los certificados de firma, identificación y cifrado.

11.1 Criterios de composición del campo CN para un certificado de empleado público con seudónimo

- Incluir obligatoriamente el PUESTO O CARGO o literal 'SEUDONIMO',
- Incluir obligatoriamente un SÍMBOLO o CARÁCTER que separe el cargo/literal del seudónimo del titular del certificado
- Incluir obligatoriamente el SEUDONIMO,
- Incluir obligatoriamente un SÍMBOLO o CARÁCTER que separe el seudónimo del organismo en que presta los servicios el titular del certificado
- Incluir obligatoriamente el NOMBRE OFICIAL DEL ORGANISMO, tal y como figura en el boletín oficial correspondiente.
- No se podrá incluir nombre y apellidos.
- No se podrá incluir el número de DNI/NIE.
- Se podrá incluir opcionalmente un literal (AUTENTICACION, FIRMA o CIFRADO) que identifique la tipología del certificado. Este identificador siempre estará al final del CN y entre paréntesis. En el caso de un nivel de aseguramiento medio/sustancial, si se agrupan varios perfiles en un único certificado, no se deberá incluir esta opción.

Ejemplos:

SUBINSPECTOR – NIP 11111111 – DIRECCION GENERAL DE POLICIA (AUTENTICACION)
SUBINSPECTOR – NIP 11111111 - DIRECCION GENERAL DE POLICIA (FIRMA)
SUBINSPECTOR – NIP 11111111 - DIRECCION GENERAL DE POLICIA
SEUDONIMO – 123456789 - DIRECCION GENERAL DE TRAFICO (AUTENTICACION)
SEUDONIMO - 123456789 - DIRECCION GENERAL DE TRAFICO (FIRMA)

11.2 Campos comunes a los dos niveles

Campo	Contenido	R	Observaciones
3. X.509v1 Field			-
3.1. Version	2 (= v3)	Sí	Integer:=2 ([RFC5280] describe la versión del certificado al usar extensiones es decir v3 su valor debe ser 2)
3.2. Serial Number	Número identificativo único del certificado.	Sí	Integer. SerialNumber = p. ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280] integer positivo, no mayor 20 octetos (1- 2^{159}) Se utilizará para identificar de manera unívoca el certificado
3.3. Issuer Distinguished Name		Sí	Todos los campos destinados a identificar/describir el prestador de servicios serán codificados en formato UTF8
3.3.1. Country (C)	ES	Sí	C = p. ej: ES (PrintableString) Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements" Size [RFC 5280] 3
3.3.2. Organization (O)	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado).	Sí	O = p. ej: MINISTERIO DE FOMENTO (String UTF8) Size [RFC 5280] 128
3.3.3. Locality (L)	Localidad/dirección del prestador de servicios de certificación		L = p. ej: MADRID (String UTF8) Size [RFC 5280] 128 Si bien el campo está estipulado para introducir la localidad, se contempla la posibilidad de incluir la dirección completa
3.3.4. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.	Sí	OU = p. ej: AUTORIDAD DE CERTIFICACION CERTICA (String UTF8) Size [RFC 5280] 128 Se contempla el nombre de la entidad que ha emitido el certificado
3.3.5. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF.	*	NIF = NIF entidad suscriptora, p. ej: S2833002 (Printable String) Size = 9
3.3.6. Organization Identifier	Identificador de la organización Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)	*	OrganizationIdentifier p. ej: VATES-S2833002.
3.3.7. Common Name (CN)	Nombre común de la organización prestadora de servicios de certificación (emisor del certificado)	Sí	CN = p. ej: CERTICA Root CA (String UTF8) Size 80 Size [RFC 5280] 80

Campo	Contenido	R	Observaciones
3.4. Validity	5 años (recomendado)	Sí	Los datos de validez creados antes del 2050 se codificarán utilizando UTCTime. A partir del 2050 se utilizará la codificación GeneralizedTime en la cual se utilizan dos dígitos más para especificar el año (4 en lugar de 2)
3.4.1. Not Before	Fecha de inicio de validez	Sí	Fecha de inicio de validez, formato: UTCTime YYMMDDHHMMSSZ
3.4.2. Not After	Fecha de fin de validez	Sí	Fecha fin de validez, formato: UTCTime YYMMDDHHMMSSZ
3.5. Subject	Todos los campos destinados a identificar/describir al custodio/responsable del certificado serán codificados utilizando UTF-8	Sí	Según la RFC5280 esta parte se ha de rellenar con carácter obligatorio Según la ETSI-QC se debe reflejar obligatoriamente el campo Country Ver RFC3739 / ETSI 101862
3.5.1. Country (C)	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas.	Sí	C = p. ej: ES (PrintableString) Se codificará de acuerdo a “ISO 3166-1-alpha-2 code elements” Size [RFC 5280] 3
3.5.2. Organization (O)	Denominación (nombre “oficial”) de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado.	Sí	O = p. ej: MINISTERIO DE INTERIOR (String UTF8) Size [RFC 5280] 128
3.5.3. Organizational Unit (OU)	Descripción del tipo de certificado	Sí	OU = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (String UTF8) Size [RFC 5280] 128
3.5.4. Organizational Unit (OU)	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado		Unidad = p. ej: DIRECCION GENERAL DE LA POLICIA (String) Size [RFC 5280] 128
3.5.5. Organizational Unit (OU)	Código DIR3 de la unidad		OU = p. ej: E04976701
3.5.6. pseudonym	Seudónimo Obligatorio según ETSI EN 319 412-2	Sí	Ej: NIP 111111111
3.5.7. Title	Debe incluir el puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado.		Title = p. ej: SUBINSPECTOR. Nombre descriptivo del puesto o cargo que ostenta el responsable del certificado (String UTF8) Size [RFC 5280] 128
3.5.8. Common Name (CN)	Se deben introducir el seudónimo y el organismo (Ver Criterios de Composición del campo CN para un empleado público con seudónimo).	Sí	Ej: SUBINSPECTOR – NIP 11111111 – DIRECCION GENERAL DE POLICIA (FIRMA) (String UTF8)) Size [RFC 5280] 132

Campo	Contenido	R	Observaciones
3.6. Subject Public Key Info	Clave pública de la persona, codificada de acuerdo con el algoritmo criptográfico.	Sí	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. (String UTF8)

(*) Se deberá incluir al menos uno de los campos SerialNumber u OrganizationIdentifier

11.2.1 Extensiones del certificado

Campo	Contenido	R	Observaciones
4. X.509v3 Extensions			-
4.1. Authority Key Identifier	Presente, de acuerdo con RFC 5280.	Sí	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.
4.1.1. Key Identifier	Presente, de acuerdo con RFC 5280.		Identificador de la clave pública del emisor (String UTF8)
4.1.2. AuthorityCertIssuer	Path de identificación de certificación		Nombre de la CA a la que corresponde la clave identificada en keyIdentifier (String UTF8) Size 128
4.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA		(Integer)
4.2. Subject Key Identifier	Presente, de acuerdo con RFC 5280.	Sí	Identificador de la clave pública del suscriptor o poseedor de claves (derivada de utilizar la función de Hash sobre la clave pública del sujeto). Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.
4.3. cRLDistributionPoint		Sí	Indica cómo se obtiene la información de CRL.
4.3.1. distributionPoint	Punto de distribución de la CRL, número 1	Sí	Web donde resida la CRL (punto de distribución 1 -http. (String UTF8)
4.3.2. distributionPoint	Punto de distribución de la CRL, número 2		Web donde resida la CRL (punto de distribución 2 – http/https o con servidor autenticado). (String UTF8)
4.4. Authority Info Access		Sí	
4.4.1. Access Method	Id-ad-ocsp	Sí	ID de On-line Certificate Status Protocol
4.4.2. Access Location	(dirección web)	Sí	URL de On-line Certificate Status Protocol. Especifica el emplazamiento de la información (String UTF8)
4.4.3. Access Method	Id-ad-caIssuers	Sí	ID de localización del certificado de la CA
4.4.4. Access Location	(dirección web)	Sí	URL de localización del certificado de la CA. Especifica el emplazamiento de la información (String UTF8)
4.5. Issuer Alternative Name	Nombre alternativo de la persona de contacto de la Entidad de Certificación emisora		
4.5.1. rfc822Name	Correo electrónico de contacto de la Entidad de Certificación emisora		Correo electrónico de contacto de la entidad de certificación emisora, p. ej: soporte.certica@mfom.es (String) Size [RFC 5280] 255

11.3 Nivel Alto, funciones segregadas en tres perfiles de certificado

11.3.1 Certificado de firma electrónica

11.3.1.1 Certificado

Campo	Contenido	R	Observaciones
2. X.509v1 Field			-
2.1. Signature Algorithm	SHA-2 con RSA Signature y longitud de clave de 2048 bits	Sí	String UTF8 (40). Identificando el tipo de algoritmo, (más laxo que el del certificado raíz), y longitud de 2048 por tratarse de un certificado de nivel alto. OID 2.16.840.1.101.3.4.2.1

11.3.1.2 Extensiones del certificado

Campo	Contenido	R	Observaciones
2.2. Key Usage		Sí	Campo crítico para determinar el uso (dependiente del certificado)
2.2.1. Digital Signature	No seleccionado “0”		Se utiliza cuando se realiza la función de autenticación
2.2.2. Content Commitment	Seleccionado “1”	Sí	Se utiliza cuando se realiza la función de firma electrónica
2.2.3. Key Encipherment	No seleccionado “0”		Se utiliza para gestión y transporte de claves
2.2.4. Data Encipherment	No seleccionado “0”		Se utiliza para cifrar datos que no sean claves criptográficas
2.2.5. Key Agreement	No seleccionado “0”		Se usa en el proceso de acuerdo de claves
2.2.6. Key Certificate Signature	No seleccionado “0”		Se usa para firmar certificados. Se utiliza en los certificados de autoridades de certificación
2.2.7. CRL Signature	No seleccionado “0”		Se usa para firmar listas de revocación de certificados
2.3. Qualified Certificate Statements		Sí	
2.3.1. QcCompliance	Indicación de certificado cualificado	Sí	OID 0.4.0.1862.1.1
2.3.2. QcEuRetentionPeriod	15 años	Sí	Integer :=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
2.3.3. QcSSCD	Uso de dispositivo seguro de firma	Sí	OID 0.4.0.1862.1.4
2.3.4. QcType- esign	Certificado de firma	Si	OID 0.4.0.1862.1.6.1
2.3.5. QcPDS	Lugar donde se encuentra la declaración PDS	Si	OID 0.4.0.1862.1.5
2.4. Certificate Policies	Políticas de certificación/DPC	Sí	

Campo	Contenido	R	Observaciones
2.4.1. Policy Identifier	OID asociado a certificado de empleado público con seudónimo de nivel alto	Sí	2.16.724.1.3.5.4.1
2.4.2. Policy Identifier	QCP-n-qscd	Si	Certificado cualificado de firma, almacenado en dispositivo seguro acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)
2.4.3. Policy Identifier	OID asociado a la DPC o PC	Sí	OID Private enterprise: p. ej: 1.3.6.1.4.1.<num prest>.1.3.4.1 u OID Country assignment (2.16…)
2.4.4. Policy Qualifier ID	Especificación de la DPC	Sí	
2.4.4.1. CPS Pointer	URL de la DPC o, en su caso, documento legal de tercero.	Sí	URL de las condiciones de uso, p. ej: www.mfom.es/certica/emision/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).
2.4.4.2. User Notice	E“: " Certificado cualificado de firma electrónica de empleado público con seudónimo, nivel alto. Consulte las condiciones de uso “n " + URL de la DPC o, en su caso, documento legal de tercero	Sí	Campo explicitText. Se recomienda que siempre se referencie a través de un link. Se recomienda longitud no superior a 200 caracteres.
2.5. Subject Alternate Names		Sí	Lugar donde se contemplarán los valores establecidos para la Identidad Administrativa
2.5.1. rfc822Name	Correo electrónico de contacto		Correo electrónico de contacto, p. ej: buzon@dgp.es (String) Size [RFC 5280] 255
2.5.2. Directory Name	Identidad administrativa	Sí	Campos específicos definidos por la Administración para los certificados RD 1671/2009. (Sequence)
2.5.2.1. Tipo de certificado	Indica la naturaleza del certificado	Sí	Tipo= CERTIFICADO CUALIFICADO DE FIRMA ELECTRONICA DE EMPLEADO PUBLICO CON SEUDONIMO, DE NIVEL ALTO (String UTF8) Size = 100 OID: 2.16.724.1.3.5.4.1.*1*
2.5.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	Sí	Entidad Suscriptora = p. ej: MINISTERIO DEL INTERIOR (String UTF8) Size = 80 OID: 2.16.724.1.3.5.4.1.2
2.5.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	Sí	NIF suscriptora = NIF entidad suscriptora, p. ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.4.1.3
2.5.2.4. Correo electrónico	Correo electrónico de contacto	O	Correo electrónico de contacto,p. ej: buzon@dgp.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.4.1.9

Campo	Contenido	R	Observaciones
2.5.2.5. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado	O	Unidad = p. ej: DIRECCION GENERAL DE LA POLICIA (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.4.1.10
2.5.2.6. Puesto o cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración.	O	Puesto = p. ej: SUBINSPECTOR (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.4.1.11
2.5.2.7. Seudónimo	Seudónimo		Seudonimo = p. ej: NIP1111 O.I.D 2.16.724.1.3.5.4.1.12

11.3.2 Certificado de autenticación

11.3.2.1 Certificado

Campo	Contenido	R	Observaciones
2. X.509v1 Field			-
2.1. Signature Algorithm	SHA-2 con RSA Signature y longitud de clave de 2048 bits	Sí	String UTF8 (40). Identificando el tipo de algoritmo, (más laxo que el del certificado raíz), y longitud de 2048 por tratarse de un certificado de nivel alto. OID 2.16.840.1.101.3.4.2.1

11.3.2.2 Extensiones del certificado

Campo	Contenido	R	Observaciones
2.2. Key Usage		Sí	Campo crítico para determinar el uso (dependiente del certificado)
2.2.1. Digital Signature	Seleccionado “1”	Sí	Se utiliza cuando se realiza la función de autenticación
2.2.2. Content Commitment	No seleccionado “0”		Se utiliza cuando se realiza la función de firma electrónica
2.2.3. Key Encipherment	No seleccionado “0/1”		Se utiliza para gestión y transporte de claves
2.2.4. Data Encipherment	No seleccionado “0”		Se utiliza para cifrar datos que no sean claves criptográficas
2.2.5. Key Agreement	No seleccionado “0/1”		Se usa en el proceso de acuerdo de claves
2.2.6. Key Certificate Signature	No seleccionado “0”		Se usa para firmar certificados. Se utiliza en los certificados de autoridades de certificación
2.2.7. CRL Signature	No seleccionado “0”		Se usa para firmar listas de revocación de certificados
2.3. Extended Key Usage		Sí	Uso extendidos del certificado
2.3.1. Email Protection	Seleccionado	Sí	Protección de mail
2.3.2. Client Authentication	Seleccionado	Sí	Autenticación cliente
2.4. Certificate Policies	Políticas de certificación/DPC	Sí	
2.4.1. Policy Identifier	OID asociado a la DPC o PC	Sí	OID Private enterprise: p. ej: 1.3.6.1.4.1.<num prest>.1.3.4.2 u OID Country assignment (2.16...)

Campo	Contenido	R	Observaciones
2.4.2. Policy Qualifier ID	Especificación de la DPC	Sí	
2.4.2.1. CPS Pointer	URL de la DPC o, en su caso, documento legal de tercero.	Sí	URL de las condiciones de uso, p. ej: www.mfom.es/certica/emision/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).
2.4.2.2. User Notice	Ej: "Certificado de empleado público con seudónimo, nivel alto, autenticación. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero	Sí	Campo explicitText. Se recomienda que siempre se referencie a través de un link. Se recomienda longitud no superior a 200 caracteres.
2.4.3. Policy Identifier	OID que indica Certificado de empleado público con seudónimo de nivel alto		2.16.724.1.3.5.4.1
2.4.4. Policy Identifier	NCP+	Si	Certificado acorde a una política normalizada, almacenado en dispositivo seguro itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)
2.5. Subject Alternate Names		Sí	Lugar donde se contemplarán los valores establecidos para la Identidad Administrativa
2.5.1. rfc822Name	Correo electrónico de contacto[9]		Correo electrónico de contacto, p. ej: buzon@dgp.es (String) Size [RFC 5280] 255
2.5.2. Directory Name	Identidad administrativa	Sí	Campos específicos definidos por la Administración para los certificados RD 1671/2009. (Sequence)
2.5.2.1. Tipo de certificado	Indica la naturaleza del certificado	Sí	Tipo= CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO(String UTF8) Size = 100 OID2.16.724.1.3.5.4.1.1
2.5.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	Sí	Entidad Suscriptora = p. ej: MINISTERIO DEL INTERIOR (String UTF8) Size = 80 OID: 2.16.724.1.3.5.4.1.2
2.5.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	Sí	NIF suscriptora = NIF entidad suscriptora, p. ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.4.1.3
2.5.2.4. Correo electrónico	Correo electrónico de contacto	O	Correo electrónico de contacto, p. ej: buzon@dgp.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.4.1.9

[9] Extensión generalmente utilizada por productos S/MIME

Campo	Contenido	R	Observaciones
2.5.2.5. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluida el responsable del certificado	O	Unidad = p. ej: DIRECCION GENERAL DE LA POLICIA (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.4.1.10
2.5.2.6. Puesto o cargo	Puesto desempeñado por el responsable del certificado dentro de la administración.	O	Puesto = p. ej: SUBINSPECTOR (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.4.1.11
2.5.3. User Principal Name (UPN)	UPN para smart card logon	O	Campo destinado a incluir el smart card logon del sistema en que trabaje el responsable del certificado.

11.3.3 Certificado de cifrado

11.3.3.1 Certificado

Campo	Contenido	R	Observaciones
2. X.509v1 Field			-
2.1. Signature Algorithm	SHA-2 con RSA Signature y longitud de clave de 2048 bits	Sí	String UTF8 (40). Identificando el tipo de algoritmo, (más laxo que el del certificado raíz), y longitud de 2048 por tratarse de un certificado de nivel alto. OID 2.16.840.1.101.3.4.2.1

11.3.3.2 Extensiones del certificado

Campo	Contenido	R	Observaciones
2.2. Key Usage		Sí	Campo crítico para determinar el uso (dependiente del certificado)
2.2.1. Digital Signature	No seleccionado “0”		No usado
2.2.2. Content Commitment	No seleccionado “0”		No usado
2.2.3. Key Encipherment	Seleccionado “1”	Sí	Se utiliza para gestión y transporte de claves
2.2.4. Data Encipherment	Seleccionado “1”	Sí	Por tratarse de un certificado de cifrado
2.2.5. Key Agreement	No seleccionado “0”		No usado
2.2.6. Key Certificate Signature	No seleccionado “0”		No usado
2.2.7. CRL Signature	No seleccionado “0”		No usado
2.3. Extended Key Usage		Sí	Uso extendidos del certificado
2.3.1. Email Protection	Seleccionado	Sí	Protección de mail
2.3.2. Client Authentication	Seleccionado	Sí	Autenticación cliente
2.4. Certificate Policies	Políticas de certificación/DPC	Sí	
2.4.1. Policy Identifier	OID asociado a la DPC o PC	Sí	OID Private enterprise: p. ej: 1.3.6.1.4.1.<num prest>.1.3.4.3, u OID Country assignment (2.16...)
2.4.2. Policy Qualifier ID	Especificación de la DPC	Sí	
2.4.2.1. CPS Pointer	URL de la DPC o, en su caso, documento legal de tercero.	Sí	URL de las condiciones de uso, p. ej: www.mfom.es/certica/emision/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).

Campo	Contenido	R	Observaciones
2.4.2.2. User Notice	Ej: "Certificado de empleado público con seudónimo, nivel alto, cifrado. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero	Sí	Campo explicitText. Se recomienda que siempre se referencie a través de un link. Se recomienda longitud no superior a 200 caracteres.
2.5. Policy Identifier	OID asociado Certificado de empleado público con seudónimo de nivel alto	Sí	2.16.724.1.3.5.4.1
2.6. Subject Alternate Names		Sí	Lugar donde se contemplarán los valores establecidos para la Identidad Administrativa
2.6.1. rfc822Name	Correo electrónico de contacto		Correo electrónico de contacto, p. ej: buzon@dgp.es (String) Size [RFC 5280] 255
2.6.2. Directory Name	Identidad administrativa	Sí	Campos específicos definidos por la Administración para los certificados RD 1671/2009. (Sequence)
2.6.2.1. Tipo de certificado	Indica la naturaleza del certificado	Sí	Tipo= CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (String UTF8) Size = 100 OID2.16.724.1.3.5.4.1.1
2.6.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	Sí	Entidad Suscriptora = p. ej: MINISTERIO DEL INTERIOR (String UTF8) Size = 80 OID: 2.16.724.1.3.5.4.1.2
2.6.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	Sí	NIF suscriptora = NIF entidad suscriptora, p. ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.4.1.3
2.6.2.4. Correo electrónico	Correo electrónico de contacto	O	Correo electrónico de contacto, p. ej: buzon@dgp.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.4.1.9
2.6.2.5. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluida el responsable del certificado	O	Unidad = p. ej: DIRECCION GENERAL DE LA POLICIA (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.4.1.10
2.6.2.6. Puesto o cargo	Puesto desempeñado por el responsable del certificado dentro de la administración.	O	Puesto = p. ej: SUBINSPECTOR (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.4.1.11

11.4 Nivel Medio/Sustancial

En el nivel de aseguramiento la configuración es libre en el sentido del número de certificados a incluir (1, 2 ó 3), derivado de este factor los usos que tengan cada uno de ellos reflejado en el Key Usage son diferentes, a continuación se presenta la opción de un único certificado.

En el ejemplo propuesto se usa un solo certificado para autenticación y firma. No se permite el uso de cifrado, para seguir las normas ETSI EN 319 412-2.

11.4.1 Certificado

Campo	Contenido	R	Observaciones
2. X.509v1 Field			-
2.1. Signature Algorithm	SHA-2 con RSA Signature y longitud de clave de 1024 bits	Sí	String UTF8 (40). Identificando el tipo de algoritmo, (más laxo que el del certificado raíz), y longitud de 1024 por tratarse de un certificado de nivel medio/sustancial. OID 2.16.840.1.101.3.4.2.1

11.4.2 Extensiones del certificado

Campo	Contenido	R	Observaciones
2.2. Key Usage		Sí	Campo crítico para determinar el uso (dependiente del certificado)
2.2.1. Digital Signature	Seleccionado “1”	Sí	Para tener uso de autenticación
2.2.2. Content Commitment	Seleccionado “1”	Sí	Necesario uso de firma
2.2.3. Key Encipherment	Seleccionado “1”	Sí	Por tratarse de un certificado de autenticación (intercambio de claves)
2.2.4. Data Encipherment	Seleccionado “0		No se permite el uso de cifrado en los certificados de empleado de nivel medio/sustancial, para seguir las normas ETSI EN 319 412-2
2.2.5. Key Agreement	No seleccionado “0”		No usado
2.2.6. Key Certificate Signature	No seleccionado “0”		No usado
2.2.7. CRL Signature	No seleccionado “0”		No usado
2.3. Extended Key Usage		Sí	Uso extendidos del certificado
2.3.1. Email Protection	Seleccionado	Sí	Protección de mail
2.3.2. Client Authentication	Seleccionado	Sí	Autenticación cliente
2.4. Qualified Certificate Statements		Sí	
2.4.1. QcCompliance	Indicación de certificado cualificado	Sí	OID 0.4.0.1862.1.1
2.4.2. QcEuRetentionPeriod	15 años	Sí	Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
2.4.3. QcType- esign	Certificado de firma	Si	OID 0.4.0.1862.1.6.1
2.4.4. QcPDS	Lugar donde se encuentra la declaración PDS	Si	OID 0.4.0.1862.1.5
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	OID asociado a la DPC o PC	Sí	OID Private enterprise: p. ej: 1.3.6.1.4.1.<num prest>.1.3.4.4 u OID Country assignment (2.16...)
2.5.2. Policy Qualifier ID	Especificación de la DPC	Sí	

Campo	Contenido	R	Observaciones
2.5.2.1. CPS Pointer	URL de la DPC o, en su caso, documento legal de tercero.	Sí	URL de las condiciones de uso, p. ej: www.mfom.es/certica/emision/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).
2.5.2.2. User Notice	P. ej: "Certificado cualificado de firma electrónica de empleado público con seudónimo, nivel medio/sustancial. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero	Sí	URL de las condiciones de uso. Se recomienda que siempre se referencie a través de un link. (String UTF8)). Se recomienda longitud no superior a 200 caracteres.
2.5.3. Policy Identifier	QCP-n	Si	Certificado cualificado de firma, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural (0)
2.5.4. Policy Identifier	OID asociado Certificado de empleado público con seudónimo de nivel medio	Sí	2.16.724.1.3.5.4.2
2.6. Subject Alternate Names		Sí	Lugar donde se contemplarán los valores establecidos para la Identidad Administrativa
2.6.1. rfc822Name	Correo electrónico de contacto[10]		Correo electrónico de contacto, p. ej: buzon@dgp.es (String) Size [RFC 5280] 255
2.6.2. Directory Name	Identidad administrativa	Sí	Campos específicos definidos por la Administración para los certificados RD 1671/2009. (Sequence)
2.6.2.1. Tipo de certificado	Indica la naturaleza del certificado	Sí	Tipo= CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (de nivel medio) (String UTF8) Size = 100 OID: 2.16.724.1.3.5.4.2.1
2.6.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	Sí	Entidad Suscriptora = p. ej: MINISTERIO DEL INTERIOR (String UTF8) Size = 80 OID: 2.16.724.1.3.5.3.2.2
2.6.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	Sí	NIF entidad suscriptora ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.3.2.3
2.6.2.4. Correo electrónico	Correo electrónico de contacto	O	Correo electrónico de contacto. P. ej: buzon@dgp.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.3.2.9
2.6.2.5. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluida el firmante del certificado	O	Unidad = p. ej: DIRECCION GENERAL DE LA POLICIA (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.3.2.10
2.6.2.6. Puesto o cargo	Puesto desempeñado por el firmante del certificado dentro de la administración.	O	Puesto = p. ej: SUBINSPECTOR (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.3.2.11

[10] Extensión generalmente utilizada por productos S/MIME

Campo	Contenido	R	Observaciones
2.6.3. User Principal Name (UPN)	UPN para smart card logon	O	Campo destinado a incluir el smart card logon de Windows para el responsable del certificado.
2.6.4. Seudónimo	Seudónimo		Seudonimo= p. ej: NIP1111 O.I.D 2.16.724.1.3.5.4.2.12

12 TRANSICION

Los nuevos perfiles de certificados de las Administraciones Públicas entraran en vigor el 1 de julio de 2016, si bien se establece un periodo máximo de 12 meses (hasta el 1 de julio de 2017) para que los Prestadores de Servicios de Confianza expidan los certificados electrónicos conforme a los requisitos recogidos en el presente anexo.
No obstante, los certificados de empleado público con seudónimo serán de aplicación con la publicación de la resolución del Secretario de Estado para la Función Pública a que hace referencia el artículo 24.3 del real Decreto 1671/2009.
Los certificados expedidos a empleados públicos acorde a las especificaciones anteriores de los perfiles serán válidos hasta el fin de su caducidad, tal y como establecen las medidas transitorias del artículo 51 del Reglamento eIDAS para los certificados de persona física.

13 CUADROS RESUMEN

Dentro del concepto **VALORES** se marcan entrecomillados y en negrita aquellos valores que deberán aparecer exactamente tal y como están aquí expresados en los campos/ extensiones indicados.

CONCEPTO	OBLIGATORIO/RECOMENDABLE	VALORES
Niveles de aseguramiento	Implícito en Objeto Identidad Administrativa Indicado en CertificatePolicies	• OID:2.16.724.1.3.5.5.1=SEDE ELECTRONICA (Nivel Alto) • OID:2.16.724.1.3.5.5.2=SEDE ELECTRONICA (Nivel Medio/sustancial) • OID:2.16.724.1.3.5.6.1=SELLO ELECTRONICO (Nivel Alto) • OID:2.16.724.1.3.5.6.2=SELLO ELECTRONICO (Nivel Medio/sustancial) • OID:2.16.724.1.3.5.7.1=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (Nivel Alto) • OID:2.16.724.1.3.5.7.2=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (Nivel Medio/sustancial) • OID:2.16.724.1.3.5.4.1=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (Nivel Alto) • OID:2.16.724.1.3.5.4.2=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (Nivel Medio/sustancial)
Objeto Identidad Administrativa	Obligatorio. OID específico por perfil definido en RD 1671/2009 y por nivel de aseguramiento	

CONCEPTO	OBLIGATORIO/RECOMENDABLE	VALORES
Algoritmos criptográficos	Obligatorios	AC raíz y subraíz (Alto y Medio/sustancial): mínimo SHA-256, RSA-4096 Certificados finales (Alto): mínimo SHA-256, RSA-2048 Certificados finales (Medio/sustancial): mínimo SHA-256, RSA-1024
Codificación UTF8	Obligatoria	
Certificado CA subordinada	Recomendable	Perfil Orientativo. Los valores proporcionados en este documento pretenden servir como ejemplos en posibles nuevas implementaciones.
Validez de los certificados	Recomendado	5 años para los certificados de Sello, Empleado Público. 27 meses para los certificados de Sede.
Criterios de composición del campo CN para un certificado de empleado público	Obligatorios	• Incluir obligatoriamente el NOMBRE, de acuerdo con lo indicado en el DNI/NIE. • Incluir obligatoriamente el PRIMER Y SEGUNDO APELLIDO, separados únicamente por un espacio en blanco, de acuerdo con lo indicado en el DNI/NIE. En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter). • Incluir obligatoriamente el número de DNI/NIE, junto con la letra de control, de acuerdo con lo indicado en el DNI/NIE. • Incluir obligatoriamente un SÍMBOLO o CARÁCTER que separe el nombre y apellidos del número de DNI. • Se podrá incluir opcionalmente el literal "DNI" antes del número de DNI/NIE. • Se podrá incluir opcionalmente un literal (AUTENTICACION, FIRMA o CIFRADO) que identifique la tipología del certificado. Este identificador siempre será al final del CN y entre paréntesis. En el caso de un nivel de aseguramiento medio/sustancial, si se agrupan varios perfiles en un único certificado, no se deberá incluir esta opción.
Criterios de composición del campo CN para un certificado de empleado público con seudónimo	Obligatorios	• Incluir obligatoriamente el PUESTO O CARGO o literal 'SEUDONIMO', • Incluir obligatoriamente un SÍMBOLO o CARÁCTER que separe el cargo/literal del seudónimo del titular del certificado • Incluir obligatoriamente el SEUDONIMO, • Incluir obligatoriamente un SÍMBOLO o CARÁCTER que separe el seudónimo del organismo en que presta los servicios el titular del certificado • Incluir obligatoriamente el NOMBRE OFICIAL DEL ORGANISMO, tal y como figura en el boletín oficial correspondiente. • Se podrá incluir opcionalmente un literal (AUTENTICACION, FIRMA o CIFRADO) que identifique la tipología del certificado. Este

CONCEPTO	OBLIGATORIO/RECOMENDABLE	VALORES
		identificador siempre estará al final del CN y entre paréntesis. En el caso de un nivel de aseguramiento medio/sustancial, si se agrupan varios perfiles en un único certificado, no se deberá incluir esta opción.

CERTIFICADO	CAMPOS OBLIGATORIOS	VALORES
SEDE ELECTRÓNICA	• Version • Serial Number • Issuer Distinguished Name (Country (C), Organization (O), Organizational Unit (OU), Common Name (CN)) • Validity (Not Before, Not After) • Subject (Country (C), Locality (L), Organization (O), Organizational Unit (OU), Organizational Unit (OU), Serial Number, OI, Business Category, jurisdictionCountryName) • Subject Alternative Names: dnsName • Subject Public Key Info • Signature Algorithm	• V3 • Número de serie • Nombre de la entidad emisora • Recomendado 27 meses • C="**ES**", L= Ciudad, O=Organización, OU= **"SEDE ELECTRONICA**", OU=Nombre descriptivo de la Sede, SN=CIF, Organization Identifier= Identificador de la organización según ETSI EN 319 412-1, BC= "Government Entity", jurisdictionCountryName='ES', • SAN: dnsName=Nombre de dominio de la Sede • Clave pública de la Sede • Algoritmo de Firma
SELLO ELECTRÓNICO	• Version • Serial Number • Issuer Distinguished Name (Country (C), Organization (O), Organizational Unit (OU), Common Name (CN)) • Validity (Not Before, Not After) • Subject (Country (C), Organization (O), Organizational Unit (OU), OI, Common Name (CN)) • Subject Public Key Info • Signature Algorithm	• V3 • Número de serie • Nombre de la entidad emisora • Recomendado 5 años • C="**ES**", O=Organización, , OU= "**SELLO ELECTRONICO**", Organization Identifier= Identificador de la organización según ETSI EN 319 412-1, • Clave pública del sello • Algoritmo de Firma
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO	• Version • Serial Number • Issuer Distinguished Name (Country (C), Organization (O), Organizational Unit (OU), Common Name (CN)) • Validity (Not Before, Not After) • Subject (Country (C), Organization (O), Organizational Unit (OU), Serial Number, Common Name (CN)) • Subject Public Key Info • Signature Algorithm	• V3 • Número de serie • Nombre de la entidad emisora • Recomendado 5 años • C="**ES**", O=Organización, OU= "**CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO**", SerialNumber=DNI/NIE del empleado, o según ETSI EN 319 412-1, CN=Nombre , apellidos y DNI/NIE del empleado • Clave pública del certificado • Algoritmo de Firma

CERTIFICADO	CAMPOS OBLIGATORIOS	VALORES
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO CON SEUDÓNIMO	• Version • Serial Number • Issuer Distinguished Name (Country (C), Organization (O), Organizational Unit (OU), Common Name (CN)) • Validity (Not Before, Not After) • Subject (Country (C), Organization (O), Organizational Unit (OU), pseudonym, Common Name (CN)) • Subject Public Key Info • Signature Algorithm	• V3 • Número de serie • Nombre de la entidad emisora • Recomendado 5 años • C="**ES**", O=Organización, OU= "**CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO**", seudónimo, CN=seudónimo + organismo • Clave pública del certificado • Algoritmo de Firma

CERTIFICADO	EXTENSIONES OBLIGATORIAS*	VALORES

SEDE ELECTRÓNICA	• Authority Key Identifier
	• Subject Key Identifier
	• Key Usage
	• cRLDistributionPoint (distributionPoint)
	• Authority Info Access (Access Method, Access Location del OCSP y de caIssuer)
	• Extended Key Usage (Server Authentication)
	• Qualified Certificate Statements
	• Certificate Policies (Policy Identifier, Policy Qualifier ID [CPS Pointer, User Notice], EU qualified certificate policy Identifier QCP-w)
	• Subject Alternative Names (Directory Name)
		• Identificador de la clave pública de la CA
		• Identificados de la clave pública del subscriptor
		• **"Digital Signature", "Key Encipherment"**
		• Información de acceso a la CRL
		• Información de acceso a OCSP, información de acceso al certificado de la CA emisora
		• Server Authentication
		• Qualified Certificate Statements:
		  o QcCompliance
		  o QcEuRetentionPeriod
		  o QcType- web
		  o QcPDS)
		• OID asignado por el PSC a la política bajo la que se emite el certificado, URL de la DPC y mensaje explícito, identificación de que es un certificado cualificado de sitio web, acorde al Reglamento UE 910/2014. EU qualified certificate policy Identifier:
		  o NIVEL ALTO: QCP-w
		  o NIVEL MEDIO/SUSTANCIAL: QCP-w

SELLO ELECTRÓNICO	• Authority Key Identifier • Subject Key Identifier • Key Usage • Extended Key Usage • CRLDistributionPoint (distributionPoint) • Authority Info Access (Access Method, Access Location del OCSP y de caIssuer)	• Identificador de la clave pública de la CA • Identificados de la clave pública del subscriptor • **"Digital Signature", "Content Commitment", "Key Encipherment", ("Data Encipherment")** • **"Email Protection", "Client Authentication"** • Información de acceso a la CRL

CERTIFICADO	EXTENSIONES OBLIGATORIAS*	VALORES
	• Qualified Certificate Statements • Certificate Policies (Policy Identifier, Policy Qualifier ID [CPS Pointer, User Notice], EU qualified certificate policy Identifier) • Subject Alternative Names (Directory Name)	• Información de acceso a OCSP, información de acceso al certificado de la CA emisora • Qualified Certificate Statements o NIVEL ALTO: **"QcCompliance", "QcEuRetentionPeriod", "QcSSCD" , QcType- eseal, QcPDS** o NIVEL MEDIO/SUSTANCIAL: **"QcCompliance", "QcEuRetentionPeriod", QcType- eseal, QcPDS** • OID asignado por el PSC a la política bajo la que se emite el certificado, URL de la DPC y mensaje explícito. EU qualified certificate policy Identifier: o NIVEL ALTO: QCP-l-qscd o NIVEL MEDIO/SUSTANCIAL: QCP-l • IDENTIDAD ADMINISTRATIVA SELLO
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO	• Authority Key Identifier • Subject Key Identifier • CRLDistributionPoint (distributionPoint,) • Authority Info Access (Access Method, Access Location del OCSP y de caIssuer) • Key Usage • Extended Key Usage • Qualified Certificate Statements • Certificate Policies (Policy Identifier, Policy Qualifier ID [CPS Pointer, User Notice], EU qualified certificate policy Identifier (solo si ALTO FIRMA o MEDIO/SUSTANCIAL)) • Subject Alternative Names (Directory Name)	• Identificador de la clave pública de la CA • Identificados de la clave pública del subscriptor • Información de acceso a la CRL • Información de acceso a OCSP, información de acceso al certificado de la CA emisora • Key Usage o FIRMA ALTO: **"Content Commitment"** o AUTENTICACIÓN ALTO: **"Digital Signature"** o CIFRADO ALTO: **"Key Encipherment", "Data Encipherment"** o FIRMA Y AUTENTICACIÓNNIVEL MEDIO/SUSTANCIAL: **"Digital Signature", "Content Commitment", "Key Encipherment",** • Extended Key Usage o AUTENTICACIÓN ALTO: **"Email Protection", "Client Authentication"** o CIFRADO ALTO: **"Email Protection", "Client Authentication"** o FIRMA Y AUTENTICACIÓN NIVEL MEDIO/SUSTANCIAL: **"Email Protection", "Client Authentication"** • Qualified Certificate Statements

CERTIFICADO	EXTENSIONES OBLIGATORIAS*	VALORES
		○ NIVEL ALTO FIRMA: **"QcCompliance", "QcEuRetentionPeriod", "QcSSCD", QcType- esign, QcPDS** ○ NIVEL MEDIO/SUSTANCIAL: **"QcCompliance", "QcEuRetentionPeriod", , QcType- esign, QcPDS** • OID asignado por el PSC a la política bajo la que se emite el certificado, URL de la DPC y mensaje explícito. EU qualified certificate policy Identifier: ○ NIVEL ALTO FIRMA: QCP-n-qscd ○ NIVEL ALTO AUTENTICACIÓN: NCP+ ○ NIVEL MEDIO/SUSTANCIAL: QCP-n • IDENTIDAD ADMINISTRATIVA EMPLEADO PUBLICO
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO CON SEUDÓNIMO	• Authority Key Identifier • Subject Key Identifier • CRLDistributionPoint (distributionPoint,) • Authority Info Access (Access Method, Access Location del OCSP y de caIssuer) • Key Usage • Extended Key Usage • Qualified Certificate Statements • Certificate Policies (Policy Identifier, Policy Qualifier ID [CPS Pointer, User Notice], EU qualified certificate policy Identifier) • Subject Alternative Names (Directory Name)	• Identificador de la clave pública de la CA • Identificados de la clave pública del subscriptor • Información de acceso a la CRL • Información de acceso a OCSP, información de acceso al certificado de la CA emisora • Key Usage ○ FIRMA ALTO: **"Content Commitment"** ○ AUTENTICACIÓN ALTO: **"Digital Signature"** ○ CIFRADO ALTO: **"Key Encipherment", "Data Encipherment"** • FIRMA Y AUTENTICACIÓN NIVEL MEDIO/SUSTANCIAL: **"Digital Signature", "Content Commitment", "Key Encipherment",** Extended Key Usage ○ AUTENTICACIÓN ALTO: **"Email Protection", "Client Authentication"** ○ **CIFRADO ALTO: "Email Protection", "Client Authentication"** ○ FIRMA Y AUTENTICACIÓN NIVEL MEDIO/SUSTANCIAL: **"Email Protection", "Client Authentication"** • Qualified Certificate Statements ○ NIVEL ALTO FIRMA: **"QcCompliance", "QcEuRetentionPeriod",**

CERTIFICADO	EXTENSIONES OBLIGATORIAS*	VALORES
		"QcSSCD", , QcType- esign, QcPDS o NIVEL MEDIO/SUSTANCIAL: **"QcCompliance", "QcEuRetentionPeriod", , QcType- esign, QcPDS** • OID asignado por el PSC a la política bajo la que se emite el certificado, URL de la DPC y mensaje explícito. . EU qualified certificate policy Identifier: o NIVEL ALTO FIRMA: QCP-n-qscd o NIVEL MEDIO/SUSTANCIAL: QCP-n • IDENTIDAD ADMINISTRATIVA EMPLEADO PUBLICO CON SEUDONIMO

(*) Las extensiones son de obligada inclusión en estos perfiles de certificados, pero deberán estar marcadas como no críticas dentro de los certificados, a menos que los estándares las establezcan como críticas.

CERTIFICADO	CAMPOS RECOMENDABLES	VALORES
SEDE ELECTRÓNICA	• Issuer Distinguished Name (Locality, Serial Number, Organization Identifier) • Subject (Common Name)	• L= Localidad del PSC • SN= NIF del emisor • Serial Number= NIF de la entidad • OI= Identificador de la organización según ETSI EN 319 412 • CN=DNS de la sede (igual que el que figura en el Subject Alernative Names)
SELLO ELECTRÓNICO	• Issuer Distinguished Name (Locality, Serial Number, Organization Identifier) • Subject (Surname, Given Name, Organization Identifier)	• L= Localidad del PSC • SN= NIF del emisor • OI= Identificador de la organización según ETSI EN 319 412-1 • Surname=Apellidos y DNI del responsable, GivenName= Nombre del responsable • CN=Nombre descriptivo del sistema • OI= Identificador de la organización según ETSI EN 319 412-1
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO	• Issuer Distinguished Name (Locality, Serial Number) • Subject (Organizational Unit (OU), Organizational Unit (OU), Organization Identifier ,Title, Surname, Given Name)	• L= Localidad del PSC • SN= NIF del emisor • OU=Unidad del Empleado, • OU=NRP o NIP, • OI= Identificador de la organización según ETSI EN 319 412-1, • Title= Puesto o cargo del empleado, • SN= Apellidos y DNI del responsable, • GN= Nombre del responsable

CERTIFICADO	CAMPOS RECOMENDABLES	VALORES
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO CON SEUDONIMO	• Issuer Distinguished Name (Locality, Serial Number, Organization Identifier) • Subject (Organizational Unit (OU), , Organization Identifier ,Title)	• L= Localidad del PSC • SN= NIF del emisor • OI= Identificador de la organización según ETSI EN 319 412-1 • OU=Unidad del Empleado, • OI= Identificador de la organización según ETSI EN 319 412-1 • Title= Puesto o cargo del empleado

CERTIFICADO	EXTENSIONES RECOMENDABLES	VALORES
SEDE ELECTRÓNICA	• Issuer Alternative Name	• rfc822Name=Correo electrónico de la CA emisora
SELLO ELECTRÓNICO	• Issuer Alternative Name • Subject Alternative Names	• rfc822Name=Correo electrónico de la CA emisora • rfc822Name=Correo electrónico de contacto del Sello
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO	• Issuer Alternative Name • Subject Alternative Names	• rfc822Name=Correo electrónico de la CA emisora • rfc822Name=Correo electrónico de contacto del empleado, User Principal Name (UPN)=nombre de inicio de sesión en Windows
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO CON SEUDÓNIMO	• Issuer Alternative Name • Subject Alternative Names	• rfc822Name=Correo electrónico de la CA emisora • rfc822Name=Correo electrónico de contacto de la unidad (genérico), User Principal Name (UPN)=nombre de inicio de sesión en Windows

CERTIFICADO	CAMPOS "IDENTIDAD ADMINISTRATIVA" FIJOS	VALORES
SELLO ELECTRÓNICO	• Tipo de certificado • Nombre de la entidad suscriptora • NIF entidad suscriptora •	• OID: 2.16.724.1.3.5.6.*x*.1 = **"SELLO ELECTRONICO"** • OID: 2.16.724.1.3.5.6..x.2 = Entidad Suscriptora (Organización) OID: 2.16.724.1.3.5.6.x.3 = NIF entidad suscriptora *Donde x tiene valor 1 para un Nivel de Aseguramiento Alto y 2 para Medio/Sustancial*
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO	• Tipo de certificado • Nombre de la entidad suscriptora • NIF entidad suscriptora • DNI/NIE del responsable • Nombre de pila • Primer apellido • Segundo apellido	• OID: 2.16.724.1.3.5.7.x.1 = **"CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO"** • OID: 2.16.724.1.3.5.7.x.2 = Entidad Suscriptora (Organización) • OID: 2.16.724.1.3.5.7.x.3 = NIF entidad suscriptora • OID: 2.16.724.1.3.5.7.x.4 = DNI/NIE responsable • OID2.16.724.1.3.5.7.x.6 = Nombre de pila del responsable del certificado

CERTIFICADO	CAMPOS "IDENTIDAD ADMINISTRATIVA" FIJOS	VALORES
		• OID: 2.16.724.1.3.5.7.x.7 = Primer apellido del responsable del certificado • OID: 2.16.724.1.3.5.7.x.8 = Segundo apellido del responsable del certificado *Donde x tiene valor 1 para un Nivel de Aseguramiento Alto y 2 para Medio/Sustancial*
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO CON SEUDÓNIMO	• Tipo de certificado • Nombre de la entidad suscriptora • NIF entidad suscriptora • seudónimo	• OID: 2.16.724.1.3.5.4.x.1 = **"CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO"** • OID: 2.16.724.1.3.5.4.x.2 = Entidad Suscriptora (Organización) • OID: 2.16.724.1.3.5.4.x.3 = NIF entidad suscriptora • *OID: 2.16.724.1.3.5.4.x.12 = seudónimo del empleado* *Donde x tiene valor 1 para un Nivel de Aseguramiento Alto y 2 para Medio/Sustancial*

CERTIFICADO	CAMPOS "IDENTIDAD" ADMINISTRATIVA OPCIONALES	
SEDE ELECTRÓNICA	• Ninguno	
SELLO ELECTRÓNICO	• DNI/NIE del responsable • Nombre de pila • Primer apellido • Segundo apellido • Correo electrónico • Denominación de sistema o componente	• OID: 2.16.724.1.3.5.6..x.4 = DNI/NIE responsable • 2.16.724.1.3.5.6.x.5 = Nombre descriptivo del sistema de sellado automático • OID: 2.16.724.1.3.5.6.x.6 = Nombre de pila del responsable del certificado • OID: 2.16.724.1.3.5.6.x.7 = Primer apellido del responsable del certificado • OID: 2.16.724.1.3.5.6.x.8 = Segundo apellido del responsable del certificado • OID: 2.16.724.1.3.5.6.x.9 = Correo electrónico de la persona responsable del sello *Donde x tiene valor 1 para un Nivel de Aseguramiento Alto y 2 para Medio/Sustancial*
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO	• Número de identificación de personal • Correo electrónico • Unidad organizativa • Puesto o cargo	• OID2.16.724.1.3.5.7.x.5 = NRP o NIP del empleado • OID: 2.16.724.1.3.5.7.x.9 = Correo electrónico del empleado • OID: 2.16.724.1.3.5.7.x.10 = Unidad del empleado • OID: 2.16.724.1.3.5.7.x.11 = Puesto o Cargo del empleado *Donde x tiene valor 1 para un Nivel de Aseguramiento Alto y 2 para Medio/Sustancial*

CERTIFICADO	CAMPOS "IDENTIDAD" ADMINISTRATIVA OPCIONALES	
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO CON SEUDÓNIMO	• Número de identificación de personal • Correo electrónico • Unidad organizativa • Puesto o cargo	• OID2.16.724.1.3.5.4.x.5 = NRP o NIP del empleado • OID: 2.16.724.1.3.5.4.x.9 = Correo electrónico del empleado • OID: 2.16.724.1.3.5.4.x.10 = Unidad del empleado • OID: 2.16.724.1.3.5.4.x.11 = Puesto o Cargo del empleado • *Donde x tiene valor 1 para un Nivel de Aseguramiento Alto y 2 para Medio/Sustancial*

14 ANEXO 1: Perfiles básicos de interoperabilidad para los certificados de persona física, representante de persona jurídica y representante de entidad sin personalidad jurídica, usados en las relaciones con la Administración General del Estado

Ante la falta de unos perfiles interoperables de persona física, jurídica, entidades sin personalidad jurídica, componente, sello de entidad, persona física con pertenencia a entidad… los recomendados en este documento han sido recogidos en el que parece un marco normativo más apropiado para ellos: la Resolución de la Política de Firma de la Administración General del Estado. De esta manera se da cumplimiento al mandato recogido en el artículo 24 del Real Decreto 1671/2009 de desarrollo parcial de la Ley 11/2007, por el que debe haber una política de firma y certificados, de la Administración General del Estado, constituida por las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación, lo que, afecta, a las relaciones de la Administración con los ciudadanos y entre sus distintos órganos.

En todo caso, los perfiles de los certificados, recogidos en esta Política de Firma y Perfiles de certificados electrónicos, estarán en continua actualización, para adaptarse al estado del arte. Especialmente, a lo que pueda derivarse de normativa de la Unión Europea. Para su actualización se convocará al grupo de trabajo correspondiente, a través de la CPCSAE.

14.1 Perfiles para los certificados de persona física, persona física representante de persona jurídica y persona física representante de entidad sin personalidad jurídica

14.1.1 Reglas para **todos:**

- Longitud mínima de clave pública del certificado de usuario: **2048 bits**.
- Longitud mínima de clave del certificado de la CA: **2048 bits**.

Transitoriamente, los certificados de usuario de **1024 bits**, se podrán seguir utilizando en tanto en cuanto las Autoridades de Certificación no completen su migración y la plataforma @Firma los dé por válidos.

14.1.2 Personas **Físicas**

14.1.2.1 Normativa técnica

ETSI ha elaborado normas europeas en cumplimiento del Mandato M/460 de la Comisión Europea para racionalizar los estándares en torno a la firma electrónica. La familia ETSI EN 319 412 especifica el contenido de los certificados expedidos a personas físicas, jurídicas o certificados de sititos web. Los nuevos certificados deberán ajustarse a dichas especificaciones.

En concreto, la parte 2 de este documento, ETSI EN **319 412-2 v2.1.1** (Part 2: *Certificate profile for certificates issued to natural persons*) define los requisitos del contenido de certificados emitidos a personas físicas. El perfil se basa en las recomendaciones IETF RFC 5280 y el estándar ITU-T X.509.

14.1.2.2 Propuesta

El Prestador de Servicio de Certificación tendrá la obligación de verificar la identidad del firmante del certificado.

- Codificación del campo Subject

Campo	**Contenido**	**Ejemplo**
Country	País	ES
Common Name	Se detalla posteriormente	
Given name	Nombre (como consta en el DNI/NIE)	Pedro
Surname	Apellidos (como consta en el DNI/NIE)	López Martínez
Serial Number	NIF del titular (NIF es el número y letra que aparece en el DNI o NIE según corresponda) o codificación acorde a ETSI EN 319 412-1	123456789Z IDCES-123456789Z

"Country" especifica el contexto en el que el resto de atributos debe ser entendido. No implica necesariamente nacionalidad del "subject" o país de emisión del certificado.

Es deseable que exista algún campo que permita la posibilidad de separar el primer apellido del segundo de forma univoca.

- Codificación del atributo Common Name

Los datos de identificación pueden incluirse en el **Common Name del Subject** del certificado. Se propone la siguiente estructura orientativa:

Obligatorios
Apellidos y Nombre del titular del certificado En MAYÚSCULAS, separados únicamente por un espacio en blanco, de acuerdo con lo indicado en el DNI/NIE. En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter)
Espacio en blanco
Guión, u otro símbolo o carácter Separa los apellidos y el nombre del número de identificación fiscal.
Espacio en blanco
Número de identificación fiscal Número de identificación fiscal del titular, NIF, de acuerdo con lo indicado en su DNI o NIE. Al NIF, también se le llama DNI o NIE.

Opcionales
Etiqueta **NOMBRE**, De usarse, va delante de apellidos y nombre del titular, separada por un espacio.
Etiqueta **NIF** o **DNI** o **NIE** El término NIF abarca tanto a DNI como a NIE. Se colocará tras el guión, u otro símbolo o carácter de separación, y delante del número de identificación fiscal, separada, de ambos, por un espacio. Caso de optar por la etiqueta DNI o NIE, en lugar de NIF, se usará aquella que corresponda.
Literal **(AUTENTICACION, FIRMA o CIFRADO)** Identifica la tipología del certificado. En el caso de que se agrupen varios perfiles en un único certificado, no se deberá incluir esta opción. Este identificador siempre estará al final del Common Name del Subject y entre paréntesis, separado, por un espacio en blanco, del número de identificación fiscal.

Ejemplos:

DE LA CAMARA ESPAÑOL JUAN ANTONIO - DNI 00000000G (AUTENTICACION)

DE LA CAMARA ESPAÑOL JUAN ANTONIO - DNI 00000000G

NOMBRE DE LA CAMARA ESPAÑOL JUAN ANTONIO - NIF 00000000G

DE LA CAMARA ESPAÑOL JUAN ANTONIO |00000000G (AUTENTICACION)

DE LA CAMARA ESPAÑOL JUAN ANTONIO |00000000G

NOMBRE ESPAÑOL ESPAÑOL JUAN - NIF 99999999R

NOMBRE EXTRANJERO EXTRANJERO JUAN – NIF X1234567H

NOMBRE EXTRANJERO EXTRANJERO JUAN – NIE X1234567H

14.1.3 **Persona Física Representante ante las Administraciones de Persona Jurídica o Entidad sin Personalidad Jurídica**

14.1.3.1 Introducción

Los “certificados de representante” permiten ofrecer a una persona física representante de una persona jurídica la herramienta de firma electrónica con la que realizar trámites con la Administración en nombre de la persona jurídica representada.

El certificado además de identificar a la persona física representante como titular/firmante y acreditar sus poderes de representación sobre la persona jurídica representada, debe incluir información sobre la misma, en cuyo nombre se actúa. En consecuencia, es necesario vincular a la persona jurídica con la firma de su representante.

El artículo 11.4 de la Ley 59/2003, de 19 de diciembre, de firma electrónica (en adelante, LFE) requiere a los prestadores que expiden certificados reconocidos que admiten una relación de representación incluir la indicación del documento público:

> *“4. Si los certificados reconocidos admiten una relación de representación incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales, de conformidad con el apartado 2 del artículo 13.”*

El artículo 3.25 del Reglamento 910/2014 de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior [eIDAS] define como «sello electrónico», los datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos. Los sellos electrónicos así definidos carecen del carácter jurídico de firma necesario para dar cumplimiento al artículo 11 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Por tanto en el Reglamento eIDAS no existen los certificados de firma de Persona Jurídica que existían en la Ley 59/2003 de firma electrónica, en los cuales la Persona Jurídica tenía capacidades de firma y no solo de garantía de origen e integridad de los datos. Por tanto se hace necesario identificar un tipo equivalente de certificado de firma de una Persona Jurídica ante las Administraciones Públicas.
Este certificado será un certificado de Persona Física que es Representante de una Persona Jurídica o Entidad sin Personalidad Jurídica, en las cuales el Representante tiene plenas capacidades para actuar en nombre de la Persona Jurídica o Entidad sin Personalidad Jurídica ante las Administraciones Públicas.

Al igual que en los certificados de firma de Persona Jurídica de la Ley 59/2003 el custodio del certificado tenía todas las capacidades para actuar en nombre de la Persona Jurídica, en el perfil normalizado propuesto para los certificados de Representante de Persona Jurídica o Entidad sin Personalidad Jurídica, el Representante deberá tener todas las capacidades para actuar en nombre de la Persona Jurídica, al menos ante las Administraciones Públicas.

14.1.3.2 Normativa técnica

ETSI ha elaborado normas europeas en cumplimiento del Mandato M/460 de la Comisión Europea para racionalizar los estándares en torno a la firma electrónica. La familia ETSI EN 319 412 especifica el contenido de los certificados expedidos a personas físicas, jurídicas o certificados de sititos web. Los nuevos certificados deberán ajustarse a dichas especificaciones.

En concreto, la parte 2 de este documento, ETSI EN **319 412-2 v2.1.1** (Part 2: *Certificate profile for certificates issued to natural persons*) define los requisitos del contenido de certificados emitidos a personas físicas. El perfil se basa en las recomendaciones IETF RFC 5280 y el estándar ITU-T X.509.

La información utilizada para definir la identidad y atributos del firmante de un certificado de persona física, sin pseudónimos, se desglosa en los siguientes campos:

- Campo “Subject”, utilizando los atributos commonName, surname (o givenName) y countryName. En el atributo SerialNumber, se puede incluir el DNI del firmante.
- Extensión “Subject Alternative Names”. No se incluye ninguna restricción.
- Extensión “Subject Directory attributes”. No deben incluirse los atributos del campo Subject.

En el caso de existir una vinculación o relación con una persona jurídica como es el caso de los certificados de persona física representante de persona jurídica, se indica que la razón social puede ser incluida en el atributo “organizationName” y el NIF en el atributo “organizationIdentifier”:

> *“Additional attributes other than those listed above may be present. In particular, when a natural person subject is associated with an organization, the subject attributes **may** also identify such organization using attributes such as **organizationName** and **organizationIdentifier**. Certificates may include one or more semantics identifiers as specified in ETSI EN 319 412-1 [i.4], clause 5 which defines the semantics for the organizationIdentifier attribute”*

Finalmente, el borrador no detalla ni determina la información a incluir en el certificado para la indicación de los poderes de representación de la persona física.

14.1.3.3 Propuesta

El Prestador de Servicio de Certificación tendrá la obligación de verificar la identidad del apoderado y del poderdante, la vigencia de los poderes y que el alcance del poder contemple capacidad para actuar en nombre del poderdante en cualquier actuación administrativa con la Administración (bien específicamente o bien a través de un poder general).

No se utilizan campos con OID propietarios para facilitar la adaptación a los perfiles. Se usan los campos "Policy Identifier" para indicar que se trata de un certificado de representación general ante las Administraciones Públicas.

Para indicar los datos de representación, se ha optado por un formato normalizado que permita el tratamiento automatizado de los datos, incluido en el campo 'Description' del Subject, dando de esta forma cumplimiento al artículo 11.4 de la Ley 59/2003.

En todo caso los certificados deberán cumplir los requisitos del Reglamento eIDAS y de los estándares europeos ETSI EN 319 412 'Certifícate Profiles'. En concreto deberán contener las extensiones QCStatements acorde a ETSI EN 319 412-5 'Certifícate Profiles. Part 5: QCStatements'

- Codificación del campo Subject

Atributos	**Contenido**	**Ejemplo**
Country	País	ES
Common Name	Ver tabla especifica	12345678Z Pedro Antonio López (R: B0085974Z) FIRMA
Given name	Nombre (como consta en el DNI/NIE)	Pedro Antonio
Surname	Apellidos (como consta en el DNI/NIE)	López Martínez
Serial Number	número DNI/NIE Opcionalmente se podrá utilizar la semántica propuesta por la norma ETSI EN319 412-1	12345678Z o IDCES-12345678Z
organizationName	Razón Social, tal como figura en los registros oficiales.	Organización. S.L.
organizationIdentifier	NIF, tal como figura en los registros oficiales. Codificado Según la Norma Europea ETSI EN 319 412-1	VATES-B0085974Z
Description (2.5.4.13)	Codificación del documento público que acredita las facultades del firmante o los datos registrales	Reg: XXX /Hoja: XXX /Tomo:XXX /Sección:XXX /Libro:XXX /Folio:XXX /Fecha: dd-mm-aaaa /Inscripción: XXX

Atributos	Contenido	Ejemplo
		Notario: Nombre Apellido1 Apellido2 /Núm Protocolo: XXX /Fecha Otorgamiento: dd-mm-aaaa En Boletines Oficiales: Boletín: XXX/ */Fecha: dd-mm-aaaa /Numero resolución: XXX*

- Codificación del documento público que acredita las facultades del firmante o los datos registrales. Se presentan varias opciones, según si se ha consultado el Registro Mercantil o un Poder Notarial, u otro tipo de registro o documento oficial.
    - En el Registro Mercantil: Reg: XXX /Hoja: XXX /Tomo:XXX /Sección:XXX /Libro:XXX /Folio:XXX /Fecha: dd-mm-aaaa /Inscripción: XXX
    - Poder Notarial: Notario: Nombre Apellido1 Apellido2 /Núm Protocolo: XXX /Fecha Otorgamiento: dd-mm-aaaa
    - En el caso de que las facultades vengan indicadas en Boletines Oficiales: Boletín: XXX/ */Fecha: dd-mm-aaaa /Numero resolución: XXX*
    - Esta codificación podrá ampliarse en un futuro para considerar otro tipo de registros y documentos oficiales para los que se detecte la necesidad de disponer de certificados de representación general ante las Administraciones Públicas. Las codificaciones se publicarán como Publicación Oficial de la Secretaria de Estado de Administraciones Públicas.

      Se considera un periodo de adaptación de un año para incluir las codificaciones de los documentos públicos acorde a las especificaciones establecidas.

  Adicionalmente el Prestador de Servicios de Certificación, si lo considera necesario, podrá incluir está información u otra complementaria en otros campos del certificado, acorde a sus Políticas de Certificación.

- Codificación del atributo Common Name

  Se propone una codificación del campo Common Name que permite al usuario identificar el certificado como uno de representación, distinguiéndolo de uno de Persona Física básico, a través del literal ‘R’. Así mismo se permite identificar la Persona Jurídica representada para facilitar la selección de certificado en caso de una Persona Física que represente a varias Personas Jurídicas.

El campo tiene un tamaño máximo de 64 caracteres según la RFC 5280.

Campo	Contenido	Ejemplo	tamaño *
NIF	número DNI/NIE	12345678Z	10
Nombre	Tal y como figura en el DNI/NIE	Pedro Antonio	
Apellido 1	Tal y como figura en el DNI/NIE	López	
Literal	(R:		4
NIF de la empresa	NIF de la empresa, tal como figura en los registros oficiales.	B0085974Z	9
Literal	)		2
Literal (opcional)	**AUTENTIC, FIRMA o CIFRADO**		8

*(contando espacio en blanco posterior)

- Codificación de la extensión Certificate Policies

  Adicionalmente al campo 'Policy Identifier' que establezca el Prestador de Servicios de Certificación para hacer referencia a la Política del certificado concreto, y a los 'Policy Identifier' con los OIDs que correspondan según la normativa Europea EN 319 412, se deberá establecer obligatoriamente los siguientes 'Policy Identifier', que determinarán las condiciones particulares del certificado de representante:

  - representante de:
    - persona jurídica,
    - entidad sin personalidad jurídica
  - con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las AAPP
  - El Prestador de Servicio de Certificación ha verificado la identidad del apoderado y del poderdante, la vigencia de los poderes y que el alcance del poder contemple capacidad para actuar en nombre del poderdante en cualquier actuación administrativa con la Administración (bien específicamente o bien a través de un poder general). Y guarda la información relevante presentada para la expedición del certificado.
  - Acorde a la especificación de perfil de certificado de representante definida en este documento.

Campo	Contenido	Ejemplo
Policy Identifier	OID = 2.16.724.1.3.5.8. Indica que el certificado es un certificado de representante de **persona jurídica**, con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las AAPP	2.16.724.1.3.5.8

Campo	Contenido	Ejemplo
Policy Identifier	OID = 2.16.724.1.3.5.9. Indica que el certificado es un certificado de representante de **entidad sin personalidad jurídica**, con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las AAPP	2.16.724.1.3.5.9

- Resto de campos del certificado.

  No se establecen requisitos para el resto de los campos del certificado, aparte de seguir la normativa y estándares europeos en materia de certificados cualificados. El Prestador de Servicios de Certificación podrá incluir la información que considere relevante en otros campos del certificado, acorde a sus Políticas de Certificación. Esto incluye emitir los certificados en Dispositivo Cualificado de Creación de Firma, en software o en servidor, emitir un único certificado para distintos usos o uno específico por uso, etc

14.2 Otros perfiles

14.2.1 Componente

Se podría plantear el uso de certificados de sello, tal y como los describe el reglamento eIDAS, para la comunicación ente máquinas. No tendrían por qué cumplir el anexo III del reglamento eIDAS si no son cualificados[11]. En este caso se recomienda que tengan una estructura de los campos Subject y Common Name similares a los especificados en este documento para los certificados de sello.

En caso contrario, pueden darse dos alternativas.

Alternativa 1:
Los datos de identificación deben estar localizados en el **Common Name del Subject** del certificado, con la siguiente estructura:

Obligatorios
Razón Social titular del certificado en MAYÚSCULAS
Espacio en blanco
Guión, u otro símbolo o carácter, que separe la razón social y el número de identificación fiscal de la razón social
Espacio en blanco
Número de identificación fiscal de la razón social
Espacio en blanco

[11] Ver considerando 65 del eIDAS : Además de autenticar el documento expedido por la persona jurídica, los sellos electrónicos pueden utilizarse para autenticar cualquier activo digital de la persona jurídica, por ejemplo, programas informáticos o servidores

Opcionales
Etiqueta **ENTIDAD** De usarse, va delante de la razón social titular, separada por un espacio.
Etiqueta **CIF** o **NIF** De usarse, va delante del número de identificación fiscal, de la razón social, y detrás del guión u otro símbolo o carácter de separación, separada, de ambos, por un espacio.

Alternativa 2:
Los datos del campo Subject del certificado deberán tener la siguiente estructura:

	COMPONENTE
Country	(PrintableString) Se codificará de acuerdo a "ISO 3166-1- alpha-2 code elements" Size [RFC 5280] 3
CommonName	Dominio del componente / descripción del componente
Organization	**Razón Social del titular del certificado**
Organizational Unit	
SerialNumber/Organization Identifier	**Número de identificación fiscal** de la organización titular del certificado

Ejemplos:

	COMPONENTE
Country	ES
CommonName	Pasarela de pagos
Organization	AGENCIA TRIBUTARIA
Organizational Unit	DIT
SerialNumber	A28000001

14.2.2 Sello

Se recomienda que los certificados de sello tengan una estructura de los campos Subject y Common Name similares a los especificados en este documento para los certificados de sello de Administraciones Públicas. Ya que son certificados con usos similares, de esta forma se favorece la interoperabilidad.

14.2.3 Pertenencia a Entidad

Aquellos certificados expedidos a personas físicas, donde también se incluya información sobre la pertenencia del sujeto a una entidad concreta, se recomienda que

tengan una estructura de los campos Subject y Common Name similares a los especificados en este documento para los certificados de Empleado Público. Ya que son certificados con usos similares, de esta forma se favorece la interoperabilidad.

15 ANEXO 2: Referencias

-
- [1] ETSI EN 319 412 Certificates Profiles
  - Part 1: Overview and common data structures
  - Part 2: Certificate profile for certificates issued to natural persons
  - Part 3: Certificate profile for certificates issued to legal persons
  - Part 4: Certificate profile for web site certificates issued to organisations
  - Part 5: QCStatements
- [2] ETSI TS 119 312 V1.1.1 Electronic Signatures and Infrastructures (ESI);
- Cryptographic Suites
- [3] ETSI EN 319 411-2. Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- [4] IETF RFC 6960. X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP.
- [5] IETF RFC 3279. Actualizada por RFC 4055, RFC 4491, RFC 5480, RFC 5758 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile.
- [6] IETF RFC 5280. Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile.
- [7] IETF RFC 3739. Actualizada por RFC 3279, RFC 5756 Internet X.509 Public Key Infrastructure. Qualified Certificates Profile.
- [8] IETF RFC 4055. Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Actualizada por RFC 5756 Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters
- [9] IETF RFC 4491 y RFC 3279. Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- [10] ISO 3166-1, alpha-2 country codes.
- [11] ISO/IEC 9594-8/ITU-T X.509.
- [12] CCN-STIC-405. Guía de seguridad de las TIC. Algoritmos y parámetros para firma electrónica segura.
- [13] 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 y por la que se deroga la Directiva 1999/93/CE
- [14] Decisión de Ejecución (UE) 2015/1505 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones técnicas y los formatos

relacionados con las listas de confianza de conformidad con el artículo 22, apartado 5, 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.
- [15] Anexo del Reglamento de Ejecución (UE) 2015/1501 de la Comisión de 8 de septiembre de 2015 sobre el marco de interoperabilidad de conformidad con el artículo 12, apartado 8, 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.
- [16] 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.
- [17] ISO / IEC 29115: 2013 Information technology -- Security techniques -- Entity authentication assurance framework
- [18] ITU X.1254 Entity authentication assurance framework
- [19] ITU X.520 - ISO/IEC 9594-6 Information technology -- Open Systems Interconnection -- The Directory -- Part 6: Selected attribute types
- [20] CA/Browser Forum. Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.
- [21] CA/Browser Forum. Guidelines For The Issuance And Management of Extended Validation Certificates.