Perfiles de certificados electrónicos

Autor:	*Consejo Superior de Administración Electrónica*
Identificador de documento:	*2.16.724.1.3.1.1.2.3*
Grupo de trabajo:	*MITyC-MPR*
Versión:	*V 1.7.6*
Fecha:	21/07/2010
Fichero:	*Perfiles de certificados v1.7.6.docx*

Historia del documento:		
Fecha:	Versión:	Descripción:
26/12/07	V 1	Creación del documento.
27/02/08	V1.5	Corrección de OIDs de certificados erróneos y distribución de Subject Modificación de comentarios al documento distribuido Añadidos cuadros resumen
28/04/2008	V1.6	Corrección OIDs Identidad Administrativa Modificación perfil sede electrónica Revisión cuadros resumen
16/06/2008	V1.7	Indicado valor QcRetentionPeriod
18/11/2009	V1.7.3	Actualización documento para recoger los campos obligatorios definidos por el RD 1679/2009 del 18/11/2009 y los OIDs registrados por el Ministerio de la Presidencia
23/06/2010	V 1.7.5	Modificación de duración máxima de certificados y corrección de errores
21/07/2010	V 1.7.6	Actualización del documento para recoger los comentarios de diversos organismos de la AGE

ÍNDICE

1 Introducción

1.1 Objeto

El presente documento describe los perfiles de certificados derivados de la Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP). Dichos certificados son: certificado de sede electrónica, certificado de sello electrónico, y certificado de empleado público. Asimismo se incluye una definición para el certificado raíz de la PKI emisora.

A continuación 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 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 LAECSP (Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos), de acuerdo con las diversas configuraciones acordadas, atendiendo a los diferentes niveles de aseguramiento.

Según el artículo 24.1 del RD 1671/2009, de Desarrollo parcial de la Ley 11/2007, 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 por el que se regula el Esquema Nacional de Interoperabilidad, 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 dentro de su ámbito de actuación. 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 11/2007, de 22 de junio, la Ley 59/2003, de 19 de diciembre, de firma electrónica y sus desarrollos normativos.

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

2 Caracterización de los perfiles de certificados

En este apartado se describen los campos que componen los diferentes perfiles. 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.
Por lo tanto, consecuentemente los perfiles definidos de certificados digitales empleados en cada nivel dispondrán de un conjunto de elementos y características que los asocia a cada nivel.

Inicialmente se definen dos niveles de aseguramiento:

- Nivel medio:
  - Este nivel corresponde a una configuración de mecanismos de seguridad apropiada para la mayoría de aplicaciones.
  - El riesgo previsto por este nivel (siguiendo la recomendación de la OCDE):
    - Infracción de seguridad (ej: el robo de identidad)
    - Puede producir pérdidas económicas moderadas
    - Pérdida de información sensible o crítica.
    - Refutación de una transacción con impacto económico significativo.
  - Asimismo, el riesgo previsto por este nivel corresponde al nivel 3 de garantía previsto en la Política Básica de Autenticación de IDABC.

- Los mecanismos de seguridad aceptables incluyen los certificados X.509 en software. En los casos de certificados emitidos a personas, se corresponde con el de un "certificado reconocido", como se define en la Ley 59/2003, de firma electrónica, para firma electrónica avanzada, sin dispositivo seguro de creación de firma.

o 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 (siguiendo la recomendación de la OCDE):
  - Infracción de seguridad
  - Puede producir pérdidas económicas importantes
  - Pérdida de información altamente sensible o crítica.
  - Refutación de una transacción con impacto económico muy significativo.

- Asimismo, el riesgo previsto por este nivel corresponde al nivel 4 de garantía previsto en la Política Básica de Autenticación de IDABC.

- 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 "firma electrónica reconocida", como se define en la Ley 59/2003, de firma electrónica.

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

Certificados y perfiles	Nivel medio	Nivel alto
Sello para la actuación automatizada	➔ Perfil único firma, autenticación y cifrado. Sw y Hw	➔ Perfil único firma, autenticación y cifrado. Dispositivo Hardware Criptográfico/HSM
Sede electrónica administrativa	➔ Perfil único autenticación y cifrado. Sw y Hw	➔ Perfil único autenticación y cifrado. Dispositivo Hardware Criptográfico /HSM

Empleado público	➔ Perfil único firma, autenticación y cifrado. Sw y Hw ➔ Perfil independiente para firma, autenticación o cifrado[1]. Sw y Hw	➔ Perfil independiente para firma, autenticación y cifrado. DSCF (Dispositivo Seguro de Creación de Firma)

Todos los certificados 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

Existen dos clasificaciones para los distintos campos: "recomendables o no" y "fijos u opcionales", dependiendo de su importancia y necesidad, quedando todos los campos tipificados en unas de estos dos grupos.

2.2.1 Campos recomendables:

Existen 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, si bien, en el uso real de 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 se consideran **recomendables** 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**". No se podrán añadir ni modificar los usos de las claves definidos en los perfiles de este documento, correspondientes al campo Key Usage. Para el certificado de sede no se podrán establecer en el campo Extended Key Usage, usos que impliquen la realización de firma electrónica (no repudio). Para el certificado de sello no se podrán establecer en el campo Extended Key Usage, usos cuya finalidad sea la identificación de una maquina.

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.

[1] El certificado de cifrado es opcional.

2.2.2 Campos fijos u opcionales:

Al margen de la categoría anterior, existe otra clasificación de campos denominados “fijos u opcionales” que atañe exclusivamente para los campos incluidos en el nuevo objeto Identidad Administrativa definido en el presente documento. Los campos fijos son aquellos 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 una “F”, aquellos considerados como FIJOS, 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 sede electrónica son:

- Fijos:
  - Descripción del tipo de certificado
  - Nombre descriptivo de la sede electrónica
  - Denominación de Nombre del dominio / dirección IP
  - Nombre de la entidad suscriptora
  - Número de Identificación Fiscal de entidad suscriptora

- Opcionales: Ninguno

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
- Número de Identificación Fiscal de entidad

o 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

3 Identificador de objetos

Como parte de la estandarización, los campos, principalmente alineados a la RFC 5280 (X509 v3), 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 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 objectId es 2.5.4.3) o serialNumber (cuyo objectId 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 nuevo, se ha optado por la siguiente opción para asignarles los ObjectIds:

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 podría utilizarlo.

Ej:

2.16.724.1.3.5.1.1=*SEDE ELECTRONICA (Nivel Alto)*
2.16.724.1.3.5.1.2=*SEDE ELECTRONICA (Nivel Medio)*
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)*
2.16.724.1.3.5.3.1*CERTIFICADO ELECTRÓNICO DE EMPLEADO PUBLICO (Nivel Alto)*
2.16.724.1.3.5.3.2= *CERTIFICADO ELECTRÓNICO DE EMPLEADO PUBLICO (Nivel Medio)*

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.

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)

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 reconocidos.

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 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, aún 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.

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 Pública Estatal.

En cuanto a las normas de codificación de los campos, en general no hay reglas complejas de nomenclatura puesto que recomendado por la RFC 5280 se usa UTF-8[2] 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.

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 Administración General del Estado.

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.

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

El personal al servicio de la Administración Pública Estatal sigue la siguiente distribución, tal y como se refleja en el Boletín Estadístico del personal al servicio de las Administraciones Públicas:

- ADMINISTRACION GENERAL DEL ESTADO
  - INSTITUCIONES SANITARIAS S. SOCIAL
  - MINISTERIOS Y OO.AA. Y AREAS VINCULADAS
    - DOCENCIA NO UNIVERSITARIA
    - CENTROS PENITENCIARIOS
    - SEGURIDAD SOCIAL (ENTIDADES GESTORAS Y SERVICIOS COMUNES)
    - PATRIMONIO NACIONAL
    - AGENCIA ESTATAL ADMINISTRACION TRIBUTARIA
    - MINISTERIOS Y OO.AA.
      - MINISTERIO DE IGUALDAD
      - MINISTERIO DE AGRICULTURA, PESCA Y ALIMENTACION
      - MINISTERIO DE ASUNTOS EXTERIORES Y COOPERACION
      - MINISTERIO DE EDUCACIÓN
      - MINISTERIO DE DEFENSA
      - MINISTERIO DE ECONOMIA Y HACIENDA
      - MINISTERIO DE CIENCIA E INNOVACIÓN
      - MINISTERIO DE FOMENTO
      - MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
      - MINISTERIO DE INTERIOR
      - MINISTERIO DE JUSTICIA
      - MINISTERIO DE MEDIO AMBIENTE
      - MINISTERIO DE PRESIDENCIA
      - MINISTERIO DE SANIDAD Y CONSUMO
      - MINISTERIO DE TRABAJO Y ASUNTOS SOCIALES
      - MINISTERIO DE VIVIENDA
      - MINISTERIO DE POLÍTICA TERRITORIAL
- FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO
- FUERZAS ARMADAS
- ADMINISTRACION DE JUSTICIA
- ENTIDADES PUBLICAS EMPRESARIALES Y ORGANISMOS PUBLICOS CON REGIMEN ESPECIFICO

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 el cuenta el formato requerido (string UTF8 [RFC 5280] size 128) siguiendo en la medida de lo posible la nomenclatura descrita en documento “Unidades.doc”

A continuación se describe una pequeña muestra:

- SECRETARIA GENERAL
- DIVISION DE PROYECTOS TECNOLOGICOS PARA LA ADMINISTRACION GENERAL DEL ESTADO
- UNIDAD DE VERIFICACION Y CONTROL
- UNIDAD DE APOYO DE LA DIRECCION GENERAL
- VICESECRETARIA GENERAL TECNICA
- GABINETE TECNICO
- UNIDAD SERVICIOS ECONOMICOS Y FINANCIEROS
- AREA DE RECURSOS HUMANOS Y ADMINISTRACION ECONOMICA
- AREA GENERAL DE APOYO ADMINISTRATIVO
- UNIDAD DE SOPORTE INFORMATICO
- UNIDAD DE RECURSOS HUMANOS

Las unidades más frecuentes vienen descritas en el fichero adjunto, aunque no se encuentran todas las existentes o en vigor en la Administración General del Estado.El documento de descripción unidades dispone tanto de las Entidades suscriptoras, como de las Unidades a las que está adscrito un puesto o cargo con las que figuran en el Registro Central de Personal a 14/11/2007, se trata de una "foto" sujeta a cambios. El documento está accesible en el portal *Funciona* del Ministerio de de la Presidencia en el enlace http://www.funciona.es/rcp/tablasportal/tablastxt.htm .

Si bien en el fichero anterior en formato de hoja de cálculo se ha representado un subconjunto de campos, el documento "Unidades" disponible en *Funciona*, tiene una estructura dividida en posiciones que explicamos a continuación, y que se describe en el fichero "Descripción", dentro del mismo portal:

CONCEPTO	POSICIONES
Código mnemotécnico	1-19
Código numérico	21-26
Denominación	28-127
Nivel de la unidad	129-129
Código numérico de la unidad de la que depende	131-136
Fecha de última actualización (AAAAMMDD)	138-145
Provincia	147-148
Localidad	150-152

⊙ 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 el cuenta el formato requerido (string UTF8 [RFC 5280] size 128), siguiendo, en la medida de lo posible, la nomenclatura descrita en documento vinculado “Tabla descripción puestos RCP-APE 14-11-2007.xls “ adjunto. Se trata de una “foto” a día 14/11/07 en el Registro Central de Personal, sujeta a variación diaria e incluye diferentes hojas en función de los colectivos de personal recogidos. Dichas descripciones están en texto libre, excepto para personal laboral de convenio único.

Dentro del documento se incluyen tres hojas con las descripciones más frecuentes de:

1. Descripciones de puestos de personal funcionario.
2. Descripciones de puestos de personal laboral de convenio único de la AGE.
3. Descripciones de puestos de personal laboral de otros convenios y fuera de convenio.

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.

Los puestos más frecuentes vienen descritos en el fichero adjunto, a continuación se describe una pequeña muestra:

- JEFE DE SECCION'
- 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

Si bien el artículo 18.2 de la LAECSP determina la inclusión del número de identificación fiscal y la denominación correspondiente, pudiendo contener la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos, se recomienda la inserción de esta identidad, dada la garantía que ello ofrece a los destinatarios de las firmas y procesos de autenticación electrónica.

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 electrónico"*
⊙ 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"*
⊙ 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"*

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, aunque el NIF correspondiente se asociaría al organismo o Departamento ministerial del que dependiera.
Ejemplo del campo “Denominación de sistema o componente informático“: “Sello electrónico de la Dirección General de Modernización Administrativa”, y como nombre de la entidad suscriptora: “Ministerio de 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 al sistema o plataforma que realiza la aplicación de la identificación y firma electrónica.
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 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”
- “060”
- “Portal oficial del Ministerio de la Presidencia”

En cuanto al empleo de un nombre de dominio o una dirección IP para designar la sede, se dispone de mayor flexibilidad en asignación de nombres de dominio y subdominio que direcciones IP. El nombre del dominio o subdominio, va a determinar en muchas ocasiones la identidad de la sede electrónica ya que no se concibe la emisión de certificados múltiples de sede electrónica para un mismo nombre de dominio, subdominio, o dirección IP.

Campos variables	Ejemplos
⊙ Descripción del tipo de certificado	*“sede electrónica”*
⊙ Nombre descriptivo de la sede electrónica (se incluyen varios ejemplos)	⊙ *“CENTRO DE TRANSFERENCIA DE TECNOLOGIAS DE LAS ADMINISTRACIONES PUBLICAS”* ⊙ *“060”* ⊙ *“PORTAL OFICIAL DE LA PRESIDENCIA”*
⊙ Denominación de Nombre del dominio / dirección IP (se incluyen varios ejemplos)	⊙ *“ctt.mpr.es”* ⊙ *“060.es”* ⊙ *“mpr.es”*
⊙ Nombre de la entidad suscriptora	*“MINISTERIO DE LA PRESIDENCIA”*
⊙ 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 nos nombres de dominio/subdominio o dirección IP 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 / dirección IP” 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.

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.

5.3 Empleado público

En el caso de los certificados del personal al servicio de las Administraciones Públicas, 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 LA PRESIDENCIA"*
⊙ Número de Identificación Fiscal de entidad suscriptora	*"S2833002"*
⊙ Dirección de correo electrónico	*"juanantonio.delacamara.espanol@mpr.es"*
⊙ Unidad a la que está adscrito el cargo o puesto que desempeña el empleado público	⊙ *"DIVISION DE PROYECTOS TECNOLOGICOS PARA LA ADMINISTRACION GENERAL DEL ESTADO"* ⊙ *"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:

1. En general, se recomienda emplear certificados específicos de cifrado, con segregación de claves, e implantar procedimientos de recuperación de claves de cifrado, procedimientos que deberán encontrarse alineados con la normativa aplicable.

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 de la administración.

Números de identificación fiscal (NIF) y personal (NIP, NRP,…)

Se concibe el número de identificación fiscal, tanto a nivel de entidad (concepto de CIF) como personal (DNI). Para designarlo se seguirá la siguiente nomenclatura:

- 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>

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 tres 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 LFE (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 las requisitos que se incluyen a continuación se ha tenido en cuenta la especificación técnica ETSI TS 102 176-1, en su versión 2.0.0 de marzo de 2007[3]. Se distinguen requerimientos criptográficos para las autoridades emisoras de los Prestadores de Servicios y para entidades o certificados finales:

Actualmente la mayoría de los prestadores utilizan como algoritmo de firma SHAwithRSA tanto en los certificados de las raíces y subraíces como en los certificados de entidades finales. Sobre el uso de SHA-1, SHA-2, y uso de longitudes de clave RSA de 1024, 2048 o 4096, hay diversidad de criterios, aunque el más generalizado es el que aplica el escenario más débil: SHA-1withRSA a 1024 para entidades finales y 2048 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.

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:

[3] Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters form Secure Electronic Signatures, Part I

Nivel Aseguramiento	Entidad	Algoritmo y longitud mínima		Observaciones
Alto y Medio	AC raíz y subraíz	SHA-1	RSA-2048	⊙ Se contemplan SHA-256 y generaciones duales que aseguren la continuidad ⊙ Igualmente, se admiten longitudes RSA de 4096.

⊙ Entidades finales:

Nivel Aseguramiento	Entidad	Algoritmo y longitud mínima		Observaciones
Alto	Certificados finales	SHA-1	RSA-2048	⊙ Se contemplan SHA-256 y generaciones duales que aseguren la continuidad.
Medio	Certificados finales	SHA-1	RSA-1024	⊙ Se recomienda usar longitudes de clave RSA 2048 o superior.

A continuación se describen los campos que componen los tres certificados derivados de la LAECSP (certificado de sede electrónica, certificado de sello electrónico y certificado de empleado público), dividiendo cada uno de ellos entre los niveles de aseguramiento en el que nos encontremos (medio 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 raíz tipo para poder ser utilizado por prestadores y Administraciones que deseen comenzar la emisión de los nuevos perfiles de certificados.

7 Certificado de SubCA

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 utilizará para identificar de manera unívoca el certificado
1.3. Signature Algorithm	SHA-1/ SHA-2 con RSA Signature , longitud de clave de 2048 bits o superior.	Sí	String UTF8 (40). Identificando el tipo de algoritmo. Al tratarse de un certificado raíz las restricciones son mayores que las de los demás certificados. OID 2.16.840.1.101.3.4.2
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	R	OU = p. ej: AUTORIDAD DE CERTIFICACION CERTICA (String UTF8) Size [RFC 5280] 128

Campo	Contenido	R	Formato/Observaciones
	la emisión del certificado.		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.	R	NIF = NIF entidad de certificación ej: S2833002 (Printable String) Size = 9
1.4.6.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 (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)
1.5.1.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 (suscriptor del certificado).	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 (suscriptor del certificado).		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

Campo	Contenido	R	Formato/Observaciones
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 ej: S2833002 (Printable String) Size = 9
1.6.6. Common Name (CN)	Nombre común de la organización prestadora de servicios de certificación (suscriptor del certificado).	Sí	CN = p. ej: CERTICA Root CA (String UTF8) Size 80 Size [RFC 5280] 80
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)

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. AuthorityCertSerialNumber			Número de serie del certificado de CA SerialNumber =.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).

Campo	Contenido	R	Formato/Observaciones
			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”		Se utiliza cuando se realiza la función de autenticación
2.3.2. Content Commitment	No seleccionado “0”		Se utiliza para realizar firma electrónica
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 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	Sí	Campo explicitText. Se recomienda que siempre se referencie a través de un link. Se recomienda longitud no

Campo	Contenido	R	Formato/Observaciones
	DPC o, en su caso, documento legal de tercero		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 ej: soporte.certica@mpr.es (String) Size [RFC 5280] 255
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 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-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- 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)
2.9. 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,

8 Certificado de sede electrónica administrativa

El prestador deberá asegurar la unicidad de los DN (Distinguished Names) de los certificados de sede electrónica administrativa.

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 = 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	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 certificación (emisor del certificado).	Sí	O = p. ej: MINISTERIO DE LA PRESIDENCIA (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 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	Sí	OU = p. ej: AUTORIDAD DE CERTIFICACION CERTICA (String UTF8) Size [RFC 5280] 128

Campo	Contenido	R	Formato/Observaciones
	la emisión del certificado.		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 ej: S2833002 (Printable String) Size = 9
1.3.6.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
1.4. Validity	3 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 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
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 organización) del suscriptor de servicios de certificación (custodio del certificado)	Sí	O = p. ej: MINISTERIO DE LA PRESIDENCIA (String UTF8) Size [RFC 5280] 128
1.5.3.Organizational Unit (OU)	Descripción del tipo de certificado	Sí	Tipo= “sede electrónica” (String UTF8) Size [RFC 5280] 128
1.5.4.Organizational Unit (OU)	El nombre descriptivo de la sede.	Sí	OU= p. ej: PORTAL 060

Campo	Contenido	R	Formato/Observaciones
1.5.5.Serial Number	Número secuencial único asignado por el prestador (no deberá haber repetidos), se recomienda usar el NIF de la entidad responsable.	Sí	SerialNumber = p. ej: S2833002. Número secuencial único asignado por el prestador (Printable String)) Size [RFC 5280] 64
1.5.6.Common Name (CN)	Denominación de nombre de dominio (DNS o IP) donde residirá el certificado.	Sí	CN= p. ej: 060.es. Denominación de nombre de dominio o IP. Conforme al estándar X.500, asegurando que dicho nombre tenga sentido y no de 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)

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

Campo	Contenido	R	Formato/Observaciones
			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 electronica
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. Ie. 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- https o LDAP con servidor autenticado). (String UTF8)
2.5.2. distributionPoint	Punto de distribución de la CRL, número 2		Web donde resida la CRL (punto de distribución 2-https o LDAP con servidor autenticado). (String UTF8)

Campo	Contenido	R	Formato/Observaciones
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)

A continuación se describen los campos diferenciados para los niveles alto y medio 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-1/ 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 1.3.14.3.2.26

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			
2.2.1.QcCompliance	Indicación de certificado reconocido		OID 0.4.0.1862.1.1
2.2.2.QcEuRetentionPeriod	15 años		Integer:=15 ([ETSI TS 101 862 v1.3.3] describe el periodo de conservación de toda la información relevante para

Campo	Contenido	R	Formato/Observaciones
			el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
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>.1.3.2.1, 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 ej: www.mpr.es/certica/emision/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).
2.3.2.2. User Notice	p.ej. "Certificado reconocido 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.rfc822Name	Correo electrónico de contacto de la sede electrónica		Correo electrónico de contacto de la sede electrónica ej: portal.060@mpr.es (String) Size [RFC 5280] 255
2.4.2.dnsName	Nombre de Dominio DNS de la Sede		Nombre Dominio DNS de la Sede ej: "060.es" (String UTF8) Size = 128
2.4.3.Directory Name	Identidad Administrativa	Sí	Campos específicos definidos por la Administración para los certificados LAECSP. (Sequence)
2.4.3.1. Tipo de certificado	Indica la naturaleza del certificado	F	OID: 2.16.724.1.3.5.1.1.1 Tipo= "sede electrónica" (String UTF8) Size = 31
2.4.3.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	F	Entidad Suscriptora = ej: MINISTERIO DE LA PRESIDENCIA (String UTF8) Size = 80 OID: 2.16.724.1.3.5.1.1.*2*

Campo	Contenido	R	Formato/Observaciones
2.4.3.3. NIF entidad suscriptora	Número único de identificación de la entidad	F	NIF = NIF entidad suscriptora ej: "S2833002" (String UTF8) Size = 9 OID: 2.16.724.1.3.5.1.1.3
2.4.3.4. Nombre descriptivo de la sede electrónica	Breve descripción de la Sede indicando un nombre	F	Nombre descriptivo de la sede electrónica, asegurando que dicho nombre tenga sentido y no de lugar a ambigüedades. Nombre sede = ej: "PORTAL 060" (String UTF8) Size = 128 OID: 2.16.724.1.3.5.1.1.4
2.4.3.5. Denominación de nombre de dominio IP	Dominio al que pertenece la Sede	F	Nombre Dominio IP = ej: "060.es" (String UTF8) Size = 128 OID: 2.16.724.1.3.5.1.1.5

8.3 Nivel Medio

8.3.1 Certificado:

Campo	Contenido	R	Formato/Observaciones
1. X.509v1 Field			-
1.1. Signature Algorithm	SHA-1/ SHA-2 con RSA Signature y longitud de clave de al menos 1024 bits	Sí	String UTF8 (40). Identificando el tipo de algoritmo, (más laxo que el del certificado de nivel alto), y longitud de al menos 1024 bits. OID 1.3.14.3.2.26

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			

Campo	Contenido	R	Observaciones
Statements			
2.2.1.QcCompliance	Indicación de certificado reconocido		OID 0.4.0.1862.1.1
2.2.2.QcEuRetentionPeriod	15 años		Integer:=15 ([ETSI TS 101 862 v1.3.3] 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. Certificate Policies	Políticas de certificación/DPC	Sí	
2.3.1.Policy Identifier	OID asociado a la DPC o PC	Sí	OID Private enterprise: ej: 1.3.6.1.4.1.<num prest>.1.3.2.2, 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 ej: www.mpr.es/certica/emision/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).
2.3.2.2. User Notice	Ej: "Certificado reconocido de sede electrónica, nivel medio. 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 de contacto de la sede electrónica		Correo electrónico de contacto de la sede electrónica ej: portal.060@mpr.es (String) Size [RFC 5280] 255
2.4.2.dnsName	Nombre de Dominio DNS de la Sede		Nombre Dominio DNS de la Sede ej: "060.es" (String UTF8) Size = 128
2.4.3.Directory Name	Identidad administrativa	Sí	Campos específicos definidos por la Administración para los certificados LAECSP. (Sequence)
2.4.3.1. Tipo de	Indica la naturaleza del	F	OID: 2.16.724.1.3.5.1.2.*1*

Campo	Contenido	R	Observaciones
certificado	certificado		Tipo= "sede electrónica" (String UTF8) Size = 31
2.4.3.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	F	Entidad Suscriptora = ej: MINISTERIO DE LA PRESIDENCIA (String UTF8) Size = 80 OID: 2.16.724.1.3.5.1.2.*2*
2.4.3.3. NIF entidad suscriptora	Número único de identificación de la entidad	F	NIF = NIF entidad suscriptora ej: "S2833002" (String UTF8) Size = 9 OID2.16.724.1.3.5.1.2.3
2.4.3.4. Nombre descriptivo de la sede electrónica	Breve descripción de la Sede indicando un nombre	F	Nombre descriptivo de la sede electrónica, asegurando que dicho nombre tenga sentido y no de lugar a ambigüedades. Nombre sede = ej: "PORTAL 060" (String UTF8) Size = 128 OID: 2.16.724.1.3.5.1.2.4
2.4.3.5. Denominación de nombre de dominio IP	Dominio al que pertenece la Sede	F	Nombre Dominio IP =ej: "060.es" (String UTF8) Size = 128 OID2.16.724.1.3.5.1.2.5

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.

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 = 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 LA PRESIDENCIA (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

Campo	Contenido	R	Observaciones
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 ej: S2833002 (Printable String) Size = 9
1.3.6. 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
1.4. Validity	3 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 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
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 suscriptor de servicios de certificación (custodio del certificado).	Sí	O = p. ej: MINISTERIO DE LA PRESIDENCIA (String UTF8) Size [RFC 5280] 128
1.5.3. Organizational Unit (OU)	Indica la naturaleza del certificado	Sí	OU = sello electrónico (String UTF8) Size [RFC 5280] 128

Campo	Contenido	R	Observaciones
1.5.4.Serial Number	Número secuencial único asignado por el prestador (no deberá haber repetidos), se recomienda usar el NIF de la entidad.	Sí	SerialNumber = p. ej: S2833002. Número secuencial único asignado por el prestador (Printable String)) Size [RFC 5280] 64
1.5.5.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 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"
1.5.6.Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)		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"
1.5.7.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 de 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)

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)

Campo	Contenido	R	Observaciones
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		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	Seleccionado “1”	Sí	Se utiliza cuando se realiza la función de firma electrónica
2.3.3.Key Encipherment	Seleccionado “1”	Sí	Se utiliza para gestión y transporte de claves
2.3.4.Data Encipherment	Seleccionado “1”	Sí	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. Extended Key Usage		Sí	Uso extendido del certificado
2.4.1.Email Protection	Seleccionado	Sí	Protección de mail
2.4.2.Client	Seleccionado	Sí	Autenticación cliente

Campo	Contenido	R	Observaciones
Authentication			
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 ie: soporte.certica@mpr.es (String) Size [RFC 5280] 255
2.6. cRLDistributionPoint		Sí	Indica cómo se obtiene la información de CRL.
2.6.1.distributionPoint	Punto de distribución de la CRL, número 1	Sí	Web donde resida la CRL (punto de distribución 1 -https o LDAP con servidor autenticado). (String UTF8)
2.6.2.distributionPoint	Punto de distribución de la CRL, número 2		Web donde resida la CRL (punto de distribución 2 – 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)

A continuación se describen los campos diferenciados para los niveles alto y medio 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-1/ 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 1.3.14.3.2.26

9.2.2 Extensiones del certificado

Campo	Contenido	R	Observaciones
2.1. Qualified Certificate Statements		Sí	
2.1.1.QcCompliance	Indicación de certificado reconocido	Sí	OID 0.4.0.1862.1.1
2.1.2.QcEuRetentionPeriod	15 años	Sí	Integer:=15 ([ETSI TS 101 862 v1.3.3] 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		OID 0.4.0.1862.1.4
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: ej: 1.3.6.1.4.1.<num prest>.1.3.3.1, u OID Country assignment (2.16...)
2.2.2.Policy Qualifier ID	Especificación de la DPC	Sí	
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 ej: www.mpr.es/certica/emision/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).
2.2.2.2. User Notice	Ej: "Certificado reconocido 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. Ie: soporte.afirma5@mpr.es (String) Size [RFC 5280] 255

Campo	Contenido	R	Observaciones
2.3.2.Directory Name	Identidad administrativa	Sí	Campos específicos definidos por la Administración para los certificados LAECSP. (Sequence)
2.3.2.1. Tipo de certificado	Indica la naturaleza del certificado	F	Tipo= sello electrónico (String UTF8) Size = 31 2.16.724.1.3.5.2.1.*1*
2.3.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	F	Entidad Suscriptora = ej: MINISTERIO DE LA PRESIDENCIA (String UTF8) Size = 80 OID: 2.16.724.1.3.5.2.1.*2*
2.3.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	F	NIF suscriptora = NIF entidad suscriptora ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.2.1.3
2.3.2.4. DNI/NIE del responsable	DNI o NIE del responsable del Sello	O	DNI/NIE responsable= ej: 00000000G (String UTF8) Size = 9 OID: 2.16.724.1.3.5.2.1.4
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 de lugar a ambigüedades. Denominación sistema = ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA". (String UTF8) Size = 128 OID: 2.16.724.1.3.5.2.1.5
2.3.2.6. Nombre de pila	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: 2.16.724.1.3.5.2.1.6 Ej: "JUAN ANTONIO"
2.3.2.7. Primer apellido	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: 2.16.724.1.3.5.2.1.7 ej: "DE LA CAMARA"
2.3.2.8. Segund	Segundo apellido del	O	SN2 = Segundo apellido del

Campo	Contenido	R	Observaciones
o apellido	responsable del certificado		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: 2.16.724.1.3.5.2.1.8 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 ej: juanantonio.delacamara.espanol@mpr.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.2.1.9

9.3 Nivel Medio

9.3.1 Certificado

Campo	Contenido	R	Observaciones
2. X.509v1 Field			-
2.1. Signature Algorithm	SHA-1/ SHA-2 con RSA Signature y longitud de clave de al menos 1024 bits	Sí	String UTF8 (40). Identificando el tipo de algoritmo, (más laxo que el del certificado de nivel alto), y longitud de al menos 1024 bits.. OID 1.3.14.3.2.26

9.3.2 Extensiones del certificado

Campo	Contenido	R	Observaciones
2.1. Qualified Certificate Statements		Sí	
2.1.1. QcCompliance	Indicación de certificado reconocido	Sí	OID 0.4.0.1862.1.1
2.1.2. QcEuRetention Period	15 años	Sí	Integer:=15 ([ETSI TS 101 862 v1.3.3] 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. Certificate Policies	Políticas de	Sí	

Campo	Contenido	R	Observaciones
	certificación/DPC		
2.2.1. Policy Identifier	OID asociado a la DPC o PC	Sí	OID Private enterprise: 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	
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 ej: www.mpr.es/certica/emision/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).
2.2.2.2. User Notice	Ej: "Certificado reconocido de sello electrónico de Administración, órgano o entidad de derecho público, nivel Medio. 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, ej: soporte.afirma5@mpr.es (String) Size [RFC 5280] 255
2.3.2. Directory Name	Identidad administrativa	Sí	Campos específicos definidos por la Administración para los certificados LAECSP. (Sequence)
2.3.2.1. Tipo de certificado	Indica la naturaleza del certificado	F	Tipo= sello electrónico (String UTF8) Size = 31 OID: 2.16.724.1.3.5.2.2.*1*
2.3.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	F	Entidad Suscriptora = ej: MINISTERIO DE LA PRESIDENCIA (String UTF8) Size = 80 OID: 2.16.724.1.3.5.2.2.*2*
2.3.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	F	NIF suscriptora = NIF entidad suscriptora ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.2.2.3

Campo	Contenido	R	Observaciones
2.3.2.4. DNI/NIE del responsable (opcional)	DNI o NIE del responsable del Sello	O	DNI/NIE responsable= ej: 00000000G (String UTF8) Size = 9 OID: 2.16.724.1.3.5.2.2.4
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 de lugar a ambigüedades. Denominación sistema = ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA". (String UTF8) Size = 128 OID: 2.16.724.1.3.5.2.2.5
2.3.2.6. Nombre de pila	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: 2.16.724.1.3.5.2.2.6 Ej: "JUAN ANTONIO"
2.3.2.7. Primer apellido	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: 2.16.724.1.3.5.2.2.7 ej: "DE LA CAMARA"
2.3.2.8. Segundo apellido	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: 2.16.724.1.3.5.2.2.8 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 ej: juanantonio.delacamara.espanol@mpr.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.2.2.9

10 Certificado de empleado público

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, 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	Sí	Integer. SerialNumber = ej: 111222.

Campo	Contenido	R	Observaciones
	del certificado.		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 LA PRESIDENCIA (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 ej: S2833002 (Printable String) Size = 9
1.3.6.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
1.4. Validity	3 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

Campo	Contenido	R	Observaciones
			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 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 LA PRESIDENCIA (String UTF8) Size [RFC 5280] 128
1.5.3.Organizational Unit (OU)	Descripción del tipo de certificado	Sí	OU = certificado electrónico de empleado público (String UTF8) Size [RFC 5280] 128
1.5.4.Organizational Unit (OU)	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado		Unidad = ej: SUBDIRECCION GENERAL DE PROCESO DE DATOS (String) Size [RFC 5280] 128
1.5.5.Organizational Unit (OU)	Número de identificación del suscriptor del certificado (supuestamente unívoco). Se corresponde con el NRP o NIP		Número identificativo = ej: A02APE1056 (String UTF8) Size = 10
1.5.6.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		Title = p. ej: ANALISTA PROGRAMADOR. Nombre descriptivo del puesto o cargo que ostenta el responsable del certificado (String UTF8) Size [RFC 5280] 128

Campo	Contenido	R	Observaciones
	certificado.		
1.5.7.Serial Number	Número secuencial único asignado por el prestador (no deberá haber repetidos), se recomienda usar el DNI/NIE del empleado público.	Sí	SerialNumber = p. ej: 00000000G. 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 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 de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 p. ej: "JUAN ANTONIO"
1.5.10. Common Name (CN)	Se recomienda 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)

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

Campo	Contenido	R	Observaciones
			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.AuthorityCertSerial Number	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.
2.3.1.distributionPoint	Punto de distribución de la CRL, número 1	Sí	Web donde resida la CRL (punto de distribución 1 -https o LDAP con servidor autenticado). (String UTF8)
2.3.2.distributionPoint	Punto de distribución de la CRL, número 2		Web donde resida la CRL (punto de distribución 2 – 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)
2.5. 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 ej: soporte.certica@mpr.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-1/ 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 1.3.14.3.2.26

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 Signatura	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

Campo	Contenido	R	Observaciones
2.2. Qualified Certificate Statements		Sí	
2.2.1.QcCompliance	Indicación de certificado reconocido	Sí	OID 0.4.0.1862.1.1
2.2.2.QcEuRetentionPeriod	15 años	Sí	Integer:=15 ([ETSI TS 101 862 v1.3.3] 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
2.3. Certificate Policies	Políticas de certificación/DPC	Sí	
2.3.1.Policy Identifier	OID asociado a la DPC o PC	Sí	OID Private enterprise: ej: 1.3.6.1.4.1.<num prest>.1.3.4.1 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 ej: www.mpr.es/certica/emision/dpc. Se recomienda que siempre se referencie a través de un link. (IA5String).
2.3.2.2. User Notice	Ej: "Certificado reconocido de personal, nivel alto, firma electrónica. 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 de la persona responsable del certificado[4]		Correo electrónico de la persona responsable del certificado ej: juanantonio.delacamara.espanol@mpr.es (String) Size [RFC 5280] 255
2.4.2.Directory Name	Identidad administrativa	Sí	Campos específicos definidos por la Administración para los certificados LAECSP. (Sequence)

[4] Extensión generalmente utilizada por productos S/MIME

Campo	Contenido	R	Observaciones
2.4.2.1. Tipo de certificado	Indica la naturaleza del certificado	F	Tipo= certificado electrónico de empleado público (String UTF8) Size = 31 OID: 2.16.724.1.3.5.3.1.*1*
2.4.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	F	Entidad Suscriptora = ej: MINISTERIO DE LA PRESIDENCIA (String UTF8) Size = 80 OID: 2.16.724.1.3.5.3.1.2
2.4.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	F	NIF suscriptora = NIF entidad suscriptora ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.3.1.3
2.4.2.4. DNI/NIE del responsable	DNI o NIE del responsable	F	DNI/NIE responsable= ej: 00000000G (String UTF8) Size = 10 OID: 2.16.724.1.3.5.3.1.4
2.4.2.5. Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente unívoco). Se corresponde con el NRP o NIP	O	Número identificativo = ej: A02APE1056 (String UTF8) Size = 10 OID: 2.16.724.1.3.5.3.1.5
2.4.2.6. Nombre de pila	Nombre de pila del responsable del certificado	F	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: 2.16.724.1.3.5.3.1.6 Ej: "JUAN ANTONIO"
2.4.2.7. Primer apellido	Primer apellido del responsable del certificado	F	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: 2.16.724.1.3.5.3.1.7 Ej: "DE LA CAMARA"
2.4.2.8. Segundo apellido	Segundo apellido del responsable del certificado	F	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).

Campo	Contenido	R	Observaciones
			OID: 2.16.724.1.3.5.3.1.8 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 ie: juanantonio.delacamara.espanol@mpr.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.3.1.9
2.4.2.10. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado	O	Unidad = ej: SUBDIRECCION GENERAL DE PROCESO DE DATOS (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.3.1.10
2.4.2.11. Puesto o cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración.	O	Puesto = ej: ANALISTA PROGRAMADOR (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.3.1.11

10.3.2 Certificado de autenticación

10.3.2.1 Certificado

Campo	Contenido	R	Observaciones
1. X.509v1 Field			-
1.1. Signature Algorithm	SHA-1/ 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 1.3.14.3.2.26

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)
2.1.1.Digital Signature	Seleccionado "1"	Sí	Se utiliza cuando se realiza la función de autenticación

Campo	Contenido	R	Observaciones
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”		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 Signatura	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. Qualified Certificate Statements		Sí	
2.3.1.QcCompliance	Indicación de certificado reconocido	Sí	OID 0.4.0.1862.1.1
2.3.2.QcEuRetentionPeriod	15 años	Sí	Integer:=15 ([ETSI TS 101 862 v1.3.3] 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		OID 0.4.0.1862.1.4
2.4. Certificate Policies	Políticas de certificación/DPC	Sí	

Campo	Contenido	R	Observaciones
2.4.1.Policy Identifier	OID asociado a la DPC o PC	Sí	OID Private enterprise: ej: 1.3.6.1.4.1.<num prest>.1.3.4.2 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 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 reconocido 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.
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[5]		Correo electrónico de la persona responsable del certificado ej: juanantonio.delacamara.espanol@mpr.es (String) Size [RFC 5280] 255
2.5.2.Directory Name	Identidad administrativa	Sí	Campos específicos definidos por la Administración para los certificados LAECSP. (Sequence)
2.5.2.1. Tipo de certificado	Indica la naturaleza del certificado	F	Tipo= certificado electrónico de empleado público (String UTF8) Size = 31 OID2.16.724.1.3.5.3.1.*1*
2.5.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	F	Entidad Suscriptora = ej: MINISTERIO DE LA PRESIDENCIA (String UTF8) Size = 80 OID: 2.16.724.1.3.5.3.1.2
2.5.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	F	NIF suscriptora = NIF entidad suscriptora ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.3.1.3

[5] Extensión generalmente utilizada por productos S/MIME

Campo	Contenido	R	Observaciones
2.5.2.4. DNI/NIE del responsable	DNI o NIE del responsable del Sello	F	DNI/NIE responsable= ej: 00000000G (String UTF8) Size = 10 OID: 2.16.724.1.3.5.3.1.4
2.5.2.5. Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente unívoco)	O	Número identificativo = ej: A02APE1056 (String UTF8) Size = 10 OID: 2.16.724.1.3.5.3.1.5
2.5.2.6. Nombre de pila	Nombre de pila del responsable del certificado	F	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: 2.16.724.1.3.5.3.1.6 Ej: "JUAN ANTONIO"
2.5.2.7. Primer apellido	Primer apellido del responsable del certificado	F	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: 2.16.724.1.3.5.3.1.7 Ej: "DE LA CAMARA"
2.5.2.8. Segundo apellido	Segundo apellido del responsable del certificado	F	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: 2.16.724.1.3.5.3.1.8 Ej: "ESPAÑOL"
2.5.2.9. Correo electrónico	Correo electrónico de la persona responsable del certificado	O	Correo electrónico de la persona responsable del certificado ie: juanantonio.delacamara.espanol@mpr.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.3.1.9
2.5.2.10. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado	O	Unidad = ej: SUBDIRECCION GENERAL DE PROCESO DE DATOS (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.3.1.10
2.5.2.11. Puesto o cargo	Puesto desempeñado por el suscriptor del certificado	O	Puesto = ej: ANALISTA PROGRAMADOR (String) Size [RFC

Campo	Contenido	R	Observaciones
	dentro de la administración.		5280] 128 OID: 2.16.724.1.3.5.3.1.11
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.

10.3.3 Certificado de cifrado

10.3.3.1 Certificado

Campo	Contenido	R	Observaciones
1. X.509v1 Field			-
1.1. Signature Algorithm	SHA-1/ 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 1.3.14.3.2.26

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	Por tratarse de un certificado de cifrado
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 Signatura	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

Campo	Contenido	R	Observaciones
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 reconocido	Sí	OID 0.4.0.1862.1.1
2.3.2.QcEuRetentionPeriod	15 años	Sí	Integer:=15 ([ETSI TS 101 862 v1.3.3] 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		OID 0.4.0.1862.1.4
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: 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 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 reconocido 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.
2.5. 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[6]		Correo electrónico de la persona responsable del certificado ej: juanantonio.delacamara.espanol@mp

[6] Extensión generalmente utilizada por productos S/MIME

Campo	Contenido	R	Observaciones
			r.es (String) Size [RFC 5280] 255
2.5.2.Directory Name	Identidad administrativa	Sí	Campos específicos definidos por la Administración para los certificados LAECSP. (Sequence)
2.5.2.1. Tipo de certificado	Indica la naturaleza del certificado	F	Tipo= certificado electrónico de empleado público (String UTF8) Size = 31 OID2.16.724.1.3.5.3.1.*1*
2.5.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	F	Entidad Suscriptora = ej: MINISTERIO DE LA PRESIDENCIA (String UTF8) Size = 80 OID: 2.16.724.1.3.5.3.1.2
2.5.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	F	NIF suscriptora = NIF entidad suscriptora ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.3.1.3
2.5.2.4. DNI/NIE del responsable	DNI o NIE del responsable del Sello	F	DNI/NIE responsable= ej: 00000000G (String UTF8) Size = 10 OID: 2.16.724.1.3.5.3.1.4
2.5.2.5. Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente unívoco)	O	Número identificativo = ej: A02APE1056 (String UTF8) Size = 10 OID: 2.16.724.1.3.5.3.1.5
2.5.2.6. Nombre de pila	Nombre de pila del responsable del certificado	F	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: 2.16.724.1.3.5.3.1.6 Ej: "JUAN ANTONIO"
2.5.2.7. Primer apellido	Primer apellido del responsable del certificado	F	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: 2.16.724.1.3.5.3.1.7 Ej: "DE LA CAMARA"
2.5.2.8. Segundo apellido	Segundo apellido del responsable del certificado	F	SN2 = Segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String

Campo	Contenido	R	Observaciones
			UTF8) Size 40 En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter). OID: 2.16.724.1.3.5.3.1.8 Ej: "ESPAÑOL"
2.5.2.9. Correo electrónico	Correo electrónico de la persona responsable del certificado	O	Correo electrónico de la persona responsable del certificado ie: juanantonio.delacamara.espanol@mpr.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.3.1.9
2.5.2.10. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado	O	Unidad = ej: SUBDIRECCION GENERAL DE PROCESO DE DATOS (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.3.1.10
2.5.2.11. Puesto o cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración.	O	Puesto = ej: ANALISTA PROGRAMADOR (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.3.1.11

10.4 Nivel Medio

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:

10.4.1 Certificado

Campo	Contenido	R	Observaciones
1. X.509v1 Field			-
1.1. Signature Algorithm	SHA-1/ 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. OID 1.3.14.3.2.26

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	Por tratarse de un certificado de cifrado
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. Qualified Certificate Statements		Sí	
2.3.1.QcCompliance	Indicación de certificado reconocido	Sí	OID 0.4.0.1862.1.1
2.3.2.QcEuRetentionPeriod	15 años	Sí	Integer:=15 ([ETSI TS 101 862 v1.3.3] 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. Certificate Policies		Sí	
2.4.1.Policy Identifier	OID asociado a la DPC o PC	Sí	OID Private enterprise: ej: 1.3.6.1.4.1.<num prest>.1.3.4.4 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 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 reconocido de personal, 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.
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[7]		Correo electrónico de la persona responsable del certificado ej: juanantonio.delacamara.espanol@mpr.es (String) Size [RFC 5280] 255
2.5.2.Directory Name	Identidad administrativa	Sí	Campos específicos definidos por la Administración para los certificados LAECSP. (Sequence)
2.5.2.1. Tipo de certificado	Indica la naturaleza del certificado	F	Tipo= certificado electronico de empleado público (String UTF8) Size = 31 OID: 2.16.724.1.3.5.3.2.*1*
2.5.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	F	Entidad Suscriptora = ej: MINISTERIO DE LA PRESIDENCIA (String UTF8) Size = 80 OID: 2.16.724.1.3.5.3.2.2
2.5.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	F	NIF suscriptora = NIF entidad suscriptora ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.3.2.3
2.5.2.4. DNI/NIE del responsable	DNI o NIE del responsable del Sello	F	DNI/NIE responsable= ej: 00000000G (String UTF8) Size = 10 OID: 2.16.724.1.3.5.3.2.4
2.5.2.5. Número	Número de identificación	O	Número identificativo = ej:

[7] Extensión generalmente utilizada por productos S/MIME

Campo	Contenido	R	Observaciones
de identificación de personal	del suscriptor del certificado (supuestamente unívoco)		A02APE1056 (String UTF8) Size = 10 OID: 2.16.724.1.3.5.3.2.5
2.5.2.6. Nombre de pila	Nombre de pila del responsable del certificado	F	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: 2.16.724.1.3.5.3.2.6 Ej: "JUAN ANTONIO"
2.5.2.7. Primer apellido	Primer apellido del responsable del certificado	F	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: 2.16.724.1.3.5.3.2.7 Ej: "DE LA CAMARA"
2.5.2.8. Segundo apellido	Segundo apellido del responsable del certificado	F	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: 2.16.724.1.3.5.3.2.8 Ej: "ESPAÑOL"
2.5.2.9. Correo electrónico	Correo electrónico de la persona responsable del certificado	O	Correo electrónico de la persona responsable del certificado ie: juanantonio.delacamara.espanol@mpr.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.3.2.9
2.5.2.10. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado	O	Unidad = ej: SUBDIRECCION GENERAL DE PROCESO DE DATOS (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.3.2.10
2.5.2.11. Puesto o cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración.	O	Puesto = ej: ANALISTA PROGRAMADOR (String) Size [RFC 5280] 128 OID: 2.16.724.1.3.5.3.2.11
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 responsable

Campo	Contenido	R	Observaciones
			del certificado.

11 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	2.16.724.1.3.5.1.1.*1*=sede electrónica (Nivel Alto) 2.16.724.1.3.5.1.2.*1*=sede electrónica (Nivel Medio) 2.16.724.1.3.5.2.1.*1*=sello electrónico (Nivel Alto) 2.16.724.1.3.5.2.2.*1*=sello electrónico (Nivel Medio)
Objeto Identidad Administrativa	Obligatorio. OID específico por perfil definido en LAECSP y por nivel de aseguramiento	2.16.724.1.3.5.3.1.*1*=certificado electrónico de empleado público (Nivel Alto) 2.16.724.1.3.5.3.2.*1*=certificado electrónico de empleado público (Nivel Medio)
Algoritmos criptográficos	Obligatorios	AC raíz y subraíz (Alto y Medio): mínimo SHA-1, RSA-2048 Certificados finales (Alto): mínimo SHA-1, RSA-2048 Certificados finales (Medio): mínimo SHA-1, RSA-1024
Codificación UTF8	Obligatoria	
Certificado CA Raíz	Recomendable	Perfil Orientativo. Los valores proporcionados en este documento pretenden servir como ejemplos en posibles nuevas implementaciones.
Validez de los certificados	Recomendado	3 años para los certificados de Sede, Sello, Empleado Público
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, 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), Organization (O), Organizational Unit (OU), Organizational Unit (OU), Serial Number, Common Name (CN)) • Subject Public Key Info • Signature Algorithm	• V3 • Número de serie • Nombre de la entidad emisora • Recomendado 3 años • C="**ES**", O=Organización, OU= "**sede electrónica**", OU=Nombre descriptivo de la Sede, SerialNumber=NIF de la entidad CN=Nombre DNS 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), Serial Number, Common Name (CN)) • Subject Public Key Info • Signature Algorithm	• V3 • Número de serie • Nombre de la entidad emisora • Recomendado 3 años • C="**ES**", O=Organización, OU= "**sello electrónico**", SerialNumber=NIF de la entidad, • Clave pública de la Sede • Algoritmo de Firma
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO	• Version • Serial Number	• V3 • Número de serie

	• 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	• Nombre de la entidad emisora • Recomendado 3 años • C="**ES**", O=Organización, OU= "**certificado electrónico de empleado público**", SerialNumber=DNI/NIE del empleado, CN=Nombre , apellidos y DNI/NIE del empleado • Clave pública de la Sede • 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) • Extended Key Usage (Server Authentication) • Qualified Certificate Statements • Certificate Policies (Policy Identifier, Policy Qualifier ID [CPS Pointer, User Notice]) • 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 • OID asignado por el PSC a la política bajo la que se emite el certificado, URL de la DPC y mensaje explícito. • IDENTIDAD ADMINISTRATIVA SEDE

SELLO ELECTRÓNICO	• Authority Key Identifier
	• Subject Key Identifier
	• Key Usage
	• Extended Key Usage
	• cRLDistributionPoint (distributionPoint)
	• Authority Info Access (Access Method, Access Location)
	• Qualified Certificate Statements
	• Certificate Policies (Policy Identifier, Policy Qualifier ID [CPS Pointer, User Notice])
	• Subject Alternative Names (Directory Name)
		• 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
		• Información de acceso a OCSP
		• Qualified Certificate Statements
		  o NIVEL ALTO: **"QcCompliance", "QcEuRetentionPeriod",**
		  o NIVEL MEDIO: **"QcCompliance", "QcEuRetentionPeriod"**

		• OID asignado por el PSC a la política bajo la que se emite el certificado, URL de la DPC y mensaje explícito. • IDENTIDAD ADMINISTRATIVA SELLO
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO	• Authority Key Identifier • Subject Key Identifier • cRLDistributionPoint (distributionPoint,) • Authority Info Access (Access Method, Access Location) • Key Usage • Extended Key Usage • Qualified Certificate Statements • Certificate Policies (Policy Identifier, Policy Qualifier ID [CPS Pointer, User Notice]) • 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 • Key Usage o FIRMA ALTO: **"Content Commitment"** o AUTENTICACIÓN ALTO: **"Digital Signature"** o CIFRADO ALTO: **"Key Encipherment", "Data Encipherment"** o FIRMA, AUTENTICACIÓN Y CIFRADO NIVEL MEDIO: **"Digital Signature", "Content Commitment", "Key Encipherment", "Data Encipherment"** • Extended Key Usage o AUTENTICACIÓN ALTO: **"Email Protection", "Client Authentication"** o CIFRADO ALTO: **"Email Protection", "Client Authentication"** o FIRMA, AUTENTICACIÓN Y CIFRADO NIVEL MEDIO: **"Email Protection", "Client Authentication"** • Qualified Certificate Statements o NIVEL ALTO: **"QcCompliance", "QcEuRetentionPeriod", "QcSSCD"** o NIVEL MEDIO: **"QcCompliance", "QcEuRetentionPeriod"** • OID asignado por el PSC a la política bajo la que se emite el certificado, URL de la DPC y mensaje explícito. • IDENTIDAD ADMINISTRATIVA EMPLEADO

		PUBLICO

CERTIFICADO	CAMPOS RECOMENDABLES	VALORES
SEDE ELECTRÓNICA	• Issuer Distinguished Name (Locality, Serial Number)	• L= Localidad del PSC • SN= NIF del emisor
SELLO ELECTRÓNICO	• Issuer Distinguished Name (Locality, Serial Number) • Subject (Surname, Given Name)	• L= Localidad del PSC • SN= NIF del emisor • Surname=Apellidos y DNI del responsable, GivenName= Nombre del responsable • CN=Nombre descriptivo del sistema
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO	• Issuer Distinguished Name (Locality, Serial Number) • Subject (Organizational Unit (OU), Organizational Unit (OU), Title, Surname, Given Name)	• L= Localidad del PSC • SN= NIF del emisor • OU=Unidad del Empleado, OU=NRP o NIP, Title= Puesto o cargo del empleado, SN= Apellidos y DNI del responsable, GN= Nombre del responsable

CERTIFICADO	EXTENSIONES RECOMENDABLES	VALORES
SEDE ELECTRÓNICA	• Issuer Alternative Name • Subject Alternative Names	• rfc822Name=Correo electrónico de la CA emisora • rfc822Name=Correo electrónico de contacto de la Sede, dnsName=Nombre de dominio de la Sede
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	CAMPOS "IDENTIDAD ADMINISTRATIVA" FIJOS	VALORES
SEDE ELECTRÓNICA	• Tipo de certificado	• OID: 2.16.724.1.3.5.1.*x.1*= **"sede electrónica"**

	• Nombre de la entidad suscriptora • NIF entidad suscriptora • Nombre descriptivo de la sede electrónica • Denominación de nombre de dominio IP	• OID: 2.16.724.1.3.5.1.x.2 = Entidad Suscriptora (Organización) • OID: 2.16.724.1.3.5.1.x.3 = NIF entidad suscriptora • OID: 2.16.724.1.3.5.1.x.4 = Nombre descriptivo de la sede electrónica • OID: 2.16.724.1.3.5.1.x.5 = Nombre DNS de la sede electrónica *Donde x tiene valor 1 para un Nivel de Aseguramiento Alto y 2 para Medio*
SELLO ELECTRÓNICO	• Tipo de certificado • Nombre de la entidad suscriptora • NIF entidad suscriptora •	• OID: 2.16.724.1.3.5.2.*x*.1 = **"sello electrónico"** • OID: 2.16.724.1.3.5.2..x.2 = Entidad Suscriptora (Organización) • OID: 2.16.724.1.3.5.2x.3 = NIF entidad suscriptora • *Donde x tiene valor 1 para un Nivel de Aseguramiento Alto y 2 para Medio*
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: 2.16.724.1.3.5.3.x.1 = **"certificado electrónico de empleado público** • OID: 2.16.724.1.3.5.3x.2 = Entidad Suscriptora (Organización) • OID: 2.16.724.1.3.5.3.x.3 = NIF entidad suscriptora • OID: 2.16.724.1.3.5.3.x.4 = DNI/NIE responsable • OID2.16.724.1.3.5.3.x.6 = Nombre de pila del responsable del certificado • OID: 2.16.724.1.3.5.3.x.7 = Primer apellido del responsable del certificado • OID: 2.16.724.1.3.5.3.x.8 = Segundo apellido del responsable del certificado *Donde x tiene valor 1 para un Nivel de Aseguramiento Alto y*

		2 para Medio

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: 2.16.724.1.3.5.2..x.4 = DNI/NIE responsable • 2.16.724.1.3.5.2.x.5 = Nombre descriptivo del sistema de sellado automático • OID: 2.16.724.1.3.5.2.x.6 = Nombre de pila del responsable del certificado • OID: 2.16.724.1.3.5.2.x.7 = Primer apellido del responsable del certificado • OID: 2.16.724.1.3.5.2.x.8 = Segundo apellido del responsable del certificado • OID: 2.16.724.1.3.5.2.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*
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO	• Número de identificación de personal • Correo electrónico • Unidad organizativa • Puesto o cargo	• OID2.16.724.1.3.5.3x.5 = NRP o NIP del empleado • OID: 2.16.724.1.3.5.3.x.9 = Correo electrónico del empleado • OID: 2.16.724.1.3.5.3.x.10 = Unidad del empleado • OID: 2.16.724.1.3.5.3.x.11 = Puesto o Cargo del empleado *Donde x tiene valor 1 para un Nivel de Aseguramiento Alto y 2 para Medio*

12 ANEXO: Referencias

- ETSI TS 101862. Qualified Certificate Profile.
- ETSI TS 102280. x.509 V.3 Certificate Profile for Certificates Issued to Natural Persons.
- IETF RFC 2560. X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP.
- 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.
- IETF RFC 5280. Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile.
- IETF RFC 3739. Actualizada por RFC 3279, RFC 5756 Internet X.509 Public Key Infrastructure. Qualified Certificates Profile.
- 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.
- 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.
- ISO 3166-1, alpha-2 country codes.
- ISO/IEC 9594-8/ITU-T X.509.
- CCN-STIC-405. Guía de seguridad de las TIC. Algoritmos y parámetros para firma electrónica segura.