Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

POLÍTICA Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS CERTIFICADOS DE REPRESENTANTE DE PERSONAS JURÍDICAS Y DE ENTIDADES SIN PERSONALIDAD JURÍDICA DE LA "AC REPRESENTACIÓN"

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM / v1.3	26/04/2016
Revisado por:	FNMT-RCM / v1.3	17/06/2016
Aprobado por:	FNMT-RCM / v1.3	24/06/2016

HISTÓRICO DEL DOCUMENTO		
Versión	**Fecha**	**Descripción**
1.0	10/07/2015	Creación del documento
1.1	20/11/2015	Expedición de los certificados de representante de Persona jurídica y de Entidad sin personalidad jurídica como reconocidos.
1.2	11/04/2016	Actualización de perfiles conforme a los estándares ETSI (mandato M460) y directrices de la DTIC.
1.3	24/06/2016	Alineación con requisitos de la auditoría conforme el estándar ETSI

Referencia: DPC/CPREP0103/SGPSC/2016

Documento clasificado como: *Público*

ÍNDICE

1. INTRODUCCIÓN

1. El presente documento forma parte integrante de la *Declaración General de Prácticas de Certificación* de la FNMT-RCM y tiene por objeto la información pública de las condiciones y características de los servicios de certificación y servicios de expedición de *Certificados* electrónicos por parte de la FNMT-RCM como *Prestador de Servicios de Confianza*, recogiendo las obligaciones y procedimientos que se compromete a cumplir en relación con la expedición del *Certificado de Representante de Persona jurídica*, del *Certificado de Representante de Entidad sin personalidad jurídica* y del *Certificado de Representante para administradores únicos y solidarios*.

2. En especial deberá tenerse presente, a efectos interpretativos de estas *Política y Prácticas de Certificación Particulares*, el apartado "Definiciones" de la *Declaración General de Prácticas de Certificación*, y, en su caso, la *Ley de Emisión del Certificado* correspondiente a cada entidad usuaria de los servicios de certificación de la FNMT-RCM.

3. Los *Certificados de Representante de Persona jurídica, de Representante* de *Entidad sin personalidad jurídica* y de *Representante para administradores únicos o solidarios* expedidos por la FNMT-RCM, cuya *Política de Certificación y Prácticas de Certificación Particulares* se definen en el presente documento, se consideran técnicamente *Certificados Reconocidos* o cualificados, de acuerdo con el Reglamento (UE) No 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, y conforme a los principios de seguridad, integridad, confidencialidad, autenticidad y no repudio previstos en la Ley 59/2003, de 19 de diciembre, de Firma electrónica (art. 11.4 y concordantes).

4. Los *Certificados de Representante para administradores únicos y solidarios* se emiten, inicialmente, para dar cobertura a las necesidades de seguridad en el tráfico jurídico para estos modos de organizar la administración de las sociedades mercantiles y, posteriormente, ampliar a otros tipos de administración en función del estado de la técnica y de las posibilidades de los *Prestadores de Servicios de Confianza* y de las personas y organizaciones destinatarias de los servicios.

2. ORGANIZACIÓN DEL DOCUMENTO

5. La *Declaración de Prácticas de Certificación* de la FNMT-RCM como *Prestador de Servicios de Confianza* está estructurada, de un lado, por la parte común de la *Declaración General de Prácticas de Certificación* (DGPC) de la FNMT-RCM, pues existen niveles de actuación análogos para todos los servicios de certificación de la Entidad y, de otro lado, por las *Políticas de Certificación y Prácticas de Certificación Particulares* aplicables a cada tipo de certificado expedido por dicha Entidad.

6. De acuerdo con lo anterior, la estructura de la *Declaración de Prácticas de Certificación de la FNMT-RCM* es la siguiente:

   1) Por una parte, la ***Declaración General de Prácticas de Certificación***, que debe considerarse cuerpo principal de la *Declaración de Prácticas de Certificación* en el que se describe, además de lo previsto en el artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, el régimen de responsabilidad aplicable a los miembros de la *Comunidad Electrónica*, los controles de seguridad aplicados a los procedimientos e instalaciones de la FNMT-RCM, en aquello que pueda ser publicado sin perjudicar la eficacia de los mismos, las normas de secreto y confidencialidad, así como cuestiones relativas a la propiedad de sus bienes y activos, a la protección de datos de carácter personal y demás cuestiones de tipo informativo general que deben ponerse a disposición del público, independientemente de su papel en la Comunidad Electrónica.

   2) Y, por otra parte, la ***Política de Certificación*** específica en la que se describen las obligaciones de las partes, los límites de uso de los *Certificados* y responsabilidades y las ***Prácticas de Certificación Particulares*** que desarrollan los términos definidos en la política correspondiente y otorgan prestaciones adicionales o específicas sobre las generales establecidas en la *Declaración General de Prácticas de Certificación*.

      Estas *Políticas de Certificación* y *Prácticas de Certificación Particulares* concretan lo articulado en el cuerpo principal de la *Declaración General de Prácticas de Certificación* y, por tanto, son parte integrante de ella, conformando, ambos, la *Declaración de Prácticas de Certificación* de la FNMT-RCM.

7. El objetivo del presente documento es la información pública del conjunto de prácticas, condiciones y características de los servicios de certificación que presta la FNMT-RCM como *Prestador de Servicios de Confianza*, en relación al ciclo de vida de los *Certificados* electrónicos de *Representante de Persona jurídica*, del *Certificado de Representante de Entidad sin personalidad jurídica* y del *Certificado de Representante para administradores únicos y solidarios*.

8. Deberá tenerse presente, a efectos interpretativos del presente anexo, el apartado "Definiciones" de la DGPC y el de este documento.

9. En resumen, estas *Políticas de Certificación* y *Prácticas de Certificación Particulares* concretan lo articulado en el cuerpo principal de la DGPC y, por tanto, son parte integrante de ella, conformando, ambos documentos, la *Declaración de Prácticas de Certificación* de la FNMT-RCM para los *Certificados de Representante de Persona jurídica*, del *Certificado de Representante de Entidad sin personalidad jurídica* y del *Certificado de Representante para administradores únicos y solidarios*. Así pues, lo descrito en este documento, sólo es

de aplicación para el conjunto de *Certificados* caracterizado e identificado en esta *Política y Prácticas Particulares de Certificación* y pueden revestir, además, especialidades plasmadas a través de la *Ley de Emisión* del *Certificado* o grupo de *Certificados* correspondiente, en caso de que existan características o funcionalidades específicas.

3. ORDEN DE PRELACIÓN

10. La presente Declaración de *Política y Prácticas de Certificación Particulares* aplica a los *Certificados de Representante de Personas jurídicas*, a los *Certificados de Representante de Entidades sin personalidad jurídica* y a los *Certificados de Representante para administradores únicos o solidarios* y tendrán prelación sobre lo dispuesto en el cuerpo principal de la *Declaración General de Prácticas de Certificación*.

Por tanto, en caso de que existiera contradicción entre el presente documento y lo dispuesto en la *Declaración General de Prácticas de Certificación*, tendrá preferencia lo aquí articulado.

4. DEFINICIONES

11. A los efectos de lo dispuesto en el presente documento, particularizando las definiciones de la *Declaración General de Prácticas de Certificación* y únicamente cuando los términos comiencen con letra mayúscula y estén en cursiva, se entenderá por:

- *Certificado de Representante de Persona jurídica:* es la certificación electrónica expedida por la FNMT-RCM que vincula un *Firmante* a unos *Datos de verificación de Firma* y confirma su identidad. Este *Certificado* se corresponde con el certificado tradicionalmente utilizado por las Administraciones Públicas para el ámbito tributario y que, posteriormente, ha sido admitido para otros ámbitos. Por tanto, este *Certificado* se expide a las P*ersonas Jurídicas* para su uso en sus relaciones con aquellas Administraciones Públicas, Entidades y Organismos Públicos, vinculados o dependientes de las mismas.
- *Certificado de Representante de Entidad sin personalidad jurídica:* es la certificación electrónica expedida por la FNMT-RCM a una *Entidad sin personalidad jurídica* que vincula un *Firmante* a unos *Datos de verificación de Firma* y confirma su identidad en el ámbito tributario y otros ámbitos admitidos por la legislación vigente.
- *Certificado de Representante para administradores únicos y solidarios*: es la certificación electrónica expedida por la FNMT-RCM que vincula un *Firmante* a con unos *Datos de verificación de Firma* y confirma su identidad. El *Firmante* actúa en representación de una *Persona jurídica* en calidad de representante legal con su cargo de administrador único o solidario inscrito en el Registro Mercantil.
- *Entidad representada*: *Persona jurídica* o *Entidad sin personalidad jurídica* en nombre de las cuales actúa el *Firmante* de un *Certificado* de los incluidos en la presente *Política y Prácticas de Certificación Particulares.*
- *Entidad sin personalidad jurídica*: son las entidades a las que se refiere el artículo 35.4 de la Ley General Tributaria y resto de legislación aplicable.

- *Firmante*: es la persona física que posee un dispositivo de creación de firma y que actúa (realiza la firma) en nombre propio o en nombre de la *Persona jurídica* a la que representa.
- *Persona jurídica*: persona o conjunto de personas agrupadas que constituyen una unidad con finalidad propia, la cual adquiere, como entidad, capacidad jurídica y de obrar distinta de la del miembro o de los miembros que la componen.
- *Prestador de Servicios de Confianza*: la persona física o jurídica que presta uno o más *Servicios de Confianza* de conformidad con lo establecido en el REGLAMENTO (UE) Nº 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
- *Representante*: Persona física que actúa en representación, legal o voluntaria, de una *Persona jurídica* o una *Entidad sin personalidad Jurídica*.
- *Servicio de Confianza*: un servicio electrónico que consiste en alguna de las siguientes actividades: la creación, verificación, validación, gestión y conservación de F*irmas Electrónicas*, sellos electrónicos, *Sellos de Tiempo*, documentos electrónicos, servicios de entrega electrónica, autenticación de sitios web y *Certificados Electrónicos*, incluidos los certificados de *Firma Electrónica* y de sello electrónico.
- *Solicitante*: persona física mayor de 18 años o menor emancipado, que previa identificación, solicita una operación relativa a un *Certificado* en nombre de la *Entidad representada*. A efectos de las presentes *Políticas y Prácticas de Certificación Particulares* coincidirá con la figura del *Representante*.

(Los términos señalados en cursiva se definen en el presente documento o en la Declaración General de Prácticas de Certificación).

5. SEUDÓNIMOS

12. En cuanto a la identificación de los *Firmantes* mediante el uso de los *Certificados* expedidos bajo la presente *Política de Certificación*, la FNMT-RCM no admite el uso de seudónimos.

6. PERFIL DE LOS CERTIFICADOS

13. Todos los *Certificados* emitidos bajo esta política son de conformidad con el estándar X.509 versión 3.

6.1. RESTRICCIONES DE LOS NOMBRES

14. La codificación de los *Certificados* sigue la recomendación RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Reocation List (CRL) Profile". Todos los campos definidos en el perfil de los *Certificados* en el anexo II de las presentes *Políticas de Certificación,* excepto en los campos que específicamente se exprese lo contrario, emplean la codificación UTF8String.

6.2. USO DE LA EXTENSIÓN POLICY CONSTRAINS

15. La extensión Policy Constrains del certificado raíz de la AC no es utilizado.

6.3. SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS

16. La extensión Certificate Policies incluye dos campos de Policy Qualifiers:

- CPS Pointer: contiene la URL donde se publica la *Declaración General de Prácticas de Certificación* y las *Políticas de Certificación* y *Prácticas de Certificación Particulares* aplicables a los *Certificados.*
- User notice: contiene un texto que puede ser desplegado en la pantalla del usuario del *Certificado* durante la verificación del mismo.

6.4. TRATAMIENTO SEMÁNTICO DE LA EXTENSIÓN "CERTIFICATE POLICY"

17. La extensión Certificate Policy incluye el campo OID de política, que identifica la política asociada al *Certificado* por parte de la FNMT–RCM, así como los dos campos relacionados en el apartado anterior.

7. RECONOCIMIENTO Y AUTENTICACIÓN DE MARCAS REGISTRADAS

18. La FNMT–RCM no asume compromiso alguno sobre el uso de signos distintivos, registrados o no, en la emisión de los *Certificados* expedidos bajo la presente *Política de Certificación.* Sólo se permite la solicitud de *Certificados* que incluyan signos distintivos cuyo derecho de uso sea propiedad de la *Entidad representada* o se encuentre debidamente autorizada. La FNMT–RCM no está obligada a verificar previamente la titularidad o registro de los signos distintivos antes de la emisión de los *Certificados* aunque figuren en registros públicos.

8. GESTIÓN DEL CICLO DE VIDA DE LAS CLAVES DEL PRESTADOR DE SERVICIOS DE CONFIANZA

19. La FNMT-RCM, en su actividad *como Prestador de Servicios de Confianza*, en relación con las claves criptográficas empleadas para la expedición de *Certificados de Persona Física,* declara que realizará la gestión descrita en el siguiente apartado.

8.1. GESTIÓN DEL CICLO DE VIDA DE LAS *CLAVES*

8.1.1. Generación de las *Claves* del *Prestador de Servicios de Confianza*

20. Las *Claves* de la FNMT-RCM, como *Prestador de Servicios de Confianza*, son generadas en circunstancias completamente controladas, en un entorno físicamente seguro y, al menos, por dos personas autorizadas para ello, utilizando sistemas hardware y software que cumplen con la normativa actual en materia de protección criptográfica, tal y como se muestra en la *Declaración General de Prácticas de Certificación*.

8.1.2. Almacenamiento, salvaguarda y recuperación de las Claves del Prestador de Servicios de Confianza

21. La FNMT-RCM utiliza los mecanismos necesarios para mantener su *Clave privada* confidencial y mantener su integridad en la forma que se muestra en la *Declaración General de Prácticas de Certificación*.

8.1.3. Distribución de los Datos de verificación de Firma del Prestador de Servicios de Confianza

22. La FNMT-RCM utiliza los mecanismos necesarios para mantener la integridad y autenticidad de su *Clave Pública*, así como su distribución en la forma que se muestra en la *Declaración General de Prácticas de Certificación*.

23. Los *Certificados de Persona Física* son expedidos por una *Autoridad de Certificación* subordinada a la *Autoridad de Certificación* raíz de la FNMT – RCM. Las características de ambas *Autoridades de Certificación* se recogen en el anexo I del presente documento.

24. Por tanto, los *Certificados* expedidos bajo la *Política de Certificación* identificada en este documento vendrán firmados electrónicamente con los *Datos de Creación de Firma* del *Prestador de Servicios de Confianza*.

25. Los *certificados raíz* de las *Autoridades de Certificación* que intervienen en la expedición de los *certificados de Persona Física* se encuentran definidos en el anexo II del presente documento.

8.1.4. Almacenamiento, salvaguarda y recuperación de las Claves Privadas de los *Titulares*

26. La FNMT-RCM bajo ningún concepto genera ni almacena las *Claves Privadas* de los *Titulares* de los *Certificados*, las cuales son generadas bajo el exclusivo control del *Solicitante*, y cuya custodia está bajo la responsabilidad del *Titular* del certificado asociado a dichas *Claves Privadas*.

8.1.5. Uso de los Datos de Creación de Firma del Prestador de Servicios de Confianza

27. Los *Datos de Creación de Firma* de la FNMT-RCM, en su actividad como *Prestador de Servicios de Confianza*, serán utilizados única y exclusivamente para los propósitos de:

1) Firma de *Certificados*.
2) Firma de las *Listas de Revocación*.
3) Otros usos previstos en esta *Declaración* y/o en la legislación aplicable.

8.1.6. Fin del ciclo de vida de las Claves del Prestador de Servicios de Confianza

28. La FNMT-RCM dispondrá de los medios necesarios para lograr que, una vez finalizado el período de validez de las *Claves* del *Prestador de Servicios de Confianza*, estas *Claves* no vuelven a ser utilizadas, bien destruyéndolas o almacenándolas de forma apropiada para dicha finalidad.

8.1.7. Ciclo de vida del hardware criptográfico utilizado para firmar Certificados

29. La FNMT-RCM dispondrá de los medios necesarios para posibilitar que el hardware criptográfico utilizado para la protección de sus *Claves* como *Prestador de Servicios de Confianza*, no sufra manipulaciones de acuerdo con el estado de la técnica a la fecha durante todo su ciclo de vida, estando situado dicho componente en un entorno físicamente seguro desde su recepción hasta su destrucción llegado el caso.

9. OPERACIÓN Y GESTIÓN DE LA INFRAESTRUCTURA DE *CLAVE PÚBLICA*; ESQUEMA NACIONAL DE INTEROPERABILIDAD Y ESQUEMA NACIONAL DE SEGURIDAD

9.1. OPERACIÓN Y GESTIÓN DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA

30. Las operaciones y procedimientos realizados para la puesta en práctica de las *Política de Certificación* reflejada en este documento se realizan siguiendo los controles requeridos por los estándares reconocidos para tal efecto, describiéndose estas actuaciones en los apartados "Controles de seguridad física, de procedimientos y de personal" y "Controles de seguridad técnica" de la *Declaración General de Prácticas de Certificación* de la FNMT-RCM.

31. Adicionalmente cabe destacar que la FNMT-RCM posee un *Sistema de Gestión de la Seguridad de la Información* (en adelante SGSI) para su Departamento CERES con el objetivo final de mantener y garantizar la seguridad de la información de los miembros de la *Comunidad Electrónica*, así como la suya propia, de forma que los servicios FNMT-RCM-CERES se presten con un razonable grado de seguridad conforme al estado actual de la técnica. El SGSI de FNMT-RCM-CERES es aplicable a los activos de información definidos en el Análisis de Riesgos realizado para todas las Áreas que componen el departamento, incluyendo como activos los servicios prestados a los miembros de la *Comunidad Electrónica*.

32. En el documento Declaración General de Prácticas de Certificación, se da respuesta concreta para todos aquellos aspectos referentes a los siguientes apartados de la norma ETSI TS 101 456:

- Gestión de la seguridad
- Clasificación y gestión de activos
- Seguridad del personal
- Seguridad física y ambiental
- Gestión de operaciones
- Sistema de gestión de accesos
- Desarrollo y mantenimiento de los sistemas de confianza
- Gestión de la continuidad de negocio y gestión de incidentes
- Terminación de la AC
- Cumplimiento de requisitos legales

- Grabación y custodia de información relativa a certificados reconocidos

9.2. INTEROPERABILIDAD

Los *Certificados* relativos a las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares* son expedidos por la FNMT – RCM conforme a la Resolución de 29 de noviembre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se publica el Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados de la Administración General del Estado y se anuncia su publicación en la sede correspondiente, y concretamente el perfil de este tipo de certificados es conforme al perfil aprobado por el Consejo Superior de Administración Electrónica, en reunión de la Comisión Permanente de 30 de mayo de 2012 y publicado en el anexo II de la citada Resolución.

10. DIFUSIÓN DE TÉRMINOS Y CONDICIONES

33. La FNMT-RCM pone a disposición de la *Comunidad Electrónica* y demás interesados, tanto el presente documento como el documento de *Declaración General de Prácticas de Certificación* de la FNMT-RCM en los que se detalla:

1) Los términos y condiciones que regulan la utilización de los *Certificados* expedidos por la FNMT-RCM.
2) La Política de Certificación aplicable a los *Certificados* expedidos por la FNMT-RCM.
3) Los límites de uso para los *Certificados* expedidos bajo esta Política de Certificación.
4) Las obligaciones, garantías y responsabilidades de las partes involucradas en la expedición y uso de los *Certificados*.
5) Los períodos de conservación de la información recabada en el proceso de registro y de los eventos producidos en los sistemas del *Prestador de Servicios de Confianza* relacionados con la gestión del ciclo de vida de los *Certificados* expedidos bajo esta *Política de Certificación*.

11. RESPONSABILIDADES Y OBLIGACIONES DE LAS PARTES

34. El presente apartado recoge las obligaciones y responsabilidades de las partes implicadas en la expedición y uso del *Certificado de Representante de Persona jurídica*, del *Certificado de Representante de Entidad sin personalidad jurídica* y del *Certificado de Representante para administradores únicos y solidarios*. En el caso de identificar obligaciones y responsabilidades específicas de cada uno de estos certificados, se expresarán en los apartados correspondientes en el presente documento.

35. Serán partes a los efectos de este apartado los siguientes sujetos:

- FNMT-RCM, en cuanto *Prestador de Servicios de Confianza*.
- Oficinas de Registro, que, a través del personal designado por la Administración competente, debe seguir los procedimientos establecidos por la FNMT-RCM en la presente *Declaración de Prácticas de Certificación* y en las *Políticas de Certificación*,

en el desempeño de sus funciones de gestión, expedición, renovación y revocación de *Certificados* y no salirse de dicho marco de actuación.

- El Colegio de Registradores de la Propiedad y Mercantiles de España (CORPME),en el caso del *Certificado de Representante para administradores únicos y solidarios*.
- La *Entidad representada* y el *Representante* (*Solicitante*).
- La *Entidad usuaria*, los terceros que confían en los *Certificados* y, en general los miembros de la *Comunidad Electrónica*.

36. FNMT-RCM no será responsable de la utilización de estos tipos de *Certificados* cuando el *Representante* o usuario del *Certificado* realice actuaciones sin facultades, extralimitándose en las mismas o en fraude de ley o de terceros, si no existe notificación fehaciente que permita trasladar los efectos pretendidos a la gestión de los *Certificados*.

11.1. RESPONSABILIDADES DE LAS PARTES

37. Para poder usar *Certificados* expedidos por la FNMT-RCM se deberá previamente formar parte de la *Comunidad Electrónica* y adquirir la condición de *Entidad Usuaria*. Para confiar en un *Certificado* expedido por la FNMT-RCM, será imprescindible comprobar el estado de validez del *Certificado* mediante el *Servicio de Información y Consulta sobre el Estado de los Certificados* de dicha Entidad.

38. De producirse esta confianza por parte de un miembro de la *Comunidad Electrónica*, *Entidad Usuaria* o por parte de un tercero, sin realizar la comprobación del estado del *Certificado*, no se obtendrá cobertura de la *Declaración de Prácticas de Certificación* y se carecerá de legitimidad alguna para reclamar o emprender acciones judiciales contra la FNMT-RCM. Por tanto, en tal caso, esta Entidad no será responsable de los daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado* expedido bajo las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares*.

11.1.1. Responsabilidad del Prestador de Servicios de Confianza

39. La FNMT-RCM únicamente responde de la correcta identificación del *Solicitante,* del *Representante* y de la *Entidad representada*. Respecto de esta información, la FNMT-RCM se limita únicamente a expresarla en un *Certificado*.

40. La FNMT-RCM únicamente responderá por deficiencias en los procedimientos propios de su actividad como *Prestador de Servicios de Confianza*, y conforme a lo dispuesto en estas *Políticas* y *Prácticas de Certificación* o en la Ley. En ningún caso será responsable de las acciones o de las pérdidas en las que incurran*, Solicitantes, Representantes*, *Entidades representadas*, *Entidades usuarias*, o, en su caso, terceros involucrados, que no se deban a errores imputables a la FNMT-RCM en los mencionados procedimientos de expedición y/o de gestión de los *Certificados*.

41. FNMT-RCM no responderá en los supuestos de caso fortuito, fuerza mayor, atentado terrorista, huelga salvaje, así como en los supuestos que se trate de acciones constitutivas de delito o falta que afecten a sus infraestructuras prestadoras, salvo que hubiera mediado culpa grave de la entidad. En todo caso, en los correspondientes contratos y/o convenios FNMT

podrá establecer cláusulas de limitación de responsabilidad adicionales a las recogidas en este documento.

42. La FNMT-RCM no responderá ante personas cuyo comportamiento en la utilización de los *Certificados* haya sido negligente, debiendo considerarse a estos efectos y en todo caso como negligencia la falta de observancia de lo dispuesto en la *Declaración de Prácticas de Certificación*, y, en especial, lo dispuesto en los apartados referidos a las obligaciones y a la responsabilidad de las partes.

43. La FNMT-RCM no responderá de ningún software que no haya proporcionado directamente.

44. La FNMT-RCM no garantiza los algoritmos criptográficos, ni responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si guardó la diligencia debida de acuerdo con el estado actual de la técnica, y procedió conforme a lo dispuesto en esta *Declaración de Prácticas de Certificación* y en la Ley.

45. En todo caso y con la condición de cláusula penal, la cuantía que la FNMT-RCM debiera satisfacer, en concepto de daños y perjuicios, por imperativo judicial a terceros perjudicados o miembros de la *Comunidad Electrónica* en cualquier ámbito de actuación público o privado, en defecto de regulación específica en los contratos o convenios, se limita a un máximo de SEIS MIL EUROS (6.000€).

46. La FNMT-RCM no establece límites adicionales en los *Certificados Electrónicos* expedidos bajo las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares* por razón de la cuantía o de la materia.

11.1.2. Responsabilidad del Solicitante

47. El *Solicitante* responderá de la veracidad y exactitud de la información presentada durante la solicitud del *Certificado*, de que cuenta con apoderamiento suficiente de la *Entidad representada* u ostenta la condición de administrador único o solidario a los efectos de la prestación del servicio.

48. El *Solicitante* mantendrá a salvo y defenderá a su costa a la FNMT-RCM contra cualquier acción que pudiera emprenderse contra esta Entidad y contra cualquier daño y perjuicio que sufra la FNMT-RCM como consecuencia de falsedades o errores graves en la información suministrada en el proceso de solicitud del *Certificado,* o como consecuencia de un acto u omisión culposa o negligente del *Solicitante*.

11.1.3. Responsabilidad de la *Entidad representada* y del *Representante*

49. Será en todo caso responsabilidad de la *Entidad representada* y del *Representante* utilizar de manera adecuada y custodiar diligentemente el *Certificado*, según el propósito y función para el que ha sido expedido, así como informar a la FNMT-RCM acerca de cualquier variación de estado o información respecto de lo reflejado en el *Certificado*, para su revocación y nueva expedición.

50. Asimismo, serán la *Entidad representada* y el *Representante* quienes deban responder, en todo caso, ante la FNMT-RCM, las *Entidades usuarias* y, en su caso, ante terceros, del uso

indebido del *Certificado*, o de la falsedad o errores de las manifestaciones en él recogidas, o actos u omisiones que provoquen daños y perjuicios a la FNMT-RCM o a terceros.

51. Será responsabilidad y, por tanto, obligación de la *Entidad representada* y del *Representante* no usar el *Certificado* en caso de que el *Prestador de Servicios de Confianza* haya cesado en la actividad como Entidad emisora de *Certificados* que realizó la expedición del *Certificado* en cuestión y no se hubiera producido la subrogación prevista en la Ley. En todo caso, la *Entidad representada* y el *Representante* no usarán el *Certificado* en los casos en los que los *Datos de Creación de Firma* del *Prestador* puedan estar amenazados y/o comprometidos, y así se haya comunicado por el Prestador o, en su caso, hubieran tenido noticia de estas circunstancias.

11.1.4. Responsabilidad de la Entidad Usuaria y terceros que confían

52. Será responsabilidad de la *Entidad usuaria*, de los terceros que confían en los *Certificados* y, en general de los miembros de la *Comunidad Electrónica*, la verificación y comprobación del estado de los *Certificados*, no cabiendo en ningún caso presumir la validez de los *Certificados* sin dichas comprobaciones.

53. No podrá considerarse que la *Entidad usuaria* y terceros que confían en los *Certificados* han actuado con la mínima diligencia debida si confían en una *Firma Electrónica* basada en un *Certificado* expedido por la FNMT-RCM sin haber observado lo dispuesto en la *Declaración de Prácticas de Certificación* y comprobado que dicha *Firma Electrónica* puede ser verificada por referencia a una *Cadena de Certificación* válida.

54. Si las circunstancias indican necesidad de garantías adicionales, la *Entidad Usuaria* deberá obtener garantías adicionales para que dicha confianza resulte razonable.

55. Asimismo, será responsabilidad de la *Entidad Usuaria* observar lo dispuesto en la *Declaración de Prácticas de Certificación* y sus posibles modificaciones futuras, con especial atención a los límites de uso establecidos para cada *Certificado* en su correspondiente *Política de Certificación*.

11.2. OBLIGACIONES Y GARANTÍAS DE LAS PARTES

11.2.1. Obligaciones y Garantías del Prestador de Servicios de Confianza

56. La FNMT-RCM no estará sujeta a otras garantías ni otras obligaciones que las establecidas en la normativa de aplicación y en la *Declaración de Prácticas de Certificación*.

57. La FNMT – RCM cumple los requisitos de las especificaciones técnicas de la norma ETSI TS 101 456 para la emisión de *Certificados reconocidos* y se compromete a continuar cumpliendo con dicha norma o aquellas que la sustituyan.

58. Sin perjuicio de lo dispuesto en la legislación sobre firma electrónica, y su normativa de desarrollo, así como en su normativa específica, el *Prestador de Servicios de Confianza* se obliga a:

59. Con carácter previo a la expedición del *Certificado*:

- Verificar que toda la información contenida en la solicitud del *Certificado* se corresponde con la aportada por el *Solicitante*.

- Comprobar que el *Solicitante* está en posesión de la *Clave Privada* que constituirá, una vez expedido el *Certificado*, los *Datos de Creación de Firma* correspondientes a los de *Datos de Verificación de Firma* que constarán en el *Certificado*, y comprobar su complementariedad.
- Garantizar que los procedimientos seguidos aseguran que las *Claves Privadas* que constituyan los *Datos de Creación de Firma* son generados sin que se realicen copias ni se produzca el almacenamiento de los mismos por parte de la FNMT-RCM.
- Realizar la comunicación de información al *Representante* y *Solicitante* de tal forma que se procure su *Confidencialidad*.
- Poner a disposición del *Solicitante, Representante* y demás interesados (http://www.ceres.fnmt.es) la *Declaración de Prácticas de Certificación* y cuanta información sea relevante para el desarrollo de los procedimientos relacionados con el ciclo de vida de los *Certificados* objeto de esta *Política de Certificación* y *Prácticas de Certificación Particulares* de conformidad con la normativa aplicable.

60. En cualquier caso, la FNMT-RCM actuará eficazmente para:

- Comprobar que el *Solicitante* del *Certificado* utiliza la *Clave Privada* correspondiente a la *Clave Publica* vinculada a la identidad de la *Entidad representada* y del *Firmante* del mismo. Para ello, la FNMT-RCM comprobará la correspondencia entre la *Clave privada* y la *Clave pública*.
- Lograr que la información incluida en el *Certificado* se base en la información proporcionada por el *Solicitante* u obtenida de registros públicos.
- No ignorar hechos notorios que puedan afectar a la fiabilidad del *Certificado.*
- Lograr que el *DN* (nombre distintivo) asignado en el *Certificado* sea único en toda la *Infraestructura de Clave Pública* de la FNMT-RCM.

61. La FNMT-RCM, en ningún caso, incluirá en un *Certificado* información distinta de la aquí mostrada, ni circunstancias, atributos específicos de los *Firmantes* o límites distintos a los previstos en la presente *Declaración de Prácticas de Certificación*.

62. Conservación de la información por la FNMT-RCM

- Conservar toda la información y documentación relativa a cada *Certificado*, en las debidas condiciones de seguridad, durante quince (15) años contados desde el momento de su expedición.
- Mantener un *Directorio* seguro y actualizado de *Certificados* en el que se identifican los *Certificados* expedidos, así como su vigencia, incluyendo en forma de *Listas de Revocación* la identificación de los *Certificados* que hayan sido revocados. La integridad de este *Directorio* se protegerá mediante la utilización de sistemas conformes con las disposiciones reglamentarias específicas que al respecto se dicten en España y, en su caso, en la UE.
- Mantener un servicio de información y consulta sobre el estado de los *Certificados*.

- Establecer un mecanismo de fechado que permita determinar con exactitud la fecha y la hora en las que se expidió un *Certificado*, o se extinguió su vigencia.
- Conservar la *Declaración de Prácticas de Certificación* durante 15 años desde su derogación por publicación de una nueva versión de la misma, en las debidas condiciones de seguridad.

63. Protección de los Datos de Carácter Personal:

- La FNMT-RCM se compromete a cumplir la legislación vigente en materia de Protección de Datos de Carácter Personal, fundamentalmente, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y el resto de normas de aplicación.
- Para informarse sobre la política de protección de datos seguida por la FNMT-RCM, y acerca del uso que de los datos se realiza, se puede consultar la DGPC.

64. Revocación de *Certificados*:

- Acerca de la revocación de *Certificados* y de las obligaciones que la FNMT-RCM se compromete a asumir al respecto, se puede consultar el procedimiento de revocación de *Certificados* reflejado en el presente documento.

65. Cese de la actividad de la FNMT-RCM como *Prestador de Servicios de Confianza*:

- A este respecto se puede consultar el apartado correspondiente de la DGPC.

11.2.2. Obligaciones de la Oficina de Registro

66. Para la gestión del ciclo de vida de los *Certificados de Representante de Persona jurídica*, los *Certificados de Representante de Entidad sin personalidad jurídica* y los *Certificados de Representante para administradores únicos y solidarios*, las *Oficinas de Registro* tienen la obligación de:

- Con carácter general, seguir los procedimientos establecidos por la FNMT-RCM en la *Política y Prácticas de Certificación* de aplicación en el desempeño de sus funciones de gestión, expedición y revocación de *Certificados* y no alterar dicho marco de actuación.
- Permitir a la FNMT-RCM el acceso a los archivos y la auditoría de sus procedimientos en relación con los datos obtenidos en calidad de *Oficina de Registro*.
- Comunicar a la FNMT-RCM, a través de los medios dispuestos para ello, cualquier evento relacionado con la gestión del ciclo de vida de los *Certificados* expedidos por la FNMT-RCM: solicitudes de expedición, renovación, etc.
- Respecto de la extinción de la validez de los *Certificados:*

  1 Comprobar diligentemente las causas de revocación y suspensión que pudieran afectar a la vigencia de los *Certificados*.

2 Comunicar a la FNMT-RCM de forma diligente las solicitudes de revocación y suspensión de los *Certificados*.

- Respecto de la Protección de Datos de Carácter Personal, será de aplicación lo dispuesto en el apartado correspondiente de la *Declaración General de Prácticas de Certificación.*
- Las Oficinas de Registro, a través del personal adscrito al servicio, por relación laboral o funcionarial, deberán ejercer funciones públicas de acuerdo con la legislación específica aplicable a la FNMT-RCM.
- Conservar toda la información y documentación relativa a los *Certificados*, cuya solicitud, renovación o revocación gestiona durante quince (15) años.
- Comprobar diligentemente las causas de revocación que pudieran afectar a la vigencia de los *Certificados*.

11.2.3. Obligaciones *del Solicitante*, de la *Entidad representada* y del *Representante*

67. Los *Solicitantes*, las *Entidades representadas* y los *Representantes* de los *Certificados de Representante de Persona jurídica*, de los *Certificados de Representante de Entidad sin personalidad jurídica* y de los *Certificados de Representante para administradores únicos y solidarios*, tienen la obligación de:

- No usar el *Certificado* fuera de los límites especificados en las presentes *Política y Prácticas de Certificación* particulares.
- Aportar información veraz en la solicitud de los *Certificados* y mantenerla actualizada, suscribiendo los contratos por persona con capacidad suficiente.
- No solicitar *Certificados* conteniendo signos distintivos, denominaciones o derechos protegidos por las normas sobre propiedad industrial o intelectual de las que no sea titular, licenciatario o cuente con autorización demostrable para su uso.
- Actuar con diligencia respecto de la custodia y conservación de los *Datos de creación de Firma* o cualquier otra información sensible como *Claves*, códigos de activación del *Certificado*, palabras de acceso, números de identificación personal, etc., así como de los soportes de los *Certificados,* lo que comprende en todo caso, la no revelación de ninguno de los datos mencionados.
- Conocer y cumplir las condiciones de utilización de los *Certificados* previstas en las condiciones de uso y en la *Declaración de Prácticas de Certificación* y en particular, las limitaciones de uso de los *Certificados.*
- Conocer y cumplir las modificaciones que se produzcan en la *Declaración de Prácticas de Certificación*.
- Solicitar la revocación del correspondiente *Certificado*, según el procedimiento descrito en el presente documento, notificando diligentemente a la FNMT-RCM, las circunstancias para la revocación o sospecha de pérdida de la *Confidencialidad*, la divulgación, modificación o uso no autorizado de los *Datos de Creación de Firma*.

- Revisar la información contenida en el *Certificado*, y notificar a la FNMT-RCM cualquier error o inexactitud.
- Verificar con carácter previo a confiar en los *Certificados,* la *Firma electrónica reconocida* del *Prestador de Servicios de Confianza* emisor del *Certificado.*
- Notificar diligentemente a la FNMT-RCM cualquier modificación de los datos aportados en la solicitud del *Certificado*, solicitando, cuando consecuentemente fuere pertinente, la revocación del mismo.
- Devolver o destruir el *Certificado* cuando así lo exija la FNMT-RCM, y no usarlo con propósito de firmar o identificarse electrónicamente cuando el *Certificado* caduque, o sea revocado.

11.2.4. Obligaciones de la Entidad Usuaria y terceros que confían

68. Las *Entidades Usuarias*, los miembros de la *Comunidad Electrónica* y, en general, los terceros que confían en los *Certificados de Representante de Persona jurídica*, en los *Certificados de Representante de Entidad sin personalidad jurídica* y en los *Certificados de Representante para administradores únicos y solidarios*, tienen la obligación de:

- Verificar con carácter previo a confiar en los *Certificados*, la *Firma Electrónica* reconocida del *Prestador de Servicios de Confianza* emisor del *Certificado*.
- Verificar que el *Certificado* en el que están confiando continúa vigente y activo.
- Verificar el estado de los *Certificados* en la *Cadena de Certificación*, a través del *Servicio de Información y Consulta sobre el Estado de los Certificados* de la FNMT-RCM.
- Comprobar las limitaciones de uso del *Certificado* que se verifica.
- Conocer las condiciones de utilización del *Certificado* conforme a las *Políticas y Declaraciones de Prácticas de Certificación* de aplicación.
- Notificar a la FNMT-RCM cualquier anomalía o información relativa al *Certificado* y que pueda ser considerada como causa de revocación del mismo, aportando todos los elementos probatorios de los que disponga.

12. CERTIFICADOS DE REPRESENTANTE DE PERSONA JURÍDICA Y DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA

12.1. RESPONSABILIDADES Y OBLIGACIONES DE LAS PARTES

69. El presente apartado recoge las obligaciones y responsabilidades de las partes implicadas en la expedición y uso del *Certificado de Representante de Persona jurídica* y del *Certificado de Representante de Entidad sin personalidad jurídica*. Por tanto, son de aplicación tanto la siguiente relación de obligaciones y responsabilidades específicas para estos dos tipos de certificados, como las ya descritas en el apartado "11 Responsabilidades y obligaciones de las partes" relativas a los tipos de C*ertificados* incluidos en el presente documento de *Políticas y Prácticas Particulares de Certificación*.

12.1.1. Responsabilidades de las partes

12.1.1.1. Responsabilidad del Prestador de Servicios de Confianza

70. Además de las responsabilidades recogidas en el apartado de responsabilidad general, la FNMT-RCM, a través de la *Oficina de Registro*, responde de la correcta identificación de la *Entidad representada* y del *Representante*, comprobando la legalidad extrínseca de los documentos aportados para acreditar el alcance de su representación, incluyendo una indicación de esta información en el *Certificado*. La FNMT-RCM no será responsable de cualesquiera daños producidos, a la *Entidad representada* o a terceros, por parte del *Solicitante* en caso de que infrinja las obligaciones de aportar documentación fidedigna o la aportada contenga inexactitudes, errores o falsedades y se produzca la expedición del *Certificado*. FNMT-RCM tampoco será responsable si el *Representante* utilizara indebidamente el *Certificado*, en caso de falta de vigencia, capacidad insuficiente, caducidad, revocación, extinción de su apoderamiento o lo utilizara más allá de su ámbito de aplicación inicial.

12.1.1.2. Responsabilidad del Solicitante

71. Es de aplicación el apartado "11 Responsabilidades y obligaciones de las partes". Además, el *Solicitante*, para este tipo de *Certificados*, será responsable de la acreditación de la personalidad jurídica de la *Entidad representada*, de la vigencia y capacidad suficiente de su apoderamiento para la solicitud y utilización de estos *Certificados*, según su propósito, y de solicitar la revocación del *Certificado* en el momento que varíen los datos del *Solicitante* o de la *Entidad representada*, siendo responsable, frente a la FNMT-RCM y frente a terceros, si el *Certificado* se utilizara después de que finalice su apoderamiento, haya sido revocado, de que tales datos hayan variado o que se utilice más allá del ámbito de aplicación del *Certificado*.

12.1.1.3. Responsabilidad de la Entidad representada y del Representante

72. Es de aplicación el apartado "11 Responsabilidades y obligaciones de las partes". Además, la *Entidad representada* y el *Representante*, para este tipo de *Certificados*, serán responsables de constatar la personalidad jurídica de la *Entidad representada*, de la vigencia y capacidad suficiente del apoderamiento del *Representante/Firmante* para la utilización de estos *Certificados*, según su propósito, y de solicitar la revocación del *Certificado* en el momento que varíen los datos del *Representante* o de la *Entidad representada*, siendo responsables, frente a la FNMT-RCM y frente a terceros, si el *Certificado* se utilizara después de que finalice el apoderamiento del *Representante*, haya sido revocado, de que tales datos hayan variado o que se utilice más allá del ámbito de aplicación inicial del *Certificado*.

12.1.1.4. Responsabilidad de la Entidad Usuaria y terceros que confían

73. Es de aplicación el apartado "11 Responsabilidades y obligaciones de las partes".

12.1.2. Obligaciones y garantías de las partes

12.1.2.1. Obligaciones y Garantías del Prestador de Servicios de Confianza

74. Sin perjuicio de lo dispuesto en la legislación sobre firma electrónica, y su normativa de desarrollo, así como en su normativa específica, el *Prestador de Servicios de Confianza* se obliga a comprobar, durante el proceso de registro y con carácter previo a la expedición del *Certificado,* los datos relativos a la personalidad jurídica de la *Entidad representada* y a la identidad y capacidad del *Representante.* Todas estas comprobaciones se realizarán según lo dispuesto en las *Prácticas de Certificación Particulares* expresadas en este documento y según los protocolos y procedimientos de registro de la FNMT-RCM.

75. En los procesos de comprobación de los extremos señalados anteriormente la FNMT-RCM podrá realizar verificaciones mediante la intervención de terceros que ostenten facultades fedatarias o de registros públicos o privados.

12.1.2.2. Obligaciones de la Oficina de Registro

76. Para la gestión del ciclo de vida de los *Certificados de Representante de Persona jurídica* y de los *Certificados de Representante de Entidad sin personalidad jurídica*, las *Oficinas de Registro* tienen la obligación de comprobar la identidad de la *Entidad representada,* así como la identidad, suficiencia del nombramiento o apoderamiento y cualesquiera circunstancias personales de los *Representantes* de los *Certificados* relevantes para el fin propio de estos, utilizando cualquiera de los medios admitidos en Derecho y conforme a lo previsto con carácter general en la DGPC y con carácter particular en las presentes *Políticas y Prácticas de Certificación Particulares*.

12.1.2.3. Obligaciones de la Entidad representada y del Representante

77. Es de aplicación el apartado “11 Responsabilidades y obligaciones de las partes”.

12.1.2.4. Obligaciones de la Entidad Usuaria y terceros que confían

78. Es de aplicación el apartado “11 Responsabilidades y obligaciones de las partes”.

12.2. PRÁCTICAS DE CERTIFICACIÓN PARTICULARES

79. El presente apartado define el conjunto de *Prácticas de Certificación* adoptadas por la FNMT-RCM como *Prestador de Servicios de Confianza* para la gestión del ciclo de vida de los *Certificados de Representante de Persona jurídica*, expedidos bajo la *Política de Certificación* identificada con el OID 1.3.6.1.4.1.5734.3.11.2. y de los *Certificados de Representante de Entidad sin personalidad jurídica*, expedidos bajo la *Política de Certificación* identificada con el OID 1.3.6.1.4.1.5734.3.11.3.

12.2.1. Servicios de gestión de las Claves

80. La FNMT-RCM, bajo ningún concepto, genera ni almacena las *Claves Privadas* de los *Firmantes*, que son generadas bajo su exclusivo control.

12.2.2. Gestión del ciclo de vida de los Certificados

81. En este apartado se definen aquellos aspectos que, si bien ya han sido apuntados en la *Declaración General de Prácticas de Certificación* de la que este documento forma parte, revisten determinadas especialidades que necesitan un mayor nivel de detalle.

82. A continuación se describe el procedimiento de solicitud por el que la *Oficina de Registro* toma los datos personales de un *Solicitante*, confirma su identidad así como la extensión y vigencia de sus facultades de representación sobre la persona jurídica y se formalizan, entre el citado *Solicitante* y la FNMT-RCM, las condiciones de uso para la posterior expedición del *Certificado de Representante de Persona jurídica* o del *Certificado de Representante de Entidad sin personalidad jurídica.*

12.2.2.1. Procedimiento de solicitud

83. El interesado accede al sitio web del *Prestador de Servicios de Confianza* de la FNMT-RCM, a través de la dirección http://www.cert.fnmt.es, donde se mostrarán las instrucciones del proceso completo de obtención del *Certificado*. El *Solicitante* deberá introducir su dirección de correo electrónico y el NIF de la *Persona Jurídica* o de la *Entidad sin personalidad jurídica*, en el punto de recogida de datos dispuesto para ello. Así mismo, el *Solicitante* manifestará su voluntad de obtener el *Certificado* para el que está realizando la solicitud y dará su consentimiento para que la FNMT-RCM pueda realizar una consulta al Sistema de Verificación de Datos de Identidad.

84. Posteriormente, se generan las *Claves Pública* y *Privada* (en un dispositivo criptográfico —Token o Tarjeta criptográfica— si el *Solicitante* dispone del mismo o en el navegador si no dispone de dicho dispositivo) que serán vinculadas al *Certificado* que se generará en una fase posterior, y la FNMT–RCM asigna a la solicitud un código único.

85. Con carácter previo el Solicitante deberá consultar las Declaraciones General y Particular de Prácticas de Certificación en la dirección http://www.ceres.fnmt.es/dpcs/ con las condiciones de uso y obligaciones para las partes.

86. Al realizar esta solicitud se envía a la FNMT-RCM la *Clave Pública* generada, junto con las correspondientes pruebas de posesión de la *Clave Privada*, para la posterior expedición del *Certificado*. El envío de la *Clave Pública* a la AC para la generación del *Certificado* se realiza mediante un formato estándar, PKCS#10 o SPKAC, utilizando un canal seguro para dicho envío.

87. La FNMT-RCM, tras recibir esta información, comprobará mediante la *Clave Pública* del peticionario, la validez de la información de la solicitud, comprobando únicamente la posesión y correspondencia de la pareja de *Claves criptográficas* por parte del peticionario.

88. Esta información no dará lugar a la generación de un *Certificado* por parte de la FNMT-RCM, en tanto que esta no reciba la confirmación, por parte de la *Oficina de Registro*, de la

identificación del *Representante* y la extensión y vigencia de sus facultades de representación sobre la entidad representada.

89. El procedimiento de solicitud del *Certificado* finaliza con el envío, por parte de la FNMT – RCM, de un correo electrónico a la dirección facilitada por el *Solicitante* donde se le indica el código de solicitud único asignado y se le informa de las siguientes fases del proceso de obtención del *Certificado*.

12.2.2.2. Confirmación de la identidad personal y la vigencia de sus facultades de representación

90. La FNMT-RCM, como *Prestador de Servicios de Confianza*, antes de expedir el *Certificado* identificará al *Solicitante* del mismo, así como los datos relativos a la personalidad jurídica de la *Entidad representada* y a la extensión y vigencia de sus facultades de representación del *Representante*, mediante personación física ante una *Oficina de Registro* con la que la FNMT- RCM tenga suscrito un acuerdo para tal fin. En este acto, el *Solicitante* y cualquier otro tercero cuya personación fuera necesaria, aportarán los datos y documentos que se les requieran y acreditarán su identidad personal así como la extensión y vigencia de sus facultades de representación sobre la *Entidad representada*.

91. En todo caso se exigirá con carácter general a los *Solicitantes* de estos *Certificados*, su personación ante una Oficina de Registro autorizada, con los siguientes medios de identificación: DNI, Tarjeta de Identidad de Extranjeros, Pasaporte u otros medios admitidos en derecho (debiendo, en estos dos últimos casos, aportar también el NIE). El encargado de acreditación de la *Oficina de Registro* verificará que los documentos aportados cumplen todos los requisitos para confirmar la identidad del *Solicitante*, del *Representante*, así como los datos relativos a la personalidad jurídica del representado. Podrá prescindirse de la personación si su firma en la solicitud de expedición ha sido legitimada en presencia notarial, sin perjuicio de la necesidad de acreditar suficientemente la extensión y vigencia de sus facultades de representación.

92. Asimismo, la FNMT-RCM, con carácter particular, comprobará, directamente o a través de tercero, los datos relativos a la constitución y, en su caso, personalidad jurídica de la entidad para la que se solicita la emisión del *Certificado*, y a la vigencia de las facultades de representación del *Solicitante* para realizar la mencionada solicitud, previa aportación de la documentación fidedigna que sea requerida para este fin, y que será custodiada por el *Prestador de Servicios de Confianza* por sí o por cuenta de la *Oficina de Registro* habilitada, con el fin de posibilitar su consulta con posterioridad. La relación que compone dicha documentación se publica en la sede electrónica de la FNMT-RCM (http://www.cert.fnmt.es).

93. Una vez que la *Oficina de Registro* ha realizado estas comprobaciones, procederá a validar los datos y a enviarlos a la FNMT-RCM, junto con el código de solicitud remitido al *Solicitante* por correo electrónico. Esta transmisión de información se realizará mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM. Los datos de carácter personal y su tratamiento quedarán sometidos a la legislación específica.

12.2.2.3. Expedición del Certificado

94. Una vez recibidos en la FNMT-RCM los datos personales del *Solicitante*, así como su código de solicitud, se procederá a la expedición del *Certificado* solicitado.

95. La expedición de *Certificados* de *Representante de Persona jurídica* o de *Representante de Entidad sin personalidad jurídica* supone la generación de documentos electrónicos que confirman la identidad del *Representante* y de la *Entidad representada*, así como su correspondencia con la *Clave Pública* asociada. La expedición de estos tipos de *Certificados* de la FNMT-RCM solo puede realizarla ella misma, en su calidad de *Prestador de Servicios de Confianza*, no existiendo ninguna otra entidad u organismo con capacidad de expedición de los mismos.

96. La FNMT-RCM, por medio de su *Firma electrónica*, autentica los *Certificados* de *Representante de Persona jurídica* y de *Representante de Entidad sin personalidad jurídica* y confirma la identidad del *Representante* y de la *Entidad representada*. Por otro lado y con el fin de evitar la manipulación de la información contenida en los *Certificados*, la FNMT-RCM utilizará mecanismos criptográficos que doten de autenticidad e integridad al *Certificado*.

97. Para la expedición del *Certificado* se seguirán los siguientes pasos:

1. Composición de los datos de identificación localizados en el campo Common Name del Subject del *Certificado*, a partir de los datos recogidos durante el proceso de solicitud del *Certificado*, conforme a la siguiente estructura:

Campo	**Contenido**
NIF	Número DNI/NIE
Espacio en blanco	
Nombre	Tal y como figura en DNI/TIE
Espacio en blanco	
Apellido 1	Tal y como figura en DNI/TIE
Espacio en blanco	
Literal	(R:
NIF de la empresa	NIF de la empresa, tal como figura en los registros oficiales.
Literal	)

Ejemplo:

00000000T Juan Español (R: Q0000000J)

Actualmente, no se contempla el uso de seudónimos como forma de identificación.

2. Composición de la identidad alternativa de los *Certificados de Representante de Persona jurídica* y de los *Certificados de Representante de Entidad sin personalidad jurídica*.

   La identidad alternativa de estos *Certificados* es distribuida en una serie de atributos, de forma que sea más sencilla la obtención de los datos del *Representante* del *Certificado* y de la *Entidad representada*. Para ello se utiliza la extensión subjectAltName definida en *X.509* versión 3, y contiene la siguiente información:

   1) la dirección de correo electrónico del *Solicitante*, y

   2) en el subcampo DirectoryName, el nombre, los apellidos y el NIF del *Representante*, así como la Razón social y el NIF de la *Entidad representada* (adicionalmente, en los *Certificados de Representante de Entidad sin personalidad jurídica*, se incluye el tipo de dicha Entidad).

3. Generación del *Certificado* conforme al Perfil del *Certificado*.

   Los formatos de los *Certificados de Representante de Persona jurídica* y de los *Certificados de Representante de Entidad sin personalidad jurídica*, expedidos por la FNMT-RCM bajo las presentes *Prácticas de Certificación*, en consonancia con la norma UIT-T X.509 versión 3 y de acuerdo con la normativa legalmente aplicable en materia de *Certificados electrónicos reconocidos*, pueden consultarse en los anexos al presente documento.

   En ellos se describen los perfiles de dichos *Certificados* y del *Certificado* de la *Autoridad de Certificación* que los expide (siempre subordinada a la *Autoridad de Certificación Raíz* de la FNMT-RCM).

   La FNMT-RCM enviará una comunicación a la dirección de correo electrónico facilitada por el *Solicitante* en la fase de solicitud del *Certificado*, informando de la disponibilidad del *Certificado* para proceder a su descarga.

12.2.2.4. Aceptación, descarga e instalación del Certificado

98. En menos de una (1) hora desde que tiene lugar la confirmación de la identidad personal del *Solicitante*, la FNMT-RCM pone el *Certificado* a disposición de este para su descarga a través de la página web desde la que hizo la solicitud, http://www.cert.fnmt.es y utilizando el mismo equipo o dispositivo desde el que solicitó el *Certificado*.

99. En este proceso guiado se le pedirá al *Solicitante* que introduzca el NIF de la *Persona jurídica* o de la *Entidad sin personalidad jurídica*, así como el correspondiente código de solicitud obtenido en dicho proceso. Este código de solicitud será empleado, como clave

concertada, para la generación por parte del *Firmante* de una firma electrónica de las condiciones de uso del *Certificado*, como requisito imprescindible para acceder a la descarga del mismo y aceptar las condiciones de utilización, remitiendo dichas condiciones firmadas a la FNMT-RCM. Si el *Certificado* aún no hubiera sido generado por cualquier motivo o existiera una incidencia, el proceso le informará de este hecho.

100. El *Solicitante* realizará, en su caso, el pago del importe correspondiente a los precios públicos aprobados por la FNMT-RCM para este tipo de *Certificados*. Para ello, dicha Entidad pone al servicio de los ciudadanos los medios de pago seguros a través de la página web desde la que se está realizando la descarga del *Certificado*.

101. Una vez realizado el pago, el *Certificado* se instalará en el soporte en el que se generaron las *Claves* durante el proceso de solicitud (Token criptográfico o, en su defecto, el *Navegador* desde el cual hizo la solicitud). En la citada página web de la FNMT-RCM se indican los *Navegadores* soportados y normas de instalación de los certificados.

12.2.2.5. Vigencia del Certificado

12.2.2.5.1. Caducidad

102. Los *Certificados de Representante de Persona jurídica* y los *Certificados de Representante de Entidad sin personalidad jurídica* expedidos por la FNMT-RCM tendrán validez durante un período de dos (2) años contados a partir del momento de la expedición del *Certificado*, siempre y cuando no se extinga su vigencia. Transcurrido este período y si el *Certificado* sigue activo, caducará, siendo necesaria la expedición de uno nuevo en caso de que la *Entidad representada* desee seguir utilizando los servicios del *Prestador de Servicios de Confianza.*

12.2.2.5.2. Extinción de la vigencia del Certificado

103. Los *Certificados de Representante de Persona jurídica* y los *Certificados de Representante de Entidad sin personalidad jurídica* expedidos por la FNMT-RCM quedarán sin efecto en los siguientes casos:

a) Terminación del período de validez del *Certificado*.

b) Cese en la actividad como *Prestador de Servicios de Confianza* de la FNMT-RCM, salvo que, previo consentimiento expreso del *Firmante*, los *Certificados* expedidos por la FNMT-RCM hayan sido transferidos a otro *Prestador de Servicios de Confianza*.

En estos dos casos [a) y b)], la pérdida de eficacia de los *Certificados* tendrá lugar desde que estas circunstancias se produzcan.

c) Suspensión o revocación del *Certificado* por cualquiera de las causas recogidas en el presente documento.

104. A los efectos enumerados anteriormente, la expedición de un *Certificado de Representante de Persona Jurídica* o de un *Certificado de Representante de Entidad sin personalidad jurídica* cuando exista otro vigente a favor de la misma *Entidad representada* y que incluye al mismo *Firmante*, conllevará la revocación inmediata del *Certificado* anterior expedido bajo las presentes *Políticas de Certificación y Prácticas de Certificación Particulares*.

12.2.2.6. Revocación del Certificado

12.2.2.6.1. Causas de revocación

105. Serán causas admitidas para la revocación de un *Certificado de Representante de Persona jurídica* o de un *Certificado de Representante de Entidad sin personalidad jurídica* las expuestas a continuación:

a) La solicitud de revocación por parte del *Firmante,* de la *Entidad representada* por este o por un tercero debidamente autorizado. En todo caso, deberá dar lugar a esta solicitud:

- La pérdida del soporte del *Certificado*.
- La utilización por un tercero de los *Datos de Creación de Firma*, correspondientes a los *Datos de Verificación de Firma* contenidos en el *Certificado* y vinculados a la identidad del *Representante* y de la *Entidad representada*.
- La violación o puesta en peligro del secreto de los *Datos de Creación de Firma*.
- La no aceptación de las nuevas condiciones que puedan suponer la expedición de nuevas *Declaraciones de Prácticas de Certificación*, durante el periodo de un mes tras su publicación.

b) Resolución judicial o administrativa que así lo ordene.

c) Fallecimiento del *Representante*.

d) Incapacidad sobrevenida, total o parcial, del *Representante*.

e) Terminación de la representación.

f) Disolución de la persona jurídica representada.

g) Inexactitudes en los datos aportados por el *Solicitante* para la obtención del *Certificado,* o alteración de los datos aportados para la obtención del *Certificado* o modificación de las circunstancias verificadas para la expedición del *Certificado,* como las relativas al cargo o a las facultades de representación, de manera que este ya no fuera conforme a la realidad

h) Contravención de una obligación sustancial de esta *Declaración de Prácticas de Certificación* por parte de la *Entidad representada,* del *Firmante* o del *Solicitante* del *Certificado* si, en este último caso, hubiese podido afectar al procedimiento de expedición del *Certificado*.

i) Contravención de una obligación sustancial de esta *Declaración de Prácticas de Certificación* por parte de una *Oficina de Registro* si hubiese podido afectar al procedimiento de expedición del *Certificado*.

j) Resolución del contrato suscrito entre la *Entidad representada* o el *Firmante* y la FNMT-RCM.

106. En ningún caso la FNMT-RCM asume obligación alguna de comprobar los extremos mencionados en las letras c) a i) del presente apartado, debiendo ser notificadas a esta

entidad de forma fehaciente mediante entrega de los documentos e informaciones necesarias para verificarlo.

107. La FNMT-RCM únicamente será responsable de las consecuencias que se desprendan de no haber revocado un *Certificado* en los siguientes supuestos:

- Que la revocación se debiera haber efectuado por solicitud fehaciente por parte del *Firmante* o de la *Entidad representada,* o por medio de los sistemas puestos a disposición por la FNMT-RCM para este fin.
- Que la solicitud de revocación o la causa que la motiva, le haya sido notificada mediante resolución judicial o administrativa.
- Que las causas c) a i) del presente apartado le sean acreditadas fehacientemente, previa identificación de la *Entidad representada, Representante* y/o *Solicitante* de la revocación o persona con facultades de representación suficientes, si se produjera el cese o la incapacidad sobrevenida del *Representante*.

108. Las actuaciones constitutivas de delito o falta de las que no tenga conocimiento la FNMT-RCM que se realicen sobre los datos y/o *Certificado* y las inexactitudes sobre los datos o falta de diligencia en su comunicación a la FNMT-RCM, producirán la exoneración de responsabilidad de la FNMT-RCM.

12.2.2.6.2. Efectos de la revocación

109. La revocación o suspensión del *Certificado de Representante de Persona jurídica* o del *Certificado de Representante de Entidad sin personalidad jurídica*, esto es, la extinción de su vigencia, surtirá efecto la fecha en que la FNMT-RCM, tras el conocimiento cierto de cualquiera de los hechos determinantes, lo incluya en su *Servicio de información y consulta sobre el estado de los certificados*.

110. La revocación del *Certificado de Representante de Persona jurídica* o del *Certificado de Representante de Entidad sin personalidad jurídica* implica, además de su extinción, la finalización de la relación y régimen de uso de dicho *Certificado* con la FNMT-RCM.

12.2.2.6.3. Procedimiento para la revocación

111. La solicitud de revocación del *Certificado de Representante de Persona jurídica* o del *Certificado de Representante de Entidad sin personalidad jurídica* podrá efectuarse durante el período de validez que consta en el *Certificado*.

112. La revocación de estos tipos de *Certificados* solamente podrá ser solicitada por la *Entidad representada* o persona con facultades de representación suficientes, en los términos recogidos en las presentes *Políticas de Certificación y Prácticas de Certificación Particulares*.

113. No obstante, la FNMT-RCM podrá revocar de oficio los *Certificados de Representante de Persona jurídica* o *de Representante de Entidad sin personalidad jurídica* en los supuestos recogidos en la presente *Declaración de Prácticas de Certificación*.

114. El *Representante* o la *Entidad representada* pueden solicitar la revocación de su *Certificado de Representante de Persona jurídica* o *de Representante de Entidad sin personalidad jurídica* conforme a alguno de los siguientes procedimientos:

A) Si la *Entidad representada* está en posesión de su *Certificado* y sus *Datos de creación de Firma* asociados, es posible autenticar su identidad con base a dicho *Certificado*, por lo que se le permite solicitar la revocación del mismo a través de Internet, o de cualquier otra vía equivalente que permita la conexión a la dirección http://www.ceres.fnmt.es, siguiendo las instrucciones expuestas en dicho sitio web. Este servicio estará disponible las veinticuatro (24) horas del día, todos los días del año, salvo por circunstancias ajenas a la FNMT-RCM u operaciones de mantenimiento. La FNMT-RCM notificará esta última circunstancia en la dirección http://www.ceres.fnmt.es, si es posible con al menos cuarenta y ocho (48) horas de antelación y tratará de solventarla en un periodo no superior a veinticuatro (24) horas.

B) Si la *Entidad representada* no está en posesión de su *Certificado* y sus *Datos de creación de Firma* asociados, podrá solicitar la revocación de dicho *Certificado* por cualquiera de las siguientes vías:

1) Personándose en una de las *Oficinas de Registro* implantadas por las *Entidades usuarias* con las que la FNMT-RCM haya suscrito el convenio correspondiente para la expedición de estos tipos de *Certificados*, donde acreditará su identidad.

2) En el teléfono 902 200 616 de la FNMT-RCM, donde se le realizarán las preguntas oportunas al objeto de verificar la verdadera identidad del peticionario. Este servicio estará disponible las veinticuatro (24) horas del día, todos los días del año.

115. Tan pronto se resuelva la revocación, el *Firmante* recibirá, a través de la dirección de correo electrónico consignada en la solicitud, la notificación de la revocación del *Certificado*.

116. Una vez que la FNMT-RCM ha procedido a la revocación del *Certificado*, se publicará en el *Directorio* seguro la correspondiente *Lista de Certificados Revocados* conteniendo el número de serie del *Certificado* revocado, la fecha y hora de revocación y la causa de la misma.

12.2.2.7. Suspensión del Certificado

117. La suspensión de un *Certificado* deja sin efecto dicho *Certificado* durante un período de tiempo y en unas condiciones determinadas.

118. La suspensión de los *Certificados* será considerada una revocación temporal de la vigencia de los mismos por lo que los procedimientos y entidades habilitadas para la solicitud y tramitación de la revocación del *Certificado* son de aplicación en el caso de la suspensión.

12.2.2.7.1. Causas de la suspensión del Certificado

119. La FNMT-RCM podrá suspender la vigencia de los *Certificados de Representante de Persona jurídica* y de los *Certificados de Representante de Entidad sin personalidad jurídica* a solicitud del legítimo interesado o de Autoridad Judicial o ante la existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los *Certificados* contempladas en el apartado "Causas de revocación" del presente documento.

120. Asimismo, la solicitud de suspensión puede deberse a la existencia de una investigación o procedimiento judicial o administrativo en curso, cuya conclusión pueda determinar que el *Certificado* efectivamente está afectado por una causa de revocación. En estos casos la FNMT-RCM, a solicitud del legítimo interesado, suspenderá la vigencia del *Certificado* por

el plazo requerido y, transcurrido este plazo, procederá a la revocación del *Certificado* salvo que a la FNMT-RCM se le solicite, de forma fehaciente por el legítimo interesado, la reactivación del mismo.

12.2.2.7.2. Procedimiento para la suspensión de Certificados

121. La solicitud de la suspensión de los *Certificados de Representante de Persona jurídica* y de los *Certificados de Representante de Entidad sin personalidad jurídica* solamente podrá ser realizada a través de las *Oficinas de Registro* implantadas por las *Entidades usuarias* con las que la FNMT-RCM haya suscrito el convenio correspondiente.

122. La FNMT-RCM procederá a suspender el *Certificado* durante un plazo de treinta (30) días, plazo tras el cual se extinguirá el *Certificado* mediante su revocación directa por parte del *Prestador de Servicios de Confianza*, la FNMT-RCM, salvo que se hubiera levantado la suspensión mediante solicitud de cancelación de la suspensión por parte de la *Entidad representada*, su *Representante* o un tercero autorizado y con facultades suficientes. No obstante lo anterior, el plazo previsto para la suspensión del *Certificado* podrá verse alterado en función de los procedimientos judiciales o administrativos que lo pudieran afectar.

123. Si durante el plazo de suspensión del *Certificado* este caducara o se solicitara su revocación, se producirán las mismas consecuencias que para los *Certificados* no suspendidos que se vieran afectados por supuestos de caducidad o de revocación respectivamente.

12.2.2.7.3. Procedimiento para la cancelación de la suspensión de Certificados

124. Podrán solicitar la cancelación de la suspensión de los *Certificados* los *Representantes* siempre que, con anterioridad a esta solicitud de cancelación de la suspensión, conserven el *Certificado* y sus *Datos de creación de Firma*, y dicha solicitud se efectúe durante los treinta (30) días siguientes a su suspensión.

125. Para ello deberán personarse ante cualquier *Oficina de Registro* con las que la FNMT-RCM haya suscrito el convenio correspondiente. En este acto el *Solicitante* aportará los datos que se le requieran y acreditará su identidad personal, como en el proceso de emisión ya descrito.

126. La personación del *Solicitante* no será indispensable si la firma de la solicitud de cancelación de la suspensión de un *Certificado* ha sido legitimada en presencia notarial.

127. Los datos personales del *Solicitante*, una vez validados por la *Oficina de Registro*, se enviarán a la FNMT-RCM mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM.

128. Una vez recibidos los datos validados por la *Oficina de Registro* de la petición de la cancelación de la suspensión la FNMT-RCM procederá a retirar este *Certificado* del *Servicio de información y consulta sobre el estado de los certificados*.

12.2.3. Comprobación del estado de revocación del Certificado

129. El estado de revocación de los *Certificados* electrónicos de *Representante de Persona jurídica* y *de Representante de Entidad sin personalidad jurídica* se podrá comprobar a través del *Servicio de información y consulta del estado de los Certificados* mediante el protocolo OCSP.

130. Este servicio estará disponible las veinticuatro (24) horas del día, todos los días del año, salvo por circunstancias ajenas a la FNMT-RCM u operaciones de mantenimiento. La FNMT-RCM notificará esta última circunstancia en la dirección http://www.cert.fnmt.es si es posible con al menos cuarenta y ocho (48) horas de antelación y tratará de solventarla en un periodo no superior a veinticuatro (24) horas.

131. El funcionamiento de este servicio es el siguiente: el *servidor OCSP* de la FNMT-RCM recibe la petición OCSP efectuada por un *Cliente OCSP* y comprueba el estado de los *Certificados* incluidos en la misma. En caso de que la petición sea válida, se emitirá una respuesta de OCSP informando acerca del estado en el que se encuentran en ese momento los *Certificados* incluidos en la petición. Dicha respuesta OCSP está firmada con los *Datos de Creación de Firma* asociados al servidor OCSP específico para la AC Representación, garantizando así la integridad y la autenticidad de la información suministrada sobre el estado de revocación de los *Certificados* consultados.

132. Será responsabilidad de la *Entidad usuaria* obtener un *Cliente OCSP* para operar con el *servidor OCSP* puesto a disposición por la FNMT-RCM.

12.3. POLÍTICA DE CERTIFICACIÓN DE LOS CERTIFICADOS DE *REPRESENTANTE DE* PERSONA JURÍDICA

12.3.1. Identificación

133. La presente *Política de Certificación* de la FNMT-RCM para la expedición de *Certificados de Representante de Persona jurídica* tiene la siguiente identificación:

Nombre: Política de Certificación de *Certificados de Representante de Persona jurídica*

Referencia / OID[1]:

- 1.3.6.1.4.1.5734.3.11.2.

Versión: 1.3

Fecha de expedición: 24 de junio de 2016

Localización: http://www.cert.fnmt.es/dpcs/

DPC relacionada: Declaración General de Prácticas de Certificación de la FNMT-RCM

Localización: http://www.cert.fnmt.es/dpcs/

[1] *Nota*: El OID o identificador de política es una referencia que se incluye en el *Certificado* al objeto de determinar un conjunto de reglas que indican la aplicabilidad de un determinado tipo de *Certificado* a la *Comunidad Electrónica* y/o clase de aplicación con requisitos de seguridad comunes.

12.3.2. Tipología del Certificado de *Representante de* Persona jurídica

134. El *Certificado de Representante de Persona jurídica* es la certificación electrónica expedida por la FNMT-RCM que vincula a un *Firmante*, unos *Datos de verificación de Firma* y confirma su identidad.

12.3.3. Comunidad y ámbito de aplicación

135. Los *Certificados* expedidos bajo esta *Política de Certificación* se consideran válidos, como parte integrante de los sistemas de identificación y firma electrónica, basados en *Certificados electrónicos reconocidos* para la relación de las *Personas Jurídicas* en sus relaciones con las Administraciones Públicas, Entidades y Organismos Públicos vinculados o dependientes de las mismas.

12.3.4. Límites de uso de los Certificados de Persona jurídica

136. No se podrá emplear este tipo de *Certificados*, por persona o entidad distinta a la FNMT-RCM, para:

- Firmar otro *Certificado*, salvo supuestos expresamente autorizados previamente.
- Firmar software o componentes.
- Generar *Sellos de tiempo* para procedimientos de *Fechado electrónico.*
- Prestar servicios a título gratuito u oneroso, salvo supuestos expresamente autorizados previamente, como serían a título enunciativo y no limitativo:
    - Prestar servicios de *OCSP*.
    - Generar *Listas de Revocación.*
    - Prestar servicios de notificación

12.4. POLÍTICA DE CERTIFICACIÓN DE LOS CERTIFICADOS DE *REPRESENTANTE DE* ENTIDAD SIN PERSONALIDAD JURÍDICA

12.4.1. Identificación

137. La presente *Política de Certificación* de la FNMT-RCM para la expedición de *Certificados de Representante de Entidad sin personalidad jurídica* tiene la siguiente identificación:

Nombre: Política de Certificación de *Certificados de Representante de Entidad sin personalidad jurídica*

Referencia / OID[2]:

[2] *Nota*: El OID o identificador de política es una referencia que se incluye en el *Certificado* al objeto de determinar un conjunto de reglas que indican la aplicabilidad de un determinado tipo de *Certificado* a la *Comunidad Electrónica* y/o clase de aplicación con requisitos de seguridad comunes.

- 1.3.6.1.4.1.5734.3.11.3.

Versión: 1.3

Fecha de expedición: 24 de junio de 2016

Localización: http://www.cert.fnmt.es/dpcs/

DPC relacionada: Declaración General de Prácticas de Certificación de la FNMT-RCM

Localización: http://www.cert.fnmt.es/dpcs/

12.4.2. Tipología del Certificado de *Representante de* Entidad sin personalidad jurídica

138. El *Certificado de Representante de Entidad sin personalidad jurídica* es la certificación electrónica expedida por la FNMT-RCM que vincula a un *Firmante*, unos *Datos de verificación de Firma* y confirma su identidad.

12.4.3. Comunidad y ámbito de aplicación

139. Los *Certificados* expedidos bajo esta *Política de Certificación* se consideran válidos como parte integrante de los sistemas de identificación y firma electrónica basados en *Certificados electrónicos reconocidos* para la relación de las *Entidades sin personalidad jurídica* en el ámbito tributario y otros ámbitos previstos de acuerdo con la correspondiente *Ley de emisión*.

12.4.4. Límites de uso de los Certificados de Entidad sin personalidad jurídica

140. No se podrá emplear este tipo de *Certificados*, por persona o entidad distinta a la FNMT-RCM, para:

- Firmar otro *Certificado*, salvo supuestos expresamente autorizados previamente.
- Firmar software o componentes.
- Generar *Sellos de tiempo* para procedimientos de *Fechado electrónico.*
- Prestar servicios a título gratuito u oneroso, salvo supuestos expresamente autorizados previamente, como serían a título enunciativo y no limitativo:
    - Prestar servicios de *OCSP*.
    - Generar *Listas de Revocación.*
    - Prestar servicios de notificación

13. CERTIFICADO DE REPRESENTANTE PARA ADMINISTRADORES ÚNICOS Y SOLIDARIOS

13.1. RESPONSABILIDADES Y OBLIGACIONES DE LAS PARTES

141. El presente apartado recoge las obligaciones y responsabilidades de las partes implicadas en la expedición y uso del *Certificado de Representante para administradores únicos y solidarios*. Por tanto, son de aplicación tanto la siguiente relación de obligaciones y responsabilidades específicas para este tipo de *Certificados*, como la ya descrita en el apartado "11 Responsabilidades y obligaciones de las partes" relativa a los tipos de C*ertificados* incluidos en el presente documento de *Políticas y Prácticas Particulares de Certificación*.

13.1.1. Responsabilidades de las partes

13.1.1.1. Responsabilidad del Prestador de Servicios de Confianza

142. La FNMT-RCM responde de la correcta identificación personal del *Representante* y, en su caso, del *Solicitante* del *Certificado*.

143. La FNMT-RCM responde de realizar la comprobación, en las bases de datos del Colegio de Registradores de la Propiedad y Mercantiles de España (CORPME), de la vigencia de las facultades del *Representante* (inscripción como administrador único o solidario) sobre la *Entidad representada*, así como de la existencia de dicha *Entidad* y su personalidad jurídica en el momento de la acreditación de la identidad personal del *Representante*.

144. La FNMT-RCM se limita únicamente a expresar la información relativa a la identidad del *Representante*, su facultad de representación (administrador único o solidario) y la identidad de la *Entidad representada*, en un *Certificado electrónico*. La FNMT-RCM, en ningún caso, será responsable de los posibles errores o discrepancias entre la realidad y la información suministrada por el CORPME.

13.1.1.2. Responsabilidad del CORPME

145. El CORPME responderá de la transmisión de la información suministrada por los registradores mercantiles titulares de la información con presunción de veracidad relativa a las facultades de representación (administrador único o solidario) del *Representante* del *Certificado,* así como de la existencia de la *Entidad representada* y su personalidad jurídica, de conformidad con la información que conste inscrita en el Registro Mercantil y que sea puesta a disposición de la FNMT-RCM.

146. El régimen de distribución de responsabilidades entre la FNMT-RCM y el CORPME, en relación con la información intercambiada entre ellas y el momento en que se recoge en la expedición de los *Certificados* y, en su caso, la revocación de los mismos, será el definido en el correspondiente acuerdo formalizado a tal fin entre ambas instituciones.

13.1.1.3. Responsabilidad del Solicitante

147. Es de aplicación el apartado "11 Responsabilidades y obligaciones de las partes".

13.1.1.4. Responsabilidad de la Entidad representada y del Representante

148. Es de aplicación el apartado "11 Responsabilidades y obligaciones de las partes".

13.1.1.5. Responsabilidad de la Entidad Usuaria y terceros que confían

149. Es de aplicación el apartado "11 Responsabilidades y obligaciones de las partes".

13.1.2. Obligaciones y garantías de las partes

13.1.2.1. Obligaciones y Garantías del Prestador de Servicios de Confianza

150. Sin perjuicio de lo dispuesto en la legislación sobre firma electrónica, y su normativa de desarrollo, así como en su normativa específica, el *Prestador de Servicios de Confianza* se obliga a:

151. Con carácter previo a la expedición del *Certificado*:

- Comprobar la identidad y circunstancias personales del *Solicitante* del *Certificado* y, en su caso, recoger la manifestación de que el *Solicitante* está autorizado por la *Entidad representada* para realizar la solicitud. En ningún caso se expedirán *Certificados* a menores de edad, salvo que ostenten la cualidad de emancipados.
- En el proceso de registro, comprobar los datos relativos a las facultades de representación (administrador único o solidario) del *Representante*, así como la existencia y la personalidad jurídica de la entidad, según la información suministrada por el CORPME. Todas estas comprobaciones se realizarán según lo dispuesto en las *Prácticas de Certificación Particulares* expresadas en este documento y según los protocolos y procedimientos de registro de la FNMT-RCM.
- Verificar que toda la información contenida en la solicitud del *Certificado* se corresponde con la aportada por el *Solicitante* y la recabada del CORPME.

152. Revocación de *Certificados*:

- La FNMT-RCM revocará de oficio los *Certificados de Representante para administradores únicos y solidarios* de los que reciba información del CORPME relativa a la inscripción del cese del *Representante* incluido en el Certificado (administrador único o solidario), a la extinción de la *Entidad representada* del *Certificado* o cualquier otra causa de revocación que legalmente sea de obligada inscripción en el Registro Mercantil.
- Adicionalmente las obligaciones que la FNMT-RCM se compromete a asumir en relación con la revocación de este tipo de *Certificados* se desarrolla en el procedimiento de revocación de *Certificados* reflejado en el presente documento.

13.1.2.2. Obligaciones de la Oficina de Registro

153. Para la gestión del ciclo de vida de los *Certificados de Representante para administradores únicos y solidarios*, las *Oficinas de Registro* tienen la obligación de comprobar la identidad y circunstancias personales de los *Solicitantes*, *Entidades representadas* y *Representantes*

de los *Certificados* relevantes para el fin propio de estos, utilizando cualquiera de los medios admitidos en Derecho y conforme a lo previsto con carácter general en la DGPC y con carácter particular en la presente *Declaración de Políticas y Prácticas de Certificación Particulares*.

13.1.2.3. Obligaciones de la Entidad representada y del Representante

154. Es de aplicación el apartado "11 Responsabilidades y obligaciones de las partes".

13.1.2.4. Obligaciones de la Entidad Usuaria y terceros que confían

155. Es de aplicación el apartado "11 Responsabilidades y obligaciones de las partes".

13.2. PRÁCTICAS DE CERTIFICACIÓN PARTICULARES

156. El presente apartado define el conjunto de *Prácticas de Certificación* adoptadas por la FNMT-RCM como *Prestador de Servicios de Confianza* para la gestión del ciclo de vida de los *Certificados de Representante para administradores únicos y solidarios*, expedidos bajo la *Política de Certificación* identificada con el OID 1.3.6.1.4.1.5734.3.11.1.

13.2.1. Servicios de gestión de las Claves

157. La FNMT-RCM, bajo ningún concepto, genera ni almacena las *Claves Privadas* de los *Firmantes*, que son generadas bajo su exclusivo control.

13.2.2. Gestión del ciclo de vida de los Certificados

158. En este apartado se definen aquellos aspectos que, si bien ya han sido apuntados en la *Declaración General de Prácticas de Certificación* de la que este documento forma parte, revisten determinadas especialidades que necesitan un mayor nivel de detalle.

A continuación se describe el procedimiento de solicitud por el que la *Oficina de Registro* toma los datos personales de un *Solicitante*, confirma su identidad y se formalizan, entre el citado *Solicitante* y la FNMT-RCM, las condiciones de uso para la posterior expedición del *Certificado de Representante para administradores únicos y solidarios*.

13.2.2.1. Procedimiento de solicitud

159. El interesado accede al sitio web del *Prestador de Servicios de Confianza* de la FNMT-RCM, a través de la dirección http://www.cert.fnmt.es, donde se mostrarán las instrucciones del proceso completo de obtención del *Certificado*. El Solicitante deberá introducir su número NIF, su primer apellido, su dirección de correo electrónico y el NIF de la *Entidad representada* en el punto de recogida de datos dispuesto para ello. Así mismo, el *Solicitante* manifestará su voluntad de obtener el *Certificado* para el que está realizando la solicitud y dará su consentimiento para que la FNMT-RCM pueda realizar una consulta al Sistema de Verificación de Datos de Identidad, así como la consulta pertinente al Registro Mercantil, al

objeto de comprobar la personalidad jurídica de la entidad representada, y la extensión y vigencia de sus facultades de representación.

160. Posteriormente se generan las *Claves Pública* y *Privada* (en un dispositivo criptográfico — Token o Tarjeta criptográfica— si el *Solicitante* dispone del mismo o en el navegador si no dispone de dicho dispositivo) que serán vinculadas al *Certificado* que se generará en una fase posterior, y la FNMT-RCM asigna a la solicitud un código único.

161. Con carácter previo el Solicitante deberá consultar las Declaraciones General y Particular de Prácticas de Certificación en la dirección http://www.ceres.fnmt.es/dpcs/ con las condiciones de uso y obligaciones para las partes.

162. Al realizar esta solicitud se envía a la FNMT-RCM la *Clave Pública* generada, junto con las correspondientes pruebas de posesión de la *Clave Privada*, para la posterior expedición del *Certificado*. El envío de la *Clave Pública* a la AC para la generación del *Certificado* se realiza mediante un formato estándar, PKCS#10 o SPKAC, utilizando un canal seguro para dicho envío.

163. La FNMT-RCM, tras recibir esta información, comprobará la validez de la información de la solicitud, la posesión y correspondencia de la pareja de *Claves criptográficas* por parte del peticionario, el tamaño de claves generadas, así como la inscripción en el CORPME de la *Entidad representada* y la cualidad de administrador único o solidario del *Representante*.

164. Esta información no dará lugar a la generación de un *Certificado* por parte de la FNMT-RCM, en tanto que esta no reciba la confirmación, por parte de la *Oficina de Registro*, de la identificación del *Solicitante* y, adicionalmente, haya verificado la personalidad jurídica de la entidad representada y la extensión y vigencia de las facultades de representación del *Representante*.

165. El procedimiento de solicitud del *Certificado* finaliza con el envío, por parte de la FNMT-RCM, de un correo electrónico a la dirección facilitada por el *Solicitante* donde se le indica el código de solicitud único asignado y se le informa de las siguientes fases del proceso de obtención del *Certificado*.

13.2.2.2. Confirmación de la identidad personal

166. La FNMT-RCM, como *Prestador de Servicios de Confianza*, antes de expedir un *Certificado de Representante para administradores únicos y solidarios* identificará al *Solicitante* del mismo, bien mediante personación física ante una *Oficina de Registro* con la que la FNMT-RCM tenga suscrito un acuerdo, bien mediante un certificado electrónico vigente que confirme la identidad de la persona física solicitante. La FNMT- RCM aceptará para tal fin *Certificados* electrónicos de persona física emitidos por dicha entidad y los C*ertificados* electrónicos incorporados al DNIe.

13.2.2.2.1. Comprobación de la identidad mediante comparecencia física

167. Los *Solicitantes* de *Certificados de Representante para administradores únicos y solidarios* deberán comparecer físicamente para formalizar el procedimiento de confirmación de identidad personal, presentándose en la *Oficina de Registro* autorizada, con los siguientes medios de identificación: DNI, Tarjeta de Identidad de Extranjeros, Pasaporte u otros medios admitidos en derecho (debiendo, en estos dos últimos casos, aportar también el

NIE). El encargado de acreditación de la *Oficina de Registro* verificará que los documentos aportados cumplen todos los requisitos para confirmar la identidad del *Solicitante*.

168. Una vez confirmada la identidad del *Solicitante* por la *Oficina de Registro*, esta procederá a validar los datos y a enviarlos a la FNMT-RCM, junto con el código de solicitud remitido al *Solicitante* por correo electrónico. Esta transmisión de información se realizará mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM. Los datos personales y su tratamiento, en su caso, quedarán sometidos a la legislación específica.

169. La personación del *Solicitante* no será indispensable si su firma en la solicitud de expedición de un *Certificado* ha sido legitimada en presencia notarial, si se emplea un certificado electrónico como medio de identificación personal conforme el siguiente apartado, o si se solicita una renovación del *Certificado*, de conformidad con lo dispuesto en el subapartado "*Renovación del Certificado*" del presente apartado de "Gestión del ciclo de vida de los *Certificados*".

13.2.2.2.2. Uso de certificados electrónicos como medio de identificación

170. La FNMT-RCM expedirá el *Certificado de Representante para administradores únicos y solidarios* sin necesidad de que el peticionario comparezca ante una *Oficina de Registro* conforme al proceso descrito en el apartado anterior si, en el proceso de solicitud de dicho *Certificado*, el *Solicitante* se identifica con un *Certificado* electrónico vigente y admitido para tal fin. La relación de dichos *Certificados* puede consultarse en la página web de solicitud de este tipo de *Certificados*.

171. No obstante, solo se permitirá la solicitud telemática del *Certificado de Representante para administradores únicos y solidarios* mediante el uso de los certificados electrónicos relacionados en el apartado anterior si en el momento de la solicitud no se ha superado el plazo máximo de 5 años desde la personación e identificación física del *Representante*, de acuerdo con lo establecido en el artículo 13.4 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

13.2.2.3. Confirmación de la vigencia de las facultades de representación

172. La FNMT-RCM, una vez ha comprobada la identidad personal del *Representante*, procede a verificar la personalidad jurídica de la entidad representada y la extensión y vigencia de las facultades de representación del *Representante,* es decir, su nombramiento e inscripción en el Registro Mercantil como administrador único o solidario mediante consulta telemática a los registros del CORPME.

173. Las comunicaciones entre FNMT-RCM y CORPME se realizan a través de la red interadministrativa SARA, mediante procesos disponibles 24x7 y mediante comunicaciones seguras.

174. La información remitida por el CORPME a la FNMT-RCM garantizará que la entidad está inscrita en el Registro Mercantil, que el *Solicitante* del *Certificado* es administrador único o solidario de la *Entidad representada* y aportará los datos registrales que se incluirán en el *Certificado* en el momento de su expedición.

13.2.2.4. Expedición del Certificado

175. Una vez realizadas las comprobaciones anteriores y recibidos en la FNMT-RCM los datos personales del *Solicitante*, así como su código de solicitud, se procederá a la expedición del *Certificado* solicitado.

176. La expedición de *Certificados de Representante para administradores únicos y solidarios* supone la generación de documentos electrónicos que confirman la identidad del *Representante* y de la *Entidad representada* así como su correspondencia con la *Clave Pública* asociada. La expedición de este tipo de *Certificados* de la FNMT-RCM solo puede realizarla ella misma, en su calidad de *Prestador de Servicios de Confianza*, no existiendo ninguna otra entidad u organismo con capacidad de expedición de los mismos.

177. La FNMT-RCM, por medio de su *Firma electrónica*, autentica los *Certificados de Representante para administradores únicos y solidarios* y confirma la identidad del *Representante* y de la *Entidad representada*. Por otro lado y con el fin de evitar la manipulación de la información contenida en los *Certificados*, la FNMT-RCM utilizará mecanismos criptográficos que doten de autenticidad e integridad al *Certificado*.

178. Para la expedición del *Certificado* se seguirán los siguientes pasos:

1. Composición de los datos de identificación localizados en el campo Common Name del Subject del *Certificado*, a partir de los datos recogidos durante el proceso de solicitud del *Certificado*, conforme a la siguiente estructura:

Campo	**Contenido**
NIF	Número DNI/NIE
Espacio en blanco	
Nombre	Tal y como figura en DNI/TIE
Espacio en blanco	
Apellido 1	Tal y como figura en DNI/TIE
Espacio en blanco	
Literal	(R:
NIF de la empresa	NIF de la empresa, tal como figura en los registros oficiales.
Literal	)

Ejemplo:

00000000T Juan Español (R: Q0000000J)

No se contempla el uso de seudónimos como forma de identificación.

2. Composición de la identidad alternativa de los *Certificados de Representante para administradores únicos y solidarios*.

   La identidad alternativa de estos *Certificados* es distribuida en una serie de atributos, de forma que sea más sencilla la obtención de los datos del *Representante* del *Certificado* y de la *Entidad representada*. Para ello se utiliza la extensión subjectAltName definida en *X.509* versión 3, y contiene la siguiente información:

   1) la dirección de correo electrónico del *Solicitante,* y,
   2) en el subcampo DirectoryName, el nombre, los apellidos, el NIF y el cargo o poder (administrativo único o solidario) del *Representante*, así como la Razón social y el NIF de la *Entidad representada.*

3. Generación del *Certificado* conforme al Perfil del *Certificado*.

   El formato del *Certificado de Representante para administradores únicos y solidarios*, expedido por la FNMT-RCM bajo las presentes *Prácticas de Certificación*, en consonancia con la norma UIT-T X.509 versión 3 y de acuerdo con la normativa legalmente aplicable en materia de *Certificados electrónicos reconocidos*, puede consultarse en los anexos al presente documento.

   En ellos se describen los perfiles de dicho *Certificado* y del *Certificado* de la *Autoridad de Certificación* que los expide (siempre subordinada a la *Autoridad de Certificación Raíz* de la FNMT-RCM).

   La FNMT-RCM enviará una comunicación a la dirección de correo electrónico facilitada por el *Solicitante* en la fase de solicitud del *Certificado*, informando de la disponibilidad del *Certificado* para proceder a su descarga.

13.2.2.5. Descarga e instalación del Certificado

179. En menos de una (1) hora desde que tiene lugar la confirmación de la identidad personal del *Solicitante* y la verificación positiva de los datos relativos a la personalidad jurídica de la entidad representada y la extensión y vigencia de las facultades de representación del *Representante,* mediante consulta online a los registros del CORPME, la FNMT-RCM pone el *Certificado* a disposición del *Solicitante* para su descarga en la página web desde la que hizo la solicitud, http://www.cert.fnmt.es y utilizando el mismo equipo o dispositivo desde el que solicitó el *Certificado*.

180. En este proceso guiado se le pedirá al *Solicitante* que introduzca su número NIF, su primer apellido, así como el correspondiente código de solicitud obtenido en dicho proceso. Este código de solicitud será empleado, como clave concertada, para la generación por parte del *Firmante* de una firma electrónica de las condiciones de uso del *Certificado*, como requisito imprescindible para acceder a la descarga del mismo y aceptar las condiciones de

utilización, remitiendo dicha firma a la FNMT-RCM. Si el *Certificado* aún no hubiera sido generado por cualquier motivo, el proceso le informará de este hecho.

181. El *Solicitante* realizará el pago del importe correspondiente a los precios públicos aprobados por la FNMT-RCM para este tipo de *Certificado*. Para ello, esta Entidad pone al servicio de los ciudadanos y organizaciones los medios de pago seguro a través de la página web desde la que se está realizando la descarga del *Certificado*.

182. Una vez realizado el pago, el *Certificado* se instalará en el soporte en el que se generaron las *Claves* durante el proceso de solicitud (Token criptográfico o, en su defecto, el *Navegador* desde el cual hizo la solicitud). En la citada página web de la FNMT-RCM se indican los *Navegadores* soportados y normas de instalación de los certificados.

13.2.2.6. Vigencia del Certificado

13.2.2.6.1. Caducidad

183. Los *Certificados de Representante para administradores únicos y solidarios* expedidos por la FNMT-RCM tendrán validez durante un período de dos (2) años contados a partir del momento de la expedición del *Certificado*, siempre y cuando no se extinga su vigencia. Transcurrido este período y si el *Certificado* sigue activo, caducará, siendo necesaria la expedición de uno nuevo en caso de que la *Entidad representada* desee seguir utilizando los servicios del *Prestador de Servicios de Confianza.* No obstante, se podrá renovar el *Certificado* en los plazos y condiciones establecidos en el apartado denominado *Renovación del Certificado*.

13.2.2.6.2. Extinción de la vigencia del Certificado

184. Los *Certificados de Representante para administradores únicos y solidarios* expedidos por la FNMT-RCM quedarán sin efecto en los siguientes casos:

a) Terminación del período de validez del *Certificado*.

b) Cese en la actividad como *Prestador de Servicios de Confianza* de la FNMT-RCM, salvo que, previo consentimiento expreso del *Firmante*, los *Certificados* expedidos por la FNMT-RCM hayan sido transferidos a otro *Prestador de Servicios de Confianza*.

   En estos dos casos [a) y b)], la pérdida de eficacia de los *Certificados* tendrá lugar desde que estas circunstancias se produzcan.

c) Suspensión o revocación del *Certificado* por cualquiera de las causas recogidas en el presente documento.

185. A los efectos enumerados anteriormente, la expedición de un *Certificado de Representante para administradores únicos y solidarios* cuando exista otro *Certificado* vigente expedido bajo la presente *Política de Certificación y Prácticas de Certificación Particulares* a favor de la misma *Entidad representada* y que incluye al mismo *Firmante*, conllevará la revocación inmediata del *Certificado* anterior. La única excepción a este caso se produce cuando la expedición de un *Certificado de Representante para administradores únicos y solidarios* sea causa de un proceso de renovación del mismo durante el periodo de tiempo de sesenta (60) días antes de su fecha de caducidad, en cuyo caso el *Certificado* que está próximo a caducar seguirá siendo válido hasta que expire el período de vigencia del mismo.

Durante este tiempo, de producirse la revocación de dicho *Certificado* conforme al apartado siguiente, se producirá la extinción de la vigencia de ambos *Certificados*.

13.2.2.7. Revocación del Certificado

13.2.2.7.1. Causas de revocación

186. Serán causas admitidas para la revocación de un *Certificado de Representante para administradores únicos y solidarios* las expuestas a continuación:

a) La solicitud de revocación por parte del *Firmante,* de la *Entidad representada* por este o por un tercero debidamente autorizado. En todo caso deberá dar lugar a esta solicitud:

- La pérdida del soporte del *Certificado*.
- La utilización por un tercero de los *Datos de Creación de Firma*, correspondientes a los *Datos de Verificación de Firma* contenidos en el *Certificado* y vinculados a la identidad del *Representante* y de la *Entidad representada*.
- La violación o puesta en peligro del secreto de los *Datos de Creación de Firma*.
- La no aceptación de las nuevas condiciones que puedan suponer la expedición de nuevas *Declaraciones de Prácticas de Certificación*, durante el periodo de un mes tras su publicación.

b) Resolución judicial o administrativa que así lo ordene.

c) Fallecimiento del *Representante*.

d) Incapacidad sobrevenida, total o parcial, del *Representante*.

e) Terminación de la representación.

f) Disolución de la persona jurídica representada.

g) Inexactitudes en los datos aportados por el *Solicitante* para la obtención del *Certificado,* o alteración de los datos aportados para la obtención del *Certificado* o modificación de las circunstancias verificadas para la expedición del *Certificado,* como las relativas al cargo o a las facultades de representación, de manera que este ya no fuera conforme a la realidad

h) Contravención de una obligación sustancial de esta *Declaración de Prácticas de Certificación* por parte de la *Entidad representada*, del *Firmante* o del *Solicitante* del *Certificado* si, en este último caso, hubiese podido afectar al procedimiento de expedición del *Certificado*.

i) Contravención de una obligación sustancial de esta *Declaración de Prácticas de Certificación* por parte de una *Oficina de Registro* si hubiese podido afectar al procedimiento de expedición del *Certificado*.

j) Resolución del contrato suscrito entre la *Entidad representada* o el *Firmante* y la FNMT-RCM.

187. En ningún caso la FNMT-RCM asume obligación alguna de comprobar los extremos mencionados en las letras c) a i) del presente apartado, debiendo ser notificadas a esta

entidad de forma fehaciente mediante entrega de los documentos e informaciones necesarias para verificarlo. Los extremos mencionados en las letras e) y f) del presente apartado serán comunicados por parte del CORPME a la FNMT-RCM, momento en el cual esta entidad procederá a la revocación del *Certificado* afectado.

188. La FNMT-RCM únicamente será responsable de las consecuencias que se desprendan de no haber revocado un *Certificado* en los siguientes supuestos:

- Que la revocación se debiera haber efectuado por solicitud fehaciente por parte del *Firmante,* de la *Entidad representada* o por medio de los sistemas puestos a disposición por la FNMT-RCM para este fin.
- Que la solicitud de revocación o la causa que la motiva, le haya sido notificada mediante resolución judicial o administrativa.
- Que las causas c) a i) del presente apartado le sean acreditadas fehacientemente, previa identificación de la *Entidad representada, Representante* y/o *Solicitante* de la revocación (o persona con facultades de representación suficientes, si se produjera el cese o la incapacidad sobrevenida del *Representante*).
- Que las causas e) y f) del presente apartado le sean comunicadas por parte del CORPME por medio de los sistemas puestos a tal fin o de forma que queden acreditadas fehacientemente, previa identificación de la *Entidad representada, Representante* y/o *Solicitante* de la revocación (o persona con facultades de representación suficientes, si se produjera el cese o la incapacidad sobrevenida del *Representante*).

189. Las actuaciones constitutivas de delito o falta de las que no tenga conocimiento la FNMT-RCM que se realicen sobre los datos y/o *Certificado* y las inexactitudes sobre los datos o falta de diligencia en su comunicación a la FNMT-RCM, producirán la exoneración de responsabilidad de la FNMT-RCM.

13.2.2.7.2. Efectos de la revocación

190. La revocación o suspensión del *Certificado de Representante para administradores únicos y solidarios*, esto es, la extinción de su vigencia, surtirá efecto la fecha en que la FNMT-RCM, tras el conocimiento cierto de cualquiera de los hechos determinantes, lo incluya en su *Servicio de información y consulta sobre el estado de los certificados*.

191. La revocación del *Certificado de Representante para administradores únicos y solidarios* implica, además de su extinción, la finalización de la relación y régimen de uso de dicho *Certificado* con la FNMT-RCM.

13.2.2.7.3. Procedimiento para la revocación

192. La solicitud de revocación del *Certificado de Representante para administradores únicos y solidarios* podrá efectuarse durante el período de validez que consta en el *Certificado*.

193. La revocación de estos tipos de *Certificados* solamente podrá ser solicitada por la *Entidad representada* o persona con facultades de representación suficientes, si se produjera el cese o la incapacidad sobrevenida del *Representante*, en los términos recogidos en las presentes *Políticas de Certificación y Prácticas de Certificación Particulares*.

194. No obstante, la FNMT-RCM podrá revocar de oficio los *Certificados de Representante para administradores únicos y solidarios* en los casos en los que el CORPME le notifique la modificación de alguno de los hechos significativos recogidos en el *Certificado*, relativos a la extinción de la personalidad jurídica de la entidad representada o de la extensión y vigencia de las facultades de representación del *Representante* y en el resto de supuestos recogidos en la presente *Declaración de Prácticas de Certificación*.

195. El *Representante* o la *Entidad representada* pueden solicitar la revocación de su *Certificado de Representante para administradores únicos y solidarios* conforme a alguno de los siguientes procedimientos:

A) Si la *Entidad representada* está en posesión de su *Certificado* y sus *Datos de creación de Firma* asociados, es posible autenticar su identidad con base a dicho *Certificado*, por lo que se le permite solicitar la revocación del mismo a través de Internet, o de cualquier otra vía equivalente que permita la conexión a la dirección http://www.ceres.fnmt.es, siguiendo las instrucciones expuestas en dicho sitio web. Este servicio estará disponible las veinticuatro (24) horas del día, todos los días del año, salvo por circunstancias ajenas a la FNMT-RCM u operaciones de mantenimiento. La FNMT-RCM notificará esta última circunstancia en la dirección http://www.ceres.fnmt.es, si es posible con al menos cuarenta y ocho (48) horas de antelación y tratará de solventarla en un periodo no superior a veinticuatro (24) horas.

B) Si la *Entidad representada* no está en posesión de su *Certificado* y sus *Datos de creación de Firma* asociados, podrá solicitar la revocación de dicho *Certificado* por cualquiera de las siguientes vías:

1) Personándose en una de las *Oficinas de Registro* implantadas por las *Entidades usuarias* con las que la FNMT-RCM haya suscrito el convenio correspondiente para la expedición de este tipo de *Certificados*, donde acreditará su identidad.

2) En el teléfono 902 200 616 de la FNMT-RCM, donde se le realizarán las preguntas oportunas al objeto de verificar la verdadera identidad del peticionario. Este servicio estará disponible las veinticuatro (24) horas del día, todos los días del año.

196. Tan pronto se resuelva la revocación, el *Firmante* recibirá, a través de la dirección de correo electrónico consignada en la solicitud, la notificación de la revocación del *Certificado*.

197. Una vez que la FNMT-RCM ha procedido a la revocación del *Certificado*, se publicará en el *Directorio* seguro la correspondiente *Lista de Certificados Revocados* conteniendo el número de serie del *Certificado* revocado, la fecha y hora de revocación y la causa de la misma.

13.2.2.8. Suspensión del Certificado

198. La suspensión de un *Certificado* deja sin efecto dicho *Certificado* durante un período de tiempo y en unas condiciones determinadas.

199. La suspensión de los *Certificados* será considerada una revocación temporal de la vigencia de los mismos por lo que los procedimientos y entidades habilitadas para la solicitud y tramitación de la revocación del *Certificado* son de aplicación en el caso de la suspensión.

13.2.2.8.1. Causas de la suspensión del Certificado

200. La FNMT-RCM podrá suspender la vigencia de los *Certificados de Representante para administradores únicos y solidarios* a solicitud del legítimo interesado o de Autoridad Judicial o ante la existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los *Certificados* contempladas en el apartado "Causas de revocación" del presente documento.

201. Asimismo, la solicitud de suspensión puede deberse a la existencia de una investigación o procedimiento judicial o administrativo en curso, cuya conclusión pueda determinar que el *Certificado* efectivamente está afectado por una causa de revocación. En estos casos la FNMT-RCM, a solicitud del legítimo interesado, suspenderá la vigencia del *Certificado* por el plazo requerido y, transcurrido este plazo, procederá a la revocación del *Certificado* salvo que a la FNMT-RCM se le solicite, de forma fehaciente por el legítimo interesado, la reactivación del mismo.

13.2.2.8.2. Procedimiento para la suspensión de Certificados

202. La solicitud de la suspensión de los *Certificados de Representante para administradores únicos y solidarios* solamente podrá ser realizada a través de las *Oficinas de Registro* implantadas por las *Entidades usuarias* con las que la FNMT-RCM haya suscrito el convenio correspondiente.

203. La FNMT-RCM procederá a suspender el *Certificado* durante un plazo de treinta (30) días, plazo tras el cual se extinguirá el *Certificado* mediante su revocación directa por parte del *Prestador de Servicios de Confianza*, la FNMT-RCM, salvo que se hubiera levantado la suspensión mediante solicitud de cancelación de la suspensión por parte de la *Entidad representada*, su *Representante* o un tercero autorizado y con facultades suficientes. No obstante lo anterior, el plazo previsto para la suspensión del *Certificado* podrá verse alterado en función de los procedimientos judiciales o administrativos que lo pudieran afectar.

204. Si durante el plazo de suspensión del *Certificado* este caducara o se solicitara su revocación, se producirán las mismas consecuencias que para los *Certificados* no suspendidos que se vieran afectados por supuestos de caducidad o de revocación respectivamente.

13.2.2.8.3. Procedimiento para la cancelación de la suspensión de Certificados

205. Podrán solicitar la cancelación de la suspensión de los *Certificados* los *Representantes* siempre que, con anterioridad a esta solicitud de cancelación de la suspensión, conserven el *Certificado* y sus *Datos de creación de Firma*, y dicha solicitud se efectúe durante los treinta (30) días siguientes a su suspensión.

206. Para ello deberán personarse ante cualquier *Oficina de Registro* con las que la FNMT-RCM haya suscrito el convenio correspondiente. En este acto el *Solicitante* aportará los datos que se le requieran y acreditará su identidad personal, como en el proceso de emisión ya descrito.

207. La personación del *Solicitante* no será indispensable si la firma de la solicitud de cancelación de la suspensión de un *Certificado* ha sido legitimada en presencia notarial.

208. Los datos personales del *Solicitante*, una vez validados por la *Oficina de Registro*, se enviarán a la FNMT-RCM mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM.

209. Una vez recibidos los datos validados por la *Oficina de Registro* de la petición de la cancelación de la suspensión la FNMT-RCM procederá a retirar este *Certificado* del *Servicio de información y consulta sobre el estado de los certificados*.

13.2.2.9. Renovación del Certificado

210. La renovación del *Certificado de Representante para administradores únicos y solidarios* se realiza siempre emitiendo nuevas claves. Se permitirá la renovación de este tipo de *Certificados* desde sesenta (60) días antes de su fecha de caducidad.

211. La identificación del *Representante*, como *Solicitante* de la renovación del *Certificado*, se realizará telemáticamente mediante el uso del *Certificado de Representante para administradores únicos y solidarios* que, estando aún activo, está próximo a caducar, siempre que en el momento de la solicitud no se haya superado el plazo máximo de 5 años desde la personación e identificación física del *Representante*, de acuerdo con lo establecido en el artículo 13.4 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

212. El proceso de renovación del *Certificado* incluirá, en la fase de descarga del mismo, el pago por parte del *Solicitante* del importe correspondiente a los precios públicos aprobados por la FNMT-RCM para este tipo de *Certificado*.

13.2.3. Comprobación del estado de revocación del Certificado

213. El estado de revocación de los *Certificados* electrónicos de *Representante para administradores únicos y solidarios* se podrá comprobar a través del *Servicio de información y consulta del estado de los Certificados* mediante el protocolo OCSP.

214. Este servicio estará disponible las veinticuatro (24) horas del día, todos los días del año, salvo por circunstancias ajenas a la FNMT-RCM u operaciones de mantenimiento. La FNMT-RCM notificará esta última circunstancia en la dirección http://www.cert.fnmt.es si es posible con al menos cuarenta y ocho (48) horas de antelación y tratará de solventarla en un periodo no superior a veinticuatro (24) horas.

215. El funcionamiento de este servicio es el siguiente: el *servidor OCSP* de la FNMT-RCM recibe la petición OCSP efectuada por un *Cliente OCSP* y comprueba el estado de los *Certificados* incluidos en la misma. En caso de que la petición sea válida, se emitirá una respuesta de OCSP informando acerca del estado en el que se encuentran en ese momento los Certificados incluidos en la petición. Dicha respuesta OCSP está firmada con los *Datos de Creación de Firma* asociados al servidor OCSP específico para la AC Representación, garantizando así la integridad y la autenticidad de la información suministrada sobre el estado de revocación de los *Certificados* consultados.

216. Será responsabilidad de la *Entidad usuaria* obtener un *Cliente OCSP* para operar con el servidor OCSP puesto a disposición por la FNMT-RCM.

13.3. POLÍTICA DE CERTIFICACIÓN DE LOS CERTIFICADOS DE REPRESENTANTE PARA ADMINISTRADORES ÚNICOS Y SOLIDARIOS

13.3.1. Identificación

217. La presente *Política de Certificación* de la FNMT-RCM para la expedición de *Certificados de Representante para administradores únicos y solidarios* tiene la siguiente identificación:

Nombre: Política de Certificación de *Certificados de Representante para administradores únicos y solidarios*

Referencia / OID[3]:

- 1.3.6.1.4.1.5734.3.11.1.

Versión: 1.3

Fecha de expedición: 24 de junio de 2016

Localización: http://www.cert.fnmt.es/dpcs/

DPC relacionada: Declaración General de Prácticas de Certificación de la FNMT-RCM

Localización: http://www.cert.fnmt.es/dpcs/

13.3.2. Tipología del Certificado de Representante para administradores únicos y solidarios

218. El *Certificado de Representante para administradores únicos y solidarios* es la certificación electrónica expedida por la FNMT-RCM que vincula al *Representante* legal (*Firmante*) de una persona jurídica, unos *Datos de verificación de Firma* y confirma su identidad.

13.3.3. Comunidad y ámbito de aplicación

219. Los *Certificados* expedidos bajo esta *Política de Certificación* se consideran válidos como parte integrante de los sistemas de identificación y firma electrónica basados en *Certificados electrónicos reconocidos* para la relación de las *Personas Jurídicas* a través de sus *Representantes* legales en sus relaciones con las administraciones públicas o en la contratación de bienes o servicios propios o concernientes a su giro o tráfico ordinario.

14. TARIFAS

220. La FNMT – RCM podrá establecer las tarifas y los medios de pago que considere oportunos en cada momento por la expedición de los *Certificados*. El precio y condiciones de pago de los *Certificados* podrán ser consultados en la página web de la FNMT – RCM o bien serán facilitados por el área comercial correspondiente bajo petición a la dirección de correo electrónico comercial.ceres@fnmt.es.

---

[3] *Nota*: El OID o identificador de política es una referencia que se incluye en el *Certificado* al objeto de determinar un conjunto de reglas que indican la aplicabilidad de un determinado tipo de *Certificado* a la *Comunidad Electrónica* y/o clase de aplicación con requisitos de seguridad comunes.

ANEXO I: IDENTIFICACIÓN DEL CERTIFICADO DE LA AUTORIDAD DE CERTIFICACIÓN AC REPRESENTACIÓN

La Autoridad de Certificación AC Representación utiliza para la firma de certificados y CRLs el certificado identificado a continuación:

Certificado de la Autoridad de Certificación "AC Representación"

- Nombre distintivo: CN = AC Representación, OU = CERES, O = FNMT-RCM, C = ES
- Número de serie: 61 C2 D4 D4 F6 A9 AE 77 55 92 66 B9 8D AF D6 21
- Período de validez desde: 30 de junio de 2015
- Período de validez hasta: 31 de diciembre de 2029
- Huella digital (sha256):

  8F D1 6A 17 99 44 D5 D1 D4 20 AF 09 40 5E DA 7A BF 2A 9C 74 28 83 E8 C2 F8 9E 0D 90 AF AF 75 4B

ANEXO II: PERFILES DE LOS CERTIFICADOS EXPEDIDOS POR LA AC REPRESENTACIÓN

PERFIL CERTIFICADO AC REPRESENTACIÓN

Campo		Contenido	Oblig	Crit	Especificaciones
1. **Version**		2	Sí		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. **Serial Number**		Número identificativo único del certificado.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. **Signature Algorithm**		Sha256withRsaEncryption	Sí		OID: 1.2.840.113549.1.1.11
4. **Issuer Distinguish Name**		Entidad emisora del certificado (CA Raíz)	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del *Prestador de Servicios de Confianza* (emisor del certificado). O=FNMT-RCM	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organizational Unit	OU=AC RAIZ FNMT-RCM	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
5. **Validity**		Hasta 31/12/2029	Sí		
6. **Subject**			Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. Organization	Denominación (nombre "oficial" de la organización) del *Prestador de Servicios de Confianza* (emisor del certificado). O=FNMT-RCM.	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	6.3. Organizational Unit	OU=CERES	Sí		UTF8 String, tamaño máximo 128 (rfc5280)

Campo			Contenido	Oblig	Crit	Especificaciones
	6.4. CommonName		CN=AC Representación	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
7. **Authority Key Identifier**			Identificador de la clave pública de la entidad raíz. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de esta CA Subordinada	Sí		RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la AC raíz.
8. **Subject Public Key Info**			Clave pública de la CA Subordinada de Representación codificada según el estándar PKCS#1 de RSA.	Sí		Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048 bits
9. **Subject Key Identifier**			Identificador de la clave pública de la CA Subordinada. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí		RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. **Key Usage**			Uso permitido de las claves certificadas.	Sí	Sí	Normalizado en norma X509 y RFC 5280
	10.1. Digital Signature		0	Sí		Ver X509 y RFC 5280
	10.2. Content Commitment		0	Sí		Ver X509 y RFC 5280
	10.3. Key Encipherment		0	Sí		Ver X509 y RFC 5280
	10.4. Data Encipherment		0	Sí		Ver X509 y RFC 5280
	10.5. Key Agreement		0	Sí		Ver X509 y RFC 5280
	10.6. Key Certificate Signature		1	Sí		Ver X509 y RFC 5280
	10.7. CRL Signature		1	Sí		Ver X509 y RFC 5280
11. **Certificate Policies**			Política de certificación	Sí		
	11.1. Policy Identifier		2.5.29.32.0 (anyPolicy)	Sí		Atendiendo a la rfc5280: "*PolicyInformation SHOULD only contain an OID.* *In a CA certificate,these policy information terms limit the set of policies for certification paths which include this certificate. When a CA does not wish to limit the set of policies for certification paths which include this certificate, it MAY assert the special policy anyPolicy, with a value of { 2 5 29 32 0 }*"
	11.2. Policy Qualifier Id			Sí		
		11.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.

Campo			Contenido	Oblig	Crit	Especificaciones
		11.2.2 User Notice	Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)	Sí		UTF8 String. Longitud máxima 200 caracteres.
12. **CRL Distribution Point**				Sí		
	12.1. Distribution Point 1		Punto de distribución 1 de la CRL (ARL) ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí		UTF8String Ruta donde reside la CRL (punto de distribución 1).
	12.2. Distribution Point 2		Punto de distribución 2 de la CRL (ARL) http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl	Sí		UTF8String. Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
13. **Authority Info Access**				Sí	No	
	13.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		OCSP (1.3.6.1.5.5.7.48.1)
	13.2. Acces Location 1		http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder	Sí		URL del servicio de OCSP
	13.3. Access Method 2		Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí		Certificado de la CA emisora: De la rfc 5280: "the idad-calssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."
	13.4. Acces Location 2		http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA raíz de la FNMTRCM.
14. **Basic Constraints**				Sí	Sí	
	14.1. cA		Valor TRUE (CA)	Sí		De la rfc 5280: "The cA boolean indicates whether the certified public key may be used to verify certificate signatures."

Campo		Contenido	Oblig	Crit	Especificaciones
	14.2. pathLenConstraint	0	Sí		Un pathLenConstraint de cero indica que no pueden existir más certificados de CA intermedios en la ruta de certificación.

PERFIL CERTIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA

Campo		Contenido	Oblig	Crit	Especificaciones
1. Version		2	Sí		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		Sha256withRsaEncryption	Sí		String UTF8 (40). Identificando el tipo de algoritmo OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del *Prestador de Servicios de Confianza* (emisor del certificado). O=FNMT-RCM	Sí		UTF8 String.
	4.3. Organizational Unit	OU=CERES	Sí		UTF8 String.
	4.4. CommonName	CN=AC Representación	Sí		UTF8 String.
5. Validity		2 años	Sí		
6. Subject		Identificación/descripción del *Representante* y de la *Entidad representada*	Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString.
	6.2. Organization	Razón social de la *Entidad Representada*	Sí		UTF8String (rfc5280). Por ejemplo: O=Entidad de pruebas
	6.3. OrganizationIdentifier	NIF de la *Entidad Representada*	Sí		Se codificará de acuerdo a ETSI EN 319 412-1. UTF8String (rfc5280). Ejemplo: organizationIdentifier= VATES-Q00000000J
	6.4. CommonName	NIF, nombre y 1er apellido del *Representante* y NIF de la *Entidad representada*.	Sí		UTF8StringPor ejemplo: CN=00000000T Juan Español (R: Q0000000J)
	6.5. Surname	Apellidos del *Representante*	Sí		UTF8String (rfc5280). Por ejemplo: SN=Español Español
	6.6. GivenName	Nombre de pila del *Representante*	Sí		UTF8String (rfc5280). Por ejemplo: givenName=Juan
	6.7. SerialNumber	NIF del *Representante*	Sí		Se codificará de acuerdo a ETSI EN 319 412-1. PrintableString (rfc5280). Ejemplo: serialNumber= IDCES-00000000T
	6.8. Description	Identificador de los documentos públicos que acreditan las facultades del *Representante* 2.5.4.13=Id de documentos públicos	Sí		UTF8 String, tamaño máximo 100 caracteres. Por ejemplo: 2.5.4.13= "Ref: XXXXX/YYYYY/ZZZZZ/12345678/20151212 120000"
7. Authority Key Identifier		Identificador de la clave pública del PSC. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí		RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la AC emisora.
8. Subject Public Key Info		Clave pública del *Firmante*, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí		Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048 bits

Campo			Contenido	Oblig	Crit	Especificaciones
9. Subject Key Identifier			Identificador de la clave pública del *Firmante*. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí		RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage			Uso permitido de las claves certificadas.	Sí	Sí	Normalizado en norma X509.
	10.1. Digital Signature		1	Sí		Ver X509 y RFC 5280.
	10.2. Content Commitment		1	Sí		Ver X509 y RFC 5280.
	10.3. Key Encipherment		1	Sí		Ver X509 y RFC 5280.
	10.4. Data Encipherment		0	Sí		Ver X509 y RFC 5280.
	10.5. Key Agreement		0	Sí		Ver X509 y RFC 5280.
	10.6. Key Certificate Signature		0	Sí		Ver X509 y RFC 5280.
	10.7. CRL Signature		0	Sí		Ver X509 y RFC 5280.
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí		Ver X509 y RFC 5280.
	11.1. Email Protection		1.3.6.1.5.5.7.3.4	Sí		Ver X509 y RFC 5280.
	11.2. Client Authentication		1.3.6.1.5.5.7.3.2	Sí		Ver X509 y RFC 5280.
12. Qualified Certificate Statements			Extensiones cualificadas.		No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.
	12.1. QcCompliance		Certificado es cualificado.	Sí		Indica que el certificado es cualificado.
	12.2. QcType		Qct-esign	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
	12.3. QcPDS		{https://www.cert.fnmt.es/pds/PDS_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_en.pdf, en}	Sí		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
	12.4. QcEuRetentionPeriod		15 años	Sí		Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otra información relevante.
13. Certificate Policies			Política de certificación	Sí		
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.11.2	Sí		Identificador de la política establecido por el Prestador.
	13.1.1. Policy Qualifier Id					
		13.1.1.1. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		13.1.1.2. User Notice	Certificado electrónico de representante de persona jurídica en sus relaciones con las AAPP, Entidades y Organismos Públicos vinculados o dependientes de las mismas	Sí		UTF8 String.
	13.2. Policy Identifier		0.4.0.194112.1.0	Sí		QCP-n: certificate policy for EU qualified certificates issued to natural persons.
	13.3. Policy Identifier		2.16.724.1.3.5.8	Sí		Identificador de la política según normativa nacional.
14. Subject Alternative Names			Identificación/descripción del *Representante* y de la *Entidad*	Sí	No	
	14.1. rfc822 Name		Correo electrónico del *Representante*	Sí		
	14.2. Directory Name					
		14.2.1. Nombre	Nombre de pila del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.1 =Nombre de pila	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.1=JUAN
		14.2.2. Apellido1	Primer apellido del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.2 =Apellido 1	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.2=ESPAÑOL

Campo			Contenido	Oblig	Crit	Especificaciones
		14.2.3. Apellido2	Segundo apellido del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.3 =Apellido 2	Opcional		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.3 =ESPAÑOL
		14.2.4. NIF	NIF del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.4=NIF	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.4=IDCES-99999999R
		14.2.5. Razón Social	Razón social de la *Entidad Representada* 1.3.6.1.4.1.5734.1.6=Razón social	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.6=Entidad de pruebas
		14.2.6. NIF de la entidad	NIF de la *Entidad Representada* 1.3.6.1.4.1.5734.1.7=NIF	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.7= VATES-Q00000000J
15. CRL Distribution Point				Sí	No	
	15.1. Distribution Point 1		Punto de distribución 1 de la CRL ldap://ldaprep.cert.fnmt.es/CN=CRL<xxx>, OU=AC%20Representacion, OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí		Ruta donde reside la CRL (punto de distribución 1). <xxx> es el identificador de la CRL particionada concreta donde se halla el certificado.
	15.2. Distribution Point 2		Punto de distribución 2 de la CRL (ARL) http://www.cert.fnmt.es/crlsrep/CRLnnn.crl	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2). <nnn> es el identificador de la CRL particionada concreta donde se halla el certificado.
16. Authority Info Access				Sí	No	
	16.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		OCSP (1.3.6.1.5.5.7.48.1)
	16.2. Acces Location 1		http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder	Sí		URL del servicio de OCSP.
	16.3. Access Method 2		Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí		Certificado de la CA emisora: De la rfc 5280: "the id-ad-calssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."
	16.4. Acces Location 2		http://www.cert.fnmt.es/certs/ACREP.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA subordinada de Representación.
17. Basic Constraints			Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	Sí	De la rf5280: "This extension MAY appear as a critical or non-critical extension in end entity certificates.
	17.1. cA		Valor FALSE (entidad final)	Sí		De la rfc 5280: "The cA boolean indicates whether the certified public key may be used to verify certificate signatures."

PERFIL CERTIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA

Campo		Contenido	Oblig	Crit	Especificaciones
1. Version		2	Sí		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		Sha256withRsaEncryption	Sí		String UTF8 (40). Identificando el tipo de algoritmo OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString.
	4.2. Organization	Denominación (nombre "oficial" de la organización) del *Prestador de Servicios de Confianza* (emisor del certificado). O=FNMT-RCM	Sí		UTF8 String.
	4.3. Organization Unit	OU=CERES	Sí		UTF8 String.
	4.4. CommonName	CN=AC Representación	Sí		UTF8 String.
5. Validity		2 años	Sí		
6. Subject		Identificación/descripción del *Representante* y de la *Entidad representada*	Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString.
	6.2. Organization	Razón social de la *Entidad Representada*	Sí		UTF8String (rfc5280). Por ejemplo: O=Entidad de pruebas
	6.3. OrganizationIdentifier	NIF de la *Entidad Representada*	Sí		Se codificará de acuerdo a ETSI EN 319 412-1. UTF8String (rfc5280). Ejemplo: organizationIdentifier= VATES-Q00000000J
	6.4. CommonName	NIF, nombre y 1er apellido del *Representante* y NIF de la *Entidad representada*.	Sí		UTF8StringPor ejemplo: CN=00000000T Juan Español (R: Q0000000J)
	6.5. Surname	Apellidos del *Representante*	Sí		UTF8String (rfc5280). Por ejemplo: SN=Español Español
	6.6. GivenName	Nombre de pila del *Representante*	Sí		UTF8String (rfc5280). Por ejemplo: givenName=Juan
	6.7. SerialNumber	NIF del *Representante*	Sí		Se codificará de acuerdo a ETSI EN 319 412-1. PrintableString (rfc5280). Ejemplo: serialNumber= IDCES-00000000T
	6.8. Description	Identificador de los documentos públicos que acreditan las facultades del *Representante* 2.5.4.13=Id de documentos públicos	Sí		UTF8 String, tamaño máximo 100 caracteres. Por ejemplo: 2.5.4.13= "Ref: XXXXX/YYYYY/ZZZZZ/12345678/20151212 120000"
7. Authority Key Identifier		Identificador de la clave pública del PSC. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí		RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la AC emisora.
8. Subject Public Key Info		Clave pública del *Firmante*, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí		Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048 bits.
9. Subject Key Identifier		Identificador de la clave pública del *Firmante*. Medio para identificar certificados que contienen una clave pública particular y facilita la	Sí		RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).

			construcción de rutas de certificación.			
10.	**Key Usage**		Uso permitido de las claves certificadas.	Sí	Sí	Normalizado en norma X509.
	10.1. Digital Signature		1	Sí		Ver X509 y RFC 5280.
	10.2. Content Commitment		1	Sí		Ver X509 y RFC 5280.
	10.3. Key Encipherment		1	Sí		Ver X509 y RFC 5280.
	10.4. Data Encipherment		0	Sí		Ver X509 y RFC 5280.
	10.5. Key Agreement		0	Sí		Ver X509 y RFC 5280.
	10.6. Key Certificate Signature		0	Sí		Ver X509 y RFC 5280.
	10.7. CRL Signature		0	Sí		Ver X509 y RFC 5280.
11.	**Extended Key Usage**		Uso mejorado o extendido de las claves	Sí		Ver X509 y RFC 5280.
	11.1. Email Protection		1.3.6.1.5.5.7.3.4	Sí		Ver X509 y RFC 5280.
	11.2. Client Authentication		1.3.6.1.5.5.7.3.2	Sí		Ver X509 y RFC 5280.
12.	**Qualified Certificate Statements**		Extensiones cualificadas.		No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.
	12.1. QcCompliance		Certificado es cualificado.	Sí		Indica que el certificado es cualificado.
	12.2. QcType		Qct-esign	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
	12.3. QcPDS		{https://www.cert.fnmt.es/pds/PDS_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_en.pdf, en}	Sí		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
	12.4. QcEuRetentionPeriod		15 años	Sí		Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otra información relevante.
13.	**Certificate Policies**		Política de certificación	Sí		
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.11.3	Sí		Identificador de la política establecido por el Prestador.
	13.1.1. Policy Qualifier Id					
		13.1.1.1. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		13.1.1.2. User Notice	Certificado electrónico de representante de entidad sin personalidad jurídica para el ámbito tributario y cualquier otro previsto por la legislación vigente	Sí		UTF8 String.
	13.2. Policy Identifier		0.4.0.194112.1.0			QCP-n: certificate policy for EU qualified certificates issued to natural persons.
	13.3. Policy Identifier		2.16.724.1.3.5.9	Sí		Identificador de la política según normativa nacional.
14.	**Subject Alternative Names**		Identificación/descripción del *Representante* y de la *Entidad*	Sí	No	
	14.1. rfc822 Name		Correo electrónico del *Representante*	Sí		
	14.2. Directory Name					
		14.2.1. Nombre	Nombre de pila del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.1 =Nombre de pila	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.1=JUAN
		14.2.2. Apellido1	Primer apellido del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.2 =Apellido 1	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.2=ESPAÑOL
		14.2.3. Apellido2	Segundo apellido del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.3 =Apellido 2	Opcional		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.3 =ESPAÑOL
		14.2.4. NIF	NIF del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.4=NIF	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.4=IDCES-99999999R
		14.2.5. Razón Social	Nombre de la *Entidad sin personalidad jurídica* representada 1.3.6.1.4.1.5734.1.6=Razón	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.6=Entidad de pruebas

			social			
		14.2.6. NIF de la entidad	NIF de la *Entidad sin personalidad jurídica* 1.3.6.1.4.1.5734.1.7=NIF	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.7= VATES-Q00000000J
		14.2.7. Tipo de ESPJ	Tipo de *Entidad sin personalidad jurídica* 1.3.6.1.4.1.5734.1.22=Tipo de entidad.	Sí		UTF8 String. Valores que puede tomar: RA - Comunidad de bienes RB - Comunidad propietarios propiedad horizontal RC - Comunidad titular montes vecinales RD - Sociedad civil RE - Herencia yacente RF - Fondo de inversión RG - Unión temporal de empresas RH - Fondo de capital-riesgo RI - Fondo de pensiones RJ - Fondo de regulación mercado hipotecario RK - Fondo de titulación hipotecaria RL - Fondo de titulación activos RM - Fondo de garantía de inversiones RN - Otros entes sin personalidad jurídica Por ejemplo: 1.3.6.1.4.1.5734.1.22=RA – Comunidad de Bienes
15. CRL Distribution Point				Sí	No	
	15.1. Distribution Point 1		Punto de distribución 1 de la CRL ldap://ldaprep.cert.fnmt.es/CN=CRL<xxx>, OU=AC%20Representacion, OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí		Ruta donde reside la CRL (punto de distribución 1). <xxx> es el identificador de la CRL particionada concreta donde se halla el certificado.
	15.2. Distribution Point 2		Punto de distribución 2 de la CRL (ARL) http://www.cert.fnmt.es/crlsrep/CRLnnn.crl	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2). <nnn> es el identificador de la CRL particionada concreta donde se halla el certificado.
16. Authority Info Access				Sí	No	
	16.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		OCSP (1.3.6.1.5.5.7.48.1)
	16.2. Acces Location 1		http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder	Sí		URL del servicio de OCSP
	16.3. Access Method 2		Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí		Certificado de la CA emisora: De la rfc 5280: “the id-ad-calssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user.”
	16.4. Acces Location 2		http://www.cert.fnmt.es/certs/ACREP.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA subordinada de Representación.
17. Basic Constraints			Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de “profundidad” permitido para las cadenas de certificación”.	Sí	Sí	De la rf5280: “This extension MAY appear as a critical or non-critical extension in end entity certificates.
	17.1. cA		Valor FALSE (entidad final)	Sí		De la rfc 5280: “The cA boolean indicates whether the certified public key may be used to verify certificate signatures.”

PERFIL CERTIFICADO DE REPRESENTANTE PARA ADMINISTRADORES ÚNICOS O SOLIDARIOS

Campo		Contenido	Oblig	Crit	Especificaciones
1. **Version**		2	Sí		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. **Serial Number**		Número identificativo único del certificado.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. **Signature Algorithm**		Sha256withRsaEncryption	Sí		OID: 1.2.840.113549.1.1.11
4. **Issuer Distinguish Name**		Entidad emisora del certificado (CA Subordinada)	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString.
	4.2. Organization	Denominación (nombre "oficial" de la organización) del *Prestador de Servicios de Confianza* (emisor del certificado). O=FNMT-RCM	Sí		UTF8 String.
	4.3. Organizational Unit	OU=CERES	Sí		UTF8 String.
	4.4. CommonName	CN=AC Representación	Sí		UTF8 String.
5. **Validity**		2 años	Sí		
6. **Subject**		Identificación/descripción del *Representante* y de la *Entidad representada*	Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString.
	6.2. Organization	Razón social de la *Entidad Representada*	Sí		UTF8String (rfc5280). Por ejemplo: O=Entidad de pruebas
	6.3. OrganizationIdentifier	NIF de la *Entidad Representada*	Sí		Se codificará de acuerdo a ETSI EN 319 412-1. UTF8String (rfc5280). Ejemplo: organizationIdentifier= VATES-Q00000000J
	6.4. CommonName	NIF, nombre y 1er apellido del *Representante* y NIF de la *Entidad representada*.	Sí		UTF8StringPor ejemplo: CN=00000000T Juan Español (R: Q0000000J)
	6.5. Surname	Apellidos del *Representante*	Sí		UTF8String (rfc5280). Por ejemplo: SN=Español Español
	6.6. GivenName	Nombre de pila del *Representante*	Sí		UTF8String (rfc5280). Por ejemplo: givenName=Juan
	6.7. SerialNumber	NIF del *Representante*	Sí		Se codificará de acuerdo a ETSI EN 319 412-1. PrintableString (rfc5280). Ejemplo: serialNumber= IDCES-00000000T
	6.8. Description	Codificación del documento público que acredita las facultades del firmante o los datos registrales.	Sí		UTF8String. Estará compuesto por la concatenación separada por comas de los siguientes datos registrales: - Registro - Hoja - Tomo - Folio - Nº de inscripción - Fecha de inscripción Por ejemplo: 2.5.4.13="Reg:XXX/Hoja: XXX/ Tomo: XXX/Folio: XXX/Fecha dd/mm/yyyy/Incripción: XX"
7. **Authority Key Identifier**		Identificador de la clave pública del PSC. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí		RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la AC emisora.

Campo			Contenido	Oblig	Crit	Especificaciones
8. **Subject Public Key Info**			Clave pública del *Firmante*, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí		Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048 bits
9. **Subject Key Identifier**			Identificador de la clave pública del *Firmante*. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí		RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. **Key Usage**			Uso permitido de las claves certificadas.	Sí	Sí	Normalizado en norma X509.
	10.1. Digital Signature		1	Sí		Ver X509 y RFC 5280.
	10.2. Content Commitment		1	Sí		Ver X509 y RFC 5280.
	10.3. Key Encipherment		1	Sí		Ver X509 y RFC 5280.
	10.4. Data Encipherment		0	Sí		Ver X509 y RFC 5280.
	10.5. Key Agreement		0	Sí		Ver X509 y RFC 5280.
	10.6. Key Certificate Signature		0	Sí		Ver X509 y RFC 5280.
	10.7. CRL Signature		0	Sí		Ver X509 y RFC 5280.
11. **Extended Key Usage**			Uso mejorado o extendido de las claves	Sí		Ver X509 y RFC 5280.
	11.1. Email Protection		1.3.6.1.5.5.7.3.4	Sí		Ver X509 y RFC 5280.
	11.2. Client Authentication		1.3.6.1.5.5.7.3.2	Sí		Ver X509 y RFC 5280.
12. **Qualified Certificate Statements**			Extensiones cualificadas.		No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.
	12.1. QcCompliance		Certificado es cualificado.	Sí		Indica que el certificado es cualificado.
	12.2. QcType		Qct-esign	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
	12.3. QcPDS		{https://www.cert.fnmt.es/pds/PDS_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_en.pdf (, en}	Sí		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
	12.4. QcEuRetentionPeriod		15 años	Sí		Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otra información relevante.
13. **Certificate Policies**			Política de certificación	Sí		
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.11.1	Sí		Identificador de la política establecido por el Prestador.
	13.1.1. Policy Qualifier Id					
		13.1.1.1. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		13.1.1.2. User Notice	Certificado electrónico de representante de persona jurídica en sus relaciones con las AAPP o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario	Sí		UTF8 String.
	13.2. Policy Identifier		0.4.0.194112.1.0			QCP-n: certificate policy for EU qualified certificates issued to natural persons.
	13.3. Policy Identifier		2.16.724.1.3.5.8	Sí		Identificador de la política según normativa nacional.
14. **Subject Alternative Names**			Identificación/descripción del *Representante* y de la *Entidad representada*	Sí	No	
	14.1. rfc822 Name		Correo electrónico del *Representante*	Sí		
	14.2. Directory Name					
		14.2.1. Nombre	Nombre de pila del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.1 =Nombre de pila	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.1=JUAN

Campo			Contenido	Oblig	Crit	Especificaciones
		14.2.2. Apellido1	Primer apellido del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.2 =Apellido 1	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.2=ESPAÑOL
		14.2.3. Apellido2	Segundo apellido del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.3 =Apellido 2	Opcional		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.3 =ESPAÑOL
		14.2.4. NIF	NIF del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.4=NIF	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.4=IDCES-99999999R
		14.2.5. Razón Social	Razón social de la *Entidad Representada* 1.3.6.1.4.1.5734.1.6=Razón social	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.6=Entidad de pruebas
		14.2.6. NIF de la entidad	NIF de la *Entidad Representada* 1.3.6.1.4.1.5734.1.7=NIF	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.7= VATES-Q00000000J
		14.2.7. Cargo / Poder	Cargo o poder del *Representante* dentro de la entidad 1.3.6.1.4.1.5734.1.20 =Cargo	Sí		UTF8 String. Dos posibles valores: - administrador único - administrador solidario Por ejemplo: 1.3.6.1.4.1.5734.1.20 =Administrador único
15. **CRL Distribution Point**				Sí	No	
	15.1. Distribution Point 1		Punto de distribución 1 de la CRL ldap://ldaprep.cert.fnmt.es/CN=CRL<xxx>, OU=AC%20Representacion, OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí		Ruta donde reside la CRL (punto de distribución 1). <xxx> es el identificador de la CRL particionada concreta donde se halla el certificado.
	15.2. Distribution Point 2		Punto de distribución 2 de la CRL http://www.cert.fnmt.es/crlsrep/CRLnnn.crl	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).). <nnn> es el identificador de la CRL particionada concreta donde se halla el certificado.
16. **Authority Info Access**				Sí	No	
	16.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		OCSP (1.3.6.1.5.5.7.48.1)
	16.2. Acces Location 1		http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder	Sí		URL del servicio de OCSP
	16.3. Access Method 2		Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí		Certificado de la CA emisora: De la rfc 5280: “the id-ad-calssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user.”
	16.4. Acces Location 2		http://www.cert.fnmt.es/certs/ACREP.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA subordinada de Representación.
17. **Basic Constraints**			Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de “profundidad” permitido para las cadenas de certificación”.	Sí	Sí	De la rf5280: “This extension MAY appear as a critical or non-critical extension in end entity certificates.
	17.1. cA		Valor FALSE (entidad final)	Sí		De la rfc 5280: “The cA boolean indicates whether the certified public key may be used to verify certificate signatures.”