POLÍTICA Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS CERTIFICADOS DE PERSONAS FÍSICAS DE LA "AC FNMT USUARIOS"

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM / v1.0	25/03/2014
Revisado por:	FNMT-RCM / v1.0	20/10/2014
Aprobado por:	FNMT-RCM / v1.0	09/10/2014

HISTÓRICO DEL DOCUMENTO		
Versión	**Fecha**	**Descripción**
1.0	25/03/2014	Creación del documento

Referencia: DPC/CPUS0100/SGPSC/2014

Documento clasificado como: *Público*

ÍNDICES

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

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 Persona Física*.

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* correspondiente a cada órgano y/u organismo o entidad usuaria de los servicios de certificación de la FNMT-RCM.

3. Los *Certificados de usuarios* 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, según lo definido en la Ley 59/2003, de firma electrónica, y la norma ETSI 101 456 del European Telecommunications Standards Institute que define los requisitos que deben cumplir las políticas de certificación de las Autoridades de Certificación que expiden certificados electrónicos con la cualidad de reconocidos (qualified) conforme al anexo I de la Directiva Europea 1999/93/CE, por la que se establece un marco comunitario para la firma electrónica.

2. ORGANIZACIÓN DEL DOCUMENTO

4. 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.

5. 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.

6. El presente documento representa, por tanto, las *Políticas de Certificación y Prácticas de Certificación Particulares* para los *Certificados* expedidos a personas físicas.

3. ORDEN DE PRELACIÓN

7. Las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares* de *Certificados de Personas Físicas* forman parte de la *Declaración de Prácticas de Certificación* 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

8. 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 Persona Física*: Certificado expedido a una persona física que actúa como *Firmante*. Este es un tipo específico de certificado expedido por la FNMT – RCM y, por tanto, estará sujeto a las condiciones establecidas en su política y prácticas de certificación particulares.
- *Firmante*: La persona física que posee un dispositivo de creación de firma y que actúa (realiza la firma) en nombre propio o en nombre del *Titular* del *Certificado*.
- *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 la que se deroga la Directiva 1999/93/CE.
- *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 su nombre .
- *Suscriptor*: Persona física que suscribe los términos y condiciones de uso de un *Certificado*. En los *Certificados de Persona Física* expedidos bajo la presente *Política*, coincide con la persona del *Titular*.
- *Titular* (de un *Certificado*): Es la persona física, mayor de 18 años o menor emancipado, cuya identidad queda vinculada a los *Datos de verificación de firma* (Clave Pública) del *Certificado* expedido por el *Prestador de Servicios de Confianza*. Por tanto, la identidad del *Titular* se vincula a lo firmado electrónicamente utilizando los *Datos de creación de firma* (Clave privada) asociados al *Certificado*.

5. SEUDÓNIMOS

9. En cuanto a la identificación de los *Titulares* 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

10. Todos los *Certificados* emitidos bajo esta política son de conformidad con el estándar X.509 versión 3. El anexo III de este documento refleja el perfil completo del *Certificado*.

6.1. RESTRICCIONES DE LOS NOMBRES

11. 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

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

6.3. SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS

13. 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"

14. 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

15. La FNMT–RCM no asume compromiso alguno sobre el uso de marcas comerciales en la emisión de los *Certificados* expedidos bajo la presente *Política de Certificación*. No se permite el uso de signos distintivos cuyo derecho de uso no sea propiedad del *Titular* por lo que la FNMT–RCM no está obligada a verificar previamente la posesión de marcas registradas y demás 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

16. 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*

17. 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

18. 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

19. 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*.

20. 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.

21. 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*.

22. 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*

23. 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

24. 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

25. 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

26. 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

27. 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.

28. 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*.

29. 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:

1) Gestión de la Seguridad.
2) Clasificación y Gestión de Activos.
3) Seguridad de Personal.
4) Seguridad física y del entorno.
5) Gestión de las Operaciones.
6) Gestión de Accesos al Sistema.
7) Gestión de incidencias y sistema de continuidad de negocio.
8) Terminación de la FNMT-RCM como *Prestador de Servicios de Confianza*.
9) Almacenamiento de la información referente a los *Certificados Reconocidos*.

9.2. INTEROPERABILIDAD

30. Los *Certificados de Persona Física* 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

31. 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*.

6) Reseña legal de interés, con referencia a las normas relativas a reclamaciones y resolución de conflictos.

11. POLÍTICA DE CERTIFICACIÓN DE LOS CERTIFICADOS DE PERSONA FÍSICA

11.1. IDENTIFICACIÓN

32. La presente *Política de Certificación* de la FNMT-RCM para la expedición de *Certificados de Persona Física* tiene la siguiente identificación:

Nombre: Política de Certificación de *Certificados de Persona Física*

Referencia / OID[1]:

- 1.3.6.1.4.1.5734.3.10.1.

Versión: 1.0

Fecha de expedición: 30 de octubre de 2014

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/

11.2. TIPOLOGÍA DEL CERTIFICADO DE PERSONA FÍSICA

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

11.3. COMUNIDAD Y ÁMBITO DE APLICACIÓN

34. La presente *Política de Certificación* es de aplicación en la expedición de *Certificados* electrónicos que tienen las siguientes características:

a) Son expedidos como *Certificados Reconocidos* atendiendo a los criterios establecidos en la Ley 59/2003, de 19 de diciembre, de firma electrónica y en la normativa técnica EESSI, concretamente ETSI TS 101 862 – "Qualified Certificate Profile".

b) Son expedidos por la FNMT-RCM como *Prestador de Servicios de Confianza* cumpliendo con los criterios establecidos en la citada Ley 59/2003 y en la normativa técnica EESSI, concretamente ETSI TS 101 456 - "Policy requirements for certification authorities issuing qualified certificates".

[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.

c) 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 que deban ser admitidos en virtud de su inclusión en las listas de servicios de confianza (TSL, por sus siglas en inglés) conforme a las especificaciones técnicas recogidas en el Anexo de la Decisión de la Comisión 2009/767/CE, de 16 de octubre de 2009 (modificada por la Decisión de la Comisión 2010/425/UE , de 28 de julio de 2010), por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las ventanillas únicas, con arreglo a la Directiva 2006/123/CE, de 12 de diciembre de 2006, del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior. Estas listas de servicios de confianza contienen información relativa a los *Proveedores de Servicios de Certificación* que expiden C*ertificados* reconocidos al público supervisados en cada Estado miembro, entre los cuales se encuentra la FNMT–RCM.

11.4. RESPONSABILIDAD Y OBLIGACIONES DE LAS PARTES

35. Las obligaciones y responsabilidades expresadas en este apartado se entienden sin perjuicio de las correspondientes derivadas de la legislación y normativa de aplicación, específicamente de las aplicables a la FNMT-RCM como *Prestador de Servicios de Confianza* y que para tal condición se establecen en el articulado en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, su reglamentación de desarrollo y 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 la que se deroga la Directiva 1999/93/CE, de conformidad con su artículo 52, "Entrada en vigor".

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

- La Administración, organismos, entidades públicas y privadas que admiten los *Certificados de Persona Física* como medios de identificación y/o firma electrónica.
- 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.
- Los *Titulares* del *Certificado*.
- FNMT-RCM, en cuanto *Prestador de Servicios de Confianza*.
- En su caso, resto de Comunidad Electrónica y terceros.

11.4.1. Derechos y obligaciones de las Administraciones

El régimen de derechos y obligaciones de las Administraciones, organismos, entidades públicas y la FNMT-RCM se regirá mediante el correspondiente acuerdo, encomienda o convenio regulador de los servicios de certificación y la legislación aplicable.

11.4.2. Obligaciones y responsabilidad de las Oficinas de Registro

37. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en este documento y en la *Declaración General de Prácticas de Certificación*, las *Oficinas de Registro* tienen la obligación de:

i) Comprobar fehacientemente la identidad y cualesquiera circunstancias personales de los *Solicitantes* de los *Certificados* relevantes para el fin propio de estos, utilizando cualquiera de los medios admitidos en Derecho, y conforme a lo previsto en la *Declaración General de Prácticas de Certificación* y con carácter particular en la presente *Declaración de Prácticas de Certificación Particulares*.

ii) Conservar toda la información y documentación relativa a los *Certificados de usuario*, cuya solicitud, renovación, suspensión o revocación gestiona durante el plazo de tiempo establecido en la legislación vigente.

iii) 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*.

iv) Informar a la FNMT-RCM de cualquier aspecto que afecte a los *Certificados* expedidos por la FNMT-RCM (ej.: solicitudes de expedición, renovación…).

v) Comunicar a la FNMT-RCM de forma diligente las solicitudes de expedición de *Certificados*.

vi) 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*.

vii) 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.*

viii) 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.

38. En todo caso la FNMT-RCM podrá repetir contra la Oficina de Registro que hubiera realizado el procedimiento de identificación, iniciando las acciones correspondientes, si la causa del daño tuviera su origen en la actuación dolosa o culposa de ésta.

11.4.3. Obligaciones y responsabilidad del Prestador de Servicios de Confianza

Las obligaciones y responsabilidades de la FNMT-RCM, como *Prestador de Servicios de Confianza*, con el *Titular* del *Certificado de Persona Física* y el resto de miembros de la *Comunidad Electrónica*, quedarán determinadas principalmente, por el documento relativo a las condiciones de utilización o el contrato de expedición del *Certificado*, y, subsidiariamente, por las presentes *Políticas y Prácticas de Certificación Particulares* y por la *Declaración General de Prácticas de Certificación*.

11.4.3.1. Con carácter previo a la emisión del Certificado

39. a) Comprobar la identidad y circunstancias personales de los *Titulares* de *Certificados* con arreglo a lo dispuesto en las presentes *Políticas y Prácticas de Certificación Particulares* (a este respecto puede consultarse el correspondiente procedimiento de registro establecido en este documento). No se emitirán *Certificados* para menores de edad salvo que ostenten y acrediten su cualidad de emancipados.

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

c) Comprobar que el interesado en solicitar la emisión de un *Certificado* está en posesión de la *Clave Privada* que constituirá, una vez emitido 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.

11.4.3.2. Identificación del Titular

40. a) Identificar a la persona física que solicite un *Certificado* exigiendo, con carácter general, su personación y estar en posesión de número de Documento Nacional de Identidad o Número de Identificación de Extranjeros. Para la identificación se procederá con arreglo al procedimiento de registro.

b) En los procesos de comprobación de los extremos antes señalados anteriormente la FNMT-RCM podrá realizar estas comprobaciones mediante la intervención de *Oficinas de Registro* autorizadas o de terceros que ostenten facultades fedatarias.

11.4.3.3. Generación de Datos de creación de Firma e información adicional

41. a) 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.

b) Poner a disposición del *Solicitante* (http://www.ceres.fnmt.es) la siguiente información:

i. Instrucciones para el *Titular*, en especial:
   - La forma en que han de custodiarse los *Datos de creación de Firma*.
   - Los mecanismos generales que garanticen la fiabilidad de la *Firma electrónica* de un documento.

- El procedimiento para comunicar la pérdida o utilización indebida de dichos *Datos*.
- Información relacionada con los *Dispositivos de creación y verificación de Firma electrónica* compatibles con los *Datos de creación y verificación de Firma* generados, y con el *Certificado* expedido.
- Las condiciones precisas de utilización del *Certificado*, sus límites de uso y la forma en que garantiza su responsabilidad patrimonial.

ii. Una descripción del método utilizado por la FNMT-RCM para comprobar la identidad del *Titular* y aquellos otros datos que figuren en el Certificado.

iii. Las certificaciones que haya obtenido la FNMT-RCM.

iv. El procedimiento aplicable para la resolución de conflictos.

v. Un ejemplar de las presentes Políticas y Prácticas de Certificación Particulares de los *Certificados de Persona Física*, disponible a través de la Sede Electrónica de la FNMT-RCM.

11.4.3.4. Conservación de la información por la FNMT-RCM

42. a) 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, de manera que puedan verificarse las firmas efectuadas con el mismo.

b) Mantener un *repositorio* 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 o suspendidos. 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, de la UE.

c) Mantener un servicio de consulta sobre la vigencia de los *Certificados*. Este servicio se describe en el apartado "Comprobación del estado del *Certificado de Persona Física*" del presente documento.

d) 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 o suspendió su vigencia.

e) Conservar las *DPCs* durante 15 años desde su modificación o derogación por publicación de una nueva *DPC*, en las debidas condiciones de seguridad.

11.4.3.5. Protección de los Datos de Carácter Personal

43. La FNMT-RCM se compromete a conocer y cumplir la legislación vigente en materia de *Protección de Datos Personales*, fundamentalmente la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. A tal efecto y con carácter enunciativo, se compromete a cumplir con las obligaciones que tal normativa establece en materia de información a los afectados, declaración de ficheros ante la Agencia Española de Protección de Datos, conservación y acceso a la información, así como con las medidas de seguridad y demás obligaciones establecidas en el Real Decreto 1720/2007. Asimismo, garantiza que la utilización de los datos personales recabados se limitará a aquellas finalidades para las cuales estos fueron recogidos.

44. 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 el apartado "Datos de Carácter Personal" de la *Declaración General de Prácticas de Certificación.*

11.4.3.6. Cese de la actividad de la FNMT-RCM como Prestador de Servicios de Certificación

45. A este respecto se puede consultar el apartado "Cese de la actividad del *Prestador de Servicios de Certificación*." de la *Declaración General de Prácticas de Certificación*.

11.4.3.7. Responsabilidad del Prestador de Servicios de Certificación

46. La FNMT-RCM únicamente responde de la correcta identificación personal del *Solicitante* y futuro *Titular*, y de incorporar esos datos a un *Certificado*. Para la aplicación de garantías, obligaciones y responsabilidades, es necesario que el hecho se haya producido en el ámbito de la *Comunidad Electrónica* según se define dicho concepto en esta *Declaración General de Prácticas de Certificación*.

47. 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 de Certificación* o en la Ley. En ningún otro caso será responsable de las acciones o de las pérdidas en las que incurran los *Titulares*, *Suscriptores*, *Entidades usuarias*, o 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*.

48. FNMT-RCM no responderá en caso de 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-RCM podrá establecer cláusulas de limitación de responsabilidad. En todo caso, la cuantía que en concepto de daños y perjuicios debiera satisfacer por imperativo judicial la FNMT-RCM a terceros perjudicados, y/o miembros de la *Comunidad electrónica* en defecto de regulación específica en los contratos o convenios, se limitan a un máximo de SEIS MIL EUROS (6.000€) euros.

49. 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 General de Prácticas de Certificación*, en la presente *Política y Prácticas de certificación particulares* y, en especial, lo dispuesto en los apartados referidos a las obligaciones y a la responsabilidad de las partes.

50. La FNMT-RCM no responderá por ningún software que no haya proporcionado directamente. No obstante, la FNMT-RCM pondrá las medidas de protección adecuadas para la protección de sus sistemas frente a *Software malicioso (Malware)* y las mantendrá diligentemente actualizadas para colaborar con los usuarios en evitar los daños que este tipo de software puede causar.

51. 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 al estado actual de la técnica, y procedió conforme a lo dispuesto en esta *Declaración de Prácticas de Certificación* y en la Ley.

11.4.4. Obligaciones y responsabilidad del Solicitante y del Titular

11.4.4.1. Responsabilidad del Solicitante

52. El *Solicitante* responderá de que la información presentada durante la solicitud del *Certificado* es verdadera.

53. El *Solicitante* mantendrá a salvo y defenderá a su costa a la FNMT-RCM contra cualquier acción que pudiese emprenderse contra esta Entidad como consecuencia de la falsedad de la información suministrada en el mencionado procedimiento de expedición del *Certificado*, o contra cualquier daño y perjuicio que sufra la FNMT-RCM como consecuencia de un acto u omisión del *Solicitante*.

11.4.4.2. Responsabilidad del Titular

54. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la *Declaración General de Prácticas de Certificación*, el *Titular* del *Certificado de Persona Física*, como firmante y custodio del *Certificado* y sus *Claves*, tiene la obligación de:

- Custodiar adecuadamente el *Certificado*, los *Datos de Creación de Firma* y, en su caso, la tarjeta o soporte del *Certificado*, poniendo los medios necesarios para impedir su utilización por personas distintas a su *Titular* o a su legítimo poseedor.
- No utilizar el *Certificado* cuando alguno de los datos incluidos en el *Certificado* sea inexacto o incorrecto, o existan razones de seguridad que así lo aconsejen.
- Comunicar a la FNMT-RCM la pérdida, extravío o sospecha de ello, del *Certificado*, de los *Datos de Creación de Firma*, de la tarjeta o soporte del *Certificado* del que es *Titular* y custodio, con el fin de iniciar, en su caso, los trámites de su revocación o suspensión.

55. Será responsabilidad del *Titular* 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.

56. Asimismo, será el *Titular* quien deba responder ante los miembros de la *Comunidad electrónica* y demás *Entidades usuarias* o, en su caso, ante terceros del uso indebido del *Certificado*, o de la falsedad de las manifestaciones en él recogidas, o actos u omisiones que provoquen daños y perjuicios a la FNMT-RCM o a terceros.

57. Será responsabilidad y, por tanto, obligación del *Titular* 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 originó la emisión del certificado en cuestión y no se hubiera

producido la subrogación prevista en la ley. En todo caso, el *Titular* no usará 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, el *Titular* hubiera tenido noticia de estas circunstancias.

11.4.5. Obligaciones y responsabilidad de la Entidad usuaria y terceros que confían en los Certificados

58. El resto de la *Comunidad Electrónica, Entidades usuarias* y los terceros regularán sus relaciones con la FNMT-RCM a través de la *Declaración General de Prácticas de Certificación*, y, en su caso, a través de estas *Políticas y Prácticas de Certificación Particulares*; todo ello sin perjuicio de lo dispuesto en la normativa sobre firma electrónica y demás normativa que resulte de aplicación.

59. Sin perjuicio de lo contenido en el párrafo anterior los miembros de la *Comunidad Electrónica, Entidades usuarias* y los terceros que confían en los *Certificados* y en las *Firmas electrónicas* generadas con los mismos, deberán cumplir las siguientes obligaciones, exonerando de cualquier responsabilidad al *Prestador de Servicios de Confianza* en caso de que alguna no sea cumplida:

- Verificar con carácter previo a confiar en los *Certificados*, la *Firma electrónica* reconocida del *Prestador de Servicios de Confianza* que expidió el *Certificado*.
- Verificar que el *Certificado* del *Titular* recibido continúa vigente.
- Verificar el estado de los *Certificados* en la cadena de certificación, mediante consulta a las *Listas de Revocación* de *Certificados* o a través del servicio *OCSP* de la FNMT-RCM.
- Comprobar las limitaciones de uso contenidas en el *Certificado* que se verifica.
- Conocer las condiciones de utilización del *Certificado* conforme a las presentes *Políticas y Prácticas de Certificación Particulares.*
- Notificar a la FNMT-RCM o a cualquier *Oficina de Registro*, 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.

60. Será responsabilidad de la *Entidad usuaria* y de los terceros que confíen en *Certificados* expedidos por la FNMT-RCM, salvo contratación de esta obligación con esta Entidad, la verificación de las *Firmas electrónicas* de los documentos, así como de los *Certificados*, no cabiendo en ningún caso presumir la autenticidad de los documentos o *Certificados* sin dicha verificación.

61. No podrá considerarse que la *Entidad usuaria* ha actuado con la mínima diligencia debida si confía en una firma electrónica basada en un *Certificado* emitido por la FNMT-RCM sin haber observado lo dispuesto en la *Declaración General de Prácticas de Certificación* y en el presente documento y comprobado que dicha firma electrónica puede ser verificada por referencia a una *Cadena de certificación* válida.

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

63. Asimismo, será responsabilidad de la *Entidad usuaria* observar lo dispuesto en la *Declaración General de Prácticas de Certificación* y sus posibles modificaciones futuras, con especial atención a los límites de uso establecidos para los *Certificados* en las presentes *Políticas de Certificación*.

11.5. LÍMITES DE USO DE LOS CERTIFICADOS DE PERSONA FÍSICA

64. Para poder usar los *Certificados* de forma diligente a la hora de confiar en documentos firmados electrónicamente con base en los mismos, se deberá previamente formar parte de la *Comunidad Electrónica*, adquirir la condición de *Entidad usuaria* o ser una tercera parte que confía en los *Certificados*, con la finalidad que puedan ser prestados por la FNMT-RCM los servicios de comprobación de vigencia de los diferentes *Certificados*.

65. En cualquier caso, fuera de la *Comunidad Electrónica*, si una *Entidad usuaria* o un tercero desean confiar en la firma electrónica realizada con uno de estos *Certificados*, sin acceder a los servicios de comprobación de la vigencia de los *Certificados* expedidos bajo esta *Política de Certificación*, no se obtendrá cobertura de las presentes *Políticas y Prácticas de Certificación Particulares*, y se carecerá de legitimidad alguna para reclamar o emprender acciones legales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado*.

66. 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. PRÁCTICAS DE CERTIFICACIÓN PARTICULARES PARA LOS CERTIFICADOS DE PERSONA FÍSICA

67. El presente documento 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 Persona Física*, expedidos bajo la presente *Política de Certificación* identificada con el OID 1.3.6.1.4.1.5734.3.10.1.

12.1. SERVICIOS DE GESTIÓN DE LAS CLAVES

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

12.2. GESTIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS

69. 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 Persona Física*.

12.2.1. Procedimiento de solicitud del Certificado de Persona Física

70. 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 de Persona Física*. El Solicitante deberá introducir su número de DNI o NIE, su primer apellido y su dirección de correo electrónico en el punto de recogida de datos dispuesto para ello. Así mismo, el *Solicitante* manifestará su voluntad de obtener un *Certificado de Persona Física* y dará su consentimiento para que la FNMT-RCM pueda realizar una consulta al Sistema de Verificación de Datos de Identidad.

71. 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.

72. 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.

73. 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.

74. 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.

75. 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 peticionario. No obstante lo anterior, se tendrá en cuenta la posibilidad de identificación electrónica del peticionario del *Certificado de Persona Física*, generándose,

en su caso, dicho Certificado sin que sea necesario que el Solicitante se persone físicamente ante una Oficina de Registro para acreditar su identidad.

76. El procedimiento de solicitud del *Certificado de Persona Física* 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. Confirmación de la identidad personal

77. La FNMT-RCM, como *Prestador de Servicios de Confianza*, antes de expedir un *Certificado de Persona Física* 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.

12.2.2.1. Comprobación de la identidad mediante comparecencia física

78. Los *Solicitantes* de *Certificados de Persona Física* deberán comparecer físicamente para formalizar el procedimiento de confirmación de identidad personal, presentándose en la *Oficina de Registro* autorizada, en posesión de su DNI, válido y vigente, o de otros medios admitidos en derecho a efectos de identificación (en los que conste su número de DNI). Cuando el *Solicitante* sea extranjero y no posea el DNI, deberá estar en posesión del Documento Nacional de Identificación de Extranjeros o el Certificado de Ciudadano de la Unión donde conste el NIE junto con Pasaporte o documento de identidad de país de origen. El encargado de acreditación de la *Oficina de Registro* verificará que los documentos aportados cumplen todos los requisitos para confirmar la identidad del *Solicitante*.

79. La personación del *Solicitante* no será indispensable si la 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 conforme el siguiente apartado, o si se solicita una renovación del *Certificado*, de conformidad con lo dispuesto en el apartado "*Renovación del Certificado de Persona Física*" del presente documento.

80. 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.

12.2.2.2. Uso de certificados electrónicos como medio de identificación

81. La FNMT-RCM expedirá el *Certificado de Persona Física* 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 perteneciente a alguno de los siguientes tipos:

- Un *Certificado de Persona Física* expedido bajo la presente *Política*.
- Un *Certificado de Identidad de Persona Física*, expedido bajo la *Política de Certificación de Certificados Reconocidos de la FNMT-RCM* identificada con el OID 1.3.6.1.4.1.5734.3.5.
- Un *Certificado* electrónico de los incorporados al DNIe.

82. No obstante, solo se permitirá la solicitud telemática del *Certificado de Persona Física* 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 *Titular* que establece el artículo 13.4 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

12.2.3. Expedición del Certificado de Persona Física

83. 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 de Persona Física*.

84. La expedición de *Certificados de Persona Física* supone la generación de documentos electrónicos que confirman la identidad del *Titular* así como su correspondencia con la *Clave Pública* asociada. La expedición de *Certificados de Persona Física* de la FNMT-RCM sólo 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.

85. La FNMT-RCM, por medio de su *Firma electrónica*, autentica los *Certificados de Persona Física* y confirma la identidad del *Titular*. 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*.

86. 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*.

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

- Comprobar que el *Solicitante* del *Certificado de Persona Física* utiliza la *Clave Privada* correspondiente a la *Clave Publica* vinculada a la identidad del *Titular* 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 de Persona Física* se base en la información proporcionada por el *Solicitante*.
- No ignorar hechos notorios que puedan afectar a la fiabilidad del *Certificado de Persona Física.*
- Lograr que el *DN* (nombre distintivo) asignado en el *Certificado* sea único en toda la *Infraestructura de Clave Pública* de la FNMT-RCM.

88. 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 de Persona Física*, a partir de los datos personales del *Solicitante* recogidos durante el proceso de solicitud del *Certificado de Persona Física*, conforme a la siguiente estructura:

Apellidos y Nombre del titular del certificado de Persona Física En MAYÚSCULAS, separados únicamente por un espacio en blanco, de acuerdo con lo indicado en el DNI/NIE del *Titular*. En caso de no existir el segundo apellido el espacio correspondiente al mismo se dejará en blanco (sin ningún carácter).
Espacio en blanco
Guion, u otro símbolo o carácter Separa los apellidos y el nombre del número de identificación fiscal.
Espacio en blanco
Número de identificación fiscal Número de identificación fiscal del *Titular*, NIF, de acuerdo con lo indicado en su DNI o NIE.

Ejemplo:

ESPAÑOL ESPAÑOL JUAN – 00000000T

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

2. Composición de la identidad alternativa del *Certificado de Persona Física*.

La identidad alternativa del *Certificado de Persona Física* contiene la misma información que el *CN*, a la que se añadirá, a voluntad del *Solicitante*, su dirección de correo electrónico, distribuida en una serie de atributos, de forma que sea más sencilla la obtención de los datos personales del *Titular* del *Certificado de Persona Física*. Se utiliza la extensión subjectAltName definida en *X.509* versión 3 para ofrecer esta información.

Dentro de dicha extensión, se utilizará el subcampo directoryName para incluir un conjunto de atributos definidos por la FNMT-RCM, que incorporan información sobre el *Titular* del *Certificado de Persona Física* en cuestión.

3. Generación del *Certificado* conforme al Perfil del *Certificado de Persona Física*.

   El formato del *Certificado de Persona Física*, expedido por la FNMT-RCM bajo la presente *Política 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 Reconocidos*, puede consultarse en los anexos al presente documento.

   En ellos se describen los perfiles de los *Certificados de Persona Física* 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 para su descarga de su *Certificado de Persona Física*.

12.2.4. Descarga e instalación del Certificado de Persona Física

89. En menos de una (1) hora desde que tiene lugar la confirmación de la identidad personal del solicitante, la FNMT-RCM pone el *Certificado de Persona Física* a disposición de este para su descarga en la página web desde la que hizo la solicitud, http://www.cert.fnmt.es.

90. En este proceso guiado se le pedirá al *Solicitante* que introduzca el número de DNI o NIE con el que se realizó el proceso de solicitud, el 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 *Titular* de una firma electrónica de las condiciones de uso del *Certificado*, como requisito imprescindible para acceder a la descarga del mismo, remitiendo dicha firma a la FNMT – RCM. Si el *Certificado de Persona Física* aún no hubiera sido generado por cualquier motivo, el proceso le informará de este hecho.

91. En el momento de la descarga del *Certificado de Persona Física*, este 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.

12.2.5. Vigencia del Certificado de Persona Física

12.2.5.1. Caducidad

92. Los *Certificados de Persona Física* expedidos por la FNMT-RCM tendrán validez durante un período de cuatro (4) 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 el *Titular* desee seguir utilizando los servicios del *Prestador de Servicios de Confianza.*

12.2.5.2. Extinción de la vigencia del Certificado

93. Los *Certificados de Persona Física* 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.

94. A los efectos enumerados anteriormente, la expedición de un *Certificado de Persona Física* cuando exista otro vigente a favor del mismo *Titular* (tanto si este es un *Certificado* expedido bajo la presente política como si es un *Certificado* FNMT Clase 2CA, expedido bajo la política con OID 1.3.6.1.4.1.5734.3.5), conllevará la revocación inmediata del *Certificado* anterior.

12.2.6. Revocación del Certificado de Persona Física

12.2.6.1. Causas de revocación

95. Serán causas admitidas para la revocación de un *Certificado de Persona Física* las expuestas a continuación:

a) La solicitud de revocación por parte del *Titular*. 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 personal del *Titular*.
- 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 o incapacidad sobrevenida, total o parcial, del *Titular*.

d) 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*, de manera que este ya no fuera conforme a la realidad.

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

f) Violación o puesta en peligro del secreto de los *Datos de Creación de Firma*.

g) 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*.

h) Resolución del contrato suscrito entre el *Titular* y la FNMT-RCM.

96. En ningún caso la FNMT-RCM asume obligación alguna de comprobar los extremos mencionados en las letras c) a f) del presente apartado, debiendo ser notificadas a esta entidad de forma fehaciente mediante entrega de los documentos e informaciones necesarias para verificarlo.

97. 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 *Titular* 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 f) del presente apartado le sean acreditadas fehacientemente, previa identificación del *Titular* y/o *Solicitante* de la revocación (o persona con facultades de representación suficientes, si se produjera incapacidad sobrevenida del *Titular*).

98. 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.

12.2.6.2. Efectos de la revocación

99. La revocación o suspensión del *Certificado de Persona Física*, esto es, la extinción de su vigencia, surtirá efecto la fecha en que la FNMT-RCM tenga conocimiento cierto de cualquiera de los hechos determinantes y desde el momento de hacerlo constar en su *Servicio de información y consulta sobre el estado de los certificados*.

100. La revocación del *Certificado de Persona Física* implica, además de su extinción, la finalización de la relación y régimen de uso de dicho *Certificado* con la FNMT-RCM.

12.2.6.3. Procedimiento para la revocación

101. La solicitud de revocación de los *Certificados de Persona Física* podrá efectuarse durante el período de validez que consta en el *Certificado*.

102. La revocación de un *Certificado de Persona Física* solamente podrá ser solicitada por el *Titular* o persona con facultades de representación suficientes, si se produjera incapacidad

sobrevenida del *Titular*, en los términos recogidos en las presentes *Políticas de Certificación y Prácticas de Certificación Particulares*.

103. No obstante, la FNMT-RCM podrá revocar de oficio los *Certificados de Persona Física* en los supuestos recogidos en la presente *Declaración de Prácticas de Certificación*.

104. El *Titular* puede solicitar la revocación de su *Certificado de Persona Física* conforme a alguno de los siguientes procedimientos:

A) Si el *Titular* está en posesión del *Certificado de Persona Física* 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 el *Titular* no está en posesión del *Certificado de Persona Física* 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, 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.

105. En todos los supuestos anteriores de estas *Prácticas de Certificación* particulares donde sea necesaria la identificación y sea posible la identificación telemática, se tendrá en cuenta por la FNMT-RCM las funcionalidades previstas para el DNIe, de acuerdo con la legislación específica.

106. 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.

12.2.7. Suspensión del Certificado de Persona Física

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

108. 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.

12.2.7.1. Causas de la suspensión del Certificado

109. La FNMT – RCM podrá suspender la vigencia de los *Certificados de Persona Física* 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.

110. 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.

12.2.7.2. Efectos de la suspensión

111. La suspensión de *Certificados* deja sin efecto el *Certificado* (extingue su vigencia) durante un período de tiempo y en unas condiciones determinadas.

12.2.7.3. Procedimiento para la suspensión de Certificados

112. La solicitud de la suspensión de los *Certificados de Persona Física* 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.

113. 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* de la FNMT-RCM, salvo que se hubiera levantado la suspensión mediante solicitud de cancelación de la suspensión por parte del *Titular* o un tercero autorizado. 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.

114. 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.

12.2.8. Renovación del Certificado de Persona Física

115. Solo se permitirá una única renovación del *Certificado de Persona Física*. El *Titular* que ya hubiera realizado una renovación de su *Certificado* y quisiera seguir utilizando un *Certificado de Persona Física* bajo las presentes *Políticas de Certificación y Prácticas de Certificación Particulares*, deberá solicitar un nuevo *Certificado* y confirmar su identidad conforme al procedimiento descrito en el apartado "Comprobación de la identidad mediante comparecencia física" de este documento.

116. Podrán solicitar la renovación de los *Certificados de Persona Física* expedidos por la FNMT-RCM los *Titulares* de los mismos, siempre que en el momento de la solicitud

tengan un *Certificado* en vigor y sus *Datos de creación de Firma* asociados y dicha solicitud se efectúe durante los sesenta (60) días anteriores a su c*aducidad*.

117. La renovación de un *Certificado de Persona Física* consistirá en la generación de nuevos *Datos de verificación de Firma* y de *creación de Firma*, así como en la expedición de un nuevo *Certificado de Persona Física*. La solicitud de renovación se hará a través de la dirección http://www.ceres.fnmt.es.

118. El antiguo *Certificado* que está próximo a caducar seguirá siendo válido hasta que expire el período de vigencia del mismo. En caso de solicitarse la revocación del *Certificado de Persona Física* durante el período de tiempo en el que el *Titular* posee dos *Certificados* activos, la FNMT-RCM procederá a revocar ambos *Certificados*.

119. El procedimiento establecido para la renovación de un *Certificado de Persona Física* no requiere la personación del peticionario, ya que se le identificará telemáticamente mediante la utilización de sus *Datos de creación de Firma*. Tanto el proceso de la solicitud como la obtención del *Certificado* se realizarán de forma telemática, requiriéndose en todo caso la generación por parte del peticionario de una *Firma electrónica avanzada*, realizada con un *Certificado electrónico* reconocido, del documento de solicitud de renovación. No obstante, solo se permitirá la renovación telemática del *Certificado de Persona Física* cuando no se haya superado el plazo máximo de 5 años desde la personación e identificación física del *Titular* que establece el artículo 13.4 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

120. Las funcionalidades del DNIe se tendrán en cuenta a los efectos de identificación de acuerdo con su legislación específica.

121. La utilización de los *Certificados de Persona Física* renovados se sujeta a las mismas condiciones generales y particulares vigentes en cada momento y establecidas para este tipo de *Certificados* en su correspondiente *Declaración de Practicas de Certificación*.

12.3. COMPROBACIÓN DEL ESTADO DEL CERTIFICADO DE PERSONA FÍSICA

122. El *Titular* del *Certificado* y las Administraciones, organismos y entidades usuarias pertenecientes a la *Comunidad Electrónica* podrán realizar la comprobación del estado de un *Certificado* en la forma y condiciones que se expresan en este apartado.

123. El estado del *Certificado de Persona Física* podrá ser comprobado, bien a través del acceso a las *Listas de Revocación*, bien a través del *Servicio de información y consulta del estado de los Certificados* a través del protocolo OCSP, por aquellas Administraciones, organismos y entidades usuarias pertenecientes a la *Comunidad Electrónica* que cuenten con un acuerdo con la FNMT-RCM para tal fin.

124. El *Titular* del *Certificado* podrá comprobar el estado de revocación de su propio *Certificado* a través de la página web de la FNMT-RCM https://www.sede.fnmt.gob.es/certificados/persona-fisica/verificar-estado siempre que cuente con los *Datos de creación de firma* asociados a dicho *Certificado* electrónico.

125. Estos servicios estarán 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

126. La FNMT-RCM ofrece el *Servicio de información y consulta del estado de los certificados* bajo los términos suscritos en el correspondiente convenio, contrato o *Ley de Emisión*. Dicho servicio funciona de la siguiente manera: el servidor OCSP recibe la petición OCSP efectuada por un Cliente OCSP registrado en el sistema 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.

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

ANEXO I: IDENTIFICACIÓN DEL CERTIFICADO DE LA AUTORIDAD DE CERTIFICACIÓN AC FNMT USUARIOS

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

Certificado de la Autoridad de Certificación "AC FNMT Usuarios"

- Nombre distintivo: CN = AC FNMT Usuarios, OU = Ceres, O = FNMT-RCM, C = ES
- Número de serie: 45 5f 3a e1 5c 21 cd ba 54 4f 82 aa 47 51 eb db
- Período de validez desde: martes, 28 de octubre de 2014 12:48:58
- Período de validez hasta: domingo, 28 de octubre de 2029 12:48:58
- Huella digital (sha1): 80 8B 72 E43B 57 4C F5 87 7C B8 41 A8 DF 88 39 6D 38 AB 94
- Huella digital (sha256): 60 12 93 CA 20 B0 9A 03 29 5D 19 62 56 C6 95 3F F9 EB A8 11 DB 8E 3C E1 40 41 3C 1B FF E9 A8 69

ANEXO II: PERFILES DE CERTIFICADOS DE AUTORIDADES DE CERTIFICACIÓN

CERTIFICADO RAÍZ DE LA FNMT-RCM

CERTIFICADO RAÍZ DE LA FNMT-RCM			
CAMPO	**CONTENIDO**	**CRÍTICA**	**OBSERVACIONES**
Campos de X509v1			
1. Versión	V3		
2. Serial Number	Número identificativo único del certificado.		*[RFC3280]: the serial number MUST be a positive integer, not longer than 20 octets (1 < SN < 2^{159}). Processing components MUST be able to interpret such long numbers.*
3. Signature Algorithm	Sha1withRsaEncryption Sha256withRsaEncryption Sha512withRsaEncryption		OID: 1.2.840.113549.1.1.5 OID: 1.2.840.113549.1.1.11 OID: 1.2.840.113549.1.1.13 Norma PKCS#1 v2.1 y RFC 3447.
4. Issuer Distinguished Name	OU=AC RAIZ FNMT -RCM O=FNMT-RCM C=ES		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements"*, en *PrintableString*.
5. Validez	Hasta 01/01/2030		El programa de inclusión de certificados raíz de Microsoft requiere que la fecha de validez sea posterior al 1/1/2010. *[RFC3280]: Validity dates before and through 2049 MUST be encoded by CAs as UTCTime, dates in 2050 and later as GeneralizedTime. Date values MUST be given in the format YYMMDDhhmmssZ resp. YYYYMMDDhhmmssZ, i.e. always including seconds and expressed as Zulu time (Universal Coordinated Time).*
6. Subject	OU=AC RAIZ FNMT -RCM O=FNMT-RCM C=ES		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements"*, en *PrintableString*. Coincidirá con el campo emisor del certificado de las AC subordinada. *[RFC3280]: The issuer name MUST be a non-empty DName. Processing components MUST be prepared to receive the following attributes: countryName,* *organizationName, organizationalUnitName, distinguishedNameQualifier, stateOrProvinceName, commonName, serialNumber, and domainComponent. Processing components SHOULD be prepared for attributes: localityName, title, surname, givenName, initials, pseudonym, and generationQualifier* *[ETSI-QC]: the issuer name MUST contain the countryName attribute. The specified country MUST be the country where the issuer CA is established.* *[ETSI-CPN]: the issuer name MUST contain the countryName and the organizationName attributes.*

CERTIFICADO RAÍZ DE LA FNMT-RCM			
CAMPO	**CONTENIDO**	**CRÍTICA**	**OBSERVACIONES**
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: 4096 bits		
Campos de X509v2			
1. issuerUniqueIdentifier	No se utilizará		
2. subjectUniqueIdentifier	No se utilizará		
Extensiones de X509v3			
1. Subject Key Identifier	Función hash SHA-1 sobre la clave pública del sujeto (AC raíz).	NO (RFC 3280)	RFC 3280: 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).
2. Authority Key Identifier	No procede		
3. KeyUsage		SI (RFCs 3280 y 3739)	
Digital Signature	0		
Non Repudiation	0		
Key Encipherment	0		
Data Encipherment	0		
Key Agreement	0		
Key Certificate Signature	1		
CRL Signature	1		
4.extKeyUsage	No se utilizará		
5. privateKeyUsagePeriod	No se utilizará		

CERTIFICADO RAÍZ DE LA FNMT-RCM			
CAMPO	**CONTENIDO**	**CRÍTICA**	**OBSERVACIONES**
6. Certificate Policies		NO	[RFC 3739] obliga la existencia de al menos un valor. La Ley de Firma Electrónica dice para los certificados reconocidos: "*La identificación del prestador de servicios de certificación que expide el certificado y su domicilio*". Se incluirá en la DPC. *[RFC3280]: 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 }.* *To promote interoperability, this profile RECOMMENDS that policy information terms consist of only an OID. Where an OID alone is insufficient, this profile strongly recommends that use of qualifiers*
Policy Identifier	anyPolicy 2 5 29 32 0		
URL CPS	http://www.cert.fnmt.es/dpcs/		
Notice Reference	NO para los certificados de AC, según RFC 5280 (sustituta de RFC 3280).		
7. Policy Mappings	No se utilizará		
8. Subject Alternate Names	No se utilizará	NO	
9. Issuer Alternate Names	No se utilizará		
10. Subject Directory Attributes	No se utilizará		
11. Basic Constraints		SI (RFC 3280)	RFC 3280. Puede especificarse el número máximo de niveles en "Path Length Constraint". Para la AC Raíz no se establecerá ningún límite de niveles de AC subordinadas. [*RFC3280] This extension MUST appear as a critical extension in all CA certificates that contain public keys used to validate digital signatures on certificates.*
Subject Type	CA		
Path Length Constraint	Ninguno		
12. Policy Constraints	No utilizado		
13. CRLDistributionPoints	No utilizado		La revocación del certificado Raíz se publicitará por otros mecanismos.
14. Auth. Information Access	No procede	NO (RFC 3280)	
15.netscapeCertType	No procede		

CERTIFICADO RAÍZ DE LA FNMT-RCM			
CAMPO	**CONTENIDO**	**CRÍTICA**	**OBSERVACIONES**
16. netscapeRevocationURL	No procede		
17. netscapeCAPolicyURL	No procede		
18. netscapeComment	No procede		

Tabla 1 - Certificado raíz de la FNMT-RCM

CERTIFICADO AUTORIDAD DE CERTIFICACIÓN "AC FNMT USUARIOS"

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		Object Identifier 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 certificación (emisor del certificado). o=FNMT-RCM	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organizational Unit	Denominación de la Unidad Organizativa ou = AC RAIZ FNMT-RCM	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
5. Validity		15 años	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 certificación (emisor del certificado). o=FNMT-RCM	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	6.3. Organizational Unit	Denominación de la Unidad Organizativa	Sí		UTF8 String, tamaño máximo 128 (rfc5280)

Campo		Contenido	Oblig	Crit	Especificaciones
		ou= Ceres			
	6.4. Common Name	cn= AC FNMT Usuarios	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 para la Administración Pública, 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
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
	10.1. Digital Signature	0	Sí		Permite realizar la operación de firma electrónica.
	10.2. Content Commitment	0	Sí		Se refiere a la cualidad de un tipo de certificado que indica al software en el que se usa que debe permitir que el usuario conozca lo que firma.
	10.3. Key Encipherment	0	Sí		Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras
	10.4. Data Encipherment	0	Sí		Se utiliza para cifrar datos que no sean claves criptográficas.
	10.5. Key Agreement	0	Sí		Para uso en el proceso de acuerdo de claves
	10.6. Key Certificate Signature	1	Sí		Se permite usa para firmar certificados. Este uso se utiliza en los certificados de autoridades de certificación.
	10.7. CRL Signature	1	Sí		Se permite para firmar listas de revocación de certificados. Este uso se utiliza en los certificados de autoridades de certificación.

Campo			Contenido	Oblig	Crit	Especificaciones
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.
		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		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		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
13. Basic Constraints				Sí	Sí	
	13.1. 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."
	13.2. pathLenConstraint		0	Sí		Un pathLenConstraint de cero indica que ningún no pueden existir más certificados de CA intermedios en la ruta de certificación.
14. Authority Info Access				Sí	No	

Campo		Contenido	Oblig	Crit	Especificaciones
	14.1. 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)
	14.2. Acces Location 1	http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder	Sí		URL del servicio de OCSP
	14.3. 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-caIssuers 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."
	14.4. 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.

Tabla 2 - Certificado Autoridad de Certificación "AC FNMT Usuarios"

ANEXO III: PERFIL DEL CERTIFICADO DE PERSONA FÍSICA

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		Object Identifier 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 certificación (emisor del certificado). o=FNMT-RCM	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organizational Unit	Denominación de la Unidad Organizativa ou= Ceres	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.4. Common Name	cn= AC FNMT Usuarios	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
5. Validity		4 años	Sí		
6. Subject		Identificación/descripción del custodio/responsable de las claves certificadas	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. SerialNumber	NIF del titular	Sí		PrintableString (rfc5280) Ejemplo: SN=00000000T
	6.3. Given Name	Nombre de pila, de acuerdo con documento de identidad	Sí		UTF8String (rfc5280). Por ejemplo: gn=Juan
	6.4. Surname	Apellidos de acuerdo con documento de identificación	Sí		UTF8String (rfc5280). Por ejemplo: sn=Español Español
	6.5. Common Name	Apellidos, Nombre y NIF del titular	Sí		UTF8String (rfc5280). Por ejemplo: cn= Español Español Juan – 00000000T
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 titular, 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
9. Subject Key Identifier		Identificador de la clave pública del titular o poseedor de claves. 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		De la rfc 5280: "The digitalSignature bit is asserted when the subject public key is used for verifying digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), such as those used in an

Campo			Contenido	Oblig	Crit	Especificaciones
						entity authentication service, a data origin authentication service, and/or an integrity service."
	10.2. Content Commitment		1	Sí		De la rfc 5280: "The contentCommitment bit is asserted when the subject public key is used to verify digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), used to provide a non-repudiation service that protects against the signing entity falsely denying some action. In the case of later conflict, areliable third party may determine the authenticity of the signed data."
	10.3. Key Encipherment		1	Sí		Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras
	10.4. Data Encipherment		0	Sí		Se utiliza para cifrar datos que no sean claves criptográficas.
	10.5. Key Agreement		0	Sí		Para uso en el proceso de acuerdo de claves
	10.6. Key Certificate Signature		0	Sí		Se permite usa para firmar certificados. Este uso se utiliza en los certificados de autoridades de certificación.
	10.7. CRL Signature		0	Sí		Se permite para firmar listas de revocación de certificados. Este uso se utiliza en los certificados de autoridades de certificación.
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí		Esta extensión indica que uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, además de o en lugar de los usos básicos que se indican en la extensión KeyUsage.
	11.1. Email Protection		1.3.6.1.5.5.7.3.4	Opcional		Protección de correo electrónico.
	11.2. Client Authentication		1.3.6.1.5.5.7.3.2	Sí		Autenticación de cliente
	11.3. AnyExtendedKeyUsage		2.5.29.37.0	Sí		
12. Qualified Certificate Statements			Extensiones cualificadas.	Sí	No	ETSI TS 101 862 define la inclusión de ciertas declaraciones para certificados cualificados
	12.1. QcCompliance		Certificado es reconocido.	Sí		Indica que el certificado es reconocido.
	12.2. 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. En este caso la Ley obliga: "Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.".
13. Certificate Policies			Política de certificación	Sí		
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.10.1	Sí		Identificador de la política
	13.2. Policy Qualifier Id					
		13.2.1. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		13.2.2. User Notice	Certificado reconocido. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM (C/Jorge Juan 106-28009-Madrid-España)	Sí		UTF8 String. Longitud máxima 200 caracteres.
14. Subject Alternative Names			Identificación/descripción del titular	Sí	No	
	14.1. rfc822 Name		Correo electrónico del titular	Opcional		
	14.2. Directory Name					
		14.2.1. Nombre	Nombre de pila del titular del certificado 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 titular del	Sí		UTF8 String. Por ejemplo:

Campo			Contenido	Oblig	Crit	Especificaciones
			certificado Id Campo/Valor: 1.3.6.1.4.1.5734.1.2 =<Apellido 1			1.3.6.1.4.1.5734.1.2=ESPAÑOL
		14.2.3. Apellido2	Segundo apellido del titular del certificado 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	Identificador de identidad del titular / custodio de las claves. (NIF). Id Campo/Valor: 1.3.6.1.4.1.5734.1.4=<NIF	Sí		UTF8 String, tamaño 9. Por ejemplo: 1.3.6.1.4.1.5734.1.4=99999999R
15. CRL Distribution Point				Sí	No	
	15.1. Distribution Point 1		Punto de distribución 1 de la CRL ldap://ldapusu.cert.fnmt.es/CN=CRL<xxx*>, CN=AC%20FNMT%20Usuarios, OU=CERES, O=FNMT-RCM, C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí		Ruta donde reside la CRL (punto de distribución 1). <xxx*> es un identificador que identificará 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://ocspusu.cert.fnmt.es/ocspusu/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 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."
	16.4. Acces Location 2		http://www.cert.fnmt.es/certs/ACUSU.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 persona física
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."

Tabla 3 - Perfil del Certificado de Persona Física