Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

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

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM / v1.4	04/03/2019
Revisado por:	FNMT-RCM / v1.4	04/03/2019
Aprobado por:	FNMT-RCM / v1.4	05/03/2019

HISTÓRICO DEL DOCUMENTO		
Versión	**Fecha**	**Descripción**
1.0	25/03/2014	Creación del documento
1.1	24/06/2016	Alineación con algunos requisitos del estándar ETSI 101 456
1.2	03/01/2017	Adaptación al estándar ETSI EN 319 412 - 2
1.3	22/12/2017	Revisión anual del documento. No se realizan cambios reseñables.
1.4	05/03/2019	Eliminación de prácticas de suspensión de certificados.

Referencia: DPC/CPUS0104/SGPSC/2019

Documento clasificado como: *Público*

ÍNDICES

ÍNDICE DE CONTENIDOS

Índices **2**

1. Introducción **4**

2. Organización del documento **4**

3. Orden de prelación **5**

4. Definiciones **5**

5. Seudónimos **6**

6. Perfil de los certificados **6**

6.1. Restricciones de los nombres *6*

6.2. Uso de la extensión Policy Constrains *6*

6.3. Sintaxis y semántica de los Policy Qualifiers *6*

6.4. Tratamiento semántico de la extensión "Certificate Policy" *6*

7. Reconocimiento y autenticación de marcas registradas **6**

8. Gestión del ciclo de vida de las claves del Prestador de Servicios de Confianza **7**

8.1. Gestión del ciclo de vida de las Claves *7*

8.1.1. Generación de las Claves del Prestador de Servicios de Confianza 7

8.1.2. Almacenamiento, salvaguarda y recuperación de las Claves del Prestador de Servicios de Confianza 7

8.1.3. Distribución de los Datos de verificación de Firma del Prestador de Servicios de Confianza 7

8.1.4. Almacenamiento, salvaguarda y recuperación de las Claves Privadas de los Firmantes 7

8.1.5. Uso de los Datos de Creación de Firma / Sello del Prestador de Servicios de Confianza 8

8.1.6. Fin del ciclo de vida de las Claves del Prestador de Servicios de Confianza 8

8.1.7. Ciclo de vida del hardware criptográfico utilizado para firmar / sellar Certificados 8

9. Operación y Gestión de la Infraestructura de Clave Pública **8**

10. Difusión de Términos y Condiciones **9**

11. Política de certificación de los Certificados de Persona Física **9**

11.1. Identificación *9*

11.2. Tipología del Certificado de Persona Física *10*

11.3. Comunidad y ámbito de aplicación *10*

11.4. Responsabilidad y obligaciones de las partes *10*

11.4.1. Derechos y obligaciones de las Administraciones 11

11.4.2. Obligaciones y responsabilidad de las Oficinas de Registro 11

11.4.3. Obligaciones y responsabilidad del Prestador de Servicios de Confianza 12
11.4.3.1. Con carácter previo a la emisión del Certificado 12
11.4.3.2. Identificación del Titular 12
11.4.3.3. Generación de Datos de creación de Firma e información adicional 13
11.4.3.4. Conservación de la información por la FNMT-RCM 13
11.4.3.5. Protección de los Datos de Carácter Personal 14
11.4.3.6. Cese de la actividad de la FNMT-RCM como Prestador de Servicios de Confianza 14
11.4.3.7. Responsabilidad del Prestador de Servicios de Confianza 14
11.4.4. Obligaciones y responsabilidad del Solicitante y del Titular 15
11.4.4.1. Responsabilidad del Solicitante 15
11.4.4.2. Responsabilidad del Titular 15
11.4.5. Obligaciones y responsabilidad de la Entidad usuaria y terceros que confían en los Certificados 16

11.5. Límites de uso de los Certificados de Persona Física 17

12. Prácticas de certificación particulares para los Certificados de Persona Física 17

12.1. Servicios de Gestión de las Claves 18

12.2. Gestión del ciclo de vida de los Certificados 18
12.2.1. Procedimiento de solicitud del Certificado de Persona Física 18
12.2.2. Confirmación de la identidad personal 19
12.2.2.1. Comprobación de la identidad mediante comparecencia física 19
12.2.2.2. Uso de certificados electrónicos como medio de identificación 19
12.2.3. Expedición del Certificado de Persona Física 20
12.2.4. Aceptación, descarga e instalación del Certificado de Persona Física 22
12.2.5. Vigencia del Certificado de Persona Física 22
12.2.5.1. Caducidad 22
12.2.5.2. Extinción de la vigencia del Certificado 22
12.2.6. Revocación del Certificado de Persona Física 23
12.2.6.1. Causas de revocación 23
12.2.6.2. Efectos de la revocación 24
12.2.6.3. Procedimiento para la revocación 24
12.2.7. Suspensión del Certificado de Persona Física 25
12.2.8. Renovación del Certificado de Persona Física 26

12.3. Comprobación del estado del Certificado de Persona Física 26

Anexo I: Identificación del certificado de la Autoridad de Certificación AC FNMT Usuarios 28

1. INTRODUCCIÓN

1. El presente documento forma parte integrante de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica (DGPC)*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 el *Certificado de Persona Física* expedido por la AC FNMT Usuarios.

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 Servicios de Confianza y de Certificación electrónica*.

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 Cualificados* de acuerdo con el Reglamento (UE) No 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, y conforme a la Ley 59/2003, de 19 de diciembre, de Firma electrónica, en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presta la FNMT – RCM.

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 Servicios de Confianza y de Certificación electrónica* (DGPC) de la FNMT-RCM, pues existen niveles de actuación análogos para todos los servicios de confianza de la Entidad y, de otro lado, por las *Políticas de Certificación y Prácticas de Certificación Particulares* aplicables a cada tipo de servicio de confianza que provee 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 Servicios de Confianza y de Certificación electrónica***, 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 las partes involucradas en los servicios de confianza, 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.

   2) Y, por otra parte, la *Política de Certificación* específica en la que se describen las obligaciones y responsabilidades de las partes, los límites de uso de los *Certificados* 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 Servicios de Confianza y de Certificación electrónica*.

Estas *Políticas de Certificación* y *Prácticas de Certificación Particulares* concretan lo articulado en el cuerpo principal de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* 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 por la AC FNMT Usuarios.

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 *Servicios de Confianza y de Certificación electrónica*.

Por tanto, en caso de que existiera contradicción entre el presente documento y lo dispuesto en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*, 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 Servicios de Confianza y de Certificación electrónica* y únicamente cuando los términos comiencen con letra mayúscula y estén en cursiva, se entenderá por:

- *Certificado de Persona Física*: *Certificado cualificado de firma electrónica* expedido por la AC FNMT Usuarios 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*.
- *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.
- *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. En la página http://www.cert.fnmt.es/dpcs/ se publica el documento que describe dichos perfiles.

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 Revocation List (CRL) Profile". Todos los campos definidos en el perfil de los *Certificados* 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 *DGPC* 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 *DGPC*.

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 *DGPC*.

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 *DGPC*.

20. Los *Certificados de Persona Física* son expedidos por una *Autoridad de Certificación* subordinada a la *Autoridad de Certificación* raíz de la FNMT – RCM. La identificación de dicha *Autoridad de Certificación* subordinada se recoge 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* / *Sello* del *Prestador de Servicios de Confianza*.

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

22. La FNMT-RCM no 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 / Sello del Prestador de Servicios de Confianza

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

    1) Firma / Sello de *Certificados*.
    2) Firma / Sello 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

24. 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 / sellar Certificados

25. 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*

26. 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 *DGPC* de la FNMT-RCM.

27. 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*.

28. En el documento DGPC, se da respuesta concreta para todos aquellos aspectos referentes a los siguientes apartados del estándar ETSI EN 319 411:

    - Controles de seguridad física
    - Controles de procedimiento
    - Controles de seguridad de personal

- Procedimientos de registro de auditoría
- Datos relevantes que serán registrados
- Cambio de Claves
- Restablecimiento de los servicios en caso de fallo o desastre
- Gestión de la continuidad de negocio y gestión de incidentes
- Terminación de la actividad de la FNMT-RCM como PSC

10. DIFUSIÓN DE TÉRMINOS Y CONDICIONES

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

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

11. POLÍTICA DE CERTIFICACIÓN DE LOS CERTIFICADOS DE PERSONA FÍSICA

11.1. IDENTIFICACIÓN

30. 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: 1.4

[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.

Fecha de expedición: 5 de marzo de 2019

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

DPC relacionada: Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica de la FNMT-RCM

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

11.2. TIPOLOGÍA DEL CERTIFICADO DE PERSONA FÍSICA

31. 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

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

33. Son expedidos como *Certificados Cualificados* conforme al Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93 (Reglamento eIDAS) y de conformidad con los requisitos establecidos en los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons".

34. Los *Certificados* expedidos bajo esta *Política de Certificación* se consideran válidos como sistemas de identificación y de firma electrónicas, de conformidad con la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, basados en *Certificados electrónicos cualificados* que son 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 Confianza* que expiden *Certificados cualificados* 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 en el Reglamento eIDAS.

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, deben 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

37. 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 confianza y la legislación aplicable.

11.4.2. Obligaciones y responsabilidad de las Oficinas de Registro

38. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en este documento y en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*, 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 *DGPC* 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 Persona física*, cuya solicitud, renovación 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 dicha Entidad (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 que pudieran afectar a la vigencia de los *Certificados*.
2. Comunicar a la FNMT-RCM de forma diligente las solicitudes de revocación de los *Certificados*.

vii) Respecto de la Protección de Datos de Carácter Personal, será de aplicación lo dispuesto en el apartado correspondiente de la *DGPC.*

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.

39. 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

40. 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 *DGPC*.

41. La FNMT – RCM cumple los requisitos de las especificaciones técnicas de la norma ETSI EN 319 412 para la emisión de *Certificados cualificados* y se compromete a continuar cumpliendo con dicha norma o aquellas que la sustituyan.

11.4.3.1. Con carácter previo a la emisión del Certificado

42. 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

43. a) Identificar a la persona física que solicite un *Certificado* exigiendo, con carácter general, su personación y estar en posesión del 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

44. 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*.
   - 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

45. 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. La integridad de este *Directorio* se protegerá mediante la utilización de sistemas conformes con las disposiciones reglamentarias específicas que al respecto se dicten en España y, en su caso, en la UE.

c) Mantener un *Servicio de información y consulta sobre el estado de validez 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 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

46. 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.

47. 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 *DGPC.*

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

48. A este respecto se puede consultar el apartado "Cese de la actividad del *Prestador de Servicios de Confianza*." de la *DGPC*.

11.4.3.7. Responsabilidad del Prestador de Servicios de Confianza

49. 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 la *DGPC*.

50. 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*.

51. 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.

52. 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 *DGPC*, 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.

53. 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.

54. 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

55. El *Solicitante* responderá de que la información presentada durante la solicitud del *Certificado* es verdadera y que la solicitud y descarga del *Certificado* se realizan desde un equipo o dispositivo que puede utilizar, con un alto nivel de confianza, bajo su control exclusivo.

56. 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

57. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la *DGPC*, el *Titular* del *Certificado de Persona Física*, como *firmante* 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*, con el fin de iniciar, en su caso, los trámites de su revocación.

58. 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.

59. 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.

60. 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* 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 / Sello* 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

61. El resto de la *Comunidad Electrónica, Entidades usuarias* y los terceros regularán sus relaciones con la FNMT-RCM a través de la *DGPC*, 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.

62. 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* o el *Sello electrónico avanzados* 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 al *Servicio de información y consulta sobre el estado de validez de los certificados* 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.

63. 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.

64. 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 *DGPC* y en el presente documento y comprobado que dicha *Firma electrónica* puede ser verificada por referencia a una *Cadena de certificación* válida.

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

66. Asimismo, será responsabilidad de la *Entidad usuaria* observar lo dispuesto en la *DGPC* 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

67. En cualquier caso, si una *Entidad usuaria* o un tercero desean confiar en la *Firma electrónica* realizada con uno de estos *Certificados*, sin acceder al *Servicio de información y consulta sobre el estado de validez 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*.

68. No se podrá emplear este tipo de *Certificados* 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

69. 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

70. La FNMT-RCM, no 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

71. En este apartado se definen aquellos aspectos que, si bien ya han sido apuntados en la *DGPC* 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

72. 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.

73. 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.

74. 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.

75. 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, y utilizando un canal seguro.

76. 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.

77. 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.

78. 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

79. 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 de firma electrónica* vigente que confirme la identidad de la persona física solicitante. La FNMT- RCM aceptará para tal fin *Certificados de firma electrónica* 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

80. 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, con los siguientes medios de identificación: Ciudadanos españoles: DNI, Pasaporte u otros medios admitidos en derecho a efectos de identificación (en los que conste su número de DNI/NIF). Ciudadanos de la UE: Tarjeta de Identificación de Extranjeros, o Certificado de Registro de Ciudadano de la Unión (donde conste el NIE) y Pasaporte o documento de identidad de país de origen, o Documento oficial de concesión del NIF y Pasaporte o documento de identidad de país de origen. Extranjeros: Tarjeta de Identificación de Extranjeros (donde conste el NIE) o Documento oficial de concesión del NIF y Pasaporte. El encargado de acreditación de la *Oficina de Registro* verificará que los documentos aportados cumplen todos los requisitos para confirmar la identidad del *Solicitante*.

81. 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 cualificado de firma electrónica* 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.

82. 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

83. 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 cualificado de firma electrónica* 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.

84. 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

85. Una vez recibidos en la FNMT-RCM los datos personales del *Solicitante*, así como su código de solicitud, y confirmada su identidad conforme al apartado anterior, se procederá a la expedición del *Certificado de Persona Física*.

86. 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.

87. La FNMT-RCM, por medio de su *Firma electrónica* o *Sello electrónico*, 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*.

88. 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*.

89. 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.

90. 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 Cualificados*, así como el *Certificado* de la *Autoridad de Certificación* que los expide (siempre subordinada a la *Autoridad de Certificación Raíz* de la FNMT-RCM). pueden consultarse en la página http://www.cert.fnmt.es/dpcs/.

   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 la descarga de su *Certificado de Persona Física*.

12.2.4. Aceptación, descarga e instalación del Certificado de Persona Física

91. En menos de una (1) hora desde que tiene lugar la confirmación de la identidad personal del *Solicitante*, la FNMT-RCM pone a disposición exclusiva del *Titular* su *Certificado de Persona Física* para que proceda a su descarga en la página web http://www.cert.fnmt.es.

92. En este proceso guiado se le pedirá al *Solicitante* que introduzca su número de DNI o NIE, 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 y como aceptación de dichas condiciones de uso, remitiéndolas firmadas 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.

93. 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

94. 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

95. 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) Revocación del *Certificado* por cualquiera de las causas recogidas en el presente documento.

96. 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. La única excepción a este caso se produce cuando la expedición de un *Certificado de Persona Física* sea causa de un proceso de renovación del mismo durante el periodo de tiempo de sesenta (60) días antes de su fecha de caducidad, en cuyo caso el *Certificado* que está próximo a caducar seguirá siendo válido hasta que expire el período de vigencia del mismo. Durante este tiempo, de producirse la revocación de dicho *Certificado* conforme al apartado siguiente, se producirá la extinción de la vigencia de ambos *Certificados.*

12.2.6. Revocación del Certificado de Persona Física

12.2.6.1. Causas de revocación

97. 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.

98. 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.

99. 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*).

100. 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

101. La revocación 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*.

102. 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

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

104. 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*.

105. 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*.

106. 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.

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

108. 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.

109. 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

110. No se contempla la suspensión de *Certificados*.

12.2.8. Renovación del Certificado de Persona Física

111. 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.

112. 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*.

113. 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.

114. El *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*.

115. 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 cualificado*, 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.

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

117. 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

118. El estado de revocación del *Certificado de Persona Física* podrá ser comprobado a través del *Servicio de información y consulta del estado de los Certificados* mediante el protocolo OCSP.

119. 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.

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

121. Será responsabilidad de la *Entidad usuaria* contar con 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 / sello 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