Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

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

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM	20/07/2023
Revisado por:	FNMT-RCM	21/08/2023
Aprobado por:	FNMT-RCM	28/08/2023

Versión	Fecha	Descripción
1.0	10/07/2015	Creación del documento
1.1	20/11/2015	Expedición de los certificados de representante de Persona jurídica y de Entidad sin personalidad jurídica como reconocidos.
1.2	11/04/2016	Actualización de perfiles conforme a los estándares ETSI (mandato M460) y directrices de la DTIC.
1.3	24/06/2016	Alineación con requisitos de la auditoría conforme el estándar ETSI
1.4	03/01/2017	Alineación con requisitos de la auditoría conforme el estándar ETSI 319 411
1.5	22/12/2017	Revisión anual.
1.6	05/03/2019	Eliminación de prácticas de suspensión de certificados.
1.7	05/06/2020	Adaptación estructura RFC3647 y Revisión Anual
1.8	18/08/2020	Extensión del ámbito de aplicación de los certificados de Representante y posibilidad de identificación con un certificado cualificado.

1.9	28/04/2021	Revisión anual. Alineamiento a Ley 6/2020 término "extinción de la personalidad jurídica". Aptdo.: 4.9.12: referencia a DGPC
2.0	28/08/2023	Revisión general conforme a S/MIME Baseline Requirements v.1.0.1 y el estándar ETSI 119 411-6, para la emisión de certificados con correo electrónico seguro. Se incluyen los certificados cualificados de sello de entidad.

Referencia: DPC/CPREP0200/SGPSC/2023

Documento clasificado como: Público

Índice de contenidos

Índice de tablas

1. INTRODUCCIÓN

1.1. OBJETO

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 la expedición del *Certificado de Representante de Persona jurídica*, del *Certificado de Representante de Entidad sin personalidad jurídica,* del *Certificado de Representante para administradores únicos y solidarios,* así como de los *Sellos de Entidad*.

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

3. Los Certificados expedidos por la FNMT-RCM, cuya Política de Certificación y Prácticas de Certificación Particulares se definen en el presente documento, se consideran 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 los principios de seguridad, integridad, confidencialidad, autenticidad y no repudio previstos en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

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

1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

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

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

a. 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 la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, 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.

b. 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 *DGPC*.

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

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

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

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

Referencia / OID[1]: 1.3.6.1.4.1.5734.3.11.1

[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.

Tipo de política asociada: QCP-n. OID: 0.4.0.194112.1.0

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

Referencia / OID: 1.3.6.1.4.1.5734.3.11.2

Tipo de política asociada: QCP-n. OID: 0.4.0.194112.1.0

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

Referencia / OID: 1.3.6.1.4.1.5734.3.11.3.

Tipo de política asociada: QCP-n. OID: 0.4.0.194112.1.0

Nombre: Política de Certificación de *Certificados de Sello de Entidad*

Referencia / OID: 1.3.6.1.4.1.5734.3.11.4.

Tipo de política asociada: QCP-l. OID: 0.4.0.194112.1.1

Nombre: Política de Certificación de *Certificados de Sello de Entidad con correo electrónico seguro*

Referencia / OID: 1.3.6.1.4.1.5734.3.11.5.

Tipo de política asociada: QCP-l. OID: 0.4.0.194112.1.1

Tipo de política SBR: Legacy Organization-Validated. OID: 2.23.140.1.5.2.1

Versión: 2.0

Fecha de expedición: 28/08/2023

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/

9. 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:

   a. Los términos y condiciones que regulan la utilización de los *Certificados* expedidos por la FNMT-RCM.

   b. La Política de Certificación aplicable a los *Certificados* expedidos por la FNMT-RCM.

   c. Los límites de uso para los *Certificados* expedidos bajo esta Política de Certificación.

   d. Las obligaciones, garantías y responsabilidades de las partes involucradas en la expedición y uso de los *Certificados*.

e. 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.

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

11. Por tanto, en caso de que existiera contradicción entre el presente documento y lo dispuesto en la DGPC, tendrá preferencia lo aquí articulado.

1.3. PARTES INTERVINIENTES

12. Las partes que intervienen en la gestión y uso de los *Servicios de Confianza* descritos en la presente *DPPP* son las siguientes:

1. Autoridad de Certificación
2. Autoridad de Registro
3. *Suscriptores* de los *Certificados*
4. Partes que confían
5. Otros participantes

1.3.1. Autoridad de Certificación

13. La FNMT-RCM es la *Autoridad de Certificación* que expide los *Certificados* electrónicos objeto de la presente *DPPP*. A estos efectos, existen las siguientes Autoridades de Certificación:

a) Autoridad de Certificación raíz. dicha Autoridad expide exclusivamente *Certificados* de Autoridades de Certificación subordinadas. El *Certificado* raíz de esta AC viene identificado por la siguiente información:

Tabla 1 – Certificado de la AC FNMT raíz

Certificado de la AC FNMT raíz	
Sujeto	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Emisor	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES

Certificado de la AC FNMT raíz	
Número de serie (hex)	5D:93:8D:30:67:36:C8:06:1D:1A:C7:54:84:69:07
Validez	No antes: 29 de octubre de 2008. No después: 1 de enero de 2030
Longitud clave pública	RSA 4.096 bits
Algoritmo de firma	RSA – SHA256
Identificador de clave	F7 7D C5 FD C4 E8 9A 1B 77 64 A7 F5 1D A0 CC BF 87 60 9A 6D

b) Autoridad de Certificación subordinada: expide los Certificados de entidad final objeto de la presente *DPPP*. El *Certificado* de dicha Autoridad viene identificado por la siguiente información:

Tabla 2 – Certificado de la AC subordinada

Certificado de la AC subordinada	
Sujeto	CN = AC Representación, OU = CERES, O = FNMT-RCM, C = ES
Emisor	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Número de serie (hex)	61 C2 D4 D4 F6 A9 AE 77 55 92 66 B9 8D AF D6 21
Validez	No antes: 30 de junio de 2015 No después: 31 de diciembre de 2029
Longitud clave pública	RSA 2048 bits
Algoritmo de firma	RSA – SHA256
Identificador de clave	8F D1 6A 17 99 44 D5 D1 D4 20 AF 09 40 5E DA 7A BF 2A 9C 74 28 83 E8 C2 F8 9E 0D 90 AF AF 75 4B

1.3.2. Autoridad de Registro

14. La Autoridad de Registro realiza las tareas de identificación del *Solicitante* de los *Certificados*, así como la comprobación de la documentación acreditativa de las circunstancias que constan en los mismos, la validación y la aprobación de las solicitudes de emisión, revocación y, en su caso, la renovación de dichos *Certificados*.

15. Podrán actuar como entidades de registro de FNMT-RCM para la validación y aprobación de las solicitudes de emisión y revocación de los *Certificados de Firma Electrónica*, aquellas Oficinas de Registro designadas por la FNMT-RCM con las que ésta suscriba el correspondiente instrumento legal para cubrir dicha finalidad. La validación y aprobación de las solicitudes de emisión de los Sellos de Entidad sólo se podrá llevar a cabo desde la *Autoridad de Registro* de la propia FNMT-RCM.

1.3.3. Suscriptores de los certificados

16. Los *Suscriptores* de los *Certificados de Firma Electrónica* son las personas físicas que mantienen bajo su uso exclusivo los *Datos de creación de firma* asociados a dichos *Certificados*.

17. Los *Suscriptores* de los *Sellos de Entidad* son las personas jurídicas a quienes se expide este tipo de *Certificados* y que están legalmente obligados por un acuerdo que describe los términos de uso del *Certificado*.

1.3.4. Partes que confían

18. Las partes que confían son aquellas personas físicas o jurídicas, diferentes del *Firmante* / *Suscriptor*, que reciben y / o usan *Certificados* expedidos por la FNMT-RCM y, como tales, les es de aplicación lo establecido por la presente *DPPP* cuando deciden confiar efectivamente en tales *Certificados*.

1.3.5. Otros participantes

19. No estipulado.

1.4. USO DE LOS CERTIFICADOS

1.4.1. Usos permitidos de los certificados

20. Los *Certificados de Firma Electrónica* y los *Sellos de Entidad* a los que aplica esta *DPPP* son *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", ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons" o ETSI EN 319 412-3 "Certificate profile for certificates issued to legal persons" respectivamente .

21. Los *Certificados de Firma Electrónica* emitidos bajo esta *Política de Certificación* son expedidos a personas físicas y 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 *Prestadores de Servicios de Confianza* que expiden *Certificados cualificados* al público supervisados en cada Estado miembro, entre los cuales se encuentra la FNMT–RCM.

22. Adicionalmente, los *Certificados con correo electrónico seguro* emitidos bajo esta DPPP, brindan un marco de "garantía razonable" que asegura que el *Suscriptor* tiene el control de la dirección de correo electrónico incluida en el Certificado. Estos Certificados pueden utilizarse para cifrar y/o firmar los mensajes de correo electrónico.

1.4.2. Restricciones en el uso de los certificados

23. 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*.

24. No se podrá emplear este tipo de *Certificados* para:

- Usos particulares o privados, salvo para relacionarse con las Administraciones o entre las partes cuando éstas lo admitan
- 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

1.5. ADMINISTRACIÓN DE POLÍTICAS

1.5.1. Entidad responsable

25. La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, con NIF Q2826004-J, es la Autoridad de Certificación que expide los *Certificados* a los que aplica esta *Declaración de Prácticas y Políticas de Certificación*.

1.5.2. Datos de contacto

26. La dirección de contacto de la FNMT-RCM como *Prestador de Servicios de Confianza* es la siguiente:

Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda

Dirección de Sistemas de Información - Departamento CERES

C/ Jorge Juan, 106

28071 – MADRID

E-mail: ceres@fnmt.es

Teléfono: +34 91 740 69 82

27. Para informar problemas de seguridad relacionados con un certificado, tales como sospecha de compromiso clave, uso indebido o fraude, envíenos un Informe de incidencia sobre certificado a la cuenta de correo electrónico: incidentes.ceres@fnmt.es.

1.5.3. Responsables de adecuación de la DPC

28. La Dirección de la FNMT-RCM dispone, dentro de sus competencias, de capacidad para especificar, revisar y aprobar los procedimientos de revisión y mantenimiento, tanto para las *Prácticas de Certificación Particulares*, como para la *Política de Certificación* correspondiente.

1.5.4. Procedimiento de aprobación de la DPC

29. La FNMT-RCM gestiona sus servicios de certificación y emite certificados con correo electrónico seguro de conformidad con la última versión de los "Requisitos base para la

emisión y gestión de certificados S/MIME de confianza"(S/MIME Baseline Requirements), Estos requisitos son establecidos por la entidad CA/Browser Forum y que pueden consultarse en la siguiente dirección https://cabforum.org/smime-br/

30. La FNMT-RCM a través de su Comité de Gestión del *Prestador de Servicios de Confianza*, vela por el cumplimiento de la presente *Declaración de Políticas y Prácticas de Certificación*, las aprueba, revisa y actualiza al menos cada 365 días para mantenerlas acorde a la última versión de los referidos requisitos, incrementando el número de versión y agregando una entrada de registro de cambios con fecha, incluso si no se realizaron otros cambios en el documento.

1.6. DEFINICIONES Y ACRÓNIMOS

1.6.1. Definiciones

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

- *Certificado de Firma Electrónica:* A efectos de la presente DPPP, es el *Certificado* cualificado que vincula un *Firmante* a unos *Datos de verificación de Firma* y confirma su identidad. Son *Certificados de Firma Electrónica*:
  - *Certificado de Representante de Persona jurídica*
  - *Certificado de Representante de Entidad sin personalidad jurídica*
  - *Certificado de Representante para administradores únicos y solidarios*
- *Certificado de Representante de Persona jurídica:* Es el *Certificado de Firma Electrónica* tradicionalmente utilizado por las Administraciones Públicas para el ámbito tributario y que, posteriormente, ha sido admitido para otros ámbitos. Por tanto, este *Certificado* se expide a las P*ersonas Jurídicas* para su uso en sus relaciones con aquellas Administraciones Públicas, Entidades y Organismos Públicos, vinculados o dependientes de las mismas y para otros usos admitidos entre las partes.
- *Certificado de Representante de Entidad sin personalidad jurídica:* Es el *Certificado de Firma Electrónica* utilizado en el ámbito tributario y otros ámbitos admitidos por la legislación vigente.
- *Certificado de Representante para administradores únicos y solidarios*: Es el *Certificado de Firma Electrónica* en el cual el *Firmante* actúa en representación de una *Persona jurídica* en calidad de *Representante* legal con su cargo de administrador único o solidario inscrito en el Registro Mercantil.
- Los *Certificados con correo electrónico seguro: a efectos de esta DPPP,* son aquellos certificados que incluyen una dirección de correo electrónico validada y bajo control del *Suscriptor* y la extensión e-mail protection que habilita para que estos certificados pueden emplearse para cifrar y/o firmar digitalmente correos electrónicos de forma segura utilizando la tecnología S/MIME.

- *Entidad representada*: *Persona jurídica* o *Entidad sin personalidad jurídica* en nombre de las cuales actúa el *Firmante* de un *Certificado* de los incluidos en la presente *Política y Prácticas de Certificación Particulares.*
- *Entidad sin personalidad jurídica*: son las entidades a las que se refiere el artículo 35.4 de la Ley General Tributaria y resto de legislación aplicable.
- *Firmante*: es la persona física que crea una firma electrónica en nombre propio o en nombre de la *Persona jurídica* o *Entidad sin personalidad jurídica* a la que representa.
- *Informe de incidencia sobre certificado (CPR):* queja de sospecha de compromiso clave, mal uso del certificado u otros tipos de fraude, compromiso, mal uso o conducta inapropiada relacionada con los certificados.
- *Persona jurídica*: persona o conjunto de personas agrupadas que constituyen una unidad con finalidad propia, la cual adquiere, como entidad, capacidad jurídica y de obrar distinta de la del miembro o de los miembros que la componen.
- *Prestador de Servicios de Confianza*: la persona física o jurídica que presta uno o más *Servicios de Confianza* de conformidad con lo establecido en el REGLAMENTO (UE) Nº 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
- *Representante*: Persona física que actúa en representación, legal o voluntaria, de una *Persona jurídica* o una *Entidad sin personalidad Jurídica*.
- *Sello de Entidad*: Declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona. Se utiliza para la automatización de procesos de firma y autenticación entre componentes informáticos.
- *Sello de Entidad con correo electrónico seguro*: *Sello de Entidad* que contiene la dirección de correo electrónico validada y bajo control del *Suscriptor* y la extensión e-mail protection que habilita para cifrar y/o firmar digitalmente correos electrónicos de forma segura utilizando la tecnología S/MIME.
- *Servicio de Confianza*: un servicio electrónico que consiste en alguna de las siguientes actividades: la creación, verificación, validación, gestión y conservación de F*irmas Electrónicas*, sellos electrónicos, *Sellos de Tiempo*, documentos electrónicos, servicios de entrega electrónica, autenticación de sitios web y *Certificados Electrónicos*, incluidos los *Certificados* de *Firma Electrónica* y de sello electrónico.
- *Solicitante*: persona física mayor de 18 años o menor emancipado, que previa identificación, solicita una operación relativa a un *Certificado* en nombre de la *Entidad representada*. A efectos de las presentes *Políticas y Prácticas de Certificación Particulares* coincidirá con la figura del *Representante*.

(Los términos señalados en cursiva se definen en el presente documento o en la DGPC).

1.6.2. Acrónimos

32. A los efectos de lo dispuesto en la presente DPPP, son de aplicación los siguientes acrónimos, cuyo significado es acorde con el estándar europeo ETSI EN 319 411 "Policy and security requirements for Trust Service Providers issuing certificates":

AC: Autoridad de Certificación

AR: Autoridad de Registro

ARL: Lista de Revocación de Autoridades de Certificación

CN: Common Name (Nombre común)

CRL: Lista de *Certificados* revocados

DN: Distinguished Name (Nombre distintivo)

DPC: Declaración de Prácticas de Certificación

DGPC: Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica

eIDAS: Reglamento 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.

ETSI: European Telecommunications Standards Institute

HSM: Módulo de seguridad criptográfico (Hardware Security Module). Es un dispositivo de seguridad que genera y protege claves criptográficas.

LCP: Política de *Certificado* ligera (Lightweight Certificate Policy)

NCP: Política de *Certificado* Normalizado

NCP+: Política de *Certificado* Normalizado Extendida

OCSP: Protocolo de internet usado para obtener el estado de un *Certificado* en línea (Online Certificate Status Protocol)

OID: Identificador de Objeto (Object IDentifier)

PIN: Personal Identification Number (Número de identificación personal)

PKCS: Public Key Cryptography Standards (Estándares PKI desarrollados por RSA Laboratorios)

SBR: CA/Browser Forum "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates" (S/MIME Baseline Requirements (SBR))

S/MIME: Secure MIME (Multipurpose Internet Mail Extensions) (Extensiones seguras para correo electrónico multipropósito)

TLS/SSL: Protocolos que proporcionan cifrado de datos y autenticación entre aplicaciones y servidores (Transport Layer Security/Secure Socket Layer protocol)

UTC: Tiempo coordinado universal (Coordinated Universal Time).

2. PUBLICACIÓN Y REPOSITORIOS

2.1. REPOSITORIO

33. La FNMT-RCM, como *Prestador de Servicios de Confianza*, mantiene un repositorio de información pública, disponible en horario 24x7, todos los días del año, en la dirección:

https://www.sede.fnmt.gob.es/descargas

2.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

34. La información relativa a la expedición de *Certificados* electrónicos objeto de la presente *DPPP* está publicada en la siguiente dirección:

https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

2.3. FRECUENCIA DE PUBLICACIÓN

35. Cualquier modificación en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* o en las *Políticas* y *Prácticas de Certificación Particulares* será publicada de forma inmediata en la URL de acceso a las mismas. Tal como se indica en el apartado 1.5.4 "Procedimiento de aprobación de la DPC", la frecuencia de revisión de las DPC será de al menos 365 días.

36. En cuanto a la frecuencia de publicación de CRL, se define en el apartado "4.9.7 Características adicionales. Frecuencia de publicación".

2.4. CONTROL DE ACCESO A LOS REPOSITORIOS

37. Todos los repositorios anteriormente citados son de acceso libre para la consulta y, en su caso, descarga de la información. Así mismo, la FNMT-RCM ha establecido controles para impedir que personas no autorizadas puedan añadir, modificar o borrar información incluida en sus repositorios y para proteger la autenticidad e integridad de dicha información.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. NOMBRES

38. La codificación de los *Certificados* sigue el estándar 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* en las *Políticas de Certificación* y *Prácticas de*

Certificación Particulares, excepto en los campos que específicamente se exprese lo contrario, emplean la codificación UTF8String.

3.1.1. Tipos de nombres

39. Los *Certificados* electrónicos de entidad final objeto de la presente *DPPP* contienen un nombre distintivo (*DN*) en el campo Subject Name, que se componen según se describe en la información relativa al perfil del *Certificado*.

40. En el procedimiento de acreditación de la identidad, como paso previo a la expedición de un *Certificados de Firma Electrónica,* la FNMT-RCM, a través de la *Oficina de Registro,* constatará la verdadera identidad del *Firmante* y conservará la documentación que la acredite.

3.1.2. Significado de los nombres

41. Todos los nombres distintivos (*DN*) del campo Subject Name son significativos. La descripción de los atributos asociados al *Suscriptor* del *Certificado* es legible por humanos (véase el apartado 7.1.4 Formato de nombres del presente documento).

42. El campo Common Name de los *Certificados de Firma Electrónica* define al *Suscriptor* al que se le ha expedido el *Certificado*.

43. El campo Common Name de los *Sellos de Entidad* es la denominación de sistema o aplicación de proceso automático para el que se expide el sello. Se deberá asegurar que dicho nombre tenga sentido y no dé lugar a ambigüedades.

44. El campo Common Name de los *Certificados de Sellos de Entidad con correo electrónico Seguro* tienen como valor el nombre de la organización.

3.1.3. Seudónimos

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

3.1.4. Reglas utilizadas para interpretar varios formatos de nombres

46. Se aplican los requisitos definidos por el estándar X.500 de referencia en la norma ISO/IEC 9594.

3.1.5. Unicidad de los nombres

47. El nombre distintivo (*DN*) asignado a los *Certificados* expedidos a un *Sujeto*, bajo las presentes DPPP y dentro del dominio del *Prestador de Servicios de Confianza,* será único.

3.1.6. Reconocimiento y autenticación de marcas registradas

48. La FNMT–RCM no asume compromiso alguno sobre el uso de signos distintivos, registrados o no, en la emisión de los *Certificados* expedidos bajo la presente *Política de Certificación.*

Solo se permite la solicitud de *Certificados* que incluyan signos distintivos cuyo derecho de uso sea propiedad del *Titular* o se encuentre debidamente autorizado. La FNMT–RCM no está obligada a verificar previamente la titularidad o registro de los signos distintivos antes de la emisión de los *Certificados,* aunque figuren en registros públicos.

3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD

3.2.1. Métodos para probar la posesión de la clave privada

49. La FNMT-RCM no genera ni almacena las Claves Privadas asociadas a los *Certificados* expedidos bajo las presentes Políticas de Certificación y Prácticas de Certificación Particulares, que son generadas bajo el exclusivo control del *Suscriptor*.

3.2.2. Validación de la autorización o control sobre el correo

50. Para validar el correo electrónico incluido en los *Certificados con correo electrónico seguro*, la FNMT-RCM utiliza el método descrito en el documento S/MIME Baseline Requirements (SBR)*: "3.2.2.2. Validating control over mailbox via email*". El resto de los métodos descritos en S/MIME Baseline Requirements (SBR) no se emplea para la validación de correos.

3.2.2.2. Validación del control sobre el buzón de correo mediante un correo electrónico

51. FNMT-RCM, previo a la emisión del certificado, enviará un código único y aleatorio al correo electrónico proporcionado por el *Suscriptor* durante la solicitud. Al que el Solicitante debe acceder para demostrar su control sobre el buzón de correo. La duración del código aleatorio será inferior a 24 horas desde su creación.

3.2.3. Autenticación de la identidad de la organización

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

53. Asimismo, la FNMT-RCM, con carácter particular, comprobará, directamente o a través de tercero, los datos relativos a la constitución y, en su caso, personalidad jurídica de la entidad para la que se solicita la emisión del *Certificado*, y a la vigencia de las facultades de representación del *Solicitante* para realizar la mencionada solicitud, previa aportación de la documentación fidedigna que sea requerida para este fin, y que será custodiada por el

Prestador de Servicios de Confianza por sí o por cuenta de la *Oficina de Registro* habilitada, con el fin de posibilitar su consulta con posterioridad. La relación que compone dicha documentación se publica en la sede electrónica de la FNMT-RCM (http://www.cert.fnmt.es).

54. Para el caso específico de los *Certificados de Representante para administradores únicos y solidarios*, la FNMT-RCM, una vez ha comprobada la identidad personal del *Representante*, procede a verificar la personalidad jurídica de la *Entidad representada* y la extensión y vigencia de las facultades de representación del *Representante,* es decir, su nombramiento e inscripción en el Registro Mercantil como administrador único o solidario mediante consulta telemática a los registros del CORPME.

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

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

57. La FNMT-RCM verifica la existencia legal, la dirección y la identidad de la organización suscriptora del *Certificado* mediante diferentes métodos, en función del tipo de organización (privada, pública o de negocio).

58. Cuando el *Suscriptor* es una entidad privada, se verificará su existencia, dirección e identidad, que está legalmente reconocida, activa en ese momento e inscrita formalmente, mediante consulta directa de la AR de la FNMT-RCM al servicio que el Registro Mercantil dispone para este fin.

59. En el caso de entidades públicas, dicha verificación se realizará mediante consulta directa de la AR de la FNMT-RCM al inventario de entes del sector público de la Intervención General de la Administración del Estado, dependiente del Ministerio de Hacienda, o al Boletín Oficial correspondiente.

60. Si la naturaleza del Suscriptor fuera distinta de los dos casos anteriores, las verificaciones relativas a la existencia legal, dirección y la identidad se realizará mediante consulta directa al registro oficial correspondiente.

61. La lista de las fuentes de consulta de Agencias de Registro es publicada en la web de la FNMT-RCM (https://www.cert.fnmt.es/registro/utilidades).

3.2.4. Autenticación de la identidad de la persona física solicitante

62. La FNMT-RCM, como Prestador de Servicios de Confianza, antes de expedir un *Certificado* identificará al *Solicitante* del mismo, bien mediante presencia física ante una persona con capacidad para realizar la acreditación con la participación de una Oficina de Registro con la que la FNMT- RCM tenga suscrito un acuerdo o a la que sea de aplicación de una norma o

una resolución administrativa, bien mediante la utilización de un *Certificado cualificado de firma electrónica* que confirme la identidad de la persona física solicitante.

3.2.4.1 Comprobación directa mediante presencia física

63. La persona con capacidad para realizar la acreditación verificará que los documentos aportados para acreditar la identidad del *Solicitante* cumplen todos los requisitos para confirmar su identidad. Dichos documentos son: 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.

64. 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.

3.2.4.2 Comprobación utilizando medios de identificación electrónica

65. La FNMT-RCM expedirá el *Certificado de Representante para administradores únicos o solidarios* sin necesidad de que el peticionario comparezca ante una *Oficina de Registro* si en el proceso de solicitud de dicho *Certificado*, el *Solicitante* se identifica utilizando un *Certificado cualificado de firma electrónica* perteneciente a alguno de los siguientes tipos:

- Un *Certificado de Persona Física* expedido por la FNMT-RCM.
- Un *Certificado de Representante para administradores únicos o solidarios.*
- Un *Certificado* electrónico de los incorporados al DNIe.

66. No obstante, solo se permitirá la solicitud telemática del *Certificado de Representante para administradores únicos o solidarios* mediante el uso de los *Certificados* electrónicos relacionados en el apartado anterior si, en el momento de la solicitud, no se ha superado el plazo máximo establecido por la legislación vigente desde la personación e identificación física del *Suscriptor,* y este certificado se obtuvo mediante acreditación de la identidad con presencia física.

3.2.5. Información no verificada del Suscriptor

67. Toda la información incorporada al *Certificado* electrónico es verificada por la *Autoridad de Registro*.

3.2.6. Validación de la autorización

68. Una vez confirmada la identidad del *Solicitante,* así como los datos relativos a la personalidad jurídica de la *Entidad representada* y a la extensión y vigencia de sus facultades de representación del Representante 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.

69. Previa a la emisión del *Certificado de Firma Electrónica*, la FNMT_RCM establece controles adicionales, como por ejemplo confirmar que el *Solicitante* no está inscrito como difunto en los registros que el Ministerio de Justicia comunica a esta Entidad para tal fin.

70. No se emitirán *Certificados* a menores de edad, salvo que ostenten y acrediten su cualidad de emancipados. La Oficina de Registro será la encargada de realizar las validaciones relativas a este punto.

3.2.7. Criterios de interoperación

71. No existen relaciones de interactividad con Autoridades de Certificación externas a FNMT-RCM.

3.2.8. Fiabilidad de las fuentes de verificación

72. La FNMT-RCM asegura la idoneidad de las fuentes como fuente de verificación fiable.

73. Antes de utilizar cualquier fuente de datos como fuente de datos confiable, la *RA* evaluará la fuente en cuanto a su confiabilidad, precisión y resistencia a la alteración o falsificación.

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RENOVACIÓN DE CLAVES

74. Bajo las presentes Políticas de Certificación, la FNMT-RCM no contempla ningún proceso de regeneración de claves.

75. Las condiciones de autenticación de una petición de renovación se desarrollan en el apartado correspondiente al proceso de renovación de *Certificados* de este documento.

3.3.1. Renovación rutinaria

76. Bajo las presentes Políticas de Certificación, la FNMT-RCM no contempla ningún proceso de renovación rutinaria.

3.3.2. Renovación después de una revocación

77. Bajo las presentes Políticas de Certificación, la FNMT-RCM no contempla ningún proceso de renovación después de una revocación.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

78. Previa a la revocación efectiva de los *Certificados*, la Autoridad de Registro identificará de forma fehaciente a los solicitantes de la Revocación para vincularlos con los datos únicos del *Certificado* a revocar.

79. Las condiciones de autenticación de una petición de revocación se desarrollan en el apartado correspondiente al proceso de revocación de *Certificados* de este documento.

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DE LOS CERTIFICADOS

4.1. SOLICITUD DE CERTIFICADOS

4.1.1. Quién puede solicitar un Certificado

80. El *Solicitante* de este tipo de *Certificados* solo puede ser una persona física, mayor de edad o menor que acredite su condición de emancipado, en posesión de su número de Documento Nacional de Identidad o Número de Identificación de Extranjeros.

4.1.2. Proceso de registro y responsabilidades

4.1.2.1 Para los Certificados de Firma Electrónica:

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

82. En este mismo proceso, para el caso de los *Certificados de Representante para administradores únicos y solidarios*, se recabará también su consentimiento para realizar la consulta pertinente al Registro Mercantil, al objeto de comprobar la personalidad jurídica de la *Entidad representada*, y la extensión y vigencia de sus facultades de representación.

83. Posteriormente se generan las *Claves Pública* y *Privada* que serán vinculadas al *Certificado* que se generará en una fase posterior, y la FNMT-RCM asigna a la solicitud un código único.

84. 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.

85. 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.

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

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

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

89. El apartado 9.8 "Responsabilidades" del presente documento establece las responsabilidades de las partes en este proceso.

4.1.2.2 Para los Sellos de Entidad:

90. Cada *Solicitante* deberá presentar una solicitud de *Certificado* y la información requerida antes de emitir un *Sello de Entidad*. El FNMT-RCM autentica y protege todas las comunicaciones frente a modificaciones con el *Solicitante.*

91. El proceso de registro incluye las siguientes fases:

- Enviar una solicitud de *Certificado* completa y aceptar los términos y condiciones aplicables. Con esta aceptación, los *Suscriptores* garantizan que toda la información contenida en la solicitud de *Certificado* es correcta.
- Se valida la dirección de correo electrónico del *Suscriptor,* enviando un código único y aleatorio al correo electrónico suministrado. Deberá acceder a su correo y seguir las indicaciones proporcionadas.
- Generar un par de claves,
- Entregar la clave pública del par de claves a la CA y
- Pagar cuando proceda las tarifas aplicables.

92. La AR de la FNMT-RCM realiza la verificación de la identidad de la Organización suscriptora y del *Representante del Suscriptor*, y comprueba que la solicitud del *Certificado* es correcta completa y debidamente autorizada, de conformidad con los requisitos definidos en el

apartado "3.2 Validación inicial de la identidad" del presente documento. FNMT-RCM podrá realizar comprobaciones adicionales a los procesos de validación descritos en el citado apartado.

93. FNMT-RCM recopilará las evidencias correspondientes a las comprobaciones realizadas y quedarán almacenadas en un repositorio.

4.2. PROCEDIMIENTO DE SOLICITUD DE CERTIFICADOS

4.2.1. Realización de las funciones de identificación y autenticación

94. El *Solicitante* aportará los datos requeridos y acreditará su identidad personal. La FNMT-RCM, a través de la *Oficina de Registro,* constatará la verdadera identidad del *Suscriptor,* la personalidad jurídica de la *Entidad representada* y la extensión y vigencia de las facultades de representación del *Representante* y conservará la documentación que la acredite. FNMT-RCM admitirá, en todo caso, la función e informe que realice la *Oficina de Registro*.

95. Para la emisión de *Certificados de Firma Electrónica*, la FNMT-RCM podrá identificar al *Solicitante*, de forma alternativa a la comparecencia en la *Oficina de Registro*, mediante el uso de un *Certificado de Firma Electrónica cualificado* según se describe en el apartado "3.2.4.2. *Comprobación utilizando medios de identificación electrónica".*

4.2.2. Aprobación o rechazo de la solicitud del certificado

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

97. La transmisión de información a la FNMT-RCM se realizará mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM.

98. La FNMT-RCM recabará de los *Solicitantes* aquella información recibida de la *Oficina de Registro*, que sea necesaria para la expedición de los *Certificados* y para la comprobación de la identidad, almacenando la información exigida por la legislación de firma electrónica durante el periodo de quince (15) años tratándola con la debida diligencia para el cumplimiento de la legislación nacional vigente en materia de protección de datos de carácter personal.

99. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

4.2.3. Tiempo en procesar la solicitud

100. La solicitud aprobada de los *Certificados de firma electrónica* es procesada automáticamente por el sistema, por lo que no hay establecido un tiempo para este proceso.

101. Para el caso de los Sellos de Entidad, se empleará el tiempo mínimo necesario desde la recepción por parte de la Oficina de Registro de la FNMT – RCM de toda la documentación

necesaria para realizar las comprobaciones requeridas de forma previa a la expedición del Certificado.

4.3. EMISIÓN DEL CERTIFICADO

4.3.1. Acciones de la AC durante la emisión

102. Una vez recibidos en la FNMT-RCM los datos personales del *Solicitante*, así como su código de solicitud, y confirmada su identidad, así como la personalidad jurídica de la *Entidad representada* y la extensión y vigencia de las facultades de representación del *Representante* conforme al apartado anterior, se procederá a la expedición del *Certificado*.

103. La expedición de los *Certificados* 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 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.

104. La FNMT-RCM, por medio de su *Firma electrónica* o *Sello electrónico*, autentica los *Certificados* 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*.

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

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

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

107. La emisión de los *Certificados de Firma Electrónica* atenderá a:

1. Composición de la estructura de datos que conforman el *Certificado*

   Con los datos recogidos durante el proceso de solicitud del *Certificado*, se procede a componer el nombre distintivo (DN) conforme al estándar X.500, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.

2. Composición de la identidad alternativa de los *Certificados*.

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

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

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

108. El formato de los *Certificados*, expedidos 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*, puede consultarse en la página http://www.cert.fnmt.es/dpcs/

4.3.2. Notificación de la emisión

109. Una vez emitido el *Certificado*, la FNMT-RCM informará al *Solicitante* sobre la disponibilidad de *Certificado* para su descarga.

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1. Proceso de aceptación

110. En el proceso de solicitud del *Certificado*, el *Solicitante* acepta las condiciones de uso y expresa su voluntad de obtener el *Certificado*, como requisitos necesarios para la generación del mismo.

111. La FNMT-RCM pone a disposición exclusiva del *Suscriptor* su *Certificado* para que proceda a su descarga en la página web http://www.cert.fnmt.es.

112. En este proceso guiado de descarga de un *Certificado de Firma Electrónica*, 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* aún no hubiera sido generado por cualquier motivo, el proceso le informará de este hecho.

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

114. Una vez realizado el pago, el *Certificado* se instalará en el soporte en el que se generaron las *Claves* durante el proceso de solicitud (Token criptográfico o, en su defecto, el *Navegador*

desde el cual hizo la solicitud). En la citada página web de la FNMT-RCM se indican los *Navegadores* soportados y normas de instalación de los *Certificados*.

4.4.2. Publicación del certificado por la AC

115. Los *Certificados* generados son almacenados en un repositorio seguro de la FNMT-RCM, con acceso restringido.

4.4.3. Notificación de la emisión a otras entidades

116. No se realizan notificaciones de emisión a otras entidades.

4.5. PAR DE CLAVES Y USO DEL CERTIFICADO

4.5.1. Clave privada y uso del certificado

117. La FNMT-RCM no genera ni almacena las *Claves Privadas* asociadas a los *Certificados* expedidos bajo la presente *Política de Certificación*. Corresponde la condición de custodio, *Suscriptor* y responsable sobre el control de las claves del *Certificado*, al *Suscriptor* del *Certificado*.

118. Los *Certificados de Firma Electrónica* emitidos bajo esta *Política de Certificación* son *certificados cualificados* expedidos a personas físicas y 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.

4.5.2. Uso del certificado y la clave pública por terceros que confían

119. Los terceros que confían en las *Firmas electrónicas* realizadas con las *Claves privadas* asociadas al *Certificado* se atendrán a las obligaciones y responsabilidades definidas en la presente *DPPP*.

4.6. RENOVACIÓN DEL CERTIFICADO

120. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.1. Circunstancias para la renovación del certificado

121. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.2. Quién puede solicitar la renovación del certificado

122. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.3. Procesamiento de solicitudes de renovación del certificado

123. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.4. Notificación de la renovación del certificado

124. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.5. Conducta que constituye la aceptación de la renovación del certificado

125. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.6. Publicación del certificado renovado

126. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.7. Notificación de la renovación del certificado a otras entidades

127. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.7. RENOVACIÓN CON REGENERACIÓN DE LAS CLAVES DEL CERTIFICADO

128. Bajo las presentes Políticas de Certificación, sólo se contempla la renovación con regeneración de claves de los *Certificados de Representante para administradores únicos y solidarios* que se llevará a cabo siempre emitiendo nuevas claves y siguiendo el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

129. Solo se permitirá una única renovación del *Certificado de Representante para administradores únicos y solidarios*. El *Titular* que ya hubiera realizado una renovación de su *Certificado* y quisiera seguir utilizando un *Certificado* 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 "3.2.3. Autenticación de la identidad de la persona física solicitante" del presente documento.

130. Podrán solicitar la renovación de los *Certificados de Representante para administradores únicos y solidarios* expedidos por la FNMT-RCM los *Titulares* de los mismos, siempre que en el momento de la solicitud tengan un *Certificado de Representante para administradores únicos y solidarios* 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*.

131. La renovación de un *Certificado de Representante para administradores únicos y solidarios* 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*. La solicitud de renovación se hará a través de la dirección http://www.ceres.fnmt.es.

132. El *Certificado de Representante para administradores únicos y solidarios* 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* durante el período de tiempo en el que el *Titular* posee dos *Certificados* activos, la FNMT-RCM procederá a revocar ambos *Certificados*.

133. La identificación del *Representante*, como *Solicitante* de la renovación del *Certificado*, se realizará telemáticamente mediante el uso del *Certificado de Representante para administradores únicos y solidarios* que, estando aún activo, está próximo a caducar, siempre que en el momento de la solicitud no se haya superado el plazo máximo de 5 años desde la personación e identificación física del *Representante*, de acuerdo con lo establecido en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

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

135. La utilización de los *Certificado de Representante para administradores únicos y solidarios* 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*.

4.7.1. Circunstancias para la renovación con regeneración de claves

136. Las claves de los *Certificados* se renovarán bajo los siguientes supuestos:

- Por caducidad próxima de las actuales claves a petición del solicitante de la renovación.
- Por compromiso de las claves u otra circunstancia de las recogidas en el apartado "*4.9 Revocación y suspensión del certificado"* de la presente *DPPP.*

4.7.2. Quién puede solicitar la renovación con regeneración de claves

137. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.3. Procesamiento de solicitudes de renovación con regeneración de claves

138. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.4. Notificación de la renovación con regeneración de claves

139. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.5. Conducta que constituye la aceptación de la renovación con regeneración de claves

140. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.6. Publicación del certificado renovado

141. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.7. Notificación de la renovación con regeneración de claves a otras entidades

142. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.8. MODIFICACIÓN DEL CERTIFICADO

143. No es posible realizar modificaciones de los *Certificados* expedidos. Por tanto, cualquier necesidad de modificación conlleva la expedición de un nuevo *Certificado*.

4.8.1. Circunstancias para la modificación del certificado

144. No se estipula la modificación.

4.8.2. Quién puede solicitar la modificación del certificado

145. No se estipula la modificación.

4.8.3. Procesamiento de solicitudes de modificación del certificado

146. No se estipula la modificación.

4.8.4. Notificación de la modificación del certificado

147. No se estipula la modificación.

4.8.5. Conducta que constituye la aceptación de la modificación del certificado

148. No se estipula la modificación.

4.8.6. Publicación del certificado modificado

149. No se estipula la modificación.

4.8.7. Notificación de la modificación del certificado a otras entidades

150. No se estipula la modificación.

4.9. REVOCACIÓN Y SUSPENSIÓN DEL CERTIFICADO

151. Los *Certificados* emitidos 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 *Suscriptor*, 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.

152. Los efectos de la revocación del *Certificado*, esto es, la extinción de su vigencia, surtirán desde la fecha en que la FNMT-RCM tenga conocimiento cierto de cualquiera de los hechos determinantes y así lo haga constar en su *Servicio de información y consulta sobre el estado de los Certificados*.

153. A los efectos enumerados anteriormente, la expedición de un *Certificado de Firma Electrónica* cuando exista otro vigente a favor del mismo *Titular*, conllevará la revocación inmediata del *Certificado* anterior. La única excepción a este caso se produce cuando la expedición de un *Certificado de Representante para administradores únicos y solidarios* sea causa de un proceso de renovación del mismo durante el periodo de tiempo de sesenta (60) días antes de su fecha de caducidad, en cuyo caso el *Certificado de Representante para administradores únicos y solidarios* 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*.

154. La FNMT-RCM pone a disposición de los Suscriptores, terceros que confían, proveedores de software y terceras partes una vía de comunicación a través de la sede electrónica de la FNMT-RCM https://www.sede.fnmt.gob.es/.

4.9.1. Circunstancias para la revocación

4.9.1.1 Circunstancias para la revocación del certificado del suscriptor

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

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

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

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

b) Resolución judicial o administrativa que así lo ordene.

c) Fallecimiento del Representante.

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

e) Terminación de la representación.

f) Extinción de la Persona jurídica representada.

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

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

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

j) Pérdida del control sobre la dirección del correo electrónico incluido en el Certificado por parte del suscriptor.

k) Resolución del contrato suscrito entre la Entidad representada o el Firmante y la FNMT-RCM, así como el impago o retrocesión del pago del importe asociado a la obtención del Certificado.

l) Cese en la actividad del Prestador de Servicios de Confianza salvo que la gestión de los Certificados electrónicos expedidos por aquél sea transferida a otro Prestador de Servicios de Confianza.

m) Incumplimiento de los requisitos definidos por los esquemas de auditorías a los que se somete la Autoridad de Certificación que expide los Certificados cubiertos por la presente DPC, con especial atención a los de algoritmia y tamaños de clave, que supongan un riesgo inaceptable por parte de las partes que confían en estos Certificados.

157. En ningún caso la FNMT-RCM asume obligación alguna de comprobar los extremos mencionados en las letras c) a j) del presente apartado, debiendo ser notificadas a esta entidad de forma fehaciente mediante entrega de los documentos e informaciones necesarias para verificarlo. Para el caso de los *Certificados de Representante para administradores únicos y solidarios*, los extremos mencionados en las letras e) y f) del presente apartado serán comunicados por parte del CORPME a la FNMT-RCM, momento en el cual esta entidad procederá a la revocación del *Certificado* afectado.

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

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

159. 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.

160. La revocación de los *Certificados* implica, además de su extinción y la imposibilidad de seguir utilizando los *Datos de creación de firma* o claves privadas asociados, la finalización de la relación y régimen de uso de dicho *Certificado* y su *Clave privada* con la FNMT-RCM.

4.9.1.2 Circunstancias para la revocación del certificado de la CA subordinada

161. La CA emisora revocará el certificado de la CA subordinada en cualquiera de las siguientes situaciones:

a) La CA subordinada solicita la revocación por escrito;

b) La CA subordinada notifica a la CA emisora que la solicitud de certificado original no fue autorizada y no otorga autorización retroactivamente;

c) La CA emisora obtiene evidencia de que la Clave privada de la CA subordinada correspondiente a la Clave pública en el Certificado sufrió un Compromiso clave o ya no cumple con los requisitos de las secciones 6.1.5 y 6.1.6,

d) La CA emisora obtiene evidencia de que el Certificado fue mal utilizado;

e) La CA emisora es consciente de que el Certificado no se emitió de acuerdo con o que la CA subordinada no ha cumplido con los requisitos SBR establecidos por la entidad CA/Browser fórum para este tipo de Certificados o esta DPC;

f) La CA emisora determina que cualquiera de la información que aparece en el Certificado es inexacta o engañosa;

g) La CA emisora o CA subordinada cesa sus operaciones por cualquier motivo y no ha hecho arreglos para que otra CA brinde apoyo de revocación para el Certificado;

h) El derecho de la CA emisora o de la CA subordinada a emitir Certificados según los requisitos SBR establecidos por la entidad CA/Browser fórum vence o se revoca o finaliza, a menos que la CA emisora haya hecho arreglos para continuar manteniendo el repositorio de CRL / OCSP; o

i) La DPC de la CA emisora requiere la revocación.

162. Se atenderá a lo dispuesto en el "Plan de Actuación ante Compromiso de la Infraestructura de Clave Pública de FNMT-RCM".

4.9.2. Quién puede solicitar la revocación

163. La revocación de un *Certificado* solamente podrá ser solicitada por:

- la *Autoridad de Certificación* y la *Autoridad de Registro*
- la *Entidad representada* o persona con facultades de representación suficientes, en la Oficina de Registro habilitada a tal efecto
- en su caso, el *Suscriptor,* a través del teléfono habilitado para tal fin (previa identificación del *Solicitante*) cuyo número se hace público en la web de la FNMT – RCM y que estará operativo en horario 24x7.

164. La FNMT-RCM podrá revocar de oficio los *Certificados* en los supuestos recogidos en la presente Declaración de Prácticas y Políticas de Certificación y en el caso específico de los *Certificados de Representante para administradores únicos y solidarios*, en los casos en los que el CORPME le notifique la modificación de alguno de los hechos significativos recogidos en el *Certificado*, relativos a la extinción de la personalidad jurídica de la *Entidad representada* o de la extensión y vigencia de las facultades de representación del *Representante* y en el resto de supuestos recogidos en la presente *Declaración de Prácticas de Certificación*.

4.9.3. Procedimiento de solicitud de la revocación

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

166. La revocación de un *Certificado* 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*.

167. El proceso de revocación puede realizarse de forma ininterrumpida 24x7, a través del teléfono +34 91 740 69 82, del Servicio de Revocación telefónica, puesto a disposición de los usuarios para esta finalidad, asegurando la revocación del *Certificado* en un plazo inferior a 24h.

168. Durante la revocación telefónica, el *Solicitante* de la revocación tendrá que confirmar los datos que se le soliciten y aportar aquellos que sean imprescindibles para la validación de forma inequívoca de su capacidad para solicitar dicha revocación.

169. Si la *Entidad representada* está en posesión de su *Certificado de Representante para administradores únicos y solidarios* 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.

170. Adicionalmente, se puede solicitar la revocación de cualquier *Certificado de Firma electrónica* a través de una *Oficina de Registro*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica. El *Solicitante* deberá presentarse en su *Oficina de Registro,* donde se acreditará su identidad, se validará su capacidad para revocar dicho *Certificado* y se consignará la causa de revocación. La Oficina enviará de forma telemática mediante la aplicación de registro los datos a la FNMT-RCM, y procederá a la revocación del *Certificado*.

171. Para el caso de los *Sellos de Entidad*, también es posible dirigir la solicitud de revocación al Área de Registro de la FNMT-RCM, siguiendo el siguiente procedimiento:

1. Solicitud del *Suscriptor*

   El *Representante del Suscriptor* enviará a la FNMT-RCM el formulario de solicitud de revocación, cumplimentado y firmado electrónicamente con alguno de los *Certificados* admitidos para la solicitud y por los canales electrónicos habilitados por esta Entidad.

2. Tramitación de la solicitud por la FNMT-RCM

   El registrador de la FNMT-RCM recibirá el contrato de revocación y realizará las mismas comprobaciones relativas a la identidad y capacidad del Representante del Suscriptor que para el caso de la solicitud de expedición y, si procediera, tramitará la revocación del Certificado.

172. Tan pronto la revocación sea efectiva, el *Suscriptor* y *Solicitante* de la revocación serán notificados a través de la dirección de correo electrónico.

173. 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, así como la fecha, hora y causa de revocación. Una vez que un *Certificado* ha sido revocado, su vigencia queda definitivamente extinguida, sin posibilidad de revertir su estado.

174. Para informar de posibles compromisos de Claves Privada, uso indebido de certificados u otros tipos de fraude, conducta inapropiada o cualquier otro asunto relacionado con los certificados, se puede enviar un CPR a la dirección de correo incidentes.ceres@fnmt.es indicada en el apartado 1.5.2.

4.9.4. Periodo de gracia de la solicitud de revocación

175. No existe periodo de gracia asociado a este proceso, pues la revocación se realiza de forma inmediata a la recepción verificada de la solicitud de revocación.

4.9.5. Plazo de tiempo para procesar la solicitud de revocación

176. La FNMT – RCM procede a la revocación inmediata del *Certificado* en el momento de verificar la identidad del *Solicitante* o, en su caso, de la veracidad de la solicitud realizada mediante resolución judicial o administrativa. En cualquier caso, la revocación efectiva del *Certificado* se realizará en menos de 24 horas desde la recepción de la solicitud de revocación.

177. En el caso de recibir un CPR a través de la cuenta de correo incidentes.ceres@fnmt.es indicada en el apartado 1.5.2, dentro de las 24 horas posteriores a su recepción, la FNMT-RCM investigará los hechos y circunstancias relacionados en la medida de lo posible y proporcionará un informe preliminar tanto al Suscriptor como a la entidad que lo presentó.

178. En dicho informe, se establecerá si el Certificado será revocado o no y, de ser así, la fecha en la que la CA lo revocará. El período desde la recepción del CPR o el aviso relacionado con la revocación hasta la revocación publicada no excederá el plazo establecido en la sección 4.9.1.1.

179. La fecha seleccionada por la CA considerará los siguientes criterios:

1. La naturaleza del presunto problema (alcance, contexto, gravedad, magnitud, riesgo de daño)
2. Las consecuencias de la revocación (impactos directos y colaterales a los Suscriptores y Partes que Confían)
3. El número de CPR recibidos sobre un Certificado o Suscriptor en particular
4. La entidad que presenta la queja
5. Legislación relevante.

4.9.6. Obligación de verificar las revocaciones por las partes que confían

180. Las terceras partes que confían y aceptan el uso de los *Certificados* emitidos por la FNMT – RCM están obligadas a verificar, por medio de uno de los mecanismos disponibles (Listas de Revocación CRL y/o OCSP), el estado de los *Certificados*:

- la *Firma Electrónica Avanzada* o el *Sello Electrónico Avanzado* del *Prestador de Servicios de Confianza* emisor del *Certificado,*
- que el *Certificado* continúa vigente y activo,
- el estado de los *Certificados* incluidos en la *Cadena de Certificación.*

4.9.7. Frecuencia de generación de CRLs

181. Las *Listas de Revocación* (*CRL*) de los *Certificados de Firma Electrónica y Sello de Entidad* se emiten al menos cada 12 horas, o cuando se produce una revocación y tienen un periodo de validez de 24 horas. Las *CRL* de los *Certificados* de *Autoridad* se emiten cada 6 meses, o cuando se produce una revocación de una *Autoridad de Certificación* subordinada y tienen un periodo de validez de 6 meses.

4.9.8. Periodo máximo de latencia de las CRLs

182. La publicación de las *Listas de Revocación* se realiza en el momento de generación de dichas Listas, por lo que el periodo de latencia entre la generación de la CRL y su publicación es nulo.

4.9.9. Disponibilidad del sistema de verificación online del estado de los certificados

183. La información relativa al estado de los *Certificados* estará disponible en línea las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema se pondrá en marcha el Plan de continuidad de negocio para solventar el incidente a la mayor brevedad posible.

4.9.10. Requisitos de comprobación en línea de la revocación

184. La comprobación en línea del estado de revocación de los *Certificados de Firma Electrónica y Sello Electrónico* puede realizarse mediante el *Servicio de información del estado de los Certificados*, ofrecido a través de OCSP según se describe en el apartado 4.10 del presente documento. El interesado en utilizar dicho servicio deberá:

- Comprobar la dirección contenida en la extensión AIA (Authority Information Access) del *Certificado*.
- Comprobar que la respuesta OCSP está firmada / sellada.

4.9.11. Otras formas de aviso de revocación disponibles

185. No definidas.

4.9.12. Requisitos especiales de revocación de claves comprometidas

186. Véase el apartado correspondiente en la *DGPC*.

4.9.13. Circunstancias para la suspensión

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

4.9.14. Quién puede solicitar la suspensión

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

4.9.15. Procedimiento para la petición de la suspensión

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

4.9.16. Límites sobre el periodo de suspensión

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

4.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE LOS CERTIFICADOS

4.10.1. Características operativas

191. La información relativa a la validación de los *Certificados* electrónicos objeto de la presente *DPPP* es accesible a través de los medios descritos en la *DGPC*.

4.10.2. Disponibilidad del servicio

192. La FNMT-RCM garantiza el acceso a este servicio, en horario 24x7, por parte de los *Usuarios* y las partes que confían en los *Certificados*, de forma segura, rápida y gratuita.

4.10.3. Características opcionales

193. No estipuladas.

4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN

194. La suscripción finalizará en el momento de extinción de la vigencia del *Certificado*, ya sea por expiración del periodo de vigencia o por revocación del mismo. De no llevarse a cabo la renovación del *Certificado* se considerará extinguida la relación entre el *Firmante* y la FNMT-RCM.

195. A los efectos enumerados anteriormente, se hace constar que la solicitud de emisión de un *Certificado de Firma Electrónica* emitido por la FNMT-RCM cuando exista otro vigente a favor del mismo *Firmante* y mismo *Suscriptor,* y perteneciente a la misma *Ley de Emisión,* conllevará la revocación del primero obtenido. Lo anteriormente descrito no sucederá en el caso de *Sello de Entidad.*

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1. Prácticas y políticas de custodia y recuperación de claves

196. La FNMT-RCM no recuperará las *Claves privadas* asociadas a los *Certificados*.

4.12.2. Prácticas y políticas de protección y recuperación de la clave de sesión

197. No estipulado.

5. CONTROLES DE SEGURIDAD FÍSICA, DE PROCEDIMIENTOS Y DE PERSONAL

198. Véase el apartado correspondiente en la *DGPC*.

5.1. CONTROLES DE SEGURIDAD FÍSICA

199. Véase el apartado correspondiente en la *DGPC*.

5.1.1. Ubicación de las instalaciones

200. Véase el apartado correspondiente en la *DGPC*.

5.1.2. Acceso Físico

201. Véase el apartado correspondiente en la *DGPC*.

5.1.3. Electricidad y Aire Acondicionado

202. Véase el apartado correspondiente en la *DGPC*.

5.1.4. Exposición al agua

203. Véase el apartado correspondiente en la *DGPC*.

5.1.5. Prevención y Protección contra incendios

204. Véase el apartado correspondiente en la *DGPC*.

5.1.6. Almacenamiento de Soportes

205. Véase el apartado correspondiente en la *DGPC*.

5.1.7. Eliminación de Residuos

206. Véase el apartado correspondiente en la *DGPC*.

5.1.8. Copias de Seguridad fuera de las instalaciones

207. Véase el apartado correspondiente en la *DGPC*.

5.2. CONTROLES DE PROCEDIMIENTO

208. Véase el apartado correspondiente en la *DGPC*.

5.2.1. Roles de Confianza

209. Véase el apartado correspondiente en la *DGPC*.

5.2.2. Número de personas por tarea

210. Véase el apartado correspondiente en la *DGPC*.

5.2.3. Identificación y autenticación para cada rol

211. Véase el apartado correspondiente en la *DGPC*.

5.2.4. Roles que requieren segregación de funciones

212. Véase el apartado correspondiente en la *DGPC*.

5.3. CONTROLES DE PERSONAL

213. Véase el apartado correspondiente en la *DGPC*.

5.3.1. Conocimientos, cualificación, experiencia y requerimientos acreditativos

214. Véase el apartado correspondiente en la *DGPC.*

5.3.2. Procedimientos de verificación de antecedentes

215. Véase el apartado correspondiente en la *DGPC*

5.3.3. Requisitos de formación

216. Véase el apartado correspondiente en la *DGPC*

5.3.4. Requisitos y frecuencia de actuación formativa

217. Véase el apartado correspondiente en la *DGPC*

5.3.5. Secuencia y frecuencia de rotación laboral

218. Véase el apartado correspondiente en la *DGPC.*

5.3.6. Sanciones por acciones no autorizadas

219. Véase el apartado correspondiente en la *DGPC*

5.3.7. Requisitos de contratación de personal

220. Véase el apartado correspondiente en la *DGPC*.

5.3.8. Suministro de documentación al personal

221. Véase el apartado correspondiente en la *DGPC*.

5.4. PROCEDIMIENTOS DE AUDITORÍA

222. Véase el apartado correspondiente en la *DGPC*.

5.4.1. Tipos de eventos registrados

223. Véase el apartado correspondiente en la *DGPC*.

5.4.2. Frecuencia de procesamiento de registros

224. Véase el apartado correspondiente en la *DGPC*.

5.4.3. Periodo de conservación de los registros

225. Véase el apartado correspondiente en la *DGPC*.

5.4.4. Protección de los registros

226. Véase el apartado correspondiente en la *DGPC*.

5.4.5. Procedimientos de copias de seguridad de los registros auditados

227. Véase el apartado correspondiente en la *DGPC*.

5.4.6. Sistemas de recolección de registros

228. Véase el apartado correspondiente en la *DGPC*.

5.4.7. Notificación al sujeto causante de los eventos

229. Véase el apartado correspondiente en la *DGPC*.

5.4.8. Análisis de vulnerabilidades

230. Véase el apartado correspondiente en la *DGPC*.

5.5. ARCHIVADO DE REGISTROS

231. Véase el apartado correspondiente en la *DGPC*.

5.5.1. Tipos de registros archivados

232. Véase el apartado correspondiente en la *DGPC*.

5.5.2. Periodo de retención del archivo

233. Véase el apartado correspondiente en la *DGPC*.

5.5.3. Protección del archivo

234. Véase el apartado correspondiente en la *DGPC*.

5.5.4. Procedimientos de copia de respaldo del archivo

235. Véase el apartado correspondiente en la *DGPC*.

5.5.5. Requisitos para el sellado de tiempo de los registros of Records

236. Véase el apartado correspondiente en la *DGPC*.

5.5.6. Sistema de archivo

237. Véase el apartado correspondiente en la *DGPC*.

5.5.7. Procedimientos para obtener y verificar la información archivada

238. Véase el apartado correspondiente en la *DGPC*.

5.6. CAMBIO DE CLAVES DE LA AC

239. Véase el apartado correspondiente en la *DGPC*.

5.7. GESTIÓN DE INCIDENTES Y VULNERABILIDADES

240. Véase el apartado correspondiente en la *DGPC*.

5.7.1. Gestión de incidentes y vulnerabilidades

241. Véase el apartado correspondiente en la *DGPC*.

5.7.2. Actuación ante datos y software corruptos

242. Véase el apartado correspondiente en la *DGPC*.

5.7.3. Procedimiento ante compromiso de la clave privada de la AC

243. Véase el apartado correspondiente en la *DGPC*.

5.7.4. Continuidad de negocio después de un desastre

244. Véase el apartado correspondiente en la *DGPC*.

5.8. CESE DE LA ACTIVIDAD DEL PRESTADOR DE SERVICIOS DE CONFIANZA

245. Véase el apartado correspondiente en la *DGPC*.

6. CONTROLES DE SEGURIDAD TÉCNICA

246. Véase el apartado correspondiente en la *DGPC*.

6.1. GENERACIÓN E INSTALACIÓN DE LAS CLAVES

6.1.1. Generación del par de claves

6.1.1.1 Generación del par de Claves de la CA

247. En relación con la generación de las *Claves* de AC que la FNMT-RCM necesita para el desarrollo de su actividad como *Prestador de Servicios de Confianza,* véase el apartado correspondiente en la *DGPC*.

6.1.1.2 Generación del par de Claves de la RA

248. No estipulado

6.1.1.3 Generación del par de Claves de los Suscriptores

249. En relación con la generación de las *Claves* del *Suscriptor,* la FNMT-RCM no genera ni almacena las *Claves Privadas* asociadas a los *Certificados* expedidos bajo las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares*, que son generadas bajo el exclusivo control del *Suscriptor*.

6.1.2. Envío de la clave privada al suscriptor

250. No existe ninguna entrega de *Clave privada* en la emisión de los *Certificados* expedidos bajo las presentes *Políticas y Prácticas de Certificación*.

251. En todo caso, si la FNMT-RCM o cualquiera de las oficinas de registro tuviera conocimiento de un acceso no autorizado a la *Clave privada* del *Suscriptor*, el *Certificado* asociado a dicha *Clave privada* será revocado.

6.1.3. Envío de la clave pública al emisor del certificado

252. La *Clave pública,* generada junto a la *Clave privada* en un dispositivo de generación y custodia de claves, es entregada a la *Autoridad de Certificación* mediante el envío de una solicitud de certificación.

6.1.4. Distribución de la clave pública de la AC a las partes que confían

253. Véase el apartado correspondiente en la *DGPC*.

6.1.5. Tamaños de claves y algoritmos utilizados

254. El algoritmo utilizado es RSA con SHA-256.

255. En cuanto al tamaño de las claves, dependiendo de cada caso, es:

- Claves de la AC FNMT raíz: 4.096 bits.
- Claves de la AC Representación Subordinada*:* 2.048 bits.
- Claves de los *Certificados de Firma Electrónica:* 2.048 bits.
- Claves de los *Sellos de Entidad:* 2.048 bits

6.1.6. Parámetros de generación de la clave pública y verificación de la calidad

256. Véase el apartado correspondiente en la *DGPC*.

6.1.7. Usos admitidos de las claves (KeyUsage field X.509v3)

257. Los *Certificados* FNMT incluyen la extensión Key Usage y, según el caso, Extended Key Usage, indicando los usos habilitados de las *Claves*.

258. El *Certificado* de la AC FNMT raíz tiene habilitados los usos de *Claves* para firmar/sellar los *Certificados* de las ACs FNMT Subordinadas y las ARLs.

259. El *Certificado* de la AC FNMT Subordinada que expide los *Certificados de Firma Electrónica* tiene habilitado exclusivamente el uso para firmar/sellar *Certificados* de entidad final y CRLs.

260. Los *Certificados de Firma Electrónica* tienen habilitado exclusivamente los usos de clave de cifrado de claves, autenticación y firma. Cuentan con los usos extendidos de autenticación, Adobe Authentic Documents Trust y Document Signing.

261. *El Sello de Entidad* tiene habilitados los usos de firma, autenticación y cifrado. Cuentan con los usos extendidos de autenticación, Adobe Authentic Documents Trust y Document Signing.

262. *El Sello de Entidad con correo electrónico seguro* tiene habilitados los usos de firma, autenticación y cifrado. Cuentan con los usos extendidos de autenticación y protección de correo.

6.2. PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE LOS MÓDULOS CRIPTOGRÁFICOS

6.2.1. Estándares para los módulos criptográficos

263. Véase el apartado correspondiente en la *DGPC*.

6.2.2. Control multi-persona (n de m) de la clave privada

264. Véase el apartado correspondiente en la *DGPC*.

6.2.3. Custodia de la clave privada

265. Las operaciones de copia, salvaguarda o recuperación de las *Claves privadas* de las *Autoridades de Certificación* de la FNMT-RCM se realizan bajo control exclusivo del personal autorizado, usando, al menos, control dual y en un entorno seguro.

6.2.4. Copia de seguridad de la clave privada

266. Véase el apartado correspondiente en la *DGPC*.

6.2.5. Archivado de la clave privada

267. Véase el apartado correspondiente en la *DGPC*.

6.2.6. Trasferencia de la clave privada a o desde el módulo criptográfico

268. Véase el apartado correspondiente en la *DGPC*.

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

269. Véase el apartado correspondiente en la *DGPC*.

6.2.8. Método de activación de la clave privada

270. Las *Claves privadas* de las *Autoridades de Certificación* son generadas y custodiadas por un dispositivo criptográfico que cumple los requisitos de seguridad FIPS PUB 140-2 Level 3.

271. Los mecanismos de activación y uso de las *Claves privadas* de la *Autoridad de Certificación* se basan en la segmentación de roles de gestión y operación que la FNMT-RCM tiene implementados con mecanismos de acceso multipersona basados en tarjetas criptográficas y sus correspondientes pines en un esquema de uso simultaneo M de N (2 de 5).

6.2.9. Método de desactivación de la clave privada

272. Véase el apartado correspondiente en la *DGPC*.

6.2.10. Método de destrucción de la clave privada

273. La FNMT-RCM destruirá o almacenará de forma apropiada las Claves del *Prestador de Servicios de Confianza* una vez finalizado el período de validez de las mismas, con la finalidad de evitar su uso inapropiado.

6.2.11. Clasificación de los módulos criptográficos

274. Véase el apartado correspondiente en la *DGPC*.

6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

6.3.1. Archivo de la clave pública

275. Véase el apartado correspondiente en la *DGPC*.

6.3.2. Periodos de operación del certificado y periodos de uso del par de claves

276. Los periodos de operación de los *Certificados* y sus *Claves* asociadas son:

- *Certificado* de la AC FNMT raíz y su par de *Claves*: hasta el 1 de enero de 2030.
- El *Certificado* de la AC subordinada que expide los *Certificados de Firma Electrónica*: hasta el 31 de diciembre de 2029.
- Los *Certificados de Firma Electrónica* y su par de *Claves:* no superior a 2 años.
- Los *Sellos de Entidad* y su par de claves: no superior a 3 años.

6.4. DATOS DE ACTIVACIÓN

6.4.1. Generación e instalación de datos de activación

277. Los datos de activación, tanto de las *Claves* de la AC FNMT raíz como de las *Claves* de la AC subordinada que expide los *Certificados de Firma Electrónica,* se generan durante la ceremonia de *Claves* de creación de dichas *Autoridades de Certificación*.

6.4.2. Protección de datos de activación

278. Los datos de activación de las *Claves privadas* de la *Autoridad de Certificación* están protegidos, conforme al método descrito en el apartado "6.2.8 Método de activación de la *Clave privada*" del presente documento, con mecanismos de acceso multipersona basados en tarjetas criptográficas y sus correspondientes pines en un esquema de uso simultaneo M de N (2 de 5).

6.4.3. Otros aspectos de los datos de activación

279. No estipulados.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

280. Véase el apartado correspondiente en la *DGPC*.

6.5.1. Requisitos técnicos específicos de seguridad informática

281. Véase el apartado correspondiente en la *DGPC*.

6.5.2. Evaluación del nivel de seguridad informática

282. Véase el apartado correspondiente en la *DGPC*.

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA

283. Véase el apartado correspondiente en la *DGPC*.

6.6.1. Controles de desarrollo de sistemas

284. Véase el apartado correspondiente en la *DGPC*.

6.6.2. Controles de gestión de la seguridad

285. Véase el apartado correspondiente en la *DGPC*.

6.6.3. Controles de seguridad del ciclo de vida

286. Véase el apartado correspondiente en la *DGPC*.

6.7. CONTROLES DE SEGURIDAD DE RED

287. Véase el apartado correspondiente en la *DGPC*.

6.8. FUENTE DE TIEMPO

288. Véase el apartado correspondiente en la *DGPC*.

6.9. OTROS CONTROLES ADICIONALES

289. Véase el apartado correspondiente en la *DGPC*.

6.9.1. Control de la capacidad de prestación de los servicios

290. Véase el apartado correspondiente en la *DGPC*.

6.9.2. Control de desarrollo de sistemas y aplicaciones informáticas

291. Véase el apartado correspondiente en la *DGPC*.

7. PERFILES DE LOS CERTIFICADOS, CRLS Y OCSP

7.1. PERFIL DEL CERTIFICADO

292. Los *Certificados de Firma Electrónica* son expedidos como "cualificados" de conformidad con 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".

293. Los *Sellos de entidad* son expedidos como "cualificados" de conformidad con los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 412-3 "Certificate profile for certificates issued to legal persons"

294. Adicionalmente, los *Certificados con correo electrónico seguro* son expedidos de conformidad con los requisitos establecido por el estándar europeo ETSI TS 119 411-6 "Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates".

7.1.1. Número de versión

295. Los *Certificados* son conformes con el estándar X.509 versión 3.

7.1.2. Extensiones del certificado

296. En la página http://www.cert.fnmt.es/dpcs/ se publica el documento que describe el perfil de los *Certificados* emitidos bajo esta política, incluyendo todas sus extensiones.

7.1.3. Identificadores de objeto de algoritmos

297. El identificador de objeto (OID) correspondiente al algoritmo criptográfico utilizado (SHA-256 with RSA Encryption) es 1.2.840.113549.1.1.11

7.1.4. Formatos de nombres

298. 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.

299. En la página http://www.cert.fnmt.es/dpcs/ se publica el documento que describe el perfil de los *Certificados* emitidos bajo esta política, incluyendo todas sus extensiones.

7.1.5. Restricciones de nombres

300. El nombre distintivo (*DN*) asignado al *Sujeto* del *Certificado*, en el ámbito de la presente *DPPP*, será único y con la composición definida en el perfil del *Certificado*.

7.1.6. Identificador de objeto de política de certificado

301. El identificador de objeto (OID) de la política de los *Certificados* es la definida en el apartado "1.2 Nombre del documento e identificación" del presente documento.

7.1.7. Empleo de la extensión restricciones de política

302. La extensión "Policy Constrains" del *Certificado* raíz de la AC no es utilizado.

7.1.8. Sintaxis y semántica de los calificadores de política

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

- CPS Pointer: contiene la URL donde se publican las *Políticas de Certificación* y *Prácticas de Servicios de confianza* aplicables a este servicio.
- User notice: contiene un texto que puede ser desplegado en la pantalla del usuario del *Certificado* durante la verificación del mismo.

7.1.9. Tratamiento semántico para la extensión "certificate policy"

304. 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.

7.2. PERFIL DE LA CRL

7.2.1. Número de versión

305. El perfil de las CRL son conformes con el estándar X.509 versión 2.

7.2.2. CRL y extensiones

306. El perfil de las CRL sigue la siguiente estructura:

Tabla 3 – Perfil de la CRL

Campos y extensiones	Valor
Versión	V2
Algoritmo de firma	Sha256WithRSAEncryption
Número de CRL	Valor incremental
Emisor	DN del emisor
Fecha de emisión	Tiempo UTC de emisión.
Fecha de próxima actualización	Fecha de emisión + 24 horas
Identificador de la clave de Autoridad	Hash de la clave del emisor
Punto de distribución	URLs del punto de distribución y ámbito de las CRLs
ExpiredCertsOnCRL	NotBefore de la CA
Certificados revocados	Lista de certificados revocados, conteniendo al menos para cada entrada, número de serie y fecha de revocación

7.3. PERFIL DE OCSP

7.3.1. Número de versión

307. Véase el apartado correspondiente en la *DGPC*.

7.3.2. Extensiones del OCSP

308. Véase el apartado correspondiente en la *DGPC*.

8. AUDITORÍAS DE CUMPLIMIENTO

309. El sistema de expedición de *Certificados* es sometido anualmente a un proceso de auditoría conforme a los estándares europeos ETSI EN 319 401 "General Policy Requirements for Trust Service Providers" y ETSI EN 319 411-1 "Policy and security requirements for Trust Service Providers issuing certificates".

310. Así mismo, los *Certificados* tienen la consideración de cualificados, por lo que la auditoría garantiza el cumplimiento con los requisitos establecidos en los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates".

311. Un auditor independiente evaluará anualmente el cumplimiento por parte de la CA de los requisitos y prácticas establecidos en esta DPC y/o los requisitos básicos y las pautas establecidas en CAB Forum's S/MIME Baseline Requirements.

8.1. FRECUENCIA DE LAS AUDITORÍAS

312. Periódicamente se elaborarán los correspondientes planes de auditorías que contemplarán como mínimo la realización de las siguientes acciones:

- Análisis de riesgos conforme a lo dictado en el Sistema de Gestión de la Seguridad de la Información: Una revisión anual y un análisis completo cada tres (3) años
- Revisión del Sistema de Gestión de la Seguridad de la Información conforme a UNE-ISO/IEC 27001 "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos"
- Calidad: ISO 9001: Una parcial anual externa más una auditoría anual interna preparatoria y una total externa cada tres (3) años, para mantenimiento de la certificación.
- Protección de datos: Una cada dos (2) años interna a realizar por el Departamento de Sistemas de Información.

313. La *Autoridad de Certificación* que expide los *Certificados de Firma Electrónica y Sello de Entidad* está sujeta a auditorías periódicas, de conformidad con el estándar europeo ETSI EN 319 401 "General Policy Requirements for Trust Service Providers", 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" o ETSI EN 319 412-3 "Certificate profile for certificates issued to legal persons" respectivamente. La auditoría es realizada anualmente por una empresa externa acreditada.

- Una auditoría cada dos (2) años de los sistemas de información de la FNMT-RCM que emplea para la prestación de Servicios de Confianza y conforme a lo dictaminado en el Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica).

314. La frecuencia del resto de auditorías adicionales, será conforme a lo estipulado en la normativa vigente correspondiente y con CAB Forum's S/MIME Baseline Requirements.

8.2. CUALIFICACIÓN DEL AUDITOR

315. Véase el apartado correspondiente en la *DGPC*.

8.3. RELACIÓN DEL AUDITOR CON LA EMPRESA AUDITADA

316. Véase el apartado correspondiente en la *DGPC*.

8.4. ELEMENTOS OBJETOS DE AUDITORÍA

317. Véase el apartado correspondiente en la *DGPC*.

8.5. TOMA DE DECISIONES FRENTE A DETECCIÓN DE DEFICIENCIAS

318. Véase el apartado correspondiente en la *DGPC*.

8.6. COMUNICACIÓN DE LOS RESULTADOS

319. Véase el apartado correspondiente en la *DGPC*.

8.7. AUTOEVALUACIÓN

320. Véase el apartado correspondiente en la *DGPC*.

9. OTROS ASUNTOS LEGALES Y DE ACTIVIDAD

9.1. TARIFAS

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

322. Véase el apartado correspondiente en la *DGPC*.

9.1.1. Tarifas de emisión o renovación de certificados

323. Véase el apartado correspondiente en la *DGPC*.

9.1.2. Tarifas de acceso a los certificados

324. No estipulado.

9.1.3. Tarifas de acceso a la información de estado o revocación

325. La FNMT-RCM ofrece los servicios de información del estado de los certificados a través de CRL o del OCSP de forma gratuita.

9.1.4. Tarifas para otros servicios

326. Véase el apartado correspondiente en la *DGPC*.

9.1.5. Política de reembolso

327. La FNMT – RCM cuenta con una política de devolución que permite la solicitud de reembolso dentro del período de desistimiento establecido, aceptando que este hecho llevará consigo la revocación automática del certificado. El procedimiento se publica en la sede electrónica de la FNMT – RCM.

9.2. RESPONSABILIDAD FINANCIERA

328. Véase el apartado correspondiente en la *DGPC*.

9.2.1. Seguro de responsabilidad civil

329. Véase el apartado correspondiente en la *DGPC*.

9.2.2. Otros activos

330. Véase el apartado correspondiente en la *DGPC*.

9.2.3. Seguros y garantías para entidades finales

331. Véase el apartado correspondiente en la *DGPC*.

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

332. Véase el apartado correspondiente en la *DGPC*.

9.3.1. Alcance de la información confidencial

333. Véase el apartado correspondiente en la *DGPC*.

9.3.2. Información no incluida en el alcance

334. Véase el apartado correspondiente en la *DGPC*.

9.3.3. Responsabilidad para proteger la información confidencial

335. Véase el apartado correspondiente en la *DGPC*.

9.4. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

336. Véase el apartado correspondiente en la *DGPC*.

9.4.1. Plan de privacidad

337. Véase el apartado correspondiente en la *DGPC*.

9.4.2. Información tratada como privada

338. Véase el apartado correspondiente en la *DGPC*.

9.4.3. Información no considerada privada

339. Véase el apartado correspondiente en la *DGPC*.

9.4.4. Responsabilidad de proteger la información privada

340. Véase el apartado correspondiente en la *DGPC*.

9.4.5. Aviso y consentimiento para usar información privada

341. Véase el apartado correspondiente en la *DGPC*.

9.4.6. Divulgación conforme al proceso judicial o administrativo

342. Véase el apartado correspondiente en la *DGPC*.

9.4.7. Otras circunstancias de divulgación de información

343. Véase el apartado correspondiente en la *DGPC*.

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

344. Véase el apartado correspondiente en la *DGPC*.

9.6. OBLIGACIONES Y GARANTÍAS

9.6.1. Obligaciones de la AC

345. Las obligaciones y responsabilidades de la FNMT-RCM, como *Prestador de Servicios de Confianza*, con el *Titular* del *Certificado* 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*.

346. La FNMT-RCM, a través de la *Oficina de Registro*, responde de la correcta identificación de la *Entidad representada* y del *Representante*, comprobando la legalidad extrínseca de los documentos aportados para acreditar el alcance de su representación, incluyendo una indicación de esta información en el *Certificado*

347. En el proceso de registro para los *Certificados de Representante para administradores únicos y solidarios*, comprobar los datos relativos a las facultades de representación (administrador único o solidario) del *Representante*, así como la existencia y la personalidad jurídica de la entidad, según la información suministrada por el CORPME. Todas estas comprobaciones se realizarán según lo dispuesto en las *Prácticas de Certificación Particulares* expresadas en este documento y según los protocolos y procedimientos de registro de la FNMT-RCM.

348. La FNMT – RCM cumple los requisitos de las especificaciones técnicas de la norma ETSI EN 319 411-2 para la emisión de *Certificados* cualificados y se compromete a continuar cumpliendo con dicha norma o aquellas que la sustituyan.

349. La FNMT-RCM emite los *Certificados con correo electrónico seguro* de conformidad con el estándar europeo ETSI TS 119 411-6 y S/MIME Baseline Requirements (SBR), requisitos establecidos por la entidad CA/Browser Forum y que pueden consultarse en la dirección https://cabforum.org/smime-br/. Asimismo, adaptará sus prácticas de expedición de dichos Certificados a la versión vigente de los citados requisitos. En caso de cualquier incoherencia entre la presente DPC y la citada versión, dichos requisitos prevalecerán sobre este documento.

350. Véase el apartado correspondiente en la *DGPC*.

9.6.2. Obligaciones de la AR

351. 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*, 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.

352. 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.

353. Véase el apartado correspondiente en la *DGPC*.

9.6.3. Obligaciones del suscriptor

354. 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.

355. No solicitar *Certificados* conteniendo signos distintivos, denominaciones o derechos protegidos por las normas sobre propiedad industrial o intelectual de las que no sea titular, licenciatario o cuente con autorización demostrable para su uso.

356. 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*.

357. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la *DGPC*, el *Titular* del *Certificado*, como *Suscriptor* del *Certificado* y sus *Claves*, tiene la obligación de:

- No usar el *Certificado* fuera de los límites especificados en las presentes *Política y Prácticas de Certificación* particulares.
- 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*.
- 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.
- Actuar con diligencia respecto de la custodia y conservación de los Datos de creación de Firma o cualquier otra información sensible como Claves, códigos de activación del *Certificado*, palabras de acceso, números de identificación personal, etc., así como de los soportes de los *Certificados*, lo que comprende en todo caso, la no revelación de ninguno de los datos mencionados.
- Conocer y cumplir las condiciones de utilización de los *Certificados* previstas en las condiciones de uso y en la Declaración de Prácticas de Certificación y en particular, las limitaciones de uso de los *Certificados*.
- Conocer y cumplir las modificaciones que se produzcan en la Declaración de Prácticas de Certificación.

358. 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.

359. 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.

360. 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.

9.6.4. Obligaciones de las partes que confían

361. Véase el apartado correspondiente en la *DGPC*.

9.6.5. Obligaciones de otros participantes

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

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

9.7. RENUNCIA DE GARANTÍAS

364. No estipulado.

9.8. LIMITACIONES DE RESPONSABILIDAD

365. La FNMT-RCM no será responsable de cualesquiera daños producidos, a la *Entidad representada* o a terceros, por parte del *Solicitante* en caso de que infrinja las obligaciones de aportar documentación fidedigna o la aportada contenga inexactitudes, errores o falsedades y se produzca la expedición del *Certificado*. FNMT-RCM tampoco será responsable si el *Representante* utilizara indebidamente el *Certificado*, en caso de falta de vigencia, capacidad insuficiente, caducidad, revocación, extinción de su apoderamiento o lo utilizara más allá de su ámbito de aplicación inicial.

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

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

368. Véase el apartado correspondiente en la *DGPC*.

9.9. INDEMNIZACIONES

369. Véase el apartado correspondiente en la *DGPC*.

9.9.1. Indemnización de la CA

370. No estipulado.

9.9.2. Indemnización de los Suscriptores

371. No estipulado.

9.9.3. Indemnización de las partes que confían

372. No estipulado.

9.10. PERIODO DE VALIDEZ DE ESTE DOCUMENTO

9.10.1. Plazo

373. La presente *Declaración de Prácticas y Políticas de Certificación* entrará en vigor en el momento de su publicación.

9.10.2. Terminación

374. La presente *Declaración de Prácticas y Políticas de Certificación* será derogada en el momento que una nueva versión del documento sea publicada. La nueva versión sustituirá íntegramente al documento anterior. La FNMT – RCM se compromete a someter dicha Declaración a un proceso de revisión anual.

9.10.3. Efectos de la finalización

375. Para los *Certificados* vigentes emitidos bajo una *Declaración de Prácticas y Políticas de Certificación* anterior, la nueva versión prevalecerá a la anterior en todo lo que no se oponga a ésta.

9.11. NOTIFICACIONES INDIVIDUALES Y COMUNICACIÓN CON LOS PARTICIPANTES

376. Véase el apartado correspondiente en la *DGPC*.

9.12. MODIFICACIONES DE ESTE DOCUMENTO

9.12.1. Procedimiento para las modificaciones

377. Véase el apartado correspondiente en la *DGPC*.

9.12.2. Periodo y mecanismo de notificación

378. Véase el apartado correspondiente en la *DGPC*.

9.12.3. Circunstancias bajo las cuales debe cambiarse un OID

379. Véase el apartado correspondiente en la *DGPC*.

9.13. RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS

380. Véase el apartado correspondiente en la *DGPC*.

9.14. NORMATIVA DE APLICACIÓN

381. Véase el apartado correspondiente en la *DGPC*.

9.15. CUMPLIMIENTO DE LA NORMATIVA APLICABLE

382. La FNMT-RCM manifiesta el cumplimiento de la normativa de aplicación.

9.16. ESTIPULACIONES DIVERSAS

383. Véase el apartado correspondiente en la *DGPC*.

9.16.1. Acuerdo íntegro

384. Véase el apartado correspondiente en la *DGPC*.

9.16.2. Asignación

385. Véase el apartado correspondiente en la *DGPC*.

9.16.3. Severabilidad

386. Véase el apartado correspondiente en la *DGPC*.

9.16.4. Cumplimiento

387. Véase el apartado correspondiente en la *DGPC*.

9.16.5. Fuerza Mayor

388. Véase el apartado correspondiente en la *DGPC*.

9.17. OTRAS ESTIPULACIONES

389. No se contemplan.