Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

POLÍTICAS Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS CERTIFICADOS DE SELLO PARA ENTIDADES

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM	19/01/2026
Revisado por:	FNMT-RCM	19/01/2026
Aprobado por:	FNMT-RCM	19/01/2026

Versión	Fecha	Descripción
1.0	19/01/2026	Creación del documento

Referencia: DPC/CPSEL0100/SGPSC/2026

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 de los *Certificados de 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.

1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

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

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

   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.

6. 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 del *Sello de Entidad*.

7. 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 Sello de Entidad*

Referencia / OID[1]: 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 G2*

Referencia / OID: 1.3.6.1.4.1.5734.3.22.1.0

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

Versión: 1.0

Fecha de expedición: 19/01/2026

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/

[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.

8. 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.

9. La presente Declaración de *Política y Prácticas de Certificación Particulares* aplica a los Sellos de Entidad y tendrán prelación sobre lo dispuesto en el cuerpo principal de la *DGPC*.

10. 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

11. 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

12. 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, jerarquía RSA: dicha Autoridad expide exclusivamente *Certificados* de Autoridades de Certificación subordinadas con algoritmia RSA. 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
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, jerarquía RSA: 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

Certificado de la AC subordinada	
Algoritmo de firma	RSA – SHA256
Identificador de clave	DC 50 96 9F D7 31 89 C9 11 E4 EF 96 5F F6 5F 82 52 46 62 53

c) Autoridad de Certificación raíz, jerarquía de curvas elípticas: dicha Autoridad expide exclusivamente *Certificados* de Autoridades de Certificación subordinadas son algoritmia de curva elíptica. El *Certificado* raíz de esta AC viene identificado por la siguiente información:

Tabla 3 – Certificado de la AC FNMT raíz G2

Certificado de la AC RAÍZ FNMT-RCM G2	
Sujeto	CN=AC RAIZ FNMT-RCM G2,ORG_ID=VATES-Q2826004J,O=FNMT-RCM, C=ES
Emisor	CN=AC RAIZ FNMT-RCM G2,ORG_ID=VATES-Q2826004J,O=FNMT-RCM, C=ES
Número de serie (hex)	1F B6 4F 91 9E C5 01 EA B1 21 28 BB 11 7A 00 3C 7C 5A EF 1A
Validez	No antes: 10 de Octubre de 2024. No después: 4 de Octubre de 2049
Longitud clave pública	EC 384 bits (P-384)
Algoritmo de firma	SHA-384 con ECDSA
Identificador de clave	E2 29 99 47 2A FF 5B 26 8A C8 34 41 66 45 AF 52 3A 08 F1 80

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

Tabla 4 – Certificado de la AC subordinada G2

Certificado de la AC subordinada	
Sujeto	CN=AC ENTIDADES G2,ORG_ID=VATES-Q2826004J,O=FNMT-RCM,C=ES
Emisor	CN=AC RAIZ FNMT-RCM G2,ORG_ID=VATES-Q2826004J, O=FNMT-RCM,C=ES
Número de serie (hex)	18 BF C8 71 81 3B C9 80 31 03 F1 5B 70 50 70 C0 56 20 4F 3D
Validez	No antes: 10 de octubre de 2024 No después: 07 de octubre de 2039
Longitud clave pública	EC 256 bits (P-256)
Algoritmo de firma	SHA-384 con ECDSA
Identificador de clave	E5 36 ED E0 98 12 92 DA 14 1B AE E1 97 50 98 FF 05 C9 5B 30

1.3.2. Autoridad de Registro

13. 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*.

14. 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

15. 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

16. 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

17. No estipulado.

1.4. USO DE LOS CERTIFICADOS

1.4.1. Usos permitidos de los certificados

18. 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 .

1.4.2. Restricciones en el uso de los certificados

19. En cualquier caso, si una *Entidad usuaria* o un tercero desean confiar en la *Firma o Sello electrónicos* realizados 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*.

20. 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

21. 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

22. 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

23. 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

24. 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

25. 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

26. 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 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.
- *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*.
- *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

27. 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)

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

28. 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

29. 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

30. 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.

31. 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

32. 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

33. 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

34. 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*.

35. En el procedimiento de acreditación de la identidad, como paso previo a la expedición de un *Certificado de Sello de Entidad,* 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

36. 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).

37. El campo Common Name de los *Certificados de Sello 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.

3.1.3. Seudónimos

38. 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

39. 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

40. El nombre distintivo (*DN*) asignado a los *Certificados* expedidos a un *Suscriptor*, 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

41. 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

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

3.2.2. Autenticación de la identidad de la organización

43. La FNMT-RCM, como *Prestador de Servicios de Confianza*, antes de expedir el *Certificado* identificará al *Solicitante* del mismo, así como los datos relativos a la personalidad jurídica de la *Entidad representada* y a la extensión y vigencia de sus facultades de representación del

Representante, mediante 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*.

44. 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).

45. 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).

46. 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.

47. 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.

48. 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.

49. 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).

3.2.3. Autenticación de la identidad de la persona física solicitante

50. La FNMT-RCM, como Prestador de Servicios de Confianza, antes de expedir un *Certificado de Sello de Entidad* identificará al *Solicitante* del mismo, comprobando mediante la utilización de un *Certificado cualificado de firma electrónica* que confirme la identidad de la persona física solicitante.

3.2.4. Información no verificada del Suscriptor

51. Toda la información incorporada al *Certificado de Sello de Entidad* es verificada por la *Autoridad de Registro*.

3.2.5. Validación de la autorización

52. La AR de la FNMT-RCM verifica que el *Solicitante* tiene suficiente capacidad de representación mediante la firma electrónica del formulario de solicitud, según se describe en el apartado 3.2.3 de la presente *DPPP*, aceptando el uso de un *Certificado* cualificado de representante de administrador único o solidario de la persona jurídica suscriptora o un *Certificado* cualificado de *Personal al servicio de la Administración Pública*, para cuya expedición ha sido acreditada la capacidad de representación.

53. Cuando el citado formulario se firma mediante un *Certificado* cualificado diferente de los mencionados en el párrafo anterior, la AR de la FNMT-RCM comprueba la facultad de representación del firmante de la solicitud mediante consulta a registros oficiales (Registro Mercantil, Boletines Oficiales, etc. en función de la naturaleza de la representación). Si del resultado de estas consultas no se obtuvieran evidencias de representación suficiente, la AR de la FNMT-RCM se pondrá en contacto con el *Suscriptor* para recabar dichas evidencias.

3.2.6. Criterios de interoperación

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

3.2.7. Fiabilidad de las fuentes de verificación

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

56. 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

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

58. 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

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

3.3.2. Renovación después de una revocación

60. 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

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

62. 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

63. Únicamente podrán solicitar *Certificados de Sello de Entidad* los *Representantes del Suscriptor*, o personas debidamente autorizados a solicitar el Certificado en nombre del *Suscriptor.*

4.1.2. Proceso de registro y responsabilidades

64. 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.*

65. 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.

66. 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.

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

68. El apartado 9.6 "Obligaciones y garantías" del presente documento establece las responsabilidades de las partes en este proceso.

4.2. PROCEDIMIENTO DE SOLICITUD DE CERTIFICADOS

4.2.1. Realización de las funciones de identificación y autenticación

69. 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*.

4.2.2. Aprobación o rechazo de la solicitud del certificado

70. La Autoridad de Registro que actúa en el proceso de expedición de Certificados es siempre la propia FNMT-RCM y, por tanto, no delega la validación a ninguna otra Autoridad de Registro.

71. La Autoridad de Registro de la FNMT-RCM, una vez realizadas las comprobaciones relativas a la prueba de posesión de la clave privada por parte del Representante del Suscriptor, así como la autenticación de la identidad de la Organización y de la persona *Solicitante* del Certificado, según se describe en el apartado "3.2 Validación inicial de la identidad" de la presente DPPP, determinará la aprobación o el rechazo de la solicitud del mismo.

72. En caso de que la información sea incorrecta o no se pueda confirmar, la AR rechazará la solicitud y se reservará el derecho de no revelar los motivos de dicha denegación. De lo contrario, se procederá a la emisión del certificado.

73. 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.

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

4.2.3. Tiempo en procesar la solicitud

75. Para el caso de los *Certificados de Sello 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. La FNMT-RCM pondrá a disposición del Solicitante un mecanismo de descarga del *Certificado.*

4.3. EMISIÓN DEL CERTIFICADO

4.3.1. Acciones de la AC durante la emisión

76. 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 de Sello de Entidad*.

77. La expedición de los *Certificados de Sello de Entidad* supone la generación de documentos electrónicos que confirman la identidad del *Suscriptor, y la persona física representante de la entidad suscriptora del Certificado,* 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.

78. La FNMT-RCM, por medio de su *Firma electrónica* o *Sello Electrónico* autentica los *Certificados* y confirma la identidad del *Suscriptor*. 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*.

79. 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*.

80. 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.

81. La emisión de los *Certificados de Sellos de Entidad* atenderá a:

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

   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.

   El atributo *CN* contiene la denominación del sistema o de la aplicación del proceso automático para el que se expide el *Certificado.*

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

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

- en el subcampo DirectoryName, el nombre, denominación del componente y el NIF de la *Entidad representada*.

3. Generación del *Certificado de Sello de Entidad* conforme al Perfil del *Certificado de Sello Electrónico* correspondiente

82. 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

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

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1. Proceso de aceptación

84. 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.

85. En este proceso guiado de descarga de un *Certificado de Sello de Entidad*, se le pedirá al *Representante del Suscriptor* que introduzca el nombre del componente, así como el correspondiente código de solicitud obtenido en dicho proceso.

86. Si el *Certificado de Sello de Entidad* aún no hubiera sido generado por cualquier motivo, el proceso le informará de este hecho.

4.4.2. Publicación del certificado por la AC

87. 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

88. 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

89. 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*.

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

90. Los terceros que confían en las *Sellos electrónicos* 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

91. 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

92. 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

93. 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

94. 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

95. 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

96. 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

97. 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

98. 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

99. Bajo las presentes Políticas de Certificación, la renovación con regeneración de claves de los Certificados se realiza siempre emitiendo nuevas claves, siguiendo el mismo proceso que el descrito para la emisión de un Certificado nuevo.

4.7.1. Circunstancias para la renovación con regeneración de claves

100. 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

101. 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

102. 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

103. 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

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

4.7.6. Publicación del certificado renovado

105. 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

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

4.8. MODIFICACIÓN DEL CERTIFICADO

107. 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

108. No se estipula la modificación.

4.8.2. Quién puede solicitar la modificación del certificado

109. No se estipula la modificación.

4.8.3. Procesamiento de solicitudes de modificación del certificado

110. No se estipula la modificación.

4.8.4. Notificación de la modificación del certificado

111. No se estipula la modificación.

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

112. No se estipula la modificación.

4.8.6. Publicación del certificado modificado

113. No se estipula la modificación.

4.8.7. Notificación de la modificación del certificado a otras entidades

114. No se estipula la modificación.

4.9. REVOCACIÓN Y SUSPENSIÓN DEL CERTIFICADO

115. 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.

116. 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*.

117. 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

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

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

a) La solicitud de revocación por parte de las personas autorizadas. En todo caso deberá dar lugar a esta solicitud:

- La utilización por un tercero de la Clave Privada asociada al *Certificado.*
- La violación o puesta en peligro del secreto de los *Datos de Creación de Firma* o de la clave privada asociada al *Certificado.*
- La no aceptación de las nuevas condiciones que puedan suponer la expedición de nuevas *Declaraciones de Prácticas y Políticas de Certificación*, durante el periodo de un mes tras su publicación

b) Resolución judicial o administrativa que así lo ordene.

c) Extinción o disolución de la personalidad jurídica del *Suscriptor*

d) Fallecimiento o incapacidad sobrevenida, total o parcial, del *Firmante* o del representante del *Suscriptor.*

e) 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 éste ya no fuera conforme a la realidad.

f) Contravención de una obligación sustancial de esta *Declaración de Prácticas y Políticas de Certificación* por parte del *Firmante* o del *Solicitante* del *Certificado* o por parte de una *Oficina de Registro* si, en este último caso, hubiese podido afectar al procedimiento de emisión del *Certificado*

g) Violación o puesta en peligro del secreto de los Datos de Creación de Firma o de la Clave Privada.

h) Resolución del contrato suscrito entre el *Firmante* o el Suscriptor y la FNMT-RCM.

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

j) 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.

k) 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 DPPP, 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.

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

121. 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 la revocación se debiera haber efectuado por haberse extinguido el contrato suscrito con el *Suscriptor.*
- Que las causas c) a i) del presente apartado le sean acreditadas fehacientemente, previa identificación de la *Entidad representada, Representante* y/o *Solicitante* de la revocación (o persona con facultades de representación suficientes, si se produjera el cese o la incapacidad sobrevenida del *Representante*).

122. 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.

123. La revocación de los *Certificados* implica, además de su extinción y la imposibilidad de seguir utilizando los *Datos de creación de firma y Sello* 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

124. 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

125. 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.

126. La FNMT-RCM podrá revocar de oficio los *Certificados* en los supuestos recogidos en la presente Declaración de Prácticas y Políticas de Certificación.

4.9.3. Procedimiento de solicitud de la revocación

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

128. El proceso de revocación puede realizarse de forma ininterrumpida 24x7, a través 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.

129. 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.

130. Adicionalmente, se puede solicitar la revocación de cualquier *Sello de Entidad*, dirigiendo 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.

131. Si la persona solicitante no puede aportar los datos requeridos o se determina que no está capacitada para solicitar la revocación, la solicitud de revocación será desestimada.

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

133. 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.

134. 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

135. 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

136. 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.

137. 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.

138. 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.

139. 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

140. 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

141. Las *Listas de Revocación* (*CRL*) de los *Sellos 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

142. 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

143. 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

144. La comprobación en línea del estado de revocación de los *Certificados de 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

145. No definidas.

4.9.12. Requisitos especiales de revocación de claves comprometidas

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

4.9.13. Circunstancias para la suspensión

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

4.9.14. Quién puede solicitar la suspensión

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

4.9.15. Procedimiento para la petición de la suspensión

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

4.9.16. Límites sobre el periodo de suspensión

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

4.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE LOS CERTIFICADOS

4.10.1. Características operativas

151. 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

152. 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

153. No estipuladas.

4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN

154. 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.

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1. Prácticas y políticas de custodia y recuperación de claves

155. 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

156. No estipulado.

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

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

5.1. CONTROLES DE SEGURIDAD FÍSICA

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

5.1.1. Ubicación de las instalaciones

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

5.1.2. Acceso Físico

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

5.1.3. Electricidad y Aire Acondicionado

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

5.1.4. Exposición al agua

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

5.1.5. Prevención y Protección contra incendios

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

5.1.6. Almacenamiento de Soportes

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

5.1.7. Eliminación de Residuos

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

5.1.8. Copias de Seguridad fuera de las instalaciones

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

5.2. CONTROLES DE PROCEDIMIENTO

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

5.2.1. Roles de Confianza

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

5.2.2. Número de personas por tarea

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

5.2.3. Identificación y autenticación para cada rol

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

5.2.4. Roles que requieren segregación de funciones

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

5.3. CONTROLES DE PERSONAL

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

5.3.1. Conocimientos, cualificación, experiencia y requerimientos acreditativos

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

5.3.2. Procedimientos de verificación de antecedentes

174. Véase el apartado correspondiente en la *DGPC*

5.3.3. Requisitos de formación

175. Véase el apartado correspondiente en la *DGPC*

5.3.4. Requisitos y frecuencia de actuación formativa

176. Véase el apartado correspondiente en la *DGPC*

5.3.5. Secuencia y frecuencia de rotación laboral

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

5.3.6. Sanciones por acciones no autorizadas

178. Véase el apartado correspondiente en la *DGPC*

5.3.7. Requisitos de contratación de personal

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

5.3.8. Suministro de documentación al personal

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

5.4. PROCEDIMIENTOS DE AUDITORÍA

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

5.4.1. Tipos de eventos registrados

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

5.4.2. Frecuencia de procesamiento de registros

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

5.4.3. Periodo de conservación de los registros

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

5.4.4. Protección de los registros

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

5.4.5. Procedimientos de copias de seguridad de los registros auditados

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

5.4.6. Sistemas de recolección de registros

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

5.4.7. Notificación al sujeto causante de los eventos

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

5.4.8. Análisis de vulnerabilidades

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

5.5. ARCHIVADO DE REGISTROS

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

5.5.1. Tipos de registros archivados

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

5.5.2. Periodo de retención del archivo

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

5.5.3. Protección del archivo

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

5.5.4. Procedimientos de copia de respaldo del archivo

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

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

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

5.5.6. Sistema de archivo

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

5.5.7. Procedimientos para obtener y verificar la información archivada

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

5.6. CAMBIO DE CLAVES DE LA AC

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

5.7. GESTIÓN DE INCIDENTES Y VULNERABILIDADES

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

5.7.1. Gestión de incidentes y vulnerabilidades

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

5.7.2. Actuación ante datos y software corruptos

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

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

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

5.7.4. Continuidad de negocio después de un desastre

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

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

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

6. CONTROLES DE SEGURIDAD TÉCNICA

205. 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

206. 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

207. No estipulado

6.1.1.3 Generación del par de Claves de los Suscriptores

208. 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

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

210. 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

211. 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

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

6.1.5. Tamaños de claves y algoritmos utilizados

213. Los algoritmos utilizados bajo el ámbito de la presente DPPP son:

- RSA con SHA 256.
- ECDSA con SHA-384 y ECDSA con SHA-256.

214. En cuanto al tamaño de las claves son:

- de al menos 2048 bits en el caso de claves RSA.
- de al menos 256 bits para el caso de claves ECDSA.

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

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

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

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

217. Los *Certificados* de la ACs FNMT-RCM raíces tiene habilitados los usos de *Claves* para firmar/sellar los *Certificados* de las ACs FNMT Subordinadas y las ARLs.

218. El *Certificado* de las ACs Subordinadas que expide los *Certificados de Sello de Entidad* tiene habilitado exclusivamente el uso para firmar/sellar *Certificados* de entidad final y CRLs.

219. Los *Certificados de Sello de Entidad* pueden tener habilitado exclusivamente los usos de clave de cifrado de claves, autenticación y firma.

220. La definición detallada de los perfiles de certificados finales y los usos admitidos de las claves se encuentra definidos en documento de perfiles de certificado disponible en http://www.cert.fnmt.es/dpcs/

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

6.2.1. Estándares para los módulos criptográficos

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

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

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

6.2.3. Custodia de la clave privada

223. 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

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

6.2.5. Archivado de la clave privada

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

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

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

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

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

6.2.8. Método de activación de la clave privada

228. 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.

229. 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 esquemas de uso simultáneo.

6.2.9. Método de desactivación de la clave privada

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

6.2.10. Método de destrucción de la clave privada

231. 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

232. 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

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

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

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

- Para la Jerarquía RSA:
  - *Certificado* de la AC raíz FNMT-RCM y su par de *Claves*: hasta el 1 de enero de 2030.
  - El *Certificado* de la AC Representación subordinada que expide los *Certificados de Sello de Entidad*: hasta el 31 de diciembre de 2029.
  - Los *Certificados de Sello de Entidad y su* par de *Claves:* no superior a 2 años.
- Para la Jerarquía Curvas Elípticas:
  - *Certificado* de la AC raíz FNMT-RCM G2 y su par de *Claves*: hasta el 4 de octubre de 2049.
  - El *Certificado* de la AC Entidades G2 subordinada que expide los *Certificados de Sello de Entidad*: hasta 07 de octubre de 2049.
  - Los *Certificados de Sello 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

235. 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 Sello de Entidad,* se generan durante la ceremonia de *Claves* de creación de dichas *Autoridades de Certificación*.

6.4.2. Protección de datos de activación

236. 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 esquemas de uso simultáneo.

6.4.3. Otros aspectos de los datos de activación

237. No estipulados.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

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

6.5.1. Requisitos técnicos específicos de seguridad informática

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

6.5.2. Evaluación del nivel de seguridad informática

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

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA

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

6.6.1. Controles de desarrollo de sistemas

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

6.6.2. Controles de gestión de la seguridad

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

6.6.3. Controles de seguridad del ciclo de vida

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

6.7. CONTROLES DE SEGURIDAD DE RED

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

6.8. FUENTE DE TIEMPO

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

6.9. OTROS CONTROLES ADICIONALES

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

6.9.1. Control de la capacidad de prestación de los servicios

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

6.9.2. Control de desarrollo de sistemas y aplicaciones informáticas

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

7. PERFILES DE LOS CERTIFICADOS, CRLS Y OCSP

7.1. PERFIL DEL CERTIFICADO

250. 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"

7.1.1. Número de versión

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

7.1.2. Extensiones del certificado

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

7.1.3. Identificadores de objeto de algoritmos

253. Los identificadores de objeto (OID) correspondientes a los algoritmos criptográficos utilizados son:

- Jerarquía RSA
  - Algoritmo *SHA-256 with RSA Encryption* cuyo OID es 1.2.840.113549.1.1.11
- Jerarquía Curva Elíptica:
  - Algoritmo *SHA-384 with ECDSA Encryption* cuyo OID es 1.2.840.10045.4.3.3
  - Algoritmo *SHA-256 with ECDSA Encryption* cuyo OID es 1.2.840.10045.4.3.2

7.1.4. Formatos de nombres

254. 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.

255. 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

256. 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

257. 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

258. La extensión "Policy Constraints" no se usa en ningún *Certificado* raíz (ni en AC RAIZ FNMT-RCM, ni en AC RAIZ FNMT-RCM G2).

7.1.8. Sintaxis y semántica de los calificadores de política

259. 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"

260. 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

261. Los perfiles de las CRLs son conformes con el estándar X.509 versión 2.

7.2.2. CRL y extensiones

262. Los perfiles de las CRLs siguen la siguiente estructura:

Tabla 5 – Perfiles de las CRLs

Campos y extensiones	Valor
Versión	V2
Algoritmo de firma	Sha256WithRSAEncryption o SHA-256 with ECDSA
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

Campos y extensiones	Valor
	entrada, número de serie y fecha de revocación

7.3. PERFIL DE OCSP

7.3.1. Número de versión

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

7.3.2. Extensiones del OCSP

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

8. AUDITORÍAS DE CUMPLIMIENTO

265. 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".

266. 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".

267. El sistema de expedición de Certificados es sometido a otras auditorías adicionales:

- Auditoría 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".
- Auditoría del Sistema de Gestión de Privacidad de la Información conforme a UNE-ISO/IEC 27701 "Sistemas de Gestión de Privacidad de la Información (SGPI). Requisitos".
- Auditoría según lo dictaminado en el Esquema Nacional de Seguridad (Real Decreto 311/2022, del 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica).
- Auditoría del Sistema de Gestión de la Calidad con arreglo a ISO 9001.
- Auditoría del Sistema de Gestión de la Responsabilidad Social en correspondencia con IQNet SR10.

- Auditoría del Plan de continuidad de negocio según ISO 22301.
- Auditoría conforme el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (RGPD / LOPD-GDD).

268. También se llevan a cabo análisis de riesgos, de acuerdo con lo dictado en el Sistema de Gestión de la Seguridad de la Información.

8.1. FRECUENCIA DE LAS AUDITORÍAS

269. Periódicamente se elaborarán los correspondientes planes de auditorías.

270. La *Autoridad de Certificación* que expide los *Certificados de 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 319 412-3 "Certificate profile for certificates issued to legal persons". La auditoría es realizada anualmente por una empresa externa acreditada.

271. Un auditor independiente evaluará anualmente el cumplimiento por parte de la CA de los requisitos y prácticas establecidos en esta DPC.

272. La frecuencia del resto de auditorías adicionales, será conforme a lo estipulado en la normativa vigente correspondiente.

8.2. CUALIFICACIÓN DEL AUDITOR

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

8.3. RELACIÓN DEL AUDITOR CON LA EMPRESA AUDITADA

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

8.4. ELEMENTOS OBJETOS DE AUDITORÍA

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

8.5. TOMA DE DECISIONES FRENTE A DETECCIÓN DE DEFICIENCIAS

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

8.6. COMUNICACIÓN DE LOS RESULTADOS

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

8.7. AUTOEVALUACIÓN

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

9. OTROS ASUNTOS LEGALES Y DE ACTIVIDAD

9.1. TARIFAS

279. 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.

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

9.1.1. Tarifas de emisión o renovación de certificados

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

9.1.2. Tarifas de acceso a los certificados

282. No estipulado.

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

283. 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

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

9.1.5. Política de reembolso

285. 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

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

9.2.1. Seguro de responsabilidad civil

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

9.2.2. Otros activos

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

9.2.3. Seguros y garantías para entidades finales

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

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

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

9.3.1. Alcance de la información confidencial

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

9.3.2. Información no incluida en el alcance

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

9.3.3. Responsabilidad para proteger la información confidencial

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

9.4. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

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

9.4.1. Plan de privacidad

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

9.4.2. Información tratada como privada

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

9.4.3. Información no considerada privada

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

9.4.4. Responsabilidad de proteger la información privada

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

9.4.5. Aviso y consentimiento para usar información privada

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

9.4.6. Divulgación conforme al proceso judicial o administrativo

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

9.4.7. Otras circunstancias de divulgación de información

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

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

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

9.6. OBLIGACIONES Y GARANTÍAS

9.6.1. Obligaciones de la AC

303. 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*.

304. 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*.

305. 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.

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

9.6.2. Obligaciones de la AR

307. 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.

308. 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.

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

9.6.3. Obligaciones del suscriptor

310. 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.

311. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la *DGPC*, el Representante de la Entidad, como *Solicitante* del *Certificado,* y/o en su caso el *Suscriptor* de los mismos, tienen la obligación de:

- No usar el *Certificado* fuera de los límites especificados en la presente *Política y Prácticas de Certificación* particulares.

- No usar el *Certificado* en caso de que el *Prestador de Servicios de Confianza* haya cesado su actividad como Entidad emisora de *Certificados* que expidió el certificado en cuestión, especialmente en los casos en los que los *Datos de Creación de Sello* del prestador puedan estar comprometidos, y así se haya comunicado.
- Aportar información veraz en la solicitud de los *Certificados* y mantenerla actualizada, suscribiendo los contratos por persona con capacidad suficiente.
- No solicitar para el *Sujeto* del certificado signos distintivos, denominaciones o derechos de propiedad industrial o intelectual de las que no sea titular, licenciatario o cuente con autorización demostrable para su uso.
- Actuar con diligencia respecto de la custodia y conservación de los *Datos de creación de Firma / Sello* o cualquier otra información sensible como *Claves*, códigos de activación del *Certificado*, palabras de acceso, números de identificación personal, etc., así como de los soportes de los *Certificados,* lo que comprende en todo caso, la no revelación de ninguno de los datos mencionados.
- Conocer y cumplir las condiciones de utilización de los *Certificados* previstas en las condiciones de uso y en la *Declaración de Prácticas de Certificación* y en particular, las limitaciones de uso de los *Certificados*
- Conocer y cumplir las modificaciones que se produzcan en la *Declaración de Prácticas de Certificación*.
- Solicitar la revocación del correspondiente *Certificado*, según el procedimiento descrito en el presente documento, notificando diligentemente a la FNMT-RCM las circunstancias para la revocación o sospecha de pérdida de la *Confidencialidad*, la divulgación, modificación o uso no autorizado de las *Claves privadas* asociadas,
- Revisar la información contenida en el *Certificado*, y notificar a la FNMT-RCM cualquier error o inexactitud.
- Verificar con carácter previo a confiar en los *Certificados,* la *Firma electrónica* o el *Sello electrónico* avanzados del *Prestador de Servicios de Confianza* emisor del *Certificado.*
- Notificar diligentemente a la FNMT-RCM cualquier modificación de los datos aportados en la solicitud del *Certificado*, solicitando, cuando consecuentemente fuere pertinente, la revocación del mismo.
- Devolver o destruir el *Certificado* cuando así lo exija la FNMT-RCM, y no usarlo con propósito de firmar o identificarse electrónicamente cuando el *Certificado* caduque, o sea revocado.

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

313. Asimismo, será el *Suscriptor* quien deba responder, en todo caso, ante la FNMT-RCM, las Entidades usuarias y, en su caso, ante terceros, del uso indebido del *Certificado*, o de la

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

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

315. Las relaciones de la FNMT-RCM y el *Suscriptor* quedarán determinadas principalmente, a los efectos del régimen de uso de los Certificados, a través del documento relativo a las condiciones de utilización o en su caso, contrato de emisión del Certificado y atendiendo a los acuerdos, convenios o documento de relación entre la FNMT-RCM y la Entidad Pública correspondiente.

9.6.4. Obligaciones de las partes que confían

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

9.6.5. Obligaciones de otros participantes

317. No estipulado.

9.7. RENUNCIA DE GARANTÍAS

318. No estipulado.

9.8. LIMITACIONES DE RESPONSABILIDAD

319. 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.

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

9.9. INDEMNIZACIONES

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

9.9.1. Indemnización de la CA

322. No estipulado.

9.9.2. Indemnización de los Suscriptores

323. No estipulado.

9.9.3. Indemnización de las partes que confían

324. No estipulado.

9.10. PERIODO DE VALIDEZ DE ESTE DOCUMENTO

9.10.1. Plazo

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

9.10.2. Terminación

326. 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

327. 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

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

9.12. MODIFICACIONES DE ESTE DOCUMENTO

9.12.1. Procedimiento para las modificaciones

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

9.12.2. Periodo y mecanismo de notificación

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

9.12.3. Circunstancias bajo las cuales debe cambiarse un OID

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

9.13. RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS

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

9.14. NORMATIVA DE APLICACIÓN

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

9.15. CUMPLIMIENTO DE LA NORMATIVA APLICABLE

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

9.16. ESTIPULACIONES DIVERSAS

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

9.16.1. Acuerdo íntegro

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

9.16.2. Asignación

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

9.16.3. Severabilidad

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

9.16.4. Cumplimiento

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

9.16.5. Fuerza Mayor

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

9.17. OTRAS ESTIPULACIONES

341. No se contemplan.