DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN DE CERTIFICADOS DE FIRMA ELECTRÓNICA CENTRALIZADA PARA EMPLEADOS PÚBLICOS

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM / 1.1	17/06/2018
Revisado por:	FNMT-RCM / 1.1	17/09/2018
Aprobado por:	FNMT-RCM / 1.1	21/09/2018

HISTÓRICO DEL DOCUMENTO			
Versión	**Fecha**	**Descripción**	**Autor**
1.0	13/06/2018	Declaración de Prácticas y Políticas de Certificación de certificados de firma electrónica centralizada para empleados públicos	FNMT-RCM
1.1	21/09/2018	La vigencia de los certificados se reduce a dos años.	FNMT-RCM

Referencia: DPC/DPCFCEP_0101/SGPSC/2018

Documento clasificado como: *Público*

Índice de contenidos

Índice de tablas

1. INTRODUCCIÓN

1. El Artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y de Orden Social habilita la prestación de servicios de seguridad por parte de la Fábrica Nacional de Moneda y Timbre, en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos, en su apartado Uno, establece que:

   "sin perjuicio de las competencias atribuidas en la Ley a los órganos administrativos en materia de registro de solicitudes, escritos y comunicaciones, se faculta a la Fábrica Nacional de Moneda y Timbre (FNMT) para la prestación de los servicios técnicos y administrativos necesarios para garantizar la seguridad, validez y eficacia de la emisión y recepción de comunicaciones y documentos a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT) en las relaciones que se produzcan entre:

   a) Los órganos de la Administración General del Estado entre sí o con los organismos públicos vinculados o dependientes de aquélla, así como las de estos organismos entre sí.
   b) Las personas físicas y jurídicas con la Administración General del Estado (AGE) y los organismos públicos vinculados o dependientes de ella"

2. De otro lado, su apartado Dos, establece:

   "Asimismo, se habilita a la FNMT a prestar, en su caso, a las Comunidades Autónomas, las entidades locales y las entidades de Derecho público vinculadas o dependientes de ellas, los servicios a que se refiere el apartado anterior, en las relaciones que se produzcan a través de técnicas y medios EIT entre sí, con la Administración General del Estado o con personas físicas y jurídicas; siempre que, previamente, se hayan formalizado los convenios o acuerdos procedentes."

3. La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, consagró el derecho de los ciudadanos a relacionarse electrónicamente con las diferentes Administraciones Públicas. El marco jurídico resultante de la aprobación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, viene a sistematizar toda la regulación relativa al procedimiento administrativo, clarificando e integrando el contenido de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y de la citada Ley 11/2007, de 22 de junio. Así mismo, la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, regula los sistemas de identificación y firma electrónicas utilizados en el ámbito de la Administración de Justicia.

4. Uno de estos sistemas de firma electrónica admitidos en el actual marco jurídico se encuentran los *Certificados electrónicos de firma electrónica del personal al servicio de la Administración Pública*.

5. La FNMT-RCM viene expidiendo este tipo de *Certificados*, como medio de identificación y de firma electrónica, desde los primeros años de aplicación de la citada Ley 11/2007. Sin embargo, muchas aplicaciones comerciales de uso cotidiano han evolucionado de tal forma que han dejado de soportar funcionalidades criptográficas necesarias para realizar firmas

electrónicas, siendo necesario utilizar complementos adicionales y un elevado grado de conocimiento técnico por parte de los usuarios de estos sistemas.

6. 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, establece un marco jurídico general para el uso de las *Firmas electrónicas*. Dicho Reglamento permite la creación de *Firmas electrónicas* a distancia en un entorno de creación de firma electrónica gestionado por un *Prestador de Servicios de Confianza* en nombre del *Firmante*.

1.1. OBJETO

7. El presente documento tiene por objeto la información pública de las condiciones y características del servicio de firma electrónica a distancia, o firma electrónica centralizada, dirigido al *Personal al servicio de la Administración*, por parte de la FNMT-RCM como *Prestador de Servicios de Confianza*, recogiendo en concreto las obligaciones que se compromete a cumplir en relación con

   - la gestión de los *Datos de creación y verificación de Firma* y de los *Certificados*, las condiciones aplicables a la solicitud, emisión, uso y extinción de la vigencia de los *Certificados* y sus *Datos de creación de Firma*, y en su caso, la existencia de procedimientos de coordinación con los Registros Públicos correspondientes que permitan el intercambio de información de manera inmediata y confidencial sobre la vigencia de los poderes indicados en los *Certificados* y que deban figurar preceptivamente inscritos en dichos registros
   - la prestación del servicio de consulta del estado de validez de los *Certificados*.

8. Además, en el presente documento se recogen, bien directamente o con referencias a la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica de la FNMT-RCM* de la que depende la presente Declaración, los detalles del régimen de responsabilidad aplicable a las partes usuarias y/o que confían en los servicios mencionados en el párrafo anterior, los controles de seguridad aplicados a sus procedimientos e instalaciones en aquello que pueda ser publicado sin perjudicar la eficacia de los mismos, y 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 que considere interesante poner a disposición del público.

1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

9. La *Declaración de Prácticas de Certificación* de la FNMT-RCM como *Prestador de Servicios de Confianza* está estructurada, de un lado, por la parte común de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* (DGPC) de la FNMT-RCM, pues existen niveles de actuación análogos para todos los servicios de confianza de la Entidad y, de otro lado, por los apartados específicos del presente documento de *Políticas de Certificación y Prácticas de Certificación Particulares*. No obstante lo anterior, la *Ley de Emisión* de cada tipo de *Certificado* o grupo de *Certificados* podrá establecer características especiales aplicables a los órganos, organismos, entidades y personal usuarios de los servicios de confianza de la FNMT-RCM.

10. 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 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, para cada servicio de confianza o conjunto o grupo de *Certificados*, identificado y diferenciado del resto por su tipología y régimen particular o diferenciador, existe una ***Política de Certificación*** específica en la que se describen las obligaciones de las partes, los límites de uso de los *Certificados* y responsabilidades y unas ***Prácticas de Certificación Particulares*** que desarrollan los términos definidos en la política correspondiente y otorgan prestaciones adicionales o específicas sobre las generales establecidas en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*.

       Estas *Políticas de Certificación* y *Prácticas de Certificación Particulares* concretan lo articulado en el cuerpo principal de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* y, por tanto, son parte integrante de ella, conformando, ambos, la *Declaración de Prácticas de Certificación* de la FNMT-RCM. No obstante, sólo son de aplicación para el conjunto de *Certificados* caracterizado e identificado en las correspondientes *Políticas 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.

    c. El presente documento representa, por tanto, las *Políticas de Certificación y Prácticas de Certificación Particulares* para los *Certificados de Firma Centralizada.*

11. El presente documento se denomina "*Declaración de Prácticas y Políticas de Certificación de certificados de firma electrónica centralizada para empleados públicos*", y en adelante será citado en este documento y con el ámbito descrito en el mismo como "*Declaración de Prácticas y Políticas Particulares*" o por su acrónimo "*DPPP*".

12. Las presentes *Políticas de Certificación y Prácticas de Certificación Particulares* forman parte de la *Declaración de Prácticas de Certificación* y tendrán prelación sobre lo dispuesto en el cuerpo principal de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica (DGPC)*.

13. En caso de que existiera contradicción entre el presente documento y lo dispuesto en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*, tendrá preferencia lo aquí articulado.

14. La presente *Política de Certificación* tiene la siguiente identificación:

Nombre: Política de Certificación de *Certificados* de firma electrónica centralizada para empleados públicos

Referencia / OID[1]:

- 1.3.6.1.4.1.5734.3.3.10.1.

Tipo de política asociada:

- QCP-n. OID: 0.4.0.194112.1.0

Versión: 1.1

Fecha de aprobación: 21 de septiembre de 2018

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/

15. El *Certificado* de firma electrónica centralizada para empleados públicos es un *Certificado* cualificado orientado a la realización de firmas a distancia o en servidor, esto es, la generación de las *Claves pública y privada* no son generadas directamente en el navegador de Internet del *Firmante* o en otro dispositivo en su poder, y tampoco se descarga su *Certificado*, sino que se generan y se almacenan en un dispositivo cualificado de creación de firma de la FNMT-RCM. Asimismo, la firma electrónica se realiza de forma centralizada, garantizándose en todo momento el control exclusivo del proceso de firma por parte del *Personal al servicio de la Administración* al que se le ha expedido el *Certificado*.

16. La FNMT-RCM interpretará, registrará, mantendrá, y publicará los procedimientos referidos en este apartado, pudiendo además recibir comunicaciones de los interesados sobre estos asuntos a través de la información de contacto expresada en el apartado 1.5.2 Datos de contacto del presente documento.

1.3. PARTES INTERVINIENTES

17. 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. *Firmantes*

[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.

4. Suscriptores de los *Certificados*
5. Partes que confían
6. Otros participantes

1.3.1. Autoridad de Certificación

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

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

Tabla 1 – Certificado de la AC FNMT raíz

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: 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

Sujeto	CN = AC Administración Pública, serialNumber = Q2826004J, OU = CERES, O = FNMT-RCM, C = ES

Emisor	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Número de serie (hex)	02
Validez	No antes: 21 de mayo de 2010. No después: 21 de mayo de 2022
Longitud clave pública	RSA 2.048 bits
Algoritmo de firma	RSA – SHA256
Identificador de clave	14 11 E2 B5 2B B9 8C 98 AD 68 D3 31 54 40 E4 58 5F 03 1B 7D

1.3.2. Autoridad de Registro

19. La Autoridad de Registro realiza las tareas de identificación del solicitante, *Personal al servicio de la Administración*, 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*.

20. Podrán actuar como entidades de registro de FNMT-RCM aquellas Oficinas de Registro designadas por el órgano, organismo o entidad Suscriptora del Certificado con las que ésta suscriba el correspondiente instrumento legal para cubrir dicha finalidad.

1.3.3. Firmantes

21. Los *Firmantes* son las personas físicas, *Personal al servicio de la Administración*, que mantienen bajo su uso exclusivo los *Datos de creación de firma* asociados a dicho *Certificado*.

1.3.4. Suscriptores de los certificados

22. Los *Suscriptores* de los *Certificados* de firma electrónica centralizada para empleados públicos son la Administración, organismos y entidades públicas representadas a través de los diferentes órganos competentes.

1.3.5. Partes que confían

23. 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*.

1.3.6. Otros participantes

24. No estipulado.

1.4. USO DE LOS CERTIFICADOS

1.4.1. Usos permitidos de los certificados

25. Los *Certificados* emitidos bajo esta *Política de Certificación* son expedidos a funcionarios, personal laboral, estatutario a su servicio y personal autorizado, al servicio de las Administraciones Públicas, órganos, organismos públicos o entidades de derecho público. Estos *Certificados* son válidos como sistemas de firma electrónica de conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y de conformidad con la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

26. La *Ley de Emisión* de estos *Certificados* podrá determinar, en defecto de normativa específica, las condiciones de uso y régimen de estos *Certificados* que permitirán la atribución a las Administraciones, organismos y entidades de los diferentes actos y resoluciones realizados por el personal a su servicio; todo ello, sin modificación legal o variación respecto de la actuación que vienen realizando estas Administraciones Públicas en los soportes tradicionales.

27. Dichos *Certificados* 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" y ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons".

1.4.2. Restricciones en el uso de los certificados

28. Constituyen límites de uso de este tipo de *Certificados* las diferentes competencias y funciones propias de la Administración Pública *Suscriptora* (actuando a través del personal a su servicio en calidad de *Firmante* de los *Certificados*), de acuerdo con su cargo, empleo y, en su caso, condiciones de autorización. La FNMT-RCM y la Administración, organismos y entidades públicas podrán fijar en los acuerdos o convenios, a través del documento de relación correspondiente o, si fuera procedente, en la *Ley de Emisión* de estos *Certificados*, otros límites adicionales.

29. FNMT-RCM no tendrá control sobre las actuaciones y usos de los *Certificados* y la *Clave privada* que se realicen por el *Personal al servicio de la Administración* en nombre de ésta, por lo que la FNMT-RCM quedará exonerada de responsabilidad a efectos de tales usos, así como de las consecuencias y efectos que pudieran producirse en el marco de reclamaciones o, en su caso, de posibles responsabilidades patrimoniales llevadas a cabo por terceros.

30. En cuanto a las actividades del personal de las *Oficinas de Registro*, la FNMT – RCM quedará sujeta a las obligaciones y responsabilidades derivadas de la legislación en materia de firma

electrónica, sin perjuicio de las especialidades contenidas en el artículo 11 del RD 1317/2001, de 30 de noviembre, por el que se desarrolla el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas fiscales, administrativas y del orden social en materia de prestación de servicios de seguridad por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, en las comunicaciones a través de medios electrónicos, informáticos y telemáticos con las Administraciones Públicas. Para poder usar los *Certificados* de *Firma electrónica* de *Personal al servicio de la Administración* de forma diligente, se deberá previamente formar parte de la *Comunidad Electrónica* y, la Administración actuante, adquirir la condición de *Suscriptor*.

31. En cualquier caso, si un tercero desea confiar en la *Firma electrónica* realizada con uno de estos *Certificados* sin acceder al *Servicio de información sobre el estado de los Certificados* emitidos bajo esta *Política de Certificación*, no se obtendrá cobertura de las presentes *Políticas de Certificación 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*.

32. Además, incluso dentro del ámbito de la *Comunidad Electrónica*, no se podrá emplear este tipo de *Certificados* para:

- Firmar o sellar otro *Certificado*, salvo supuestos expresamente autorizados previamente.
- Usos particulares o privados, salvo para relacionarse con las Administraciones cuando éstas lo admitan.
- Firmar o sellar 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 por ejemplo serían a título enunciativo:
    - Prestar servicios de *OCSP*.
    - Generar *Listas de Revocación.*
    - Prestar servicios de notificación

1.5. ADMINISTRACIÓN DE POLÍTICAS

1.5.1. Entidad responsable

33. 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

34. 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: 902 181 696

1.5.3. Responsables de adecuación de la DPC

35. 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

36. La FNMT – RCM, a través de su Comité de Gestión del *Prestador de Servicios de Confianza*, vela por el cumplimiento de las *Declaraciones de Políticas y Prácticas de Certificación*, las aprueba y realiza el pertinente proceso de revisión de las mismas, con una periodicidad anual.

1.6. DEFINICIONES Y ACRÓNIMOS

1.6.1. Definiciones

37. A los efectos de lo dispuesto en la presente *DPPP*, cuando los términos comiencen con letra mayúscula y estén en cursiva, se tendrán en cuenta de forma general las definiciones expresadas en la DGPC y, en particular, las expresadas a continuación:

- *Certificado de Firma Centralizada:* en el presente documento de DPPP, se refiere siempre al *Certificado* electrónico expedido por la FNMT-RCM al *Personal al servicio de la Administración*, orientado a la realización de firmas en remoto o en servidor. Esto significa que la generación de las *Claves pública y privada* se generan y almacenan en un entorno seguro perteneciente a la FNMT-RCM, garantizándose en todo momento el control exclusivo del uso de dichas Claves por parte del *Firmante* (*Personal al servicio de la Administración*).
- *Declaración de Prácticas de Certificación (DPC):* declaración puesta a disposición del público de manera fácilmente accesible, por vía electrónica y de forma gratuita por parte de la FNMT-RCM. Tiene la consideración de documento de seguridad en el que se detallan, en el marco eIDAS, las obligaciones que los *Prestadores de Servicios de Confianza* se comprometen a cumplir en relación con la gestión de los *Datos de creación y verificación de firma* y de los *Certificados* electrónicos, las condiciones aplicables a la solicitud, expedición, uso y extinción de la vigencia de los *Certificados*, las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de *los Certificados.*
- *Declaración de Prácticas y Políticas Particulares (DPPP): DPC* particular que aplica a la expedición de un conjunto determinado de *Certificados* expedidos por la

FNMT-RCM bajo las condiciones particulares recogidas en dicha Declaración, y que le son de aplicación las Políticas particulares definidas en la misma.

- *Firmante*: *Personal al servicio de la Administración* que hace uso de sus *Datos de creación de firma.*
- *Organismo de supervisión:* organismo designado por un Estado miembro como responsable de las funciones de supervisión en materia de prestación de servicios de confianza, de conformidad con el artículo 17 del Reglamento eIDAS. En España, actualmente es el Ministerio de Energía, Turismo y Agenda Digital.
- *Personal al servicio de la Administración*: Funcionarios, personal laboral, estatutario a su servicio, personal autorizado o personal al servicio de la Administración Pública o de la Administración de Justicia, órgano, organismo público o entidad de derecho público.
- *Responsable de Operaciones de Registro*: Persona física nombrada por el representante de la Administración pública, organismo público o entidad de derecho público, bajo cuya responsabilidad se realizan las tareas asignadas a la *Oficina de Registro*, con las obligaciones y responsabilidades asignadas en las presentes *Políticas y Prácticas de Certificación Particulares*.
- *Sede electrónica*: Dirección electrónica, disponible para los ciudadanos a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública, o bien a uno o varios organismos públicos o entidades de Derecho Público en el ejercicio de sus competencias.
- *Suscriptor*: La administración pública, órgano, organismo público o entidad de derecho público.

1.6.2. Acrónimos

38. 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

39. La FNMT-RCM, como 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

40. 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

41. 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.

42. En cuanto a la frecuencia de publicación de CRL, se define en el apartado "4.10.3 Características adicionales. Frecuencia de publicación".

2.4. CONTROL DE ACCESO A LOS REPOSITORIOS

43. 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

44. 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

45. 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*.

46. El campo Common Name define al *Personal al servicio de la Administración* al que se le ha expedido el *Certificado*.

Seudónimos

47. Los *Certificados de Firma centralizada* que la FNMT – RCM expida bajo las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares* haciendo uso de seudónimos, indicarán claramente esta característica, de conformidad con el Reglamento eIDAS y la normativa nacional aplicable.

48. En el procedimiento de acreditación de la identidad, como paso previo a la expedición de un *Certificados de Firma centralizada* con seudónimo, 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. Unicidad de los nombres

49. El nombre distintivo (*DN*) asignado al *Certificado* dentro del dominio del *Prestador de Servicios de Confianza* será único.

3.1.3. Reconocimiento y autenticación de marcas registradas

50. 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

51. El *Solicitante*, *Personal al servicio de la Administración*, genera sus *Claves pública y privada* en el sistema de la FNMT-RCM, después de haber sido registrado en el mismo y una vez validada dicha generación por parte de la *Oficina de Registro*, tras el proceso de acreditación de la identidad del citado *Solicitante* y recabada su voluntad para la expedición del *Certificado de Firma centralizada*.

52. Después de informar al *Solicitante* que se le va a expedir su *Certificado*, el sistema genera la pareja de *Claves*, de forma que la *Clave privada* queda almacenada de forma protegida, garantizando su uso bajo el control exclusivo del *Personal al servicio de la Administración*.

3.2.2. Autenticación de la identidad de la organización

53. Las actividades de comprobación de la identidad del *Personal al servicio de la Administración*, *Solicitantes* de los *Certificados*, serán realizadas por el personal autorizado de las *Oficinas de Registro* implantadas por el órgano, organismo o entidad de la Administración Pública en cuestión. Por tanto, queda así garantizada la identidad de la Administración, *Suscriptora* del *Certificado*, que se corresponde, en cada caso, con el organismo o entidad donde el personal presta sus servicios. Por tanto y a estos efectos las *Oficinas de Registro* no serán autoridades delegadas o dependientes de la FNMT-RCM.

3.2.3. Autenticación de la identidad de la persona física solicitante

54. Se hace constar que la FNMT-RCM, en función de la relación de personal usuario dependiente remitida por la Administración, organismos o entidad pública, considerará, bajo responsabilidad de los correspondientes órganos, organismos y/o entidades, que actuarán a través de las *Oficinas de Registro*, que este personal se encuentra con su cargo vigente, que su número de Identificación Personal, empleo o autorización es auténtico y está en vigor y, por tanto, habilitados para obtener y usar el *Certificado*. FNMT-RCM, no tendrá, en este tipo de *Certificado*, la responsabilidad de comprobar el cargo o empleo del citado personal, así como que estos requisitos se mantienen durante toda la vida del *Certificado*, al no ostentar, la FNMT-RCM, relación jurídica funcionarial, administrativa o laboral con tal personal, más allá del documento de condiciones de utilización o, en su caso, contrato de emisión, cuyo efecto es estrictamente instrumental para el desempeño de las funciones propias del cargo.

55. Las actividades de comprobación anteriores serán realizadas por los responsables de las *Oficinas de Registro* implantadas por el órgano, organismo o entidad de la Administración Pública en cuestión, y que se corresponde, en cada caso, con el organismo o entidad donde el personal presta sus servicios. Por tanto y a estos efectos las *Oficinas de Registro* no serán autoridades delegadas o dependientes de la FNMT-RCM.

Comprobación directa mediante presencia física

56. Los *Solicitantes* de *Certificados de Firma centralizada* deberán comparecer físicamente para formalizar el procedimiento de confirmación de identidad personal, con alguno de los medios

de identificación admitidos en derecho conforme a la legislación nacional vigente, presentándose en la *Oficina de Registro* designada a tal efecto por el órgano, organismo o entidad pública *Suscriptora* de la que depende el personal a su servicio. Dicha *Oficina de Registro* es creada por la Administración *Suscriptora*, que notifica a la FNMT-RCM la relación de personas habilitadas para realizar estas actividades de Registro, de acuerdo con los procedimientos establecidos a tal efecto, así como cualquier variación en la estructura de dicha Oficina.

Comprobación indirecta mediante medios de aseguramiento equivalente a la presencia física de conformidad con el Derecho nacional

57. No será necesaria la personación cuando a la *Oficina de Registro* del órgano competente de la Administración le conste la identidad u otras circunstancias permanentes de los solicitantes de los *Certificados* (identidad, vigencia del cargo y demás condiciones a incluir en el *Certificado*) en virtud de la relación preexistente entre dichos *Solicitantes* y la Administración donde prestan servicio, si queda garantizado que dichos *Solicitantes* (*Personal al servicio de la Administración*) han sido identificados mediante personación física (de conformidad con el proceso descrito en el párrafo anterior), y el período de tiempo transcurrido desde dicha personación física es menor de cinco años.

3.2.4. Información no verificada del Suscriptor

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

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RENOVACIÓN DE CLAVES

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

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

60. 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

61. El *Solicitante* de este tipo de *Certificados* solo puede ser *Personal al servicio de la Administración*.

4.1.2. Proceso de registro y responsabilidades

62. El *Solicitante*, *Personal al servicio de la Administración*, a través de la aplicación web de solicitud de *Certificados* desarrollada a tal efecto, deberá aceptar las condiciones de uso del *Certificado* e introducirá sus datos identificativos: número de DNI, primer apellido, NIF del organismo al que pertenece y su dirección de correo electrónico al que se enviará un código de solicitud.

63. La FNMT-RCM, podrá acordar con las Administraciones, organismos y entidades públicas que así lo soliciten, la creación de *Oficinas de Registro* delegadas con el fin de centralizar la realización de los procedimientos de registro con destino a otras Administraciones, vinculadas o dependientes, que no dispongan de medios suficientes para hacerlo en aplicación de las leyes sobre racionalización del gasto.

64. El apartado 9.8 "Responsabilidades" 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

65. En el supuesto que se actúe mediante comparecencia en la *Oficina de Registro*, el *Solicitante* aportará los datos que se le requieran, acreditará su identidad personal y su condición de *Personal al servicio de la Administración*. En el caso de la expedición de *Certificados de firma centralizada* con seudónimo, la FNMT-RCM, a través de la *Oficina de Registro,* constatará la verdadera identidad del *Firmante* y conservará la documentación que la acredite. FNMT-RCM admitirá, en todo caso, la función e informe que realice la *Oficina de Registro* designada por la Administración.

66. El *Solicitante* suscribirá las condiciones de uso del *Certificado*, y se le dotará de unas credenciales de identificación que usará en la aplicación de solicitud del *Certificado* (usuario y una parte de la contraseña de acceso a la misma).

67. La FNMT-RCM podrá identificar al *Solicitante*, de forma alternativa a la comparecencia en la *Oficina de Registro*, mediante el uso de un *Certificado electrónico cualificado* expedido al *Personal al servicio de la Administración,* garantizando así la autenticidad de todos los campos a incluir en el *Certificado de firma centralizada* a expedir, siempre que no hayan transcurrido más de cinco años desde que se procedió a la identificación del *Firmante*.

4.2.2. Aprobación o rechazo de la solicitud del certificado

68. Una vez confirmadas por la *Oficina de Registro* la identidad del *Solicitante* y la vigencia del cargo o empleo, y suscrito el documento de condiciones de utilización o, en su caso, el contrato de solicitud por el citado *Solicitante* y la *Oficina de Registro*, ésta procederá a validar los datos y a enviarlos firmados, junto con el código de solicitud recogido en la fase de solicitud. De esta forma, el *Solicitante* queda registrado en el sistema de la FNMT-RCM, si bien todavía no se generan las *Claves*.

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

70. La FNMT-RCM recabará de los *Solicitantes* solo 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.

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

4.2.3. Tiempo en procesar la solicitud

72. La solicitud es procesada automáticamente por el sistema, por lo que no hay establecido un tiempo para este proceso.

4.3. EMISIÓN DEL CERTIFICADO

4.3.1. Acciones de la AC durante la emisión

73. Como se ha visto anteriormente, el *Solicitante*, *Personal al servicio de la Administración,* ha sido registrado con un alto nivel de seguridad en el sistema, como paso previo a generación de las *Claves pública y privada*.

74. La FNMT-RCM envía una notificación a la dirección de correo electrónico del *Solicitante*, comunicándole la otra parte de la contraseña que conforma sus credenciales de identificación, completando así la información que se le facilitó en la *Oficina de Registro*.

75. Posteriormente, el *Solicitante* se identificará ante el sistema con las credenciales recibidas más un segundo factor de autenticación que será remitido a su dirección de correo electrónico[2] y, una vez verificada su identidad, solicitará expresamente la emisión de su *Certificado de firma centralizada.* De esta forma, la infraestructura vincula de forma segura los datos de identificación proporcionados por el Solicitante, según se ha descrito en el apartado "4.1.2 Proceso de registro" del presente documento, con el proceso de generación de su *Certificado*.

76. En ese momento, el sistema generará en un HSM protegido las *Claves pública y privada,* y expedirá al *Personal al servicio de la Administración* el *Certificado de firma centralizada* solicitado. Así mismo, el sistema requiere que el *Solicitante* establezca su número personal (PIN) que le será requerido para realizar las operaciones que usen su *Clave privada*. Este PIN no es conocido (ni almacenado) en ningún momento por el sistema de la FNMT-RCM.

77. La emisión de *Certificados* supone la generación de documentos electrónicos que confirman la identidad del personal*,* su relación, cargo o empleo con la Administración Pública, así como su correspondencia con la *Clave Pública* asociada. La emisión de *Certificados* de la FNMT-RCM sólo puede realizarla ella misma, en calidad de *Prestador de Servicios de Confianza*, no existiendo ninguna otra entidad u organismo con capacidad de emisión de los mismos. La

[2] La FNMT-RCM podrá utilizar otros medios de comunicación para transmitir este segundo factor de autenticación, previa autorización del *Solicitante*, como por ejemplo el uso de teléfonos móviles cuyo número haya sido previamente acreditado.

Autoridad de Certificación de la FNMT-RCM solo acepta solicitudes de generación de *Certificados* provenientes de fuentes autorizadas. Todos los datos contenidos en cada solicitud están protegidos contra alteraciones a través de mecanismos de firma o sello electrónicos realizados mediante el uso de *Certificados* emitidos a dichas fuentes autorizadas.

4.3.2. Notificación de la emisión

78. Una vez generadas las *Claves* y el *Certificado*, el sistema informa de este hecho al *Personal al servicio de la Administración*.

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1. Proceso de aceptación

79. En el proceso de solicitud del Certificado, el *Personal al servicio de la Administración* acepta las condiciones de uso y expresa su voluntad de obtener el Certificado, como requisitos necesarios para la generación del mismo.

4.4.2. Publicación del certificado por la AC

80. 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

81. 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

82. El *Certificado de Firma Centralizada* es la certificación electrónica emitida por la FNMT-RCM que vincula al *Firmante* con unos *Datos de verificación de Firma* y confirma, de forma conjunta:

- la identidad del *Firmante* (*Personal al servicio de la Administración*), incluyendo en su caso, su número de identificación personal, cargo, puesto de trabajo y/o condición de autorizado, y
- la identidad del *Suscriptor* del *Certificado*, donde el *Firmante* ejerce sus competencias, presta sus servicios, o desarrolla su actividad.

83. Este *Certificado* se emite por la FNMT-RCM por cuenta de la Administración correspondiente a la que la FNMT-RCM presta los servicios técnicos, administrativos y de seguridad necesarios como *Prestador de Servicios de Confianza*.

84. El *Certificado de Firma Centralizada* es expedido por la FNMT-RCM basándose en actuaciones de identificación y registro realizadas por la red de *Oficinas de Registro* designadas por el órgano, organismo o entidad *Suscriptora* del *Certificado*. Las "*Leyes de*

Emisión" podrán establecer, en el ámbito de actuación de las Administraciones Públicas, *Oficinas de Registro* comunes para este ámbito de actuación con efectos uniformes para cualesquiera Administraciones, organismos y/o entidades públicas.

85. La *Ley de Emisión* suplirá, atendiendo a las diferentes funcionalidades del ámbito de actuación de los *Certificados*, elementos o campos ordinariamente expresados en el propio *Certificado*, atendiendo a la especialidad de actuación de las diferentes Administraciones Públicas.

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

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

4.6. RENOVACIÓN DEL CERTIFICADO

87. La renovación del *Certificado* consiste en la emisión de un nuevo *Certificado* sin cambiar ninguna información del *Firmante*, *Clave pública* o cualquier otra información que aparezca en el mismo. 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

88. El proceso de "regeneración de las claves" consiste en la expedición de un nuevo certificado con una clave pública, un número de serie y un periodo de vigencia del certificado diferentes a los anteriores, manteniéndose el contenido del campo subject del antiguo certificado.

89. Bajo las presentes Políticas de Certificación, la FNMT-RCM no contempla este proceso de regeneración de claves. Si el *Firmante* quisiera seguir utilizando un *Certificado de Firma Centralizada* bajo las presentes *Políticas de Certificación y Prácticas de Certificación Particulares* una vez que su *Certificado* ha perdido su vigencia, deberá solicitar un nuevo *Certificado* y confirmar su identidad conforme al procedimiento descrito en el apartado "4.1 Solicitud de Certificados de este documento".

4.8. MODIFICACIÓN DEL CERTIFICADO

90. No es posible realizar modificaciones de los certificados expedidos. Por tanto, cualquier necesidad de modificación conlleva la expedición de un nuevo certificado.

4.9. REVOCACIÓN DEL CERTIFICADO

91. Los efectos de la revocación del *Certificado de Firma Centralizada*, esto es, la extinción de su vigencia, conllevará automáticamente la extinción de la vigencia de los *Datos de creación de firma* asociados a éste. Dichos efectos surtirán desde la fecha en que la FNMT-RCM tenga conocimiento cierto de cualquiera de los hechos determinantes y así lo hará constar en su *Servicio de información y consulta sobre el estado de los certificados*.

4.9.1. Circunstancias para la revocación

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

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

a) La solicitud de revocación formulada por el *Firmante* (*Personal al servicio de la Administración*) o por el *Suscriptor* (*Administración* donde el *Firmante* presta sus servicios) mediante personal debidamente autorizado. En todo caso deberá dar lugar a esta solicitud:

- La utilización por un tercero de los *Datos de Creación de Firma*, correspondientes a los *Datos de Verificación de Firma* contenidos en el *Certificado* y vinculados a la identidad personal del *Firmante*.
- La violación o puesta en peligro del secreto de los *Datos de Creación de Firma* o de la información necesaria para acceder a los mismos.
- La terminación de la relación del *Personal al servicio de la Administración* con ésta.
- 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) Cancelación de las credenciales de identificación del *Firmante.*

c) Resolución judicial o administrativa que así lo ordene.

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

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*, de manera que este 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* si, en este último caso, hubiese podido afectar al procedimiento de expedición del *Certificado*.

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

h) 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*.

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

j) Violación o puesta en peligro del secreto de los *Datos de Creación de Firma* del *Prestador de Servicios de Confianza*.

k) 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*.

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

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

- Que la revocación se debiera haber efectuado por solicitud fehaciente por parte del *Firmante* o del *Suscriptor*, por medio de los sistemas puestos a disposición por la FNMT-RCM para este fin.
- Que la solicitud de revocación o la causa que la motiva, le haya sido notificada mediante resolución judicial o administrativa.
- Que las causas d) a g) del presente apartado le sean acreditadas fehacientemente, previa identificación del *Solicitante* autorizado de la revocación.

96. 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.

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

98. La revocación del *Certificado de Firma Centralizada* implica, además de su extinción y la imposibilidad de seguir utilizando los *Datos de creación de firma* asociados, la finalización de la relación y régimen de uso de dicho *Certificado* y su *Clave privada* con la FNMT-RCM.

4.9.2. Quién puede solicitar la revocación

99. La revocación de un *Certificado de Firma Centralizada* solamente podrá ser solicitada por el *Suscriptor* a través de la *Oficina de Registro* habilitada para tal efecto o por el *Firmante*, bien a través de dicha *Oficina de Registro*, bien 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.

100. No obstante, la FNMT-RCM podrá revocar de oficio los *Certificados de Firma Centralizada* en los supuestos recogidos en la presente *Declaración de Prácticas y Políticas de Certificación*.

4.9.3. Procedimiento de solicitud de la revocación

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

102. A continuación, se describe el procedimiento a observar por la *Oficina de Registro* por el que se formaliza la solicitud de revocación de un *Certificado*.

103. El peticionario de la revocación del Certificado introducirá, en la aplicación desarrollada a tal efecto, los datos identificativos del *Firmante*: número de DNI, primer apellido, NIF del organismo al que pertenece y su dirección de correo electrónico al que se confirmará la revocación de su *Certificado*. De esta forma, la infraestructura vincula de forma segura los datos de identificación proporcionados por la *Oficina de Registro*, con el proceso de revocación del *Certificado.*

104. En todo caso, FNMT-RCM recibirá de la Administración, organismo y/o entidad, aquella información relevante a efectos de la revocación de un *Certificado* a través de la *Oficina de Registro*.

105. La *Oficina de Registro* remitirá los registros tramitados a la FNMT-RCM para que ésta proceda a la revocación del *Certificado*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

106. FNMT-RCM considerará que el peticionario de la revocación de un *Certificado* de este tipo cuenta con la autorización correspondiente si la petición es realizada a través de su *Oficina de Registro*. FNMT-RCM no realizará valoración alguna sobre la conveniencia o no de la revocación solicitada, cuando sea realizada a través de la citada *Oficina de Registro*.

107. El *Firmante*, *Personal al servicio de la Administración,* también podrá solicitar la revocación mediante el número de 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.

108. Tan pronto se resuelva la revocación, el *Firmante* recibirá, a través de la dirección de correo electrónico[3] consignada en la solicitud, la notificación de la revocación del *Certificado*.

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

[3] La FNMT-RCM podrá utilizar otros medios de comunicación para notificar este hecho, previa autorización del *Solicitante*, como por ejemplo mensajes mediante el uso de teléfonos móviles cuyo número haya sido previamente acreditado.

4.9.4. Periodo de gracia de la solicitud de revocación

110. 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

111. 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.

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

112. Las terceras partes que confían y aceptan el uso de los *Certificados* emitidos por la FNMT – RCM están obligadas a verificar:

- 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

113. Las *Listas de Revocación* (*CRL*) de los *Certificados de Firma Centralizada* 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

114. 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

115. 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

116. La comprobación en línea del estado de revocación del *Certificado de Firma Centralizada* 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

117. No definidas.

4.9.12. Requisitos especiales de revocación de claves comprometidas

118. No existen requisitos especiales para el caso de revocación de certificados causada por un compromiso de claves, siendo de aplicación lo descrito para el resto de las causas de revocación.

4.9.13. Circunstancias para la suspensión

119. No se contempla la suspensión de certificados.

4.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE LOS CERTIFICADOS

4.10.1. Características operativas

120. La información relativa a la validación de los *Certificados* electrónicos objeto de la presente *DPPP* es accesible a través de los siguientes medios:

a. Listas de Certificados Revocados:

i. AC RAIZ. Accesos:

1. ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint
2. http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

ii. AC Subordinada Administración Pública. Accesos:

1. ldap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,CN=AC%20Administraci%F3n%20P%FAblica,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
2. http://www.cert.fnmt.es/crlsacap/ CRL<xxx*>.crl

b. Servicio de comprobación del estado de certificados (OCSP):

i. AC RAIZ. Acceso:

http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder

ii. AC Subordinada Administración Pública. Acceso:

http://ocspap.cert.fnmt.es/ocspap/OcspResponder

4.10.2. Disponibilidad del servicio

121. 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.

4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN

122. A efectos de las presentes *Políticas y Prácticas de Certificación Particulares* la suscripción finalizará en el momento en el que quede sin efecto el *Certificado de Firma Centralizada*. De no llevarse a cabo la renovación del *Certificado* se considerará extinguida la relación entre el *Firmante* y la FNMT-RCM.

123. Los *Certificados de Firma Centralizada* 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, una vez acreditada la ausencia de oposición de los *Suscriptores*, 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.

124. A los efectos enumerados anteriormente, se hace constar que la solicitud de emisión de un *Certificado de Firma Centralizada* emitido por la FNMT-RCM cuando exista otro vigente a favor del mismo *Firmante* y mismo *Suscriptor,* y perteneciente a la misma *Ley de Emisión,* conllevará la revocación del primero obtenido.

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1. Prácticas y políticas de custodia y recuperación de claves

125. La FNMT-RCM no recuperará las *Claves privadas* asociadas a los *Certificados de Firma Centralizada*. En el caso de pérdida del PIN que protege el acceso a dicha *Clave* por parte del *Firmante,* se deberá revocar dicho *Certificado* y solicitar la emisión de uno nuevo.

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

126. No estipulado.

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

127. Véase el apartado correspondiente en la DGPC.

6. CONTROLES DE SEGURIDAD TÉCNICA

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

6.1. GENERACIÓN E INSTALACIÓN DE LAS CLAVES

6.1.1. Generación del par de claves

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

130. Las *Claves privadas* asociadas a los *Certificados de Firma Centralizada* son generadas y custodiadas por el módulo de activación de firma de la FNMT-RCM, de forma que el acceso a dichas *Claves* se realiza por medios que garantizan, con un alto nivel de confianza, el control exclusivo por parte del *Firmante*.

6.1.2. Envío de la clave privada al suscriptor

131. Las *Claves privadas* asociadas a los *Certificados de Firma Centralizada* son generadas en un dispositivo de creación de firma bajo el control exclusivo del *Firmante*, donde quedarán custodiadas para su uso. Por tanto, no existe ninguna entrega de la *Clave privada* al *Firmante*.

132. No obstante, en caso de que la FNMT-RCM o cualquiera de las oficinas de registro tengan conocimiento de un acceso no autorizado a la *Clave privada* del *Firmante*, el *Certificado de Firma Centralizada* asociado a dicha *Clave privada* será revocado.

6.1.3. Envío de la clave pública al emisor del certificado

133. La *Clave pública* generada junto a la *Clave privada* sobre el dispositivo de generación y custodia de claves es entregada a la Autoridad de Certificación mediante el envío de una solicitud de certificación en formato PKCS#10.

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

134. La FNMT-RCM distribuye las *Claves públicas,* tanto de la AC raíz como de la AC Subordinada que expide los *Certificados de Firma Centralizada,* a través de varios medios, como son mediante publicación en su sede electrónica (www.sede.fnmt.gob.es) o en el apartado 1.3.1 del presente documento.

6.1.5. Tamaños de claves y algoritmos utilizados

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

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

- Claves de la AC FNMT raíz: 4.096 bits.
- Claves de la AC FNMT Subordinada que expide los *Certificados de Firma Centralizada:* 2.048 bits.
- Claves de los *Certificados de Firma Centralizada:* 2.048 bits.

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

137. Las *Claves públicas* de los *Certificados de Firma Centralizada* están codificadas de acuerdo con RFC5280 y PKCS#1.

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

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

139. El *Certificado* de la AC FNMT raíz tiene habilitados los usos de *Claves* para firmar/sellar los *Certificados* de las ACs FNMT Subordinadas y las ARLs. El *Certificado* de la AC FNMT Subordinada que expide los *Certificados de Firma Centralizada* tiene habilitado exclusivamente el uso para firmar/sellar *Certificados* de usuario final (*Certificados de Firma Centralizada*) y CRLs.

140. El *Certificado de Firma Centralizada* expedido a los usuarios, como *Firmantes*, tiene habilitado exclusivamente el uso de firma electrónica.

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

6.2.1. Estándares para los módulos criptográficos

141. Los *Datos de creación de Firma* del *Prestador de Servicios de Confianza* se encuentran protegidos por un dispositivo criptográfico que cumple con los requisitos de seguridad FIPS PUB 140-2 Nivel 3. Las operaciones de firma de *Certificados, Listas de Revocación,* estructuras de datos relativas a la validez de los *Certificados y Sellos de Tiempo electrónicos* son llevadas a cabo dentro del dispositivo criptográfico, que dota de *Confidencialidad* a los *Datos de creación de Firma* del *Prestador de Servicios de Confianza*.

142. Si los *Datos de creación de Firma* tuvieran que encontrarse fuera del dispositivo criptográfico en alguna circunstancia, la FNMT-RCM aplicará las medidas técnicas y organizativas apropiadas para garantizar su *Confidencialidad*.

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

143. La FNMT-RCM garantiza que toda operación en la que intervengan las *Claves privadas* de sus Autoridades de Certificación requiere la aprobación de al menos dos personas.

6.2.3. Custodia de la clave privada

144. 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.

145. En cuanto a las *Claves privadas* correspondientes a los *Certificados de Firma Centralizada* expedidos a los usuarios finales (*Firmantes*), quedan custodiadas en los sistemas de la FNMT-RCM de forma que únicamente el *Firmante* puede acceder a su *Clave privada*. El acceso queda garantizado mediante el uso de sus credenciales de identificación y su PIN de firma (únicamente conocidos por el *Firmante*), más un segundo factor de autenticación como es una contraseña de un solo uso.

6.2.4. Copia de seguridad de la clave privada

146. Se mantiene una copia de los ficheros y componentes necesarios para, en caso de contingencia, posibilitar la restauración del entorno de seguridad del dispositivo criptográfico, en sobres de seguridad debidamente custodiados dentro de un armario ignífugo, que solo pueden ser obtenidos por personal autorizado.

6.2.5. Archivado de la clave privada

147. La FNMT-RCM podrá efectuar una copia de seguridad de los *Datos de creación de firma* asociados a los *Certificados de Firma Centralizada* garantizando que el grado de seguridad de los datos duplicados es del mismo nivel que el de los datos originales y que el número de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio. No se duplican los *Datos de creación de firma* para ninguna otra finalidad.

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

148. La generación de las *Claves privadas* de las Autoridades de Certificación se realiza según lo descrito en el apartado "6.1 Generación e instalación de las Claves". Por tanto, no es posible la transferencia dichas *Claves*, si bien existe un procedimiento de recuperación de las mismas como medida de contingencia, como se describe en el apartado "6.2.4 Copia de seguridad de la clave privada".

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

149. La FNMT-RCM dispone de los medios necesarios para asegurar que el hardware criptográfico utilizado para la protección de sus *Claves* como *Prestador de Servicios de Confianza:*

- No ha sido manipulado durante su transporte, mediante un proceso de inspección del material suministrado que incluye controles para detectar su autenticidad y posible manipulación.
- Funciona correctamente, mediante procesos de monitorización continua, inspecciones periódicas de mantenimiento preventivo y servicio de actualización de software y firmware.

- Permanece en un entorno físicamente seguro desde su recepción hasta su destrucción, llegado el caso.

6.2.8. Método de activación de la clave privada

150. 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.

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

152. Los mecanismos de activación y uso de las *Claves privadas* de los *Certificados de Firma Centralizada* de entidad final se basan en el uso, por parte del *Firmante*, de sus credenciales de identificación y su PIN de firma (únicamente conocidos por él), más un segundo factor de autenticación como es una contraseña de un solo uso.

6.2.9. Método de desactivación de la clave privada

153. Una persona con el rol de administrador puede proceder a la desactivación de la clave de las Autoridades de Certificación mediante la detención del sistema. Para su reactivación se actuará según lo descrito en el apartado "6.2.8 Método de activación de la clave privada".

154. En cuanto a la desactivación de las *Claves privadas* de los *Certificados de Firma Centralizada* de entidad final, éstas estarán desactivadas mientras el *Firmante* no esté autenticado en el sistema de firma centralizada.

6.2.10. Método de destrucción de la clave privada

155. 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.

156. En el caso de las *Claves privadas* de los *Certificados de Firma Centralizada* de entidad final, éstas serán destruidas una vez agotado su periodo de uso o cuando finalice la relación de los *Firmantes* con la FNMT-RCM. Adicionalmente, si el *Firmante* introduce erróneamente un número determinado de veces consecutivas su PIN de firma, tanto su *Clave* como el *Certificado* de firma quedarán destruidas. Dicha destrucción será precedida de la revocación del *Certificado de Firma Centralizada* correspondiente a dicha *Clave privada*.

6.2.11. Clasificación de los módulos criptográficos

157. Los módulos criptográficos cumplen con los requisitos de seguridad necesarios para garantizar la protección de las *Claves*, según lo indicado en el apartado "6.2.1 Estándares para los módulos criptográficos" del presente documento.

6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

6.3.1. Archivo de la clave pública

158. Los *Certificados de Firma Centralizada*, y por lo tanto sus *Claves públicas* asociadas, son conservadas por la FNMT-RCM durante el periodo de tiempo exigido por la legislación vigente, de acuerdo con lo establecido en el presente documento.

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

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

- *Certificado* de la AC FNMT raíz y su par de *Claves*: hasta el 1 de enero de 2030.
- El *Certificado* de la AC subordinada que expide los *Certificados de Firma Centralizada* y su par de *Claves*: hasta el 21 de mayo de 2022.
- Los *Certificados de Firma Centralizada* y su par de *Claves:* no superior a 2 años.

6.4. DATOS DE ACTIVACIÓN

6.4.1. Generación e instalación de datos de activación

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

161. En cuanto a los datos de activación de las *Claves* de los *Certificados de Firma Centralizada,* son generados por el módulo de activación de firma en el mismo entorno protegido contra manipulaciones que el dispositivo de creación de firma del *Prestador de Servicios de Confianza*, garantizando que dicha generación sólo puede ser realizada bajo el exclusivo control del que será el *Firmante.*

6.4.2. Protección de datos de activación

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

163. El PIN que protege el acceso a la *Clave privada* del *Certificado de Firma Centralizada* es confidencial, personal e intransferible. Por tanto, el *Firmante*, que además necesita un segundo factor de autenticación para activar su *Clave privada*, es responsable de la protección de sus datos de activación.

6.4.3. Otros aspectos de los datos de activación

164. No estipulados.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

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

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA

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

6.7. CONTROLES DE SEGURIDAD DE RED

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

6.8. FUENTE DE TIEMPO

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

7. PERFILES DE LOS CERTIFICADOS, CRLS Y OCSP

7.1. PERFIL DEL CERTIFICADO

169. Los *Certificados de Firma Centralizada* son de conformidad con el estándar europeo ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons".

7.1.1. Número de versión

170. Los *Certificados de Firma Centralizada* son conformes con el estándar X.509 versión 3.

7.1.2. Extensiones del certificado

171. En la página http://www.cert.fnmt.es/dpcs/ se publica el documento que describe el perfil de los *Certificados de Firma Centralizada*, incluyendo todas sus extensiones.

7.1.3. Identificadores de objeto de algoritmos

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

7.1.4. Formatos de nombres

173. La codificación de los *Certificados de Firma Centralizada* 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 estos *Certificados,* excepto en los campos que específicamente se exprese lo contrario, emplean la codificación UTF8String.

7.1.5. Restricciones de nombres

174. El nombre distintivo (*DN*) asignado al *Suscriptor* del *Certificado* dentro del dominio del *Prestador de Servicios de Confianza* será único y con la composición definida en el perfil del *Certificado*.

7.1.6. Identificador de objeto de política de certificado

175. El identificador de objeto (OID) de la política del *Certificado de Firma Centralizada* 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

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

7.1.8. Sintaxis y semántica de los calificadores de política

177. 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"

178. 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

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

7.2.2. CRL y extensiones

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

Tabla 3 – Perfil de la CRL

Campos y extensiones	Valor
Versión	V2

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

7.3. PERFIL DE OCSP

7.3.1. Número de versión

181. Los *Certificados* utilizados por el *Servicio de información y consulta sobre el estado de validez de los certificados*, vía OCSP, son conformes con el estándar X.509 versión 3.

7.3.2. Extensiones del OCSP

182. Las respuestas OCSP del *Servicio de información y consulta sobre el estado de validez de los certificados* incluyen, para las peticiones que lo soliciten, la extensión global "nonce", que se utiliza para vincular una petición con una respuesta, de forma que se puedan prevenir ataques de repetición.

183. Adicionalmente se incluye la extensión "Extended Revoked Definition" en los casos en los que se consulta por un *Certificado* que a la AC le consta como no emitido. De esta forma, el servicio responde a la consulta de certificados no emitidos por la AC como *Certificado* revocado.

8. AUDITORÍAS DE CUMPLIMIENTO

184. La FNMT-RCM mantendrá un sistema específico con el fin de realizar un registro de eventos para todas aquellas operaciones como: la emisión, validación y revocación de los

Certificados, emisión de *Listas de Revocación*, información sobre el estado de los *Certificados* y emisión de *Sellos de tiempo electrónicos*.

185. Con el objetivo de minimizar el impacto sobre los sistemas en producción, las auditorías sobre los sistemas en producción afectados se planifican en las franjas horarias de baja actividad.

8.1. FRECUENCIA DE LAS AUDITORÍAS

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

- Análisis de riesgos conforme a lo dictado en el Sistema de Gestión de la Seguridad de la Información: Una revisión anual y un análisis completo cada tres (3) años
- Revisión del Sistema de Gestión de la Seguridad de la Información conforme a UNE-ISO/IEC 27001 "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos"
- Calidad: ISO 9001: Una parcial anual externa más una auditoría anual interna preparatoria y una total externa cada tres (3) años, para mantenimiento de la certificación.
- Protección de datos: Una cada dos (2) años interna a realizar por el Departamento de Sistemas de Información.
- La *Autoridad de Certificación* que expide los *Certificados de Firma Centralizada* está sujeta a auditorías periódicas, de conformidad con el estándar europeo ETSI EN 319 401 "General Policy Requirements for Trust Service Providers". Auditoría realizada anualmente por una empresa externa acreditada.
- Una auditoría cada dos (2) años de los sistemas de información de la FNMT-RCM que emplea para la prestación de Servicios de Confianza y conforme a lo dictaminado en el Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica).

8.2. CUALIFICACIÓN DEL AUDITOR

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

8.3. RELACIÓN DEL AUDITOR CON LA EMPRESA AUDITADA

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

8.4. ELEMENTOS OBJETOS DE AUDITORÍA

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

8.5. TOMA DE DECISIONES FRENTE A DETECCIÓN DE DEFICIENCIAS

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

8.6. COMUNICACIÓN DE LOS RESULTADOS

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

9. OTROS ASUNTOS LEGALES Y DE ACTIVIDAD

9.1. TARIFAS

192. FNMT-RCM aplicará a las Administraciones Públicas las tarifas aprobadas por la Subsecretaría de la cual depende para la prestación de los *Servicios de Confianza* o, en su defecto, las tarifas acordadas en el convenio o encomienda de gestión formalizado para tal efecto.

9.1.1. Tarifas de emisión o renovación de certificados

193. La determinación de tarifas aplicables a la emisión o renovación de *Certificados* seguirá lo establecido en el apartado "9.1 Tarifas" del presente documento.

9.1.2. Tarifas de acceso a los certificados

194. No estipulado.

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

195. 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

196. La determinación de tarifas aplicables a otros servicios seguirá lo establecido en el apartado "9.1 Tarifas" del presente documento.

9.1.5. Política de reembolso

197. No estipulada.

9.2. RESPONSABILIDAD FINANCIERA

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

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

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

9.4. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

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

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

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

9.6. OBLIGACIONES Y GARANTÍAS

9.6.1. Obligaciones de la AC

202. Las obligaciones y responsabilidades de la FNMT-RCM, como *Prestador de Servicios de Confianza*, con la persona asociada al *Certificado*, y que actúa como *Firmante*, y con 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 la presente *Declaración de Prácticas y Políticas de Certificación*.

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

204. La FNMT – RCM no pone a disposición de los *Firmantes* los *Certificados de Firma Centralizada* para su recuperación.

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

9.6.2. Obligaciones de la AR

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

9.6.3. Obligaciones de los firmantes

207. La persona física asociada al *Certificado*, que actúa como *Firmante,* debe cumplir las normas de seguridad relacionadas con la custodia y uso del PIN, como dato confidencial, personal e intransferible que garantiza el acceso a sus *Claves privadas*. Por tanto, dicho *Firmante* debe observar las siguientes cautelas relacionadas con el PIN:

- Conservar su confidencialidad, evitando comunicarlo a otras personas.
- Memorizarlo y no anotarlo en ningún documento físico ni electrónico.
- Cambiarlo en el momento en que tenga sospechas de que pueda ser conocido por otra persona.
- Notificar a la FNMT-RCM cualquier posible pérdida de control sobre su *Clave privada*, al objeto de revocar su *Certificado de Firma Centralizada* y sus *Claves* asociadas.
- Abstenerse de escoger un PIN fácilmente deducible de sus datos personales o predecibles (fecha de nacimiento, teléfono, series de números consecutivos, repeticiones del mismo carácter, etc.).

- Seguir la política de seguridad de la FNMT-RCM en relación con la composición del PIN, periodicidad de modificación del mismo, etc.

9.6.4. Obligaciones de las partes que confían

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

9.6.5. Obligaciones de otros participantes

209. No estipulado.

9.7. RENUNCIA DE GARANTÍAS

210. No estipulado.

9.8. RESPONSABILIDADES

9.8.1. Responsabilidad del Prestador de Servicios de Confianza

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

9.8.2. Responsabilidad del Solicitante

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

9.8.3. Responsabilidad del *Firmante*

213. La persona asociada al *Certificado* que actúa como *Firmante* tiene la obligación de:

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

214. Será responsabilidad del *Firmante* 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.

215. En todo caso, el *Firmante* no usará los *Datos de creación de firma* asociados a su *Certificado de Firma Centralizada* en los casos en los que éste haya expirado su periodo de vigencia, o los *Datos de Creación de Firma / Sello* del Prestador puedan estar amenazados y/o comprometidos y así se haya comunicado por el Prestador o, en su caso, el *Firmante* conociera, sospechara o hubiera tenido noticia de estas circunstancias. Si el *Firmante* contraviniera esta obligación, será responsable de las consecuencias de los actos, documentos o transacciones firmadas en estas condiciones, así como de los costes, daños y perjuicios que

pudieran derivarse, para la FNMT-RCM o para terceros, en caso de utilizar el *Certificado* más allá de su período de vigencia.

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

217. Será responsabilidad del *Firmante* el uso que realice de su *Certificado* en caso de que el *Prestador de Servicios de Confianza* haya cesado en la actividad como Entidad emisora de *Certificados* y no se hubiera producido la subrogación prevista en la ley. En todo caso, el *Firmante* no usará los *Datos de creación de firma* asociados a su *Certificado de Firma Centralizada* en los casos en los que éste haya expirado su periodo de vigencia, o los *Datos de Creación de Firma / Sello* del *Prestador* puedan estar amenazados y/o comprometidos y así se haya comunicado por el *Prestador* o, en su caso, el *Firmante* hubiera tenido noticia de estas circunstancias.

9.8.4. Responsabilidad de la Entidad usuaria y terceros que confían

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

9.9. INDEMNIZACIONES

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

9.10. PERIODO DE VALIDEZ DE ESTE DOCUMENTO

9.10.1. Plazo

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

9.10.2. Terminación

221. La presente *Declaración de Practicas 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

222. Para los certificados vigentes emitidos bajo una *Declaración de Practicas 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

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

9.12. MODIFICACIONES DE ESTE DOCUMENTO

9.12.1. Procedimiento para las modificaciones

224. Las modificaciones de la presente *Declaración de Prácticas y Políticas de Certificación* serán aprobadas por la Dirección del departamento Ceres, que quedarán reflejadas en la correspondiente acta del Comité de Gestión del Prestador, de conformidad con el procedimiento interno aprobado mediante el documento "Procedimiento de revisión y mantenimiento de las políticas de certificación y declaración de prácticas de servicios de confianza".

9.12.2. Periodo y mecanismo de notificación

225. El Comité de Gestión del PSC revisará anualmente la presente *Declaración de Prácticas y Políticas de Certificación* y, en cualquier caso, cada vez que deba llevarse a cabo alguna modificación de las mismas.

226. Cualquier modificación en la presente *Declaración de Prácticas y Políticas de Certificación* será publicada de forma inmediata en la URL de acceso a las mismas.

227. Si las modificaciones a realizar no conllevan cambios significativos en cuanto al régimen de obligaciones y responsabilidades de las partes o relativos a una modificación de las políticas de prestación de los servicios, la FNMT-RCM no informará previamente a los usuarios, limitándose a publicar una nueva versión de la declaración afectada en su página web.

9.12.3. Circunstancias bajo las cuales debe cambiarse un OID

228. Las modificaciones significativas de las condiciones de los servicios, régimen de obligaciones y responsabilidades o limitaciones de uso pueden ocasionar un cambio de política del servicio y su identificación (OID), así como el enlace a la nueva declaración de política del servicio. En este caso, la FNMT-RCM podrá establecer un mecanismo de información de los cambios propuestos y, en su caso, de recogida de opiniones de las partes afectadas.

9.13. RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS

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

9.14. NORMATIVA DE APLICACIÓN

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

9.15. CUMPLIMIENTO DE LA NORMATIVA APLICABLE

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

9.16. ESTIPULACIONES DIVERSAS

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

9.17. OTRAS ESTIPULACIONES

233. No se contemplan