Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

POLÍTICA Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS CERTIFICADOS CONSULARES DE LA "AC CONSULARES"

	NAME	DATE
Prepared by:	FNMT-RCM	14/10/2024
Revised by:	FNMT-RCM	14/11/2024
Approved by:	FNMT-RCM	15/11/2024

VERSION	DATE	DESCRIPTION
1.0	15/11/2024	Creación del documento

Referencia: DPC/DCPCON_0100/SGPSC/2023
Documento clasificado como: *Público*

Índice de Contenidos

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 el *Certificado Consular* expedido por la AC Consulares G2, concretamente para los españoles residentes o no residentes en el extranjero que quieran solicitar un certificado, y no se hallen en posesión de su Documento Nacional de Identidad (DNI) en vigor por causa lícita o no hayan dispuesto nunca del mismo.

2. En especial deberá tenerse presente, a efectos interpretativos de estas *Política y prácticas de certificación Particulares*, el apartado "Definiciones" de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*.

3. Los *Certificados Consulares* 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, modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital (en adelante, Reglamento (UE) nº 910/2014), que establece un marco más homogéneo en lo que respecta a la identificación electrónica, definiendo nuevos estándares de seguridad, y conforme a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presta la FNMT – RCM.

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 confianza de la Entidad y, de otro lado, por los apartados específicos del presente documento que constituye la *Declaración de Políticas y Prácticas de Certificación Particulares*. No obstante, 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.

5. Por tanto, 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, existen unas ***Políticas de Certificación*** específicas 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*.

   Esta *Declaración de Políticas 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 de Certificación Particulares* 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.

6. El presente documento define el conjunto de *Prácticas de Certificación* adoptadas por la FNMT-RCM como *Prestador de Servicios de Confianza* para la gestión del ciclo de vida de los *Certificados Consulares* para los españoles que residen en el extranjero y no tienen DNI por causa lícita (o teniéndolo, este haya perdido su vigencia).

   Nombre: Política de Certificación de *Certificados Consulares*

   Referencia / OID[1]: 1.3.6.1.4.1.5734.3.26.1.0

   Tipo de política asociada: 0.4.0.194112.1.0

   Versión: 1.0

   Fecha de expedición: 15/11/2024

[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.

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

7. Las presentes Políticas y Prácticas de Certificación Particulares de Certificados Consulares 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.*

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

9. La FNMT-RCM pone así, 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.*

1.3. PARTES INTERVINIENTES

10. Las partes que intervienen en la gestión y uso de los *Servicios de Confianza* descritos en la presente *Declaración de Políticas de Certificación y Prácticas de Certificación Particulares (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. Autoridades de Certificación

11. La FNMT-RCM es la *Autoridad de Certificación* que expide los Certificados electrónicos objeto de la presente *Declaración de Políticas y Prácticas de Certificación Particulares (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 RAIZ FNMT-RCM G2

Certificado de la AC RAIZFNMT-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 del 2024; No después: 4 de octubre de 2049
Longitud clave pública	ECC 384
Algoritmo de firma	SHA-384 ECDSA
Identificador de clave	A4:D6:B7:70:E7:65:A9:BF:17:EC:D7:B5:E0:3B:85:2D:61:2F:A7:1D

b) Autoridades de Certificación subordinadas: expiden 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 CONSULARES 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)	43 5A 58 19 18 E0 46 DB 23 CA 63 DA E0 FA 06 87 31 1B 4C 35
Validez	No antes: 10 de octubre de 2024; No después: 07 de octubre de 2039
Longitud clave pública	ECDSA (P-256)
Algoritmo de firma	SHA-384 with ECDSA
Identificador de clave	F3:A6:1C:1B:06:71:63:2E:0A:93:51:FF:0D:2D:E6:66:A0:05:84:D7

1.3.2. Autoridad de Registro

12. La Autoridad de Registro realiza tareas de identificación del solicitante, titular de los certificados, así como la comprobación de la documentación y evidencias acreditativas 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.

1.3.3. Suscriptores de los certificados

13. Los *Suscriptores* de los *Certificados Consulares* serán bajo el planteamiento expuesto en el presente informe, los ciudadanos españoles residentes o no residentes en el extranjero que, por causa lícita, no se hallan en posesión de su Documento Nacional de Identidad o que, teniéndolo, no se halla en vigor, que mantienen bajo su uso exclusivo los *Datos de creación de firma* asociados a dichos *Certificados*.

1.3.4. Partes que confían

14. Las partes que confían son aquellas personas físicas o jurídicas, diferentes del *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

15. No estipulado.

1.4. USO DE LOS CERTIFICADOS

1.4.1. Usos permitidos de los certificados

16. Los *Certificados Consulares* a los que aplica esta *DPPP* son *Certificados Cualificados* conforme al Reglamento (UE) nº 910/2014 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”.
17. El *Certificado Consular* es la certificación electrónica expedida por la FNMT-RCM que vincula a un *Suscriptor* con unos *Datos de verificación de Firma* y confirma su identidad.

18. Los *Certificados de firma electrónica* emitidos bajo esta *Política de Certificación* son expedidos a personas físicas y se consideran válidos como sistemas de identificación y de firma electrónicas, de conformidad con la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, basados en Certificados electrónicos cualificados que son admitidos en virtud de su inclusión en las listas de servicios de confianza (TSL, por sus siglas en inglés) conforme a las especificaciones técnicas recogidas en el Anexo de la Decisión de la Comisión 2009/767/CE, de 16 de octubre de 2009 (modificada por la Decisión de la Comisión 2010/425/UE , de 28 de julio de 2010), por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las ventanillas únicas, con arreglo a la Directiva 2006/123/CE, de 12 de diciembre de 2006, del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior. Estas listas de servicios de confianza contienen información relativa a los *Prestadores de Servicios de Confianza* que

expiden *Certificados* cualificados al público supervisados en cada Estado miembro, entre los cuales se encuentra la FNMT–RCM

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 electrónica* realizada con uno de estos *Certificados*, sin acceder al *Servicio de información y consulta sobre el estado de validez de los certificados* expedidos bajo esta *Política de Certificación*, no se obtendrá cobertura de las presentes *Políticas y Prácticas de Certificación Particulares*, y se carecerá de legitimidad alguna para reclamar o emprender acciones legales contra la FNMT RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado*.

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

- Firmar otro *Certificado*, salvo supuestos expresamente autorizados previamente.
- Firmar software o componentes.
- Generar *Sellos de tiempo* para procedimientos de *Fechado electrónico*.
- Prestar servicios a título gratuito u oneroso, salvo supuestos expresamente autorizados previamente, como serían a título enunciativo y no limitativo:
  - Prestar servicios de *OCSP*.
  - Generar *Listas de Revocación*.
  - Prestar servicios de notificación

1.5. ADMINISTRACIÓN DE POLÍTICAS

1.5.1. Entidad responsable

21. La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, Entidad Empresarial, Medio Propio (en lo sucesivo, FNMT-RCM), 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 Servicios Digitales e Innovación- 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 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

26. A los efectos de lo dispuesto en el presente documento, particularizando las definiciones de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* y únicamente cuando los términos comiencen con letra mayúscula y estén en cursiva, se entenderá por:

- *Certificado Consular*: Certificado cualificado de Firma Electrónica cuyo *Suscriptor* es una persona física con nacionalidad española, mayor de edad, residente o no residente en el extranjero, en posesión de un Número de Identificación Consular Central (NICC) y que no se halle en posesión de su Documento Nacional de Identidad (DNI) en vigor por causa lícita o no haya dispuesto nunca del mismo, conforme a lo dispuesto en el Real Decreto 991/2024, de 1 de octubre, sobre inscripción de las personas de nacionalidad española en los Registros de Matrícula de las Oficinas Consulares en el extranjero. Este es un tipo específico de certificado expedido por la FNMT – RCM y, por tanto, estará sujeto a las condiciones establecidas en su Política y Prácticas de Certificación Particulares.
- *Número de Identificación Consular Central:* Número identificativo único e intransferible y permanente, otorgado por el Registro Matricular Consular, en coordinación con el Ministerio del Interior, conforme Real Decreto 991/2024, de 1 de octubre, sobre inscripción de las personas de nacionalidad española en los Registros de Matrícula de las Oficinas Consulares en el extranjero.
- *Servicio de Confianza*: Un servicio electrónico que consiste en alguna de las siguientes actividades: la creación, verificación, validación, gestión y conservación de Firmas Electrónicas, sellos electrónicos, Sellos de Tiempo, documentos electrónicos, servicios de entrega electrónica, autenticación de sitios web y Certificados Electrónicos, incluidos los certificados de Firma Electrónica y de sello electrónico.
- *Suscriptor*: Persona física que suscribe los términos y condiciones de uso de un Certificado. En los Certificados Consulares expedidos bajo la presente Política, coincide con la persona del Titular.

- *Titular (de un Certificado)*: Es la persona física, con nacionalidad española, mayor de edad, ya sea residente habitual en el exterior o se encuentre allí transitoriamente, en posesión de un Número de Identificación Consular Central (NICC) y que no se halle en posesión de su Documento Nacional de Identidad (DNI) en vigor por causa lícita o no haya dispuesto nunca del mismo, cuya identidad queda vinculada a los Datos de verificación de firma (Clave Pública) del Certificado expedido por el Prestador de Servicios de Confianza. Por tanto, la identidad del Titular se vincula a lo firmado electrónicamente utilizando los Datos de creación de firma (Clave Privada) asociados al Certificado.

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
NICC: Número de Identificación Consular Central
OCSP: Protocolo de internet usado para obtener el estado de un Certificado en línea (Online Certificate Status Protocol)
OID: Identificador de Objeto (Object IDentifier)
PKCS: Public Key Cryptography Standards (Estándares PKI desarrollados por RSA Laboratorios)
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.

31. En cuanto a la frecuencia de publicación de CRL, se define en el apartado "4.9.7 Frecuencia de generación de CRLs".

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 compone según se describe en la información relativa al perfil del *Certificado.*

En el procedimiento de acreditación de la identidad, como paso previo a la expedición de un *Certificado Consular* de firma electrónica, la FNMT-RCM, a través de la Oficina de Registro, constatará la verdadera identidad del Suscriptor.

3.1.2. Significado de los nombres

35. 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).

36. El campo Common Name de los *Certificados Consulares* define al *Suscriptor* al que se le ha expedido el *Certificado*.

3.1.3. Seudónimos

37. 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

38. 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

39. 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

40. 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

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

3.2.2. Autenticación de la identidad de la organización

42. Los *Certificados* expedidos bajo las presentes *Políticas de Certificación y Prácticas de Certificación Particulares* no incorporan información de relación del Suscriptor (siempre una persona física) con ninguna organización, por lo que no es de aplicación la validación de dicha información.

3.2.3. Autenticación de la identidad de la persona física solicitante

43. La FNMT-RCM, como *Prestador de Servicios de Confianza*, antes de expedir un *Certificado Consular* identificará al *Solicitante* del mismo utilizando aquellos medios que garanticen la verificación de los atributos específicos de la persona con un nivel alto de confianza, de conformidad con el Reglamento (UE) nº 910/2014 en su artículo 24.1.c). Para ello, se prevé la utilización de la video-identificación como un método reconocido a

escala nacional que aporta una seguridad equivalente, en términos de fiabilidad, a la presencia física de los solicitantes, de acuerdo con lo establecido en el artículo 7.2 de la Ley 6/2020, de 11 de noviembre.

44. La FNMT-RCM desarrollará los controles oportunos para comprobar la veracidad de la información incluida en el *Certificado*.

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

45. La FNMT-RCM podrá expedir el *Certificado Consular* mediante la identificación del *Solicitante* utilizando métodos de identificación reconocidos a escala nacional que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, de conformidad con el Reglamento (UE) nº 910/2014, como es, la identificación remota por vídeo de un solicitante. Se exige verificar la autenticidad y validez del documento de identidad, así como su correspondencia con el solicitante del certificado. Para ello, el sistema de identificación remota por vídeo empleado en el proceso deberá incorporar los medios técnicos y organizativos necesarios para verificar la autenticidad, vigencia e integridad de los documentos de identificación utilizados, verificar la correspondencia del titular del documento con el solicitante que realiza el proceso, mediante tecnologías como el reconocimiento facial, y verificar que este es una persona viva que no está siendo suplantada.

46. El *Solicitante* se identificará a través del sistema de identificación remota por video no asistida (asíncrona). La verificación de identidad se basará en un reconocimiento facial mediante procedimientos biométricos, la aportación del documento de identificación requerido para acreditar su identidad y la obtención de otras evidencias. Dicha acreditación se realizará de conformidad con el art. 24.1.c) del Reglamento (UE) nº 910/2014; el artículo 7.2 de la Ley 6/2020, de 11 de noviembre y cumpliendo las condiciones y requisitos organizativos y técnicos establecidos por la Orden ETD/465/2021 de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

3.2.4. Información no verificada del Suscriptor

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

3.2.5. Validación de la autorización

48. Una vez confirmada la identidad del *Solicitante,* se procederá a validar los datos junto con el código de solicitud remitido al *Solicitante* por correo electrónico. Esta transmisión de información se realizará mediante comunicaciones seguras establecidas para tal fin. Los datos personales y su tratamiento, en su caso, quedarán sometidos a la legislación específica.

49. Previa a la emisión del *Certificado*, la FNMT-RCM establece controles adicionales como, por ejemplo, confirmar que el solicitante no está inscrito como difunto en los registros que el Ministerio de Justicia comunica a esta Entidad para tal fin.

50. No se emitirán *Certificados* a menores de edad.

3.2.6. Criterios de interoperación

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

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RENOVACIÓN DE CLAVES

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

53. 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

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

3.3.2. Renovación después de una revocación

55. 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

56. Previa a la revocación efectiva de los *Certificados*, la Autoridad de Registro identificará de forma fehaciente al *Solicitante* de la *Revocación* para vincularle con los datos únicos del *Certificado* a revocar.

57. 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

58. El *Solicitante* de este tipo de *Certificados* sólo puede ser una persona física, mayor de edad, residente o no residente en el extranjero, en posesión de su Número de Identificación Consular Central (NICC) y que no se halle en posesión de su Documento Nacional de Identidad (DNI) en vigor por causa lícita o no haya dispuesto nunca del mismo.

4.1.2. Proceso de registro y responsabilidades

59. El interesado accede al sitio web del *Prestador de Servicios de Confianza* de la FNMT-RCM, a través de la dirección http://www.cert.fnmt.es, donde se mostrarán las instrucciones del proceso completo de obtención del *Certificado Consular*. El Solicitante deberá introducir su Número de Identificador Personal (ID Number) del Pasaporte, su

primer apellido y su dirección de correo electrónico en el punto de recogida de datos dispuesto para ello. Así mismo, el *Solicitante* manifestará su voluntad de obtener un *Certificado Consular* y dará su consentimiento para que la FNMT-RCM pueda realizar una consulta al Sistema de Registro de Matrícula Consular.

60. Posteriormente se generan las *Claves Pública y Privada* (en el navegador) que serán vinculadas al *Certificado* que se generará en una fase posterior, y la FNMT – RCM asigna a la solicitud un código único.

61. Con carácter previo el Solicitante deberá consultar las Declaraciones General y Particular de Prácticas de Certificación en la dirección http://www.ceres.fnmt.es/dpcs/ con las condiciones de uso y obligaciones para las partes.

62. Al realizar esta solicitud se envía a la FNMT-RCM la *Clave Pública* generada, junto con las correspondientes pruebas de posesión de la *Clave Privada*, para la posterior expedición del *Certificado*. El envío de la *Clave Pública* a la AC para la generación del *Certificado* se realiza mediante un formato estándar, PKCS#10 o SPKAC, y utilizando un canal seguro.

63. La FNMT-RCM, tras recibir esta información comprobará, mediante la *Clave Pública* del *Solicitante*, la validez de la información de la solicitud, la posesión y correspondencia de la pareja de *Claves* criptográficas por parte del *Solicitante*, así como el tamaño de las claves generadas.

64. Esta información no dará lugar a la generación de un *Certificado* por parte de la FNMT-RCM, en tanto que esta no reciba la confirmación de la identificación electrónica del *Solicitante*, realizada a través de su identificación remota por vídeo con la posterior confirmación de la identidad de los *Solicitantes* por parte del agente cualificado con formación previa.

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

66. 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

67. Para la emisión de *Certificados Consulares*, la FNMT-RCM identificará al *Solicitante* mediante el sistema de identificación remota por video no asistido de la FNMT-RCM, según se describe en el apartado “3.2.3.1. *Comprobación indirecta mediante medios de aseguramiento equivalente a la presencia física de conformidad con el Derecho nacional”*. Para poder iniciar el proceso de verificación de la identidad, el *Solicitante* deberá haber realizado previamente la solicitud del *Certificado Consular* y obtenido el correspondiente código de solicitud. Adicionalmente, también el *Solicitante* deberá aceptar las condiciones de uso y política de privacidad.

68. Tras obtener las evidencias para comprobar la identidad por medios a distancia, la FNMT-RCM, a través de un operador cualificado y autorizado por la *Autoridad de Registro*, revisará el proceso de identificación grabado y comprobará las evidencias generadas por

el sistema para aceptar o rechazar la validez del proceso de identificación, de conformidad con la normativa aplicable sobre las causas de rechazo de la video identificación.

69. Los datos personales recabados para realizar la verificación de la identidad serán almacenados por la FNMT-RCM durante los plazos de tiempo establecidos por la normativa específica de aplicación.

4.2.2. Aprobación o rechazo de la solicitud del certificado

70. En los *Certificados Consulares*, una vez confirmada la identidad del *Solicitante*, la solicitud deberá ser revisada por un agente que haya recibido, previamente, formación específica sobre las características verificables por el método de identificación, sus procedimientos, métodos de prueba y métodos comunes de falsificación. Para ello, el agente se encargará de verificar la identidad del *Solicitante* en base a los datos recibidos junto al código de solicitud. Si los datos son correctos y se verifica su cumplimiento, además de comprobarse la conformidad con las medidas de seguridad determinadas para tal efecto, se procederá a la expedición del Certificado desde la FNMT-RCM.

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

72. La FNMT-RCM recabará de los *Solicitantes* aquella información 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.

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

4.2.3. Tiempo en procesar la solicitud

74. La solicitud aprobada de los *Certificados Consulares* procesada automáticamente por el sistema en tiempo real, 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

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

76. La expedición de *Certificados Consular* supone la generación de documentos electrónicos que confirman la identidad del *Titular*, así como su correspondencia con la *Clave Pública* asociada. La expedición de *Certificados Consulares* 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.

77. La FNMT - RCM, por medio de su *Firma electrónica* o *Sello electrónico*, autentica los *Certificados Consulares* y confirma la identidad del *Titular*. Por otro lado, y con el fin de

evitar la manipulación de la información contenida en los *Certificados*, la FNMT - RCM utilizará mecanismos criptográficos que doten de autenticidad e integridad al *Certificado*.

78. 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.*

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

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

80. La emisión de los *Certificados Consulares* atenderá a:

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

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

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

81. 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 emisión de certificado

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

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1. Proceso de aceptación

83. 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.

84. La FNMT-RCM pondrá a disposición exclusiva del *Titular* su *Certificado Consular* para que proceda a su descarga en la página web http://www.cert.fnmt.es.

85. En este proceso guiado de descarga, se le pedirá al *Solicitante* que introduzca su número de Identificador Personal (ID Number) del Pasaporte, el primer apellido, así como el correspondiente código de solicitud obtenido en dicho proceso. Este código de solicitud será empleado, como clave concertada, para la generación por parte del *Titular* de una firma electrónica de las condiciones de uso del *Certificado*, como requisito para acceder a la descarga del mismo y como aceptación de dichas condiciones de uso, remitiéndolas firmadas a la FNMT –RCM. Si el *Certificado Consular* aún no hubiera sido generado por cualquier motivo, el proceso le informará de este hecho.

86. En el momento de la descarga del *Certificado Consular*, este se instalará en el soporte en el que se generaron las *Claves* durante el proceso de solicitud (*Navegador* desde el cual hizo la solicitud). En la citada página web de la FNMT-RCM se indican los *Navegadores* soportados y normas de instalación de los certificados.

4.4.2. Publicación del certificado por la AC

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 *Titular* del *Certificado*.

90. Los *Certificados Consular* emitidos bajo esta *Política de Certificación* son certificados cualificados expedidos a personas físicas y se consideran válidos como sistemas de identificación y de firma electrónicas, de conformidad con la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

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

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

4.6. RENOVACIÓN DEL CERTIFICADO

92. 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

93. 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

94. 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

95. 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

96. 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

97. 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

98. 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

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

4.6.8. Procesamiento de solicitudes de modificación del certificado

100. No se estipula la modificación.

4.7. RENOVACIÓN CON REGENERACIÓN DE LAS CLAVES DEL CERTIFICADO

101. Bajo las presentes Políticas de Certificación, la renovación con regeneración de claves de los *Certificados Consulares* 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

102. Las claves de los *Certificados* se renovarán por caducidad próxima de las actuales claves, a petición del solicitante de la renovación.

4.7.2. Quién puede solicitar la renovación con regeneración de claves

103. 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

104. 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

105. 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

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

4.7.6. Publicación del certificado renovado

107. 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

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

4.8. MODIFICACIÓN DEL CERTIFICADO

109. 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

110. No se estipula la modificación.

4.8.2. Quién puede solicitar la modificación del certificado

111. No se estipula la modificación.

4.8.3. Procesamiento de solicitudes de modificación del certificado

112. No se estipula la modificación.

4.8.4. Notificación de la modificación del certificado

113. No se estipula la modificación.

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

114. No se estipula la modificación.

4.8.6. Publicación del certificado modificado

115. No se estipula la modificación.

4.8.7. Notificación de la modificación del certificado a otras entidades

116. No se estipula la modificación.

4.9. REVOCACIÓN DEL CERTIFICADO

117. Los *Certificados Consulares* expedidos por la FNMT-RCM quedarán sin efecto en los siguientes casos:

a) Terminación del período de validez del *Certificado*.

b) Cese en la actividad como *Prestador de Servicios de Confianza* de la FNMT-RCM, salvo que, previo consentimiento expreso del *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.

118. Los efectos de la revocación del *Certificado*, esto es, la extinción de su vigencia, surtirán efecto desde 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*.

119. A los efectos enumerados anteriormente, la expedición de un *Certificado Consular* cuando exista otro vigente a favor del mismo *Titular*, conllevará la revocación inmediata del *Certificado* anterior.

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

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

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

a) La solicitud de revocación por parte del *Suscriptor*. En todo caso deberá dar lugar a esta solicitud:

- La pérdida del soporte del *Certificado*
- La utilización por un tercero de los *Datos de Creación de Firma*, correspondientes a los *Datos de Verificación de Firma* contenidos en el *Certificado* y vinculados a la identidad personal del *Titular*.
- La violación o puesta en peligro del secreto de los *Datos de Creación de Firma* 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 de Certificación*, durante el periodo de un mes tras su publicación.

b) Resolución judicial o administrativa que así lo ordene.

c) Fallecimiento o incapacidad sobrevenida, total o parcial, del *Titular.*

d) Inexactitudes en los datos aportados por el *Solicitante* para la obtención del *Certificado*, o alteración de los datos aportados para la obtención del *Certificado* o modificación de las circunstancias verificadas para la expedición del *Certificado*, de manera que este ya no fuera conforme a la realidad.

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

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

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

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

i) 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.*

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

123. 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 *Suscriptor* o por medio de los sistemas puestos a disposición por la FNMT-RCM para este fin.
- Que la solicitud de revocación o la causa que la motiva, le haya sido notificada mediante resolución judicial o administrativa.
- Que las causas c) a f) del presente apartado le sean acreditadas fehacientemente, previa identificación del *Suscriptor* y/o *Solicitante* de la revocación (o persona con facultades de representación suficientes, si se produjera incapacidad sobrevenida del *Suscriptor*).

124. La FNMT-RCM podrá revocar de oficio los *Certificados* de los *Suscriptores* cuando se den las causas b) a i) del presente apartado.

125. 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.

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

4.9.1.2 Circunstancias para la revocación del certificado de la CA subordinada

127. 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

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

- la *Autoridad de Certificación* y la *Autoridad de Registro*
- el *Suscriptor* o persona autorizada
- 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.

129. 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

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

131. La revocación de un *Certificado Consular* solamente podrá ser solicitada por el *Titular* o persona con facultades de representación suficientes, si se produjera incapacidad sobrevenida del *Titular*, en los términos recogidos en las presentes *Políticas de Certificación y Prácticas de Certificación Particulares.*

132. 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. Este servicio estará disponible las veinticuatro (24) horas del día, todos los días del año, salvo por circunstancias ajenas a la FNMT-RCM u operaciones de mantenimiento. La FNMT-RCM notificará las operaciones de mantenimiento o indisponibilidad del servicio en http://www.ceres.fnmt.es, si es posible con al menos cuarenta y ocho (48) horas de antelación y tratará de solventarla en un periodo no superior a veinticuatro (24) horas.

133. 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.

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

135. 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.

4.9.4. Periodo de gracia de la solicitud de revocación

136. 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

137. 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

138. 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, y
- el estado de los *Certificados* incluidos en la *Cadena de Certificación.*

4.9.7. Frecuencia de generación de CRLs

139. Las *Listas de Revocación* (CRL) de los *Certificados Consulares* 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

140. 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

141. 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

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

143. No definidas.

4.9.12. Requisitos especiales de revocación de claves comprometidas

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

4.9.13. Circunstancias para la suspensión

145. No se contempla la suspensión de Certificados.

4.9.14. Quién puede solicitar la suspensión

146. No se contempla la suspensión de Certificados.

4.9.15. Procedimiento para la petición de la suspensión

147. No se contempla la suspensión de Certificados.

4.9.16. Límites sobre el periodo de suspensión

148. No se contempla la suspensión de Certificados.

4.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE LOS CERTIFICADOS

4.10.1. Características operativas

149. 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

150. 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

151. No estipuladas.

4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN

152. 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 *Suscriptor* y la FNMT-RCM.

153. A los efectos enumerados anteriormente, se hace constar que la solicitud de emisión de un *Certificado Consular* emitido por la FNMT-RCM cuando exista otro vigente a favor del 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

154. La FNMT-RCM no recuperará las *Claves privadas* de los Titulares de los *Certificados*.

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

155. No estipulado.

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

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

5.1. CONTROLES DE SEGURIDAD FÍSICA

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

5.1.1. Ubicación de las instalaciones

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

5.1.2. Acceso Físico

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

5.1.3. Electricidad y Aire Acondicionado

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

5.1.4. Exposición al agua

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

5.1.5. Prevención y Protección contra incendios

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

5.1.6. Almacenamiento de Soportes

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

5.1.7. Eliminación de Residuos

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

5.1.8. Copias de Seguridad fuera de las instalaciones

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

5.2. CONTROLES DE PROCEDIMIENTO

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

5.2.1. Roles de confianza

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

5.2.2. Número de personas por tarea

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

5.2.3. Identificación y autenticación para cada rol

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

5.2.4. Roles que requieren segregación de funciones

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

5.3. CONTROLES DE PERSONAL

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

5.3.1. Conocimientos, cualificación, experiencia y requerimientos acreditativos

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

5.3.2. Procedimientos de verificación de antecedentes

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

5.3.3. Requisitos de formación

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

5.3.4. Requisitos y frecuencia de actualización formativa

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

5.3.5. Secuencia y frecuencia de rotación laboral

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

5.3.6. Sanciones por acciones no autorizadas

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

5.3.7. Requisitos de contratación de personal

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

5.3.8. Suministro de documentación al personal

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

5.4. PROCEDIMIENTOS DE AUDITORÍA

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

5.4.1. Tipos de eventos registrados

181. Véase el apartado correspondiente en la *DGPC*

5.4.2. Frecuencia de procesamiento de registros

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

5.4.3. Periodo de conservación de los registros

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

5.4.4. Protección de los registros

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

5.4.5. Procedimientos de copias de seguridad de los registros auditados

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

5.4.6. Sistemas de recolección de registros

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

5.4.7. Notificación al sujeto causante de los eventos

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

5.4.8. Análisis de vulnerabilidades

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

5.5. ARCHIVADO DE REGISTROS

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

5.5.1. Tipos de registros archivados

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

5.5.2. Periodo de retención del archivo

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

5.5.3. Protección del archivo

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

5.5.4. Procedimientos de copia de respaldo del archivo

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

5.5.5. Requisitos para el sellado de tiempo de los registros

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

5.5.6. Sistema de archivo

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

5.5.7. Procedimientos para obtener y verificar la información archivada

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

5.6. CAMBIO DE CLAVES DE LA AC

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

5.7. GESTIÓN DE INCIDENTES Y VULNERABILIDADES

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

5.7.1. Gestión de incidentes y vulnerabilidades

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

5.7.2. Actuación ante datos y software corruptos

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

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

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

5.7.4. Continuidad de negocio después de un desastre

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

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

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

6. CONTROLES DE SEGURIDAD TÉCNICA

204. 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

205. 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

206. No estipulado.

6.1.1.3. Generación del par de Claves de los Suscriptores

207. 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

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

209. En todo caso, si la FNMT-RCM 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

210. La *Clave pública*, generada por el *Suscriptor* 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 la solicitud del *Certificado*.

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

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

6.1.5. Tamaños de claves y algoritmos utilizados

212. Los algoritmos utilizados son:

- Para la AC FNMT G2 raíz: ecdsa-with-SHA384.
- Para la subordinada, AC Consulares: ecdsa-with-SHA384.
- Para los *Certificados Consulares*: ecdsa-with-SHA256.

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

- Claves de la AC FNMT-RCM G2 raíz: ECC P-384.
- Claves de la AC Consulares G2 Subordinada: ECC P-256.
- Claves de los *Certificados Consulares*: ECC P-256 o RSA Encryption con una longitud de 2048 bits.

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

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

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

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

216. El *Certificado* de la AC FNMT-RCM G2 raíz tiene habilitados los usos de *Claves* para firmar/sellar los *Certificados* de las ACs FNMT Subordinadas y las ARLs.

217. El *Certificado* de la AC Consulares que expide los *Certificados Consulares* tiene habilitado exclusivamente el uso para firmar/sellar *Certificados* de entidad final y CRLs.

218. Los *Certificados Consulares* tienen habilitado exclusivamente los usos de autenticación y firma en todos los casos y añadiendo el uso de clave de cifrado en los *Certificados Consulares* con clave RSA.

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

6.2.1. Estándares para los módulos criptográficos

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

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

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

6.2.3. Custodia de la clave privada

221. 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

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

6.2.5. Archivado de la clave privada

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

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

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

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

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

6.2.8. Método de activación de la clave privada

226. 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.

227. 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

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

6.2.10. Método de destrucción de la clave privada

229. 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

230. 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

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

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

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

- *Certificado* de la AC FNMT G2 raíz y su par de *Claves*: hasta el 04 de octubre de 2049.
- El *Certificado* de la AC subordinada que expide los *Certificados Consulares*: hasta el 07 de octubre de 2039.
- Los *Certificados Consulares* y su par de *Claves*: no superior a 4 años.

6.4. DATOS DE ACTIVACIÓN

6.4.1. Generación e instalación de datos de activación

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

6.4.2. Protección de datos de activación

234. 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

235. No estipulados.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

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

6.5.1. Requisitos técnicos específicos de seguridad informática

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

6.5.2. Evaluación del nivel de seguridad informática

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

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA

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

6.6.1. Controles de desarrollo de sistemas

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

6.6.2. Controles de gestión de la seguridad

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

6.6.3. Controles de seguridad del ciclo de vida

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

6.7. CONTROLES DE SEGURIDAD DE RED

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

6.8. FUENTE DE TIEMPO

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

6.9. OTROS CONTROLES ADICIONALES

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

6.9.1. Control de la capacidad de prestación de los servicios

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

6.9.2. Control de desarrollo de sistemas y aplicaciones informáticas

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

7. PERFILES DE LOS CERTIFICADOS, CRLS Y OCSP

7.1. PERFIL DEL CERTIFICADO

248. Los Certificados Consulares son expedidos como "cualificados" de conformidad con los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons".

7.1.1. Número de versión

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

7.1.2. Extensiones del certificado

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

251. Todos los certificados emitidos bajo estas políticas de certificación contendrán una extensión no crítica, qcStatements, usando el qcStatement-2 predefinido en el RFC 3739, en el que todos los valores en sematicsInformation serán:

- semanticsIdentifier: id-etsi-qcs-semanticsId-Natural
- nameRegistrationAuthorities: https://exteriores.gob.es (del tipo URI generalName)

7.1.3. Identificadores de objeto de algoritmos

252. Los identificadores de objeto (OIDs) correspondiente a los algoritmos criptográficos utilizados son:

- Para *la AC FNMT G2 raíz* y la AC Consular G2 *Subordinada* es 1.2.840.10045.4.3.3 (ecdsa-with-SHA384).
- Para los *Certificados Consulares* es 1.2.840.10045.4.3.2 (ecdsa-with-SHA256).

7.1.4. Formatos de nombres

253. 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.

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

255. La semántica de campo serialNumber será la siguiente:

EX:ES-XXXXXXXXT,

donde "xxxxxxxxT" es el Número de Identificación Consular Central (NICC) que es un número identificativo único e intransferible y permanente, otorgado por el Registro Matricular Consular, en coordinación con el Ministerio del Interior, conforme al Real Decreto 991/2024, de 1 de octubre, sobre inscripción de las personas de nacionalidad española en los Registros de Matrícula de las Oficinas Consulares en el extranjero.

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 del *Certificado Consular* 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 Constrains" del *Certificado* raíz de la AC no es utilizada.

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 publica la *DGPC* y las *Políticas de Certificación y Prácticas de Certificación Particulares* aplicables a los *Certificados*.

- User notice: contiene un texto que puede ser desplegado en la pantalla del usuario del *Certificado* durante la verificación del mismo.

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

7.2.2. CRL y extensiones

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

Tabla 3 – Perfil de la CRL

Campos y extensiones	Valor
Versión	V2
Algoritmo de firma	ecdsa-with-SHA384
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
ExpiredCertsOnCRL	NotBefore de la CA
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

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 Consulares* está sujeta a auditorías periódicas, de conformidad con el estándar europeo ETSI EN 319 401 "General Policy Requirements for Trust Service Providers", ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons". La auditoría es realizada anualmente por una empresa externa acreditada.

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

8.2. CUALIFICACIÓN DEL AUDITOR

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

8.3. RELACIÓN DEL AUDITOR CON LA EMPRESA AUDITADA

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

8.4. ELEMENTOS OBJETO DE AUDITORÍA

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

8.5. TOMA DE DECISIONES FRENTE A DETECCIÓN DE DEFICIENCIAS

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

8.6. COMUNICACIÓN DE LOS RESULTADOS

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

8.7. AUTOEVALUACIÓN

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

9. OTROS ASUNTOS LEGALES Y DE ACTIVIDAD

9.1. TARIFAS

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

9.1.1. Tarifas de emisión o renovación de certificados

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

9.1.2. Tarifas de acceso a los certificados

280. No estipulado.

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

281. 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

282. Véase el apartado correspondiente en la DGPC. .

9.1.5. Política de reembolso

283. Los Certificados emitidos bajo esta *DPPP* no conllevan gasto alguno para los *Suscriptores*, por lo que no procede establecer política de reembolso.

9.2. RESPONSABILIDAD FINANCIERA

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

9.2.1. Seguro de responsabilidad civil

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

9.2.2. Otros activos

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

9.2.3. Seguros y garantías para entidades finales

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

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

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

9.3.1. Alcance de la información confidencial

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

9.3.2. Información no incluida en el alcance

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

9.3.3. Responsabilidad para proteger la información confidencial

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

9.4. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

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

9.4.1. Plan de privacidad

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

9.4.2. Información tratada como privada

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

9.4.3. Información no considerada privada

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

9.4.4. Responsabilidad de proteger la información privada

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

9.4.5. Aviso y consentimiento para usar información privada

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

9.4.6. Divulgación conforme al proceso judicial o administrativo

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

9.4.7. Otras circunstancias de divulgación de información

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

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

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

9.6. OBLIGACIONES Y GARANTÍAS

9.6.1. Obligaciones de la AC

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

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

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

9.6.2. Obligaciones de la AR

304. 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 Consulares*, 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.

305. 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.

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

9.6.3. Obligaciones del Suscriptor

9.6.3.1. Responsabilidad del Solicitante

307. 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.

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

9.6.3.2. Responsabilidad del Suscriptor

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

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

310. Será responsabilidad del *Titular* informar a la FNMT-RCM acerca de cualquier variación de estado o información respecto de lo reflejado en el *Certificado*, para su revocación y nueva expedición.

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

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

9.6.4. Obligaciones de las partes que confían

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

9.6.5. Obligaciones de otros participantes

314. No estipulado.

9.7. RENUNCIA DE GARANTÍAS

315. No estipulado.

9.8. LÍMITES DE RESPONSABILIDAD

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

9.9. INDEMNIZACIONES

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

9.9.1. Indemnización de la CA

318. No estipulado.

9.9.2. Indemnización de los Suscriptores

319. No estipulado.

9.9.3. Indemnización de las partes que confían

320. No estipulado.

9.10. PERIODO DE VALIDEZ DE ESTE DOCUMENTO

9.10.1. Plazo

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

9.10.2. Terminación

322. 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

323. 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

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

9.12. MODIFICACIONES DE ESTE DOCUMENTO

9.12.1. Procedimiento para las modificaciones

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

9.12.2. Periodo y mecanismo de notificación

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

9.12.3. Circunstancias bajo las cuales debe cambiarse un OID

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

9.13. RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS

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

9.14. NORMATIVA DE APLICACIÓN

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

9.15. CUMPLIMIENTO DE LA NORMATIVA APLICABLE

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

9.16. ESTIPULACIONES DIVERSAS

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

9.16.1. Acuerdo íntegro

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

9.16.2. Asignación

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

9.16.3. Severabilidad

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

9.16.4. Cumplimiento

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

9.16.5. Fuerza Mayor

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

9.17. OTRAS ESTIPULACIONES

337. No se contemplan.