



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

**POLÍTICAS Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES APLICABLES A LOS SERVICIOS  
DE CERTIFICACIÓN Y FIRMA ELECTRÓNICA EN EL ÁMBITO DE ORGANIZACIÓN Y  
FUNCIONAMIENTO DE LAS ADMINISTRACIONES PÚBLICAS, SUS ORGANISMOS Y ENTIDADES  
VINCULADAS O DEPENDIENTES**

|                | <b>NOMBRE</b>   | <b>FECHA</b> |
|----------------|-----------------|--------------|
| Elaborado por: | FNMT-RCM        | 06/11/2008   |
| Revisado por:  | FNMT-RCM / v1.1 | 5/5/2009     |
| Aprobado por:  | FNMT-RCM / v1.1 | 5/5/2009     |

| <b>HISTÓRICO DEL DOCUMENTO</b> |              |   |              |
|--------------------------------|--------------|---|--------------|
| <b>Versión</b>                 | <b>Fecha</b> | <b>Descripción</b>  | <b>Autor</b> |
| 1.0                            | 06/11/2008   | Creación del documento  | FNMT-RCM     |
| 1.1                            | 5/5/2009     | Ampliación de la vigencias de los certificados a cuatro años. | FNMT-RCM     |
|                                |              |   |              |

**Referencia:** DPC/PCPAA0101/SGPSC/2008

**Documento clasificado como:** *Público*

## ÍNDICES

### ÍNDICE DE CONTENIDOS

|  |           |
|--|-----------|
| Índices .....  | 2         |
| Índice de contenidos.....  | 2         |
| Índice de Tablas .....   | 5         |
| <b>1. Preliminar .....</b>   | <b>6</b>  |
| <b>2. Introducción.....</b>  | <b>7</b>  |
| <b>3. Organización del documento.....</b>  | <b>7</b>  |
| <b>4. Orden de prelación.....</b>  | <b>9</b>  |
| <b>5. Gestión del ciclo de vida de las claves del prestador de servicios de certificación.....</b>   | <b>10</b> |
| 5.1. <i>Gestión del ciclo de vida de las Claves</i> .....  | 10        |
| 5.1.1. Generación de las <i>Claves del Prestador de Servicios de Certificación</i> .....   | 10        |
| 5.1.2. Almacenamiento, salvaguarda y recuperación de las Claves del Prestador de Servicios de Certificación .....  | 10        |
| 5.1.3. Distribución de los Datos de verificación de Firma del Prestador de Servicios de Certificación  | 10        |
| 5.1.4. Almacenamiento, salvaguarda y recuperación de las Claves Privadas de la Administración, Organismos y Entidades públicas usuarias.....   | 20        |
| 5.1.5. Uso de los Datos de Creación de Firma del Prestador de Servicios de Certificación .....   | 21        |
| 5.1.6. Fin del ciclo de vida de las <i>Claves del Prestador de Servicios de Certificación</i> .....  | 21        |
| 5.1.7. Ciclo de vida del hardware criptográfico utilizado para firmar <i>Certificados</i> .....  | 21        |
| <b>6. Operación y Gestión de la Infraestructura de <i>Clave Pública</i>; Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad .....</b>   | <b>21</b> |
| 6.1. <i>operación y gestión de la infraestructura de clave pública</i> .....   | 21        |
| 6.2. <i>Esquema nacional de interoperabilidad y esquema nacional de seguridad</i> .....  | 22        |
| <b>7. Terminación de la FNMT-RCM en su actividad como Prestador de Servicios de Certificación .....</b>  | <b>22</b> |
| <b>8. Difusión de Términos y Condiciones .....</b>   | <b>22</b> |
| <b>9. Aspectos organizativos.....</b>  | <b>23</b> |
| <b>10. Certificados emitidos para el personal al servicio de las Administraciones Públicas, Organismos y entidades públicas vinculadas o dependientes (en adelante personal al servicio de la Administración Pública) .....</b>                                    | <b>24</b> |
| 10.1. <i>Política de Certificación de los Certificados emitidos para el personal al servicio de las Administraciones Públicas, Organismos y entidades públicas vinculadas o dependientes (en adelante personal al servicio de la Administración Pública)</i> ..... | 24        |
| 10.2. <i>Identificación</i> .....  | 24        |

|            |   |           |
|------------|---|-----------|
| 10.2.1.    | Tipología del Certificado para personal al servicio de las Administraciones Públicas: (funcionarios, personal laboral, estatutario a su servicio y personal autorizado, en adelante denominado como personal al servicio de las Administraciones Públicas)..... | 24        |
| 10.2.2.    | Gestión de la Política de Certificación.....  | 26        |
| 10.2.3.    | Comunidad y ámbito de aplicación.....   | 27        |
| 10.2.4.    | Responsabilidad y obligaciones de las partes .....  | 28        |
| 10.2.5.    | Límites de uso de los <i>Certificados</i> para personal al servicio de la Administración Pública .....  | 30        |
| 10.3.      | <i>Prácticas de certificación particulares para los Certificados emitidos para personal al servicio de la Administración Pública</i> .....  | 31        |
| 10.3.1.    | Servicios de Gestión de las <i>Claves</i> de los <i>Titulares</i> .....   | 31        |
| 10.3.2.    | Preparación de los <i>Dispositivos Seguros de Creación de Firma</i> .....   | 31        |
| 10.3.3.    | Gestión del ciclo de vida de los <i>Certificados</i> .....  | 32        |
| 10.3.3.1.  | Procedimiento de solicitud del Certificado para personal al servicio de la Administración Pública   | 32        |
| 10.3.3.2.  | Personación ante las Oficinas de Registro .....   | 34        |
| 10.3.3.3.  | Comparecencia y documentación.....  | 35        |
| 10.3.3.4.  | Emisión del Certificado para personal al servicio de la Administración Pública.....   | 35        |
| 10.3.3.5.  | Publicación del Certificado de personal al servicio de la Administración Pública .....  | 42        |
| 10.3.3.6.  | Descarga e instalación del Certificado de personal al servicio de la Administración Pública   | 43        |
| 10.3.3.7.  | Período de validez del Certificado de personal al servicio de la Administración Pública..   | 43        |
| 10.3.3.8.  | Revocación del Certificado de personal al servicio de la Administración Pública .....   | 43        |
| 10.3.3.9.  | Suspensión del Certificado de personal al servicio de la Administración Pública.....  | 44        |
| 10.3.3.10. | Comprobación del estado del Certificado del personal al servicio de la Administración ..  | 46        |
| 10.3.4.    | Exclusiones y requisitos adicionales a ETSI TS 101 456 .....  | 46        |
| 10.3.5.    | Modelos de formulario.....  | 46        |
| <b>11.</b> | <b>Certificados emitidos para la identificación de sedes electrónicas de la Administración Pública, Organismos y entidades públicas vinculadas o dependientes.....</b>  | <b>47</b> |
| 11.1.      | <i>Política de Certificación de los Certificados emitidos para la identificación de sedes electrónicas de la Administración Pública, Organismos y entidades públicas vinculadas o dependientes</i> .....  | 47        |
| 11.1.1.    | Identificación .....  | 47        |
| 11.1.2.    | Tipología del <i>Certificado</i> para la identificación de sedes electrónicas de la Administración Pública, Organismos y entidades públicas vinculadas o dependientes.....  | 48        |
| 11.1.3.    | Gestión de la Política de Certificación.....  | 50        |
| 11.1.4.    | Comunidad y ámbito de aplicación.....   | 51        |
| 11.1.5.    | Responsabilidad y obligaciones de las partes .....  | 52        |
| 11.1.6.    | Límites de uso de los <i>Certificados</i> para la identificación de sedes electrónicas .....  | 54        |
| 11.2.      | <i>Prácticas de certificación particulares para los Certificados emitidos para la identificación de sedes electrónicas de la Administración Pública, Organismos y entidades públicas vinculadas o dependientes</i> .....  | 55        |
| 11.2.1.    | Servicios de Gestión de las <i>Claves</i> de los <i>Usuarios</i> y <i>Titulares</i> .....   | 55        |
| 11.2.2.    | Gestión del ciclo de vida de los <i>Certificados</i> .....  | 55        |
| 11.2.2.1.  | Registro de los <i>Titulares</i> de <i>Certificados</i> de sede electrónica ámbito público .....  | 55        |
| 11.2.2.2.  | Procedimiento de solicitud del Certificado para la identificación de sedes electrónicas ...   | 56        |
| 11.2.2.3.  | Presolicitud .....  | 56        |
| 11.2.2.4.  | Confirmación de las identidades y requisitos de las partes .....  | 57        |
| 11.2.2.5.  | Personación del Solicitante ante las Oficinas de Registro.....  | 58        |
| 11.2.2.6.  | Comparecencia y documentación.....  | 58        |
| 11.2.2.7.  | Envío de información a la FNMT-RCM.....   | 58        |
| 11.2.2.8.  | Extensión de la función de registro e identificación a otros <i>Certificados</i> emitidos por la FNMT-RCM.....  | 59        |



|            |  |    |
|------------|--|----|
| 11.2.2.9.  | Emisión del Certificado para la identificación de sede electrónica.....  | 59 |
| 11.2.2.10. | Publicación del Certificado de identificación de sede electrónica .....  | 65 |
| 11.2.2.11. | Descarga e instalación del Certificado de identificación de sede electrónica .....   | 65 |
| 11.2.2.12. | Período de validez del Certificado de identificación de sede electrónica.....  | 66 |
| 11.2.2.13. | Revocación del Certificado de identificación de sede electrónica .....   | 66 |
| 11.2.2.14. | Procedimiento por el que se obtienen los datos personales del Solicitante de la revocación, se confirma su identidad y la capacidad para realizar dicha solicitud y la formalización de la misma.... | 66 |
| 11.2.2.15. | Suspensión del Certificado de identificación de sede electrónica .....   | 68 |
| 11.2.2.16. | Cancelación de la suspensión del Certificado de identificación de sede electrónica .....   | 68 |
| 11.2.2.17. | Comprobación del estado del Certificado de identificación de sede electrónica .....  | 69 |
| 11.2.3.    | Exclusiones y requisitos adicionales a ETSI TS 101 456 .....   | 69 |
| 11.2.4.    | Modelos de formulario.....   | 70 |

**12. Certificados emitidos para la Actuación administrativa automatizada de la Administración Pública, organismos y entidades públicas vinculadas o dependientes..... 71**

|            |  |    |
|------------|--|----|
| 12.1.      | <i>Política de Certificación de los Certificados emitidos para la actuación administrativa automatizada de la Administración Pública, Organismos y entidades públicas vinculadas o dependientes.....</i>                   | 71 |
| 12.1.1.    | Identificación .....   | 71 |
| 12.1.2.    | Tipología del Certificado para la actuación administrativa automatizada de la Administración Pública, organismos y entidades públicas vinculadas o dependientes.....   | 72 |
| 12.1.3.    | Gestión de la Política de Certificación.....   | 73 |
| 12.1.4.    | Comunidad y ámbito de aplicación.....  | 74 |
| 12.1.5.    | Responsabilidad y obligaciones de las partes .....   | 75 |
| 12.1.6.    | Límites de uso de los Certificados para la actuación administrativa automatizada mediante sellos electrónicos .....  | 77 |
| 12.2.      | <i>Prácticas de certificación particulares para los Certificados emitidos para la actuación administrativa automatizada de la Administración Pública, Organismos y entidades públicas, vinculadas o dependientes .....</i> | 78 |
| 12.2.1.    | Servicios de Gestión de las Claves de los Usuarios y Titulares.....  | 79 |
| 12.2.2.    | Gestión del ciclo de vida de los Certificados .....  | 79 |
| 12.2.2.1.  | Registro de los Titulares.....   | 79 |
| 12.2.2.2.  | Procedimiento de solicitud del Certificado para la actuación administrativa automatizada de la Administración Pública .....  | 79 |
| 12.2.2.3.  | Emisión del Certificado para la actuación administrativa automatizada de la Administración Pública.....  | 82 |
| 12.2.2.4.  | Publicación del Certificado para la actuación administrativa automatizada .....  | 88 |
| 12.2.2.5.  | Descarga e instalación del Certificado para la actuación administrativa automatizada .....   | 88 |
| 12.2.2.6.  | Período de validez del Certificado para la actuación administrativa automatizada.....  | 89 |
| 12.2.2.7.  | Revocación del Certificado para la actuación administrativa automatizada .....   | 89 |
| 12.2.2.8.  | Procedimiento por el que se obtienen los datos personales del Solicitante de la revocación, se confirma su identidad y la capacidad para realizar dicha solicitud y la formalización de la misma....                       | 90 |
| 12.2.2.9.  | Suspensión del Certificado para la actuación administrativa automatizada .....   | 91 |
| 12.2.2.10. | Cancelación de la suspensión del Certificado para la actuación administrativa automatizada   | 91 |
| 12.2.2.11. | Comprobación del estado del Certificado para la actuación administrativa automatizada  | 92 |
| 12.2.3.    | Exclusiones y requisitos adicionales a ETSI TS 101 456 .....   | 92 |
| 12.2.4.    | Modelos de formulario.....   | 93 |



## ÍNDICE DE TABLAS

|   |    |
|---|----|
| <b>Tabla 1 Certificado raíz</b> .....   | 15 |
| <b>Tabla 2 Certificado CA APE</b> .....   | 20 |
| <b>Tabla 3 Identificación Política Certificación – Personal APE</b> .....                   | 24 |
| <b>Tabla 4 Composición de la identidad alternativa del sujeto. Personal APE</b> .....       | 38 |
| <b>Tabla 5 Extensión extKeyUsage. Personal APE</b> .....                                    | 38 |
| <b>Tabla 6 Perfil del Certificado: Personal APE</b> .....                                   | 42 |
| <b>Tabla 7 Identificación Política Certificación – Sede Electrónica APE</b> .....           | 47 |
| <b>Tabla 8 Composición del subcampos directoryName. Sede electrónica APE</b> .....          | 61 |
| <b>Tabla 9 Extensión extKeyUsage. Sede Electrónica APE</b> .....                            | 61 |
| <b>Tabla 10 Perfil del Certificado de Sede Electrónica - APE</b> .....                      | 65 |
| <b>Tabla 11 Identificación Política Certificación – Actuación Automatizada APE</b> .....    | 71 |
| <b>Tabla 12 Composición del subcampos directoryName. Actuación automatizada APE</b> .....   | 85 |
| <b>Tabla 13 Perfil del Certificado de Actuación Administrativa Automatizada - APE</b> ..... | 88 |



## 1. PRELIMINAR

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. El marco jurídico resultante desde la aprobación de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP), consagra el derecho de los ciudadanos a comunicarse con las diferentes administraciones públicas. El ejercicio de este derecho ha de estar ligado a la implementación, en el ámbito de las Administraciones Públicas y sus organismos y entidades vinculados o dependientes, de las infraestructuras y nuevos sistemas electrónicos, informáticos y telemáticos previstos en la referida normativa, todos ellos necesarios para el desarrollo y ejecución previsto.
4. Dentro de los diferentes sistemas de identificación y autenticación electrónica que las Administraciones Públicas pueden utilizar y a los que se refiere la presente Declaración, se encuentran:

- 1) **Firma electrónica del personal** al servicio de las Administraciones Públicas.
- 2) Sistemas de firma electrónica basados en la utilización de Certificados en dispositivo seguro o medio equivalente que permita identificar la **sede electrónica** y el establecimiento con ella de comunicaciones seguras.
- 3) Sistemas de firma electrónica para la **actuación administrativa automatizada**.





## 2. INTRODUCCIÓN

5. El presente documento forma parte integrante de la *Declaración General de Prácticas de Certificación* de la FNMT-RCM y tiene por objeto la información pública de las condiciones y características de los servicios de certificación y servicios de emisión de *Certificados* electrónicos por parte de la FNMT-RCM como *Prestador de Servicios de Certificación*, recogiendo, en particular las obligaciones y procedimientos que se compromete a cumplir en relación con la emisión de **Certificados para la identificación de sedes electrónicas, sistemas de firma electrónica para la actuación administrativa automatizada y Certificados emitidos para personal al servicio de las Administraciones Públicas.**
6. En especial deberá tenerse presente, a efectos interpretativos de estas *Políticas y Prácticas de Certificación Particulares*, el apartado “Definiciones” de la *Declaración General de Prácticas de Certificación*, y, en su caso, la *Ley de Emisión* (ver apartado 4, siguiente) correspondiente a cada órgano y/u organismo o entidad usuaria de los servicios de certificación de la FNMT-RCM.
7. Los *Certificados* emitidos por la FNMT-RCM para el personal al servicio de las administraciones públicas cuya *Política de Certificación y Prácticas de Certificación Particulares* se definen en el presente documento se consideran técnicamente *Certificados Reconocidos*, según lo definido en la Ley 59/2003 de Firma Electrónica y la norma ETSI 101 456, y válidos para la realización de *firma electrónica* por parte del personal al servicio de las administraciones públicas y según lo definido en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP)
8. Los *Certificados* emitidos por la FNMT-RCM para la identificación electrónica de las sedes electrónicas de las administraciones públicas cuya *Política de Certificación y Prácticas de Certificación Particulares* se definen en el presente documento se consideran técnicamente *Certificados Reconocidos* según lo definido en la Ley 59/2003 de firma electrónica y válidos para la identificación de las sedes electrónicas según lo definido en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP).
9. Los *Certificados* emitidos por la FNMT-RCM para los sistemas de firma electrónica para la actuación administrativa automatizada cuya *Política de Certificación y Prácticas de Certificación Particulares* se definen en el presente documento se consideran técnicamente *Certificados Reconocidos* según lo definido en la Ley 59/2003 de firma electrónica y válidos para la actuación administrativa automatizada según lo definido en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP).

## 3. ORGANIZACIÓN DEL DOCUMENTO

10. La *Declaración de Prácticas de Certificación* de la FNMT-RCM como *Prestador de Servicios de Certificación* está estructurada, de un lado, por la parte común de la *Declaración General de Prácticas de Certificación* (DGPC) de la FNMT-RCM, pues existen niveles de actuación análogos para todos los servicios de certificación de la Entidad y, de otro lado, por los apartados específicos de los servicios de Certificación a que se refiere la misma que, estructurado en Anexos, son las *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 certificación de la FNMT-RCM.

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

- 1) Por una parte, la ***Declaración General de Prácticas de Certificación***, que debe considerarse cuerpo principal de la *Declaración de Prácticas de Certificación* (apartados 1 al 9) en el que se describe, además de lo previsto en el artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, el régimen de responsabilidad aplicable a 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.
- 2) Y, por otra parte, estructurado en Anexos para cada 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 *DGPC* principal definida en el apartado 1, anterior.

Estas *Políticas de Certificación* y *Prácticas de Certificación Particulares* concretan lo articulado en el cuerpo principal de la *Declaración General de Prácticas de Certificación* 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, como se ha dicho 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.

12. El presente documento representa, por tanto, las Políticas de Certificación y Prácticas de Certificación Particulares para los Certificados emitidos para:

- 1) **Personal al servicio de las Administraciones Públicas,**
- 2) **Identificación de sedes electrónicas,**
- 3) **Sistemas de firma electrónica para la actuación administrativa automatizada.**



#### 4. ORDEN DE PRELACIÓN

13. El orden de prelación es el siguiente:

- Las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares* de *Certificados* emitidos para el personal al servicio de las Administraciones Públicas españolas, así como de *Certificados* para la identificación de sedes electrónicas y sistemas de firma electrónica para la actuación administrativa automatizada forman parte de la *Declaración de Prácticas de Certificación* y tendrán prelación, en lo que corresponda y con carácter particular sobre cada tipo de *Certificado*, sobre lo dispuesto en el cuerpo principal de la *Declaración General de Prácticas de Certificación*.

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

- La *Ley de Emisión* de cada *Certificado* o grupo de *Certificados* constituirá, en su caso y por su singularidad, norma especial sobre lo dispuesto en las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares* para los diferentes órganos y organismos o entidades públicas usuarias de los servicios de la FNMT-RCM, cuando así lo requiera la naturaleza de sus competencias o funciones. La *Ley de Emisión*, en caso de que se constituya, quedará recogida en el documento de relación a formalizar entre la FNMT-RCM y las Administraciones, organismos y entidades públicas, y/o en las condiciones de utilización o contrato de emisión, y/o en el propio *Certificado*.
- En los *Certificados* electrónicos correspondientes a este Anexo y que se refieren a: **Personal al servicio de las Administraciones Públicas, identificación de Sedes electrónicas, Sistemas de firma electrónica para la actuación administrativa automatizada a través de Sello electrónico**, la *Ley de Emisión* (sin perjuicio de lo que pudiera establecerse en los acuerdos o convenios con las Administraciones, organismos y entidades titulares, atendiendo al correspondiente régimen de competencias), tendrá los siguientes campos, los cuales, total o parcialmente, podrán ser incluidos en el propio *Certificado* o en el documento de condiciones de utilización:
  - Sistema de identificación electrónica del *Titular* y de autenticación de los documentos electrónicos que se produzcan.
  - Ámbito de uso, que coincidirá con el régimen de competencias del *Titular* y deberá ser universal en todo el ámbito de las Administraciones Públicas, organismos y entidades.
  - Limitación de responsabilidad, con indicación en su caso, de límites económicos para los actos y transacciones públicas.
  - Firmante/custodio, que deberá coincidir con la persona que tenga la condición de responsable de la correspondiente *Oficina de Registro* o, en su caso, con la del representante del órgano administrativo que ejerza estas funciones.



- Vigencia, caso que no coincida con la duración general fijada en esta Declaración.
- Sistema de validación. Plataforma común.
- Protocolo de Protección de Datos y de seguridad.

## 5. GESTIÓN DEL CICLO DE VIDA DE LAS CLAVES DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

14. (Queda recogida expresamente en estas *Políticas de Certificación y Prácticas de Certificación Particulares* la gestión del ciclo de vida de las claves del PSC, ya que se utilizará un *Certificado Raíz* diferente al utilizado hasta ahora).
15. La FNMT-RCM en su actividad *como Prestador de Servicios de Certificación*, en relación con las claves criptográficas empleadas para la emisión de *Certificados* para los *Certificados* emitidos para **personal al servicio de las Administraciones Públicas, identificación de sedes electrónicas**, sistemas de firma electrónica para la **actuación administrativa automatizada** declara que realizará la siguiente gestión:

### 5.1. GESTIÓN DEL CICLO DE VIDA DE LAS CLAVES

#### 5.1.1. Generación de las Claves del Prestador de Servicios de Certificación

16. Las *Claves* de la FNMT-RCM, como *Prestador de Servicios de Certificación*, son generadas en circunstancias completamente controladas, en un entorno físicamente seguro y, al menos, por dos personas autorizadas para ello, utilizando sistemas hardware y software que cumplen con la normativa actual en materia de protección criptográfica, tal y como se muestra en el apartado “Gestión del ciclo de vida de las Claves del Prestador de Servicios de Certificación” de la *Declaración General de Prácticas de Certificación*.

#### 5.1.2. Almacenamiento, salvaguarda y recuperación de las Claves del Prestador de Servicios de Certificación

17. La FNMT-RCM utiliza los mecanismos necesarios para mantener su *Clave privada* confidencial y mantener su integridad en la forma que se muestra en el apartado “Gestión del ciclo de vida de las Claves del Prestador de Servicios de Certificación” de la *Declaración General de Prácticas de Certificación*.

#### 5.1.3. Distribución de los Datos de verificación de Firma del Prestador de Servicios de Certificación

18. La FNMT-RCM utiliza los mecanismos necesarios para mantener la integridad y autenticidad de su *Clave Pública*, así como su distribución en la forma que se muestra en el apartado “Gestión del ciclo de vida de las Claves del Prestador de Servicios de Certificación” de la *Declaración General de Prácticas de Certificación*.
19. Los campos del *Certificado Raíz* correspondiente a la jerarquía de certificación de los *Certificados* para personal al servicio de la Administración Pública se pueden ver en la siguiente tabla:



| CAMPO                               | CONTENIDO   | CRÍTICA | OBSERVACIONES  |
|-------------------------------------|---|---------|--|
| <b>Campos de X509v1</b>             |   |         |  |
| <b>1. Versión</b>                   | V3  |         |  |
| <b>2. Serial Number</b>             | Aleatorio   |         | <i>[RFC3280]: the serial number MUST be a positive integer, not longer than 20 octets ( <math>1 &lt; SN &lt; 2^{159}</math>). Processing components MUST be able to interpret such long numbers.</i>   |
| <b>3. Signature Algorithm</b>       | Sha1withRsaEncryption<br>Sha256withRsaEncryption<br>Sha512withRsaEncryption |         | OID: 1.2.840.113549.1.1.5<br>OID: 1.2.840.113549.1.1.11<br>OID: 1.2.840.113549.1.1.13<br>Norma PKCS#1 v2.1 y RFC 3447.   |
| <b>4. Issuer Distinguished Name</b> | OU=AC RAIZ FNMT -RCM<br>O=FNMT-RCM<br>C=ES                                  |         | Todos los <i>DirectoryString</i> codificados en UTF8. El atributo "C" ( <i>countryName</i> ) se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements", en <i>PrintableString</i> .  |
| <b>5. Validez</b>                   | Hasta 01/01/2030  |         | El programa de inclusión de certificados raíz de Microsoft requiere que la fecha de validez sea posterior al 1/1/2010.<br><br><i>[RFC3280]: Validity dates before and through 2049 MUST be encoded by CAs as UTCTime, dates in 2050 and later as GeneralizedTime. Date values MUST be given in the format YYMMDDhhmmssZ resp. YYYYMMDDhhmmssZ, i.e. always including seconds</i> |

|                   |  |  |   |
|-------------------|--|--|---|
|                   |  |  | <i>and expressed as Zulu time (Universal Coordinated Time).</i>   |
| <b>6. Subject</b> | OU=AC RAIZ FNMT -RCM<br><br>O=FNMT-RCM<br><br>C=ES |  | <p>Todos los <i>DirectoryString</i> codificados en UTF8. El atributo “C” (<i>countryName</i>) se codificará de acuerdo a “<i>ISO 3166-1-alpha-2 code elements</i>”, en <i>PrintableString</i>.</p> <p>Coincidirá con el campo emisor del certificado de las AC subordinada.</p> <p><i>[RFC3280]: The issuer name MUST be a non-empty DName. Processing components MUST be prepared to receive the following attributes: countryName,</i></p> <p><i>organizationName, organizationalUnitName, distinguishedNameQualifier, stateOrProvinceName, commonName, serialNumber, and domainComponent. Processing components SHOULD be prepared for attributes: localityName, title, surname, givenName, initials, pseudonym, and generationQualifier</i></p> <p><i>[ETSI-QC]: the issuer name MUST contain the countryName attribute. The specified country MUST be the country where the issuer CA is established.</i></p> <p><i>[ETSI-CPN]: the issuer name MUST contain the</i></p> |

|                                    |   |                       |   |
|------------------------------------|---|-----------------------|---|
|                                    |   |                       | <i>countryName and the organizationName attributes.</i>   |
| <b>7. Subject Public Key Info</b>  | Algoritmo: RSA Encryption<br>Longitud: 4096 bits                |                       |   |
| <b>Campos de X509v2</b>            |   |                       |   |
| <b>1. issuerUniqueIdentifier</b>   | No se utilizará   |                       |   |
| <b>2. subjectUniqueIdentifier</b>  | No se utilizará   |                       |   |
| <b>Extensiones de X509v3</b>       |   |                       |   |
| <b>1. Subject Key Identifier</b>   | Función hash SHA-1 sobre la clave pública del sujeto (AC raíz). | NO (RFC 3280)         | RFC 3280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo <i>subjectPublicKey</i> del sujeto (excluyendo etiqueta, longitud y número de bits no usados). |
| <b>2. Authority Key Identifier</b> | No procede  |                       |   |
| <b>3. KeyUsage</b>                 |   | SI (RFCs 3280 y 3739) |   |
| <b>Digital Signature</b>           | 0   |                       |   |
| <b>Non Repudiation</b>             | 0   |                       |   |
| <b>Key Encipherment</b>            | 0   |                       |   |
| <b>Data Encipherment</b>           | 0   |                       |   |
| <b>Key Agreement</b>               | 0   |                       |   |
| <b>Key Certificate Signature</b>   | 1   |                       |   |
| <b>CRL Signature</b>               | 1   |                       |   |
| <b>4.extKeyUsage</b>               | No se utilizará   |                       |   |
| <b>5. privateKeyUsagePeriod</b>    | No se utilizará   |                       |   |

|                                   |   |    |  |
|-----------------------------------|---|----|--|
| <b>6. Certificate Policies</b>    |   | NO | [RFC 3739] obliga la existencia de al menos un valor.  |
| <b>Policy Identifier</b>          | anyPolicy 2 5 29 32 0   |    | La Ley de Firma Electrónica dice para los certificados reconocidos: “La identificación del prestador de servicios de certificación que expide el certificado y su domicilio”. Se incluirá en la DPC.   |
| <b>URL CPS</b>                    | <a href="http://www.cert.fnmt.es/dpcs/">http://www.cert.fnmt.es/dpcs/</a> |    |  |
| <b>Notice Reference</b>           | NO para los certificados de AC, según RFC 5280 (sustituta de RFC 3280).   |    | <p>[RFC3280]:<br/><i>PolicyInformation SHOULD only contain an OID</i></p> <p><i>In a CA certificate, these policy information terms limit the set of policies for certification paths which include this certificate. When a CA does not wish to limit the set of policies for certification paths which include this certificate, it MAY assert the special policy anyPolicy, with a value of { 2 5 29 32 0 }.</i></p> <p><i>To promote interoperability, this profile RECOMMENDS that policy information terms consist of only an OID. Where an OID alone is insufficient, this profile strongly recommends that use of qualifiers</i></p> |
| <b>7. Policy Mappings</b>         | No se utilizará   |    |  |
| <b>8. Subject Alternate Names</b> | No se utilizará   | NO |  |
| <b>9. Issuer Alternate Names</b>  | No se utilizará   |    |  |

|   |                 |                  |   |
|---|-----------------|------------------|---|
| <b>10. Subject Directory Attributes</b>   | No se utilizará |                  |   |
| <b>11. Basic Constraints Subject Type</b> | CA              | SI<br>(RFC 3280) | RFC 3280. Puede especificarse el número máximo de niveles en "Path Length Constraint". Para la AC Raíz no se establecerá ningún límite de niveles de AC subordinadas.<br><br><i>[RFC3280] This extension MUST appear as a critical extension in all CA certificates that contain public keys used to validate digital signatures on certificates.</i> |
| <b>Path Length Constraint</b>             | Ninguno         |                  |   |
| <b>12. Policy Constraints</b>             | No utilizado    |                  |   |
| <b>13. CRLDistributionPoints</b>          | No utilizado    |                  | La revocación del certificado Raíz se publicitará por otros mecanismos.   |
| <b>14. Auth. Information Access</b>       | No procede      | NO<br>(RFC 3280) |   |
| <b>15.netscapeCertType</b>                | No procede      |                  |   |
| <b>16. netscapeRevocationURL</b>          | No procede      |                  |   |
| <b>17. netscapeCAPolicyURL</b>            | No procede      |                  |   |
| <b>18. netscapeComment</b>                | No procede      |                  |   |

**Tabla 1 Certificado raíz**

20. Por otra parte, los *Certificados* emitidos bajo las *Políticas de Certificación* identificadas en este documento vendrán firmados electrónicamente con los *Datos de Creación de Firma* del *Prestador de Servicios de Certificación* y que se corresponden con los campos del siguiente *Certificado*.

| CAMPO                        | CONTENIDO   | CRÍTICA | OBSERVACIONES  |
|------------------------------|---|---------|--|
| <b>Campos de X509v1</b>      |   |         |  |
| 1. Versión                   | V3  |         |  |
| 2. Serial Number             | Aleatorio   |         | [RFC3280]: the serial number <b>MUST</b> be a positive integer, not longer than 20 octets ( $1 < SN < 2^{159}$ ). Processing components <b>MUST</b> be able to interpret such long numbers.  |
| 3. Signature Algorithm       | Sha1withRsaEncryption<br>Sha256withRsaEncryption<br>Sha512withRsaEncryption |         | OID: 1.2.840.113549.1.1.5<br>OID: 1.2.840.113549.1.1.11<br>OID: 1.2.840.113549.1.1.13<br>Norma PKCS#1 v2.1 y RFC 3447.   |
| 4. Issuer Distinguished Name | OU= AC RAIZ FNMT-RCM<br>O=FNMT-RCM<br>C=ES                                  |         | Coincide con el campo asunto del certificado de la AC Raíz.<br><br>Todos los <i>DirectoryString</i> codificados en UTF8. El atributo “C” ( <i>countryName</i> ) se codificará de acuerdo a “ISO 3166-1-alpha-2 code elements”, en <i>PrintableString</i> .<br><br>[ETSI-CPN]: the issuer name <b>MUST</b> contain the <i>countryName</i> and the <i>organizationName</i> attributes. |
| 5. Validez                   | Hasta 03/11/2023  |         | 15 años a partir de la constitución de la AC.  |

|                                    |  |               |   |
|------------------------------------|--|---------------|---|
| <b>6. Subject</b>                  | OU=AC APE<br><br>O=FNMT-RCM<br><br>C=ES  |               | Todos los <i>DirectoryString</i> codificados en UTF8. El atributo “C” ( <i>countryName</i> ) se codificará de acuerdo a “ISO 3166-1-alpha-2 code elements”, en <i>PrintableString</i> .   |
| <b>7. Subject Public Key Info</b>  | Algoritmo: RSA Encryption<br><br>Longitud: 2048 bits   |               |   |
| <b>Campos de X509v2</b>            |  |               |   |
| <b>1. issuerUniqueIdentifier</b>   | No se utilizará  |               |   |
| <b>2. subjectUniqueIdentifier</b>  | No se utilizará  |               |   |
| <b>Extensiones de X509v3</b>       |  |               |   |
| <b>1. Subject Key Identifier</b>   | Función hash SHA-1 sobre la clave pública del sujeto (AC subordinada).   | NO (RFC 3280) | RFC 3280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo <i>subjectPublicKey</i> del sujeto (excluyendo etiqueta, longitud y número de bits no usados).   |
| <b>2. Authority Key Identifier</b> | Función de hash SHA-1 sobre la clave pública de la AC emisora (AC Raíz). NO SE INCLUYE la identificación del certificado de la AC emisora (en este caso, DN de la AC Raíz, número de serie de la AC Raíz). | NO (RFC 3280) | RFC 3280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo <i>subjectPublicKey</i> de la AC emisora (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo <i>Subject Key Identifier</i> de la AC emisora (AC Raíz). |
| <b>3. KeyUsage</b>                 |  | SI (RFCs)     |   |

|                                  |   |                 |   |
|----------------------------------|---|-----------------|---|
| <b>Digital Signature</b>         | 0   | 3280 y<br>3739) |   |
| <b>Non Repudiation</b>           | 0   |                 |   |
| <b>Key Encipherment</b>          | 0   |                 |   |
| <b>Data Encipherment</b>         | 0   |                 |   |
| <b>Key Agreement</b>             | 0   |                 |   |
| <b>Key Certificate Signature</b> | 1   |                 |   |
| <b>CRL Signature</b>             | 1   |                 |   |
| <b>4.extKeyUsage</b>             | No se utilizará   |                 |   |
| <b>5. privateKeyUsagePeriod</b>  | No se utilizará   |                 |   |
| <b>6. Certificate Policies</b>   |   | NO              | RFC 3739 obliga la existencia de al menos un valor.<br><br>La Ley de Firma Electrónica dice para los certificados reconocidos: “La identificación del prestador de servicios de certificación que expide el certificado y su domicilio”. Se incluirá en la DPC.<br><br><i>[RFC3280]:<br/>PolicyInformation<br/>SHOULD only contain an<br/>OID.<br/><br/>In a CA certificate, these<br/>policy information terms<br/>limit the set of policies for<br/>certification paths which<br/>include this certificate.<br/>When a CA does not wish</i> |
| <b>Policy Identifier</b>         | anyPolicy 2 5 29 32 0   |                 |   |
| <b>URL CPS</b>                   | <a href="http://www.cert.fnmt.es/dpcs/">http://www.cert.fnmt.es/dpcs/</a> |                 |   |
| <b>Notice Reference</b>          | NO para los certificados de AC, según RFC 5280 (sustituta de RFC 3280).   |                 |   |

|   |                 |            |  |
|---|-----------------|------------|--|
|   |                 |            | <p><i>to limit the set of policies for certification paths which include this certificate, it MAY assert the special policy anyPolicy, with a value of { 2 5 29 32 0 }.</i></p> <p><i>To promote interoperability, this profile RECOMMENDS that policy information terms consist of only an OID. Where an OID alone is insufficient, this profile strongly recommends that use of qualifiers</i></p> |
| <b>7. Policy Mappings</b>               | No se utilizará |            |  |
| <b>8. Subject Alternate Names</b>       | No se utilizará | NO         |  |
| <b>9. Issuer Alternate Names</b>        | No se utilizará |            |  |
| <b>10. Subject Directory Attributes</b> | No se utilizará |            |  |
| <b>11. Basic Constraints</b>            |                 | SI         | <p>RFC 3280. Puede especificarse el número máximo de niveles en "Path Length Constraint". Para la AC subordinada se limita a 0 el número de ACs dependiente de esta.</p> <p>[RFC3280] This extension MUST appear as a critical extension in all CA certificates that contain public keys used to validate digital signatures on certificates.</p>  |
| <b>Subject Type</b>                     | CA              | (RFC 3280) |  |
| <b>Path Length Constraint</b>           | 0               |            |  |

|                                     |   |    |  |
|-------------------------------------|---|----|--|
| <b>12. Policy Constraints</b>       | No utilizado  |    |  |
| <b>13. CRLDistributionPoints</b>    | LDAP:<br><br>ldap://ldapfnmt.cert.fnmt.es/<br>CN=CRL,OU= AC RAIZ<br>FNMT-RCM, O=FNMT-<br>RCM, C=ES<br>?authorityRevocationList;binary?base<br>?objectclass=cRLDistributionPoint<br><br>HTTP:<br><br>http://www.cert.fnmt.es/crls/<br>ARLFNMTRCM.crl | NO | El programa de certificados raíz de Microsoft obliga a que los certificados emitidos por la AC Raíz tengan punto de distribución de CRL y que sea público. Véase también extensión <i>Auth. Information Access</i> . |
| <b>14. Auth. Information Access</b> | No  |    | Contendrá información de localización del OCSP Responder de la FNMT.   |
| <b>15.netscapeCertType</b>          | No procede  |    |  |
| <b>16.netscapeRevocationURL</b>     | No procede  |    |  |
| <b>17.netscapeCAPolicyURL</b>       | No procede  |    |  |
| <b>18.netscapeComment</b>           | No procede  |    |  |

**Tabla 2 Certificado CA APE**

**5.1.4. Almacenamiento, salvaguarda y recuperación de las Claves Privadas de la Administración, Organismos y Entidades públicas usuarias**

21. La FNMT-RCM bajo ningún concepto genera ni almacena las *Claves Privadas* de sus *Titulares*, las cuales son generadas bajo su exclusivo control, y cuya custodia está bajo la responsabilidad de los diferentes firmantes, órganos, organismos y entidades a las que se encuentren vinculadas o de las que dependan.



#### 5.1.5. Uso de los Datos de Creación de Firma del Prestador de Servicios de Certificación

22. Los *Datos de creación de Firma* de la FNMT-RCM, en su actividad como *Prestador de Servicios de Certificación*, serán utilizadas única y exclusivamente para los propósitos de:
- 1) Firma de Certificados.
  - 2) Firma de las Listas de Revocación.
  - 3) Otros usos previstos en esta Declaración y/o en la legislación aplicable.

#### 5.1.6. Fin del ciclo de vida de las Claves del Prestador de Servicios de Certificación

23. La FNMT-RCM dispondrá de los medios necesarios para lograr que una vez finalizado el período de validez de las *Claves del Prestador de Servicios de Certificación*, estas *Claves* no vuelven a ser utilizadas, bien destruyéndolas o almacenándolas de forma apropiada para dicha finalidad.

#### 5.1.7. Ciclo de vida del hardware criptográfico utilizado para firmar *Certificados*

24. La FNMT-RCM dispondrá de los medios necesarios para posibilitar que el hardware criptográfico utilizado para la protección de sus *Claves* como *Prestador de Servicios de Certificación*, no sufra manipulaciones de acuerdo con el estado de la técnica a la fecha durante todo su ciclo de vida, estando situado dicho componente en un entorno físicamente seguro desde su recepción hasta su destrucción llegado el caso.

### 6. OPERACIÓN Y GESTIÓN DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA; ESQUEMA NACIONAL DE INTEROPERABILIDAD Y ESQUEMA NACIONAL DE SEGURIDAD

#### 6.1. OPERACIÓN Y GESTIÓN DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA

25. Las operaciones y procedimientos realizados para la puesta en práctica de las *Políticas de Certificación* reflejadas en este documento se realizan siguiendo los controles requeridos por los estándares reconocidos para tal efecto, describiéndose estas actuaciones en los apartados “Controles de seguridad física, de procedimientos y del personal” y “Controles de seguridad técnica” de la *Declaración General de Prácticas de Certificación* de la FNMT-RCM.
26. De forma informativa cabe decir que la FNMT-RCM posee un *Sistema de Gestión de la Seguridad de la Información* (en adelante SGSI) para su Departamento CERES con el objetivo final de mantener y garantizar la seguridad de la información de los miembros de la *Comunidad Electrónica*, así como la suya propia, de forma que el servicio prestado por la FNMT-RCM-CERES tenga los niveles suficientes de fiabilidad que exige el Mercado. El SGSI de la FNMT-RCM-CERES es aplicable a los activos de información definidos en el Análisis de Riesgos realizado para todas las Áreas que componen el departamento, incluyendo como activos los servicios prestados a los miembros de la *Comunidad Electrónica*.



27. En el documento Declaración General de Prácticas de Certificación, se da respuesta concreta para todos aquellos aspectos referentes a los siguientes apartados de la norma ETSI TS 101 456:

- 1) Gestión de la Seguridad.
- 2) Clasificación y Gestión de Activos.
- 3) Seguridad de Personal.
- 4) Seguridad física y del entorno.
- 5) Gestión de las Operaciones.
- 6) Gestión de Accesos al Sistema.
- 7) Gestión de incidencias y sistema de continuidad de negocio.
- 8) Terminación de la FNMT-RCM como *Prestador de Servicios de Certificación*.
- 9) Almacenamiento de la información referente a los *Certificados Reconocidos*.

## 6.2. ESQUEMA NACIONAL DE INTEROPERABILIDAD Y ESQUEMA NACIONAL DE SEGURIDAD

28. Hasta que se proceda al desarrollo normativo previsto en el artículo 42, de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los ciudadanos a los Servicios Públicos, la FNMT-RCM adoptará los criterios, recomendaciones y políticas de interoperabilidad y seguridad previstas en estas *Políticas de Certificación y Prácticas de Certificación Particulares*, así como los estándares de uso generalizado, procurando en su aplicación la máxima extensión en el ámbito de las diferentes Administraciones públicas.

## 7. TERMINACIÓN DE LA FNMT-RCM EN SU ACTIVIDAD COMO PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

29. Esta circunstancia y sus consecuencias se describen en el apartado “Cese de la actividad del Prestador de Servicios de Certificación”, de la *Declaración General de Prácticas de Certificación*.

## 8. DIFUSIÓN DE TÉRMINOS Y CONDICIONES

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

- 1) Los términos y condiciones que regulan la utilización de los Certificados expedidos por la FNMT-RCM, con expresión, en su caso, de la correspondiente Ley de Emisión.
- 2) La Política de Certificación aplicable a los Certificados expedidos por la FNMT-RCM.
- 3) Los límites de uso para los Certificados expedidos bajo esta Política de Certificación.
- 4) Las obligaciones, garantías y responsabilidades de las partes envueltas en la emisión y uso de los Certificados.



- 5) Los períodos de conservación de la información recabada en el proceso de registro y de los eventos producidos en los sistemas del Prestador de Servicios de Certificación relacionados con la gestión del ciclo de vida de los Certificados emitidos bajo esta Política de Certificación.
- 6) Reseña legal de interés, con referencia a las normas relativas a reclamaciones y resolución de conflictos.

## **9. ASPECTOS ORGANIZATIVOS**

31. La FNMT-RCM es una entidad pública empresarial de las previstas en el artículo 43.1.b), de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, que, como organismo público, tiene personalidad jurídica pública diferenciada, patrimonio y tesorería propios, y autonomía de gestión en los términos de dicha ley.
32. Está adscrita al Ministerio de Economía y Hacienda, el cual, a través de la Subsecretaría de Economía y Hacienda, ejercerá la dirección estratégica y el control de eficacia de la Entidad en los términos previstos en los artículos 43 y 59, de la Ley 6/1997, de 14 de abril, citada.
33. La FNMT-RCM cuenta con una larga trayectoria histórica en la realización de sus actividades industriales, así como el respaldo del Estado, y desde la entrada en vigor del artículo 81, de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social y sus modificaciones, ha contribuido a impulsar la extensión de los servicios a los que ha sido facultada y el reconocimiento del entorno privado en este nuevo sector que representa la certificación electrónica y las redes telemáticas abiertas, alcanzando un destacado puesto en la prestación de los servicios de certificación.
34. En el desarrollo de esta actividad la FNMT-RCM ha alcanzado la acreditación de su sistema de gestión de la calidad de acuerdo a la normativa ISO 9001:2000, otorgado por AENOR e IQNET para la prestación de servicios de certificación de firma electrónica, de sellado de tiempo y de desarrollo de sistemas operativos criptográficos para tarjetas inteligentes.
35. Asimismo ha acreditado sus *Políticas de Certificación* para la emisión de *Certificados Reconocidos* conforme al estándar europeo ETSI TS 101 456, a través de una entidad independiente.



**10. CERTIFICADOS EMITIDOS PARA EL PERSONAL AL SERVICIO DE LAS ADMINISTRACIONES PÚBLICAS, ORGANISMOS Y ENTIDADES PÚBLICAS VINCULADAS O DEPENDIENTES (EN ADELANTE PERSONAL AL SERVICIO DE LA ADMINISTRACIÓN PÚBLICA)**

**10.1. POLÍTICA DE CERTIFICACIÓN DE LOS CERTIFICADOS EMITIDOS PARA EL PERSONAL AL SERVICIO DE LAS ADMINISTRACIONES PÚBLICAS, ORGANISMOS Y ENTIDADES PÚBLICAS VINCULADAS O DEPENDIENTES (EN ADELANTE PERSONAL AL SERVICIO DE LA ADMINISTRACIÓN PÚBLICA)**

**10.2. IDENTIFICACIÓN**

36. La presente *Política de Certificación* de la FNMT-RCM para la expedición de *Certificados* para personal al servicio de la Administración Pública tiene la siguiente identificación:

|                 |   |
|-----------------|---|
| Nombre          | <i>Política de Certificación de Certificados</i> para personal al servicio de la Administración Pública de España |
| Referencia/OID  | 1.3.6.1.4.1.5734.3.14   |
| Versión         | 1.0   |
| Fecha Emisión   | de 1 de Agosto de 2007  |
| Localización    | <a href="http://www.cert.fnmt.es/dpcs/">http://www.cert.fnmt.es/dpcs/</a>   |
| DPC relacionada | Declaración General de Prácticas de Certificación de la FNMT-RCM  |
| Localización    | <a href="http://www.cert.fnmt.es/dpcs/">http://www.cert.fnmt.es/dpcs/</a>   |

**Tabla 3 Identificación Política Certificación – Personal APE**

**10.2.1. Tipología del Certificado para personal al servicio de las Administraciones Públicas: (funcionarios, personal laboral, estatutario a su servicio y personal autorizado, en adelante denominado como personal al servicio de las Administraciones Públicas).**

37. El *Certificado* para el personal al servicio de las Administraciones Públicas, es la certificación electrónica emitida por la FNMT-RCM que vincula a su *Titular* (la Administración, órgano, organismo o entidad pública) con unos Datos de verificación de Firma y confirma, de forma conjunta:

- la identidad del firmante y custodio de las *Claves* (personal al servicio de las Administraciones públicas que realiza firmas electrónicas utilizando el *Certificado* en





- nombre de la Administración actuante), número de identificación personal, cargo, puesto de trabajo y/o condición de autorizado y,
- al *Titular del Certificado*, que es el órgano, organismo o entidad de la Administración Pública, bien sea ésta General, autonómica, local o institucional, donde ejerce sus competencias, presta sus servicios, o desarrolla su actividad.
38. Este *Certificado* se emite por la FNMT-RCM por cuenta de la Administración Pública correspondiente a la que la FNMT-RCM presta los servicios técnicos, administrativos y de seguridad necesarios como prestador de servicios de certificación.
39. El *Certificado* para personal al servicio de la Administración Pública es desarrollado por la FNMT-RCM mediante una infraestructura PKI específica y ad hoc, basada en actuaciones de identificación y registro realizadas por la red de Oficinas de Registro designadas por el órgano, organismo o entidad Titular 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.
40. 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.
41. Este *Certificado*, es emitido con el perfil técnico correspondiente a los *Certificados Reconocidos* con base en los criterios establecidos para tales *Certificados* en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, en la normativa especial de la FNMT-RCM y en la normativa técnica EESSI, concretamente ETSI TS 101 456 - “Policy requirements for certification authorities issuing qualified certificates” y ETSI TS 101 862 - “Qualified Certificate Profile”, tanto en lo referente al *Prestador de Servicios de Certificación* como a la generación de los *Datos de Verificación de Firma* y al contenido del propio *Certificado*.
42. Se hace constar expresamente que el *Certificado* emitido bajo esta política, constituye un Certificado distinto al previsto en el Anexo II de la *Declaración General de Prácticas de Certificación* para identidad de persona física, con independencia de los aspectos comunes y coincidentes, pues, adicionalmente a su identidad personal en su condición de personal al servicio de las Administraciones Públicas (funcionarial, laboral, estatutario, orgánico, etc.), se consigna la relación, número de identificación, vínculo, cargo o condición del *Titular del Certificado* con el órgano, organismo o entidad de la Administración Pública a la que pertenece y la propia identidad de la Administración, bien directamente en el propio Certificado, bien en la *Ley de Emisión*.
43. El *Certificado* emitido para el personal al servicio de la Administración pública no se registrará por lo dispuesto en la Ley de firma electrónica a efectos del *Certificado* de persona jurídica de acuerdo con lo dispuesto en el artículo 7.6 de la cita Ley, por lo que será de aplicación la normativa específica correspondiente y, en su defecto, las *Declaraciones General y Particulares de Certificación* de la FNMT-RCM.



### 10.2.2. Gestión de la Política de Certificación

44. La FNMT-RCM dispone, específicamente, de una Política de Certificación efectiva en relación con los Certificados emitidos para el personal al servicio de la Administración General del Estado y, en su caso, otras Administraciones Públicas del ámbito de aplicación de la Ley 11/2007, de 22 de junio, LAECSP y, en particular, declara que:

- La FNMT-RCM tiene capacidad para especificar, revisar, y aprobar la *Política de Certificación* de estos *Certificados Reconocidos*, a través de su Dirección General y demás órganos directivos de la misma.
- La FNMT-RCM dispone (apartado 10.2) de unas *Prácticas de Certificación Particulares* en las que se detallan las prácticas de certificación empleadas para la expedición de *Certificados* conformes a la *Política de Certificación* aquí expuesta para este tipo de *Certificado*.
- La FNMT-RCM dispone, dentro de las competencias de la Dirección y demás órganos directivos de la misma, 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.
- La FNMT-RCM realiza análisis de riesgos para evaluar las amenazas del sistema y proponer las medidas de seguridad adecuadas (salvaguardas) para todas las áreas implicadas.
- Las *Prácticas de Certificación Particulares* se ponen a disposición del público mediante el URL:

<http://www.cert.fnmt.es/dpcs/>

- La *Ley de Emisión* de cada tipo o grupo de *Certificados*, en caso de establecerse, podrá ser de acceso restringido total o parcialmente por razones de seguridad al tratarse de un sistema de certificación de uso en el ámbito de las Administraciones públicas y el personal correspondiente.
- La *Política de Certificación* de *Certificados* emitidos para el personal de la Administración Pública se pone a disposición del público mediante el URL:

<http://www.cert.fnmt.es/dpcs/>

- Esta *Política de Certificación* recoge las obligaciones y responsabilidades generales de las partes implicadas en la emisión y uso de los *Certificados* para el personal de la Administración y emitidos por la FNMT-RCM bajo a esta *Política de Certificación*, sin perjuicio de las especialidades que pudieran existir en el contrato o convenio correspondiente o si procede en la *Ley de Emisión*.
- Se dispone de un *OID* específico para identificar la *Política de Certificación* aquí desarrollada, siendo el *OID* asignado en el marco de la numeración de la FNMT-RCM: 1.3.6.1.4.1.5734.3.14.
- La *Política de Certificación* de la FNMT-RCM para el presente *Certificado Reconocido* se define en base al documento ETSI TS 101 456, en concreto en su apartado 8, cumpliéndose los requisitos expuestos en los apartado 6 y 7 con las



exclusiones señaladas en el apartado 8.2 (que se exponen en el apartado **Exclusiones y Requisitos Adicionales a ETSI TS 101456** de la presente *Política de Certificación*). En caso de discrepancia entre este documento y la referida norma, prevalecerá este documento.

### 10.2.3. Comunidad y ámbito de aplicación

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

- a) Son expedidos como *Certificados Reconocidos* con base en los criterios establecidos para tal en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y en la normativa técnica EESSI, concretamente ETSI TS 101 862 – “Qualified Certificate Profile”.
- b) Son expedidos por la FNMT-RCM como *Prestador de Servicios de Certificación* cumpliendo con los criterios establecidos en la Ley 59/2003, de 19 de diciembre, citada y en la normativa técnica EESSI, concretamente ETSI TS 101 456 - “Policy requirements for certification authorities issuing qualified certificates”.
- c) La *Tarjeta criptográfica* de la FNMT-RCM utilizada como *Dispositivo seguro de creación de Firma*, cumple técnicamente con los criterios establecidos en la Ley 59/2003, de 19 de diciembre, de firma electrónica para tales dispositivos. No obstante, en el ámbito de los *Certificados* de la presente *Política de Certificación*, existen otros dispositivos que realizan funciones como *Dispositivos seguros de creación de Firma* de conformidad con las normas legales y técnicas sobre tales dispositivos.

Los *Certificados* emitidos bajo esta *Política de Certificación* son expedidos para las Administraciones Públicas, del ámbito de aplicación de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos que forman parte de la *Comunidad Electrónica*, tal y como se define en el apartado **Definiciones** de la *Declaración General de Prácticas de Certificación* de la FNMT-RCM. En el marco de esta *Política de Certificación*, los *Usuarios destinatarios* se corresponden con personal de la Administración Pública del Reino de España, bien sea un órgano, organismo, entidad de la Administración general, Autónoma o Local del Estado

- d) A los efectos de las *Prácticas de Certificación Particulares* aplicable a los servicios de certificación y firma electrónica, en el ámbito de organización y funcionamiento de la Administración General del Estado y del resto de Administraciones públicas, así como sus organismos y entidades vinculadas o dependientes, el alcance de la definición Comunidad Electrónica se referirá, solamente, a los *Titulares* y firmantes/custodios de los *Certificados* emitidos al amparo de una infraestructura PKI (infraestructura de clave pública) específica del órgano y/o organismo correspondiente que esté encomendada a la FNMT-RCM, para el desarrollo de las diferentes competencias y funciones públicas propias del cargo, de la relación funcional, de las funciones del empleado público, o de la condición de autorizado en relación con los órganos y organismos dotados de *sede electrónica* a los que pertenezcan o con los que se relacionen estos usuarios.
- e) Los *Certificados* emitidos bajo esta *Política de Certificación* se consideran válidos como parte integrante de sistemas de firma electrónica y, por tanto, adecuados para el

desarrollo a efectos interadministrativos y de comunicación con el ciudadano de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP). En especial, se considera que pueden formar parte de sistemas de firma electrónica que sean conformes y/o equivalentes a lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica y resultan adecuados para garantizar la identificación de los participantes en las relaciones entre administraciones y con los ciudadanos y, en su caso, la autenticidad e integridad de los documentos electrónicos, así como su utilización para la generación de firma electrónica reconocida

- f) 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.

#### 10.2.4. Responsabilidad y obligaciones de las partes

46. Serán partes a los efectos de este apartado los siguientes sujetos:

- La Administración, organismos, entidades públicas representadas a través de los diferentes órganos competentes y que dependiendo de la *Ley de Emisión* (si la hubiere) podrán conformarse como *Titulares* responsables.
- Oficinas de Registro, que, a través del personal designado por la Administración competente, serán responsables de los requisitos y condiciones que ostenten los *Titulares* y firmantes/custodios del *Certificado*.
- Los firmantes y custodios del *Certificado* y sus *Claves*, que será el personal al servicio de las Administraciones, organismos y entidades públicas.
- FNMT-RCM, en cuanto *Prestador de Servicios de Certificación*.
- En su caso, resto de Comunidad Electrónica y terceros.

47. El régimen de derechos y obligaciones de las Administraciones, organismos, entidades públicas y la FNMT-RCM se regirá mediante el correspondiente acuerdo o convenio regulador de los servicios de certificación. En estos acuerdos o convenios podrá establecerse la *Ley de Emisión* de estos *Certificados*. La *Ley de Emisión* también podrá establecerse con el contenido y finalidad prevista en esta Declaración.

48. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en este documento y en la *Declaración General de Prácticas de Certificación*, la Administración *Titular* del *Certificado* y/o el responsable de la *Oficina de Registro* tienen la obligación de:

- No realizar registros o tramitar solicitudes de personal que preste sus servicios en una entidad diferente a la que representa como *Oficina de Registro*, sin perjuicio de la creación de *Oficinas de Registro* centralizadas o de convenios entre administraciones para efectuar registros.

- Comprobar fehacientemente los datos del personal al servicio de las Administraciones públicas como usuario del *Certificado*, que actuará como firmante y custodio del mismo, referidos a su identidad y a la condición del cargo, puesto de trabajo, empleo o cualquier otro dato que refleje o caracterice la relación de éste con la Administración, organismo o entidad a la que presta sus servicios
  - Solicitar la revocación o suspensión del *Certificado* del personal al servicio del órgano al que representa la *Oficina de Registro* cuando alguno de los datos referidos a la condición del cargo, puesto de trabajo, empleo o cualquier otro que refleje o caracterice la relación del usuario firmante y custodio del *Certificado* con el *Titular*, u órgano, organismo o entidad pública, en la que presta sus servicios, sea inexacto, incorrecto o haya variado.
  - Solicitar a la FNMT-RCM, a través de la *Oficina de Registro*, la revocación del *Certificado* cuando alguno de los datos referidos a la condición del cargo, puesto de trabajo, empleo o cualquier otro dato que refleje o caracterice la relación del personal al servicio de las Administraciones Públicas con el órgano, organismo o entidad, *Titular* del *Certificado*, donde presta sus servicios, sea inexacto, incorrecto, haya variado o sea de necesaria revocación por razones de seguridad.
  - Solicitar a la FNMT-RCM, a través de la *Oficina de Registro*, la revocación del *Certificado* cuando, directamente o a través de comunicación del personal al servicio de las Administraciones Públicas y custodio del *Certificado*, exista pérdida, extravío de la tarjeta o soporte del *Certificado*, o presunción de ello.
  - Descargar el *Certificado* y sus claves directamente en la tarjeta criptográfica que se proporcione a su personal. No conservar las claves privadas de los *Titulares* en los equipos de la *Oficina de Registro*, de conformidad con las directrices de la FNMT-RCM plasmadas en los manuales de procedimiento que se entregan a las *Oficinas de Registro*, en las presentes *Políticas de Certificación y Prácticas de Certificación Particulares* y en la *Declaración General de Prácticas de Certificación*.
49. Las relaciones de la FNMT-RCM con el *Titular* y el personal al servicio de las Administraciones públicas que realizará firmas electrónicas con el *Certificado* proporcionado por el citado *Titular* quedarán determinadas principalmente, a los efectos del régimen de uso de los *Certificados*, a través del documento relativo a las condiciones de utilización o, en su caso, contrato de emisión del *Certificado*, y, subsidiariamente, por las presentes *Políticas de Certificación y Prácticas de Certificación Particulares* y por la *Declaración General de Prácticas de Certificación*, atendiendo a los acuerdos, convenios o documento de relación entre la FNMT-RCM y la Administración Pública correspondiente.
50. Las relaciones de la Administración Pública *Titular* del *Certificado* y de su personal con la FNMT-RCM, se realizarán siempre a través de la *Oficina de Registro* y su responsable. La FNMT-RCM no realizará ninguna acción solicitada por el personal al servicio de las Administraciones públicas, firmante y custodio del *Certificado*, que no esté autorizada por el responsable de la *Oficina de Registro* o por el *Titular del Certificado*.
51. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la *Declaración General de Prácticas de Certificación*, el personal al servicio de las Administraciones Públicas, como firmante y custodio del *Certificado* y sus *Claves*, tiene la obligación de:



- No utilizar el *Certificado* cuando alguno de los datos referidos al cargo, puesto de trabajo, empleo o cualquier otro sea inexacto o incorrecto o no refleje o caracterice su relación, con el órgano, organismo o entidad en la que presta sus servicios; o, existan razones de seguridad que así lo aconsejen.
- Realizar un uso adecuado del *Certificado* en base a las competencias y facultades atribuidas por el cargo, puesto de trabajo o empleo como personal al servicio de las Administraciones Públicas.
- Comunicar al responsable de la *Oficina de Registro*, la pérdida, extravío, o sospecha de ello, de la tarjeta o soporte del *Certificado* del que es usuario y custodio, con el fin de iniciar, en su caso, los trámites de su revocación.

52. El resto de la *Comunidad Electrónica* y los terceros regularán sus relaciones con la FNMT-RCM a través de la *Declaración General de Prácticas de Certificación*, y; en su caso, a través de estas *Políticas de Certificación y Prácticas de Certificación Particulares*; todo ello sin perjuicio de lo dispuesto en la normativa sobre firma electrónica y demás normativa que resulte de aplicación.

#### 10.2.5. Límites de uso de los *Certificados* para personal al servicio de la Administración Pública

53. Constituyen límites de uso de este tipo de *Certificados* las diferentes competencias y funciones propias de las Administraciones Públicas Titulares (actuando a través del personal a su servicio en calidad de *firmante* y custodio 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.

54. FNMT-RCM no tendrá control sobre las actuaciones y usos de los *Certificados* que se realicen por el personal al servicio de las Administraciones públicas en nombre de éstas y por las Oficinas de Registro, 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.

55. Para poder usar los *Certificados* para personal al servicio de la Administración Pública de forma diligente, se deberá previamente formar parte de la Comunidad Electrónica y, la Administración actuante, adquirir la condición de *Titular*.

56. En cualquier caso, si un tercero desea confiar en la firma electrónica realizada con uno de estos *Certificados* sin acceder a los servicios de comprobación de la vigencia 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*.

57. Además, incluso dentro del ámbito de la *Comunidad Electrónica*, no se podrán emplear este tipo de *Certificados*, por persona o entidad distinta a la FNMT-RCM, para:





- Firmar otro *Certificado*, salvo supuestos expresamente autorizados previamente.
- Usos particulares o privados.
- Firmar software o componentes.
- Generar sellos de tiempo para procedimientos de *Fecha 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

### 10.3. PRÁCTICAS DE CERTIFICACIÓN PARTICULARES PARA LOS CERTIFICADOS EMITIDOS PARA PERSONAL AL SERVICIO DE LA ADMINISTRACIÓN PÚBLICA

58. La FNMT-RCM en su labor como *Prestador de Servicios de Certificación* y para demostrar la necesaria fiabilidad para la prestación de dichos servicios, ha desarrollado una *Declaración de Prácticas de Certificación* cuyo objeto es la información pública sobre las condiciones generales de prestación de los servicios de certificación por parte de la FNMT-RCM en su condición de *Prestador de Servicios de Certificación*.
59. En especial deberá tenerse presente, a efectos interpretativos del presente anexo el apartado “Definiciones” de la *Declaración General de Prácticas de Certificación*.
60. El Presente documento trae causa y forma parte integrante de la *Declaración de Prácticas de Certificación* de la FNMT-RCM y define el conjunto de prácticas particulares adoptadas por la FNMT-RCM como *Prestador de Servicios de Certificación* para la gestión del ciclo de vida de los *Certificados* para personal al servicio de la Administración Pública, expedidos bajo la *Política de Certificación* de Certificados para personal al servicio de a la Administración Pública identificada con el OID 1.3.6.1.4.1.5734.3.14.

#### 10.3.1. Servicios de Gestión de las Claves de los Titulares

61. La FNMT-RCM, bajo ningún concepto, genera ni almacena las *Claves Privadas* de los *Titulares*, que son generadas bajo su exclusivo control y con la intervención de la *Oficina de Registro* correspondiente y cuya custodia esta bajo responsabilidad del personal al servicio de la Administración Pública.

#### 10.3.2. Preparación de los Dispositivos Seguros de Creación de Firma

62. La FNMT-RCM proporciona a las Administraciones Públicas Titulares para su entrega al personal de su dependencia, *Tarjetas criptográficas* para la generación de sus *Claves Privadas* y el almacenamiento de los *Certificados*.
63. La *Tarjeta criptográfica* es entregada a los *Usuarios* y Administraciones públicas *Titulares* sin ningún tipo de contenido, con las utilidades software necesarias para conseguir una integración con los Navegadores más utilizados. Así mismo, en ese momento se le proporcionan los códigos necesarios para el acceso a dicha tarjeta para que, posteriormente,





desde su puesto o desde el puesto de la propia *Oficina de Registro*, generen sus *Claves* e inserte el *Certificado* en la *Tarjeta Criptográfica*.

64. La FNMT-RCM proporciona este tipo de tarjetas ya que permite a los *Titulares* y personal a su servicio mantener el “exclusivo control” sobre los *Datos de creación de Firma*.

### 10.3.3. Gestión del ciclo de vida de los *Certificados*

65. Se definen aquí aquellos aspectos que, si bien ya han sido apuntados en la *Declaración General de Prácticas de Certificación* de la que este documento forma parte, revisten determinadas especialidades que necesitan un mayor nivel de detalle.

#### 10.3.3.1. Procedimiento de solicitud del *Certificado* para personal al servicio de la Administración Pública

66. A continuación se describe el procedimiento de solicitud por el que la *Oficina de Registro* toma los datos del personal al servicio de la Administración Pública, confirma su identidad, vigencia del cargo o empleo y se formaliza, entre el citado personal y la FNMT-RCM el documento de condiciones de utilización o el contrato de emisión, según proceda por el cargo del personal, según lo previsto en el documento de relación, o convenio o acuerdo de la FNMT-RCM con el órgano, organismo y/o entidad para la posterior emisión de un *Certificado* para personal al servicio de la Administración Pública.

67. Se hace constar que FNMT-RCM, en función de la relación de *Titulares* y 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 funcional, 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.

68. 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.

69. Las actuaciones serán las siguientes, una vez realizadas satisfactoriamente por la *Oficina de Registro* lo señalado anteriormente:

- 1) Obtención de la Tarjeta criptográfica y del software de generación o importación de los *Datos de creación y de verificación de Firma* en la Tarjeta

La *Tarjeta criptográfica* es un *Dispositivo seguro de creación de Firma* que debe ser empleada para generar los *Datos de creación y de verificación de Firma*, en su caso, importar el *Certificado* correspondiente y realizar firmas electrónicas.



El *Titular* deberá proceder, con carácter previo a la fase de presolicitud, obtener dicha *Tarjeta* a través de la *Oficina de Registro* correspondiente. Además de la *Tarjeta criptográfica*, la Administración Pública *Titular* deberá obtener el software necesario para la generación de las *Claves* por la propia *Tarjeta*, o, en su caso, la importación del correspondiente *Certificado*.

En el procedimiento de obtención de *Certificados*, la FNMT-RCM facilitará los elementos necesarios para activar, en la *Oficina de Registro*, el software pertinente para generar las *Claves* criptográficas que le permitan proteger la seguridad de sus comunicaciones a través de mecanismos de cifrado, así como autenticarse y firmar electrónicamente de conformidad con la Ley 11/2007, de 22 de junio, LAECSP, constituyéndose en este último caso como *Datos de creación y de verificación de Firma*.

Se hace constar que, a efectos de los elementos necesarios para la activación del *Certificado*, FNMT-RCM los adquirirá del mercado buscando la máxima pluralidad de proveedores. FNMT-RCM, exigirá a los proveedores las garantías necesarias de idoneidad y titularidad de derechos de propiedad industrial e intelectual necesarios, así como aquellas que sean pertinentes en materia de seguridad informática. No obstante lo anterior, FNMT-RCM no será responsable de los daños y perjuicios y/o funcionamiento defectuoso que estos elementos puedan producir en los usos que puedan realizarse, ya sean estos por culpa de los usuarios interesados o por defectos de origen de los elementos, limitándose la FNMT-RCM a transmitir las reclamaciones y quejas a los diferentes proveedores.

Los *Datos de creación de Firma* que se encuentran en la *Tarjeta criptográfica* permanecerán siempre bajo el exclusivo control del *Titular* y del personal al servicio de la Administración Pública como usuario y custodio de tales *Certificados*, no guardándose copia de ellos por la FNMT-RCM, ni por la *Oficina de Registro*.

La FNMT-RCM fabricará estas tarjetas para mayor seguridad del proceso, bien directamente o a través de entidades colaboradoras. FNMT-RCM emitirá *Certificados* para *tarjetas criptográficas* que estén debidamente homologadas como *Dispositivos Seguros de Creación de Firma* por los organismos correspondientes y/o sean aptas técnicamente para almacenar los *Certificados* emitidos por la Entidad.

Una vez obtenido este soporte y el software necesario para la operativa que desee realizar, el interesado procederá según se dispone a continuación.

## 2) Presolicitud

El interesado se persona en la *Oficina de Registro* o desde el equipo del puesto donde desempeña las funciones, siempre que esté autorizado por la *Oficina de Registro*, y accede al *sitio web* del *Prestador de Servicios de Certificación*, la FNMT-RCM, a través de la dirección

<http://ape.cert.fnmt.es/appsUsuario/solicitudmeh/solicitudCertInicio.do>

donde se mostrarán las instrucciones del proceso completo. Deberá introducir su NIF o NIE, en el punto de recogida de datos dispuesto para ello; y/o número de identificación funcional o laboral. Posteriormente, se generarán las *Claves Pública* y *Privada* (en *Tarjeta criptográfica*) que serán vinculadas al *Certificado*,

convirtiéndose en datos de verificación y creación de firma respectivamente, y se asigna e indica al interesado un código de solicitud.

Con carácter previo, el personal al servicio de la Administración Pública y el órgano, organismo o entidad pública *Titular* deberán consultar la *Declaración General de Prácticas de Certificación*, y las presentes *Políticas de Certificación y Prácticas de Certificación Particulares* en la dirección

<http://www.cert.fnmt.es/dpcs/>

con las condiciones de uso y obligaciones propias como usuario y *Titular*, respectivamente, del *Certificado*, que se plasmarán en el documento de condiciones de utilización o, si procede, el contrato de emisión.

Al realizar esta presolicitud se envía a la FNMT-RCM la *Clave Pública* generada, junto con las correspondientes pruebas de posesión de la *Clave Privada*, para la posterior emisión del *Certificado*.

La FNMT-RCM, tras recibir esta información, y realizadas las comprobaciones pertinentes por la *Oficina de Registro*, comprobará mediante la *Clave Pública* del peticionario la validez de la información de la presolicitud firmada, comprobando, únicamente, la posesión y correspondencia de la pareja de *Claves* criptográficas por parte del peticionario.

Esta información no dará lugar a la generación de un *Certificado* por parte de la FNMT-RCM, en tanto que ésta no reciba firmada, por la *Oficina de Registro*, la solicitud del *Certificado* realizada por la Administración *Titular*.

Al realizarse la generación de las claves en el interior de la *Tarjeta Criptográfica*, la operación de presolicitud puede desarrollarse en la *Oficina de Registro* correspondiente, no perdiéndose en ningún momento la característica de confidencialidad y control exclusivo, por parte del *Titular*, de la *Clave Privada*.

### 3) Confirmación de la identidad personal, cargo o empleo

#### 10.3.3.2. Personación ante las Oficinas de Registro

70. La personación se realizará ante *Oficina de Registro* designada a tal efecto por el órgano, organismo o entidad pública *Titular* de la que depende el personal a su servicio.
71. A estos efectos FNMT-RCM tendrá en cuenta las funcionalidades previstas en la legislación aplicable en relación con el DNIe, así como los sistemas de identificación y comprobación del cargo, función o empleo aplicables en las Administraciones Públicas, por lo que el requisito de personación podrá ser sustituido por otros procedimientos que permitan la identificación, siempre que estén amparados por la intervención de la *Oficina de Registro*. En estos supuestos de procedimientos especiales de identificación propios del ámbito público, no será necesaria la personación cuando por el órgano competente de la Administración se proceda a certificar los requisitos de identidad, vigencia del cargo y demás condiciones a comunicar a la *Oficina de Registro*, de acuerdo con lo previsto en el artículo 13.1 in fine de la Ley 59/2003 de Firma electrónica y artículo 19 de la Ley 11/2007, LAECSP.

#### 10.3.3.3. *Comparecencia y documentación*

72. En el supuesto que se actúe mediante comparecencia ante la *Oficina de Registro*, el personal al servicio de la Administración Pública aportará los datos que se le requieran, acreditará su identidad personal y su condición de personal al servicio de la Administración Pública, sin perjuicio de aplicación de lo previsto en el párrafo anterior. FNMT-RCM estará y admitirá, en todo caso, la función e informe que realice la *Oficina de Registro* designada por la Administración.

1. Envío de información a la FNMT-RCM

Una vez confirmada, por la *Oficina de Registro*, la identidad de su personal, 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 personal y la *Oficina de Registro*, ésta procederá a validar los datos y a enviarlos, junto con el código de solicitud recogido en la fase de presolicitud.

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

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.

2. Extensión de la función de registro e identificación a otros *Certificados* emitidos por la FNMT-RCM.

Los miembros de la *Comunidad Electrónica* podrán recibir la prestación de servicios de certificación y firma electrónica de la FNMT-RCM, basada en la emisión de *Certificados* electrónicos pertenecientes a diferentes *Leyes de Emisión* y en soportes distintos, mediante la aceptación de las condiciones que, específicamente, se le exhibirán a instancia de la FNMT-RCM en las diferentes *webs* y demás soportes de servicios de los miembros de la *Comunidad Electrónica*, de acuerdo con lo establecido en la legislación sectorial correspondiente y con las limitaciones establecidas en la legislación reguladora del tratamiento de datos de carácter personal.

En la prestación de los servicios señalados en el párrafo anterior, se podrán extender los efectos de las actuaciones derivadas del registro e identificación, con los límites temporales previstos en la legislación de firma electrónica, así como la reguladora del DNI-e.; todo ello sin perjuicio de las especialidades que puedan derivarse del ámbito de las Administraciones Públicas.

#### 10.3.3.4. *Emisión del Certificado para personal al servicio de la Administración Pública*

73. Una vez recibidos en la FNMT-RCM los datos personales del personal solicitante, la información que describe su relación con la Administración Pública, así como el código de solicitud obtenido en la fase de presolicitud, se procederá a la emisión del *Certificado*.

74. 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 su calidad de *Prestador de Servicios de*



- Certificación*, no existiendo ninguna otra entidad u organismo con capacidad de emisión de los mismos.
75. La FNMT-RCM, por medio de su *Firma electrónica*, autentica los *Certificados* y confirma la identidad de sus *Titulares*, así como la vigencia del cargo o empleo de su personal, de conformidad con la información recibida por la *Oficina de Registro*. 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*.
76. La FNMT-RCM en ningún caso incluirá en un *Certificado* información distinta de la aquí mostrada, ni circunstancias, atributos específicos de los firmantes o límites distintos a los previstos en los acuerdos, convenios y, en su caso, a los previstos en la *Ley de Emisión* correspondiente.
77. En cualquier caso, la FNMT-RCM actuará eficazmente para:
- Comprobar que la *Oficina de Registro* o, en su caso, el personal firmante y custodio del *Certificado* utilizan la *Clave Privada* correspondiente a la *Clave Pública* vinculada a la identidad del *Titular* del mismo. Para ello, la FNMT-RCM comprobará la correspondencia entre la *Clave privada* y la *Clave pública*.
  - Lograr que la información incluida en el *Certificado* se base en la información proporcionada por la *Oficina de Registro* correspondiente.
  - No ignorar hechos notorios que puedan afectar a la fiabilidad del *Certificado*.
  - Lograr que el *DN* (nombre distintivo) asignado en el *Certificado* sea único en toda la *Infraestructura de Clave Pública* de la FNMT-RCM.
78. Para la emisión del *Certificado* se seguirán los siguientes pasos:
1. Composición del nombre distintivo (DN) del personal al servicio de la Administración Pública.  
  
Con los datos personales del citado personal 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 de lugar a ambigüedades. No se contempla el uso de seudónimos como forma de identificación.  
  
El *DN* para el personal al servicio de la Administración Pública está compuesto de los siguientes elementos:  
  
DN=CN, OU, OU, OU, O, C  
  
El conjunto de atributos OU, OU, OU, O, C representa la rama del directorio en la que se encuentra ubicada la entrada correspondiente al personal al servicio de la Administración Pública en cuestión.  
  
El atributo *CN* contiene los datos de identificación del personal al servicio de la Administración Pública que para el caso de los *Certificados de Identidad* de personal al servicio de la Administración Pública, seguirá la siguiente sintaxis:

**CN= NOMBRE a1 a2 n – NIF 12345678A**

Donde:



NOMBRE y NIF son etiquetas <sup>[1]</sup>

n, a1 y a2 son los nombres, primer y segundo apellido del personal al servicio de la Administración Pública respectivamente<sup>[2]</sup>

12345678A es su correspondiente NIF <sup>[3]</sup>.

[1] Las etiquetas siempre van en mayúsculas y se separan del valor por un espacio en blanco. Las duplas <etiqueta, valor> se separan entre ellas con un espacio en blanco, un guión y otro espacio en blanco (“ – ”)

[2] Con todos sus caracteres en mayúsculas, excepto la letra eñe, que irá siempre en minúscula. No se incluirán símbolos (comas, guiones, etc.) ni caracteres acentuados.

[3] NIF del personal al servicio de la Administración Pública = 8 cifras + 1 letra mayúscula, sin ningún tipo de separación entre ellas. En el caso que un NIF ocupe menos de 8 cifras, se incluirán ceros al comienzo del número hasta completar las 8 cifras.

Una vez compuesto el nombre distintivo (*DN*) que identificará al personal al servicio de la Administración Pública, se crea la correspondiente entrada en el directorio, procurando que el nombre distintivo sea único en toda la *Infraestructura de Clave Pública del Prestador de Servicios de Certificación*.

2. Composición de la identidad alternativa del personal al servicio de la Administración Pública.

La identidad alternativa del personal al servicio de la Administración Pública, tal como se contempla en la presente tipología de *Certificados* contiene la misma información que el *CN*, así como el cargo, órgano, organismo o entidad pública en la que presta sus servicios, que será el *Titular del Certificado*, empleo y número de identificación, distribuida en una serie de atributos, de forma que sea más sencilla la obtención de los datos personales del personal al servicio de la Administración Pública. Se utiliza la extensión *subjectAltName* definida en *X.509* versión 3 para ofrecer esta información.

Dentro de dicha extensión, se utilizará el subcampo *directoryName* para incluir un conjunto de atributos definidos por la FNMT-RCM, que incorporan información sobre el personal al servicio de la Administración Pública y la Administración *Titular* en cuestión, siguiendo el siguiente criterio:

| Tipo Certificado                              | Información      | Atributo FNMT | OID (*)     |
|---|------------------|---------------|-------------|
| Personal al Servicio de la Administración [1] | Nombre           | fnmtNombre    | fnmtoid.1.1 |
|   | Primer apellido  | fnmtApellido1 | fnmtoid.1.2 |
|   | Segundo apellido | fnmtApellido2 | fnmtoid.1.3 |

|  |                                   |                           |              |
|--|-----------------------------------|---------------------------|--------------|
|  | NIF                               | fnmtNif                   | fnmtoid.1.4  |
|  | Cargo                             | fnmtAPECargo              | fnmtoid.1.38 |
|  | Entidad en la que presta servicio | fnmtAPEEntidad            | fnmtoid.1.39 |
|  | Situación laboral                 | fnmtAPEsituacion          | fnmtoid.1.40 |
|  | Número identificación             | fnmtAPENIP                | fnmtoid.1.44 |
|  | Unidad Organizativa               | fnmtAPEUnidadOrganizativa | fnmtoid.1.45 |

**Tabla 4 Composición de la identidad alternativa del sujeto. Personal APE**

[1] Por otra parte, además del subcampo *directoryName* de la extensión *subjectAltName*, en el caso de que se haya aportado una dirección de correo electrónico por el personal al servicio de la Administración Pública durante el proceso de solicitud de emisión del *Certificado*, ésta estará incluida en el subcampo *rfc822Name*.

(\*) fnmtoid: 1.3.6.1.4.1.5734: Espacio de numeración asignado a la Fabrica Nacional de Moneda y Timbre – Real Casa de la Moneda por el IANA.

Además se incluirán las extensiones necesarias para poder realizar el proceso de “login” en Sistemas Operativos Windows con Tarjeta Criptográfica, que se considera son:

|                      |  |
|----------------------|--|
| <b>4.extKeyUsage</b> | Autenticación de cliente: 1.3.6.1.5.5.7.3.2<br>Inicio de sesión de tarjeta inteligente: 1.3.6.1.4.1.311.20.2.2 |
|----------------------|--|

**Tabla 5 Extensión extKeyUsage. Personal APE**

3. Generación del *Certificado* conforme al Perfil del Certificado de personal al servicio de la Administración Pública.

El formato del *Certificado* de personal al servicio de la Administración Pública, expedido por la FNMT-RCM bajo la *Política de Certificación de Certificados* emitidos, para el personal al servicio de la Administración Pública, por la FNMT-RCM, en consonancia con la norma UIT-T X.509 versión 3 y de acuerdo con la normativa legalmente aplicable en materia de *Certificados Reconocidos*, contiene los siguientes campos:

| CAMPO                        | CONTENIDO  | OBSERVACIONES  |
|------------------------------|--|--|
| 1. Versión                   | V3   |  |
| 2. Serial Number             | Secuencial   | [RFC3280]: the serial number MUST be a positive integer, not longer than 20 octets ( $1 < SN < 2^{159}$ ). Processing components MUST be able to interpret such long numbers.  |
| 3. Signature Algorithm       | Sha1withRsaEncryption<br>Sha256withRsaEncryption   | OID: 1.2.840.113549.1.1.5<br>OID: 1.2.840.113549.1.1.11<br><br>Norma PKCS#1 v2.1 y RFC 3447.   |
| 4. Issuer Distinguished Name | OU= AC APE<br>O=FNMT-RCM<br>C=ES   | Todos los <i>DirectoryString</i> codificados en UTF8. El atributo "C" ( <i>countryName</i> ) se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements", en <i>PrintableString</i> .<br><br>[ETSI-CPN]: the issuer name MUST contain the <i>countryName</i> and the <i>organizationName</i> attributes.   |
| 5. Validez                   | 48 meses   | 48 meses a partir del momento de la emisión.   |
| 6. Subject                   | CN= "Identidad del Titular del Certificado"<br>OU= "Organizacion_Entidad"<br>OU=AC APE<br>O=FNMT-RCM<br>C=ES | Todos los <i>DirectoryString</i> codificados en UTF8. El atributo "C" ( <i>countryName</i> ) se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements", en <i>PrintableString</i> . El atributo "SN" ( <i>serialNumber</i> ) se codificará en <i>PrintableString</i> .<br><br>La Ley de Firma Electrónica establece para los certificados reconocidos: "La identificación del firmante, en el supuesto de personas físicas, debe realizar por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal". El número de serie convierte en único el nombre del sujeto. Todos los <i>DirectoryString</i> codificados en UTF8.<br><br>[ETSI-CPN]: The subject field of EE certificates for natural persons SHALL include at least the <i>commonName</i> or the <i>givenName</i> and <i>surname</i> attribute. |
| 7. Subject Public Key Info   | Algoritmo: RSA Encryption<br>Longitud: 2048 bits   |  |
| 8. issuerUniqueIdentifier    | No se utilizará  |  |
| 9. subjectUniqueIdentifier   | No se utilizará  |  |
| 10. Subject Key Identifier   | Función hash SHA-1 sobre la clave pública del sujeto.  | RFC 3280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo <i>subjectPublicKey</i> del sujeto (excluyendo etiqueta, longitud y número de bits no usados).  |

| CAMPO |                           | CONTENIDO  | OBSERVACIONES  |
|-------|---------------------------|--|--|
| 11.   | Authority Key Identifier  | Función de hash SHA-1 sobre la clave pública de la AC emisora (AC subordinada). NO SE incluye la identificación del certificado de la AC emisora (en este caso, DN de la AC Raíz, número de serie de la AC Subordinada). | RFC 3280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo <i>subjectPublicKey</i> de la AC emisora (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo <i>Subject Key Identifier</i> de la AC emisora (AC subordinada).   |
| 12.   | KeyUsage                  |  |  |
|       | Digital Signature         | 1  | Si es necesario que tenga la misma operatividad que FNMT Clase 2 CA, tendrá La Norma ETSI TS 102 280 V1.1.1 (2004-03) – “X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons” recomienda el uso exclusivo del bit de no repudio para certificados destinados a validar el compromiso con el contenido firmado, tales como firmas electrónicas sobre transacciones o acuerdos.<br><br>En el <i>Technical Corrigendum 3</i> de la ITU-T X509 de 04/2004, el bit de no-repudio es renombrado a <b>contentCommitment</b> . En este documento se recoge lo siguiente:<br><br>“ <i>Note that it is not incorrect to refer to this keyUsage bit using the identifier nonRepudiation. However, the use of this identifier has been deprecated. Regardless of the identifier used, the semantics of this bit are as specified in this Directory Specification.</i> ” |
|       | Non Repudiation           | 1  |  |
|       | Key Encipherment          | 1  |  |
|       | Data Encipherment         | 1  |  |
|       | Key Agreement             | 0  |  |
|       | Key Certificate Signature | 0  |  |
|       | CRL Signature             | 0  |  |
| 13.   | extKeyUsage               | Autenticación de cliente:<br>1.3.6.1.5.5.7.3.2<br>Protección de correo electrónico:<br>1.3.6.1.5.5.7.3.4<br>Inicio de sesión de tarjeta inteligente:<br>1.3.6.1.4.1.311.20.2.2   | [RFC3280]: Certificate using applications MAY require that a particular purpose be indicated in order for the certificate to be acceptable to that application. If a CA includes extended key usages to satisfy such applications, but does not wish to restrict usages of the key, the CA can include the special keyPurposeID anyExtendedKeyUsage. If the anyExtendedKeyUsage key purpose is present, the extension SHOULD NOT be critical.  |
| 14.   | privateKeyUsagePeriod     | No se utilizará  |  |
| 15.   | Certificate Policies      |  | RFC 3739 obliga la existencia de al menos un valor.  |
|       | Policy Identifier         | OID asociado a la DPC o PC de certificado de firma de usuario final.<br>(fnmtPolCertPersonalAdministracion)<br>1.3.6.1.4.1.5734.3.14   | La Ley de Firma Electrónica dice para los certificados reconocidos: “La identificación del prestador de servicios de certificación que expide el certificado y su domicilio”. Se incluirá en la DPC.   |
|       | URL CPS                   | <a href="http://www.cert.fnmt.es/dpcs/">http://www.cert.fnmt.es/dpcs/</a>  | In an end entity certificate, these policy information terms indicate the policy under which the certificate has been issued and   |



| CAMPO                              | CONTENIDO  | OBSERVACIONES  |
|------------------------------------|--|--|
|                                    |  | <i>the purposes for which the certificate may be used.</i>   |
| <b>Notice Reference</b>            | Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM ( C/Jorge Juan 106-28009-Madrid-España)   |  |
| <b>16. qcStatements</b>            | id-etsi-qcs-QcCompliance<br>id-etsi-qcs-QcSSCD<br>id-etsi-qcs-QcLimitValue : 0€<br>Id-etsi-qcs-<br>QcRetentionPeriod: 15 años  | ETSI TS 101 862 define la inclusión de las siguientes declaraciones para certificados cualificados:<br>1.- <b>id-etsi-qcs-QcCompliance</b> – Indica que el certificado es cualificado. Solo si no está explícito en las políticas indicadas en la extensión correspondiente.<br>2.- <b>id-etsi-qcs-QcLimitValue</b> – Opcional. Indica el valor límite para transacciones. (No Aplicable).<br>3.- <b>id-etsi-qcs-QcRetentionPeriod</b> – Opcional. Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otro información relevante. En este caso la Ley obliga: <b>"Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo."</b> . Dado que la FNMT va a conservar la información de manera indefinida, y que la norma no establece un valor para indicar un período indefinido, no se incluirá este QC y se indicará en la DPC.<br>4.- <b>id-etsi-qcs-QcSSCD</b> – Opcional. Indica que la clave privada correspondiente al certificado está almacenada en un dispositivo seguro de creación de firma de acuerdo al Anexo III de la Directiva del Parlamento Europeo 1999/93/EC, sobre un framework comunitario para firmas electrónicas. |
| <b>17. Subject Alternate Names</b> | Nombre RFC822= email<br>Dirección del directorio:<br>OID.1.3.6.1.4.1.5734.1.1=Nom<br>OID.1.3.6.1.4.1.5734.1.2=Ape1<br>OID.1.3.6.1.4.1.5734.1.3=Ape2<br>OID.1.3.6.1.4.1.5734.1.4=NIF<br>OID.1.3.6.1.4.1.5734.1.38=fnmtA<br>PECargo<br>OID.1.3.6.1.4.1.5734.1.39=fnmtA<br>PEEntidad<br>OID.1.3.6.1.4.1.5734.1.40=fnmtA<br>PESituacion<br>OID.1.3.6.1.4.1.5734.1.44=fnmtA<br>PENIP<br>OID.1.3.6.1.4.1.5734.1.45=fnmtU<br>nidadOrganizativa<br>OID.1.3.6.1.4.1.5734.1.15<br>=fnmtPropCIF | Por interoperatividad con las aplicaciones ya desplegadas que hacen uso del formato de identificación de los certificados FNMT Clase 2 CA, se mantiene el contenido de SubjectAltName.   |



| CAMPO                        | CONTENIDO  | OBSERVACIONES  |
|------------------------------|--|--|
|                              | UPN:<br>OID.1.3.6.1.4.1.311.20.2.3=email<br>(Cadena UTF8 codificada en<br>ASN1)  |  |
| 18. Issuer Alternate Names   | No se utilizará  |  |
| 19. Basic Constraints        |  | <i>[RFC 3280] This extension MAY appear as a critical or non-critical extension in end entity certificates.</i>  |
| Subject Type                 | Entidad Final  |  |
| Path Constraint Length       | No utilizado   |  |
| 20. Policy Constraints       | No utilizado   |  |
| 21. CRLDistributionPoints    | LDAP:<br>ldap://ldapape.cert.fnmt.es:<br>puerto/CN=CRLnnn,OU= AC<br>APE, O=FNMT, C=ES<br>?certificateRevocationList;binary?base<br>?objectclass=cRLDistribution<br>Point<br>HTTP:<br>http://www.cert.fnmt.es/crls<br>ape/CRLnnn.crl          |  |
| 22. Auth. Information Access | OCSP:<br><a href="http://ocspape.cert.fnmt.es/ocspape/OcspResponder">http://ocspape.cert.fnmt.es/ocspape/OcspResponder</a><br>CA:<br><a href="http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt">http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt</a> | Contendrá información de localización del OCSP Responder. URL resuelta a diferentes servidores. Ley de Firma Electrónica: <b>"Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro"</b> . |
| 23. netscapeCertType         | sSLCLIENT,sMIME  | Tipo de certificado según Netscape   |
| 24. fnmtTipoCertificado      | 1.3.6.1.4.1.5734.1.33:<br>"Personal adscrito a la<br>Administración"   | Tipo de certificado para Personal adscrito a la Administración   |

**Tabla 6 Perfil del Certificado: Personal APE**

10.3.3.5. *Publicación del Certificado de personal al servicio de la Administración Pública*

79. Una vez generado el *Certificado* por parte del *Prestador de Servicios de Certificación*, se publicará en el *Directorio*, concretamente en la entrada correspondiente al nombre distintivo del personal al servicio de la Administración Pública, tal como se ha definido en el apartado "Emisión del Certificado" de este documento
80. Si en el proceso de solicitud el personal al servicio de la Administración Pública proporcionó una dirección de correo electrónico, se le enviará una comunicación de la disposición de su *Certificado* para su descarga.

*10.3.3.6. Descarga e instalación del Certificado de personal al servicio de la Administración Pública*

81. Una vez transcurrido el tiempo establecido desde que el personal al servicio de la Administración Pública se persona en la *Oficina de Registro* para acreditar su identidad, vigencia del cargo o empleo, y una vez que el *Certificado* haya sido generado, se pone a su disposición o a la de la *Oficina de Registro* un mecanismo de descarga de *Certificado* en la dirección

<http://ape.cert.fnmt.es/appsUsuario/descargameh/descargaCertInicio.jsp>

82. accediendo a la opción “Descarga de su Certificado”.

83. En este proceso guiado se le pedirá al personal al servicio de la Administración Pública o al responsable o encargado de la *Oficina de Registro* que introduzca el NIF o NIE con el que se realizó el proceso de presolicitud, así como el código de solicitud devuelto por el sistema al finalizar dicho proceso. Si el *Certificado* no ha sido aún generado por cualquier motivo, se le indicará este hecho en el momento que intente su descarga.

84. Si el *Certificado* ya ha sido puesto a disposición del personal al servicio de la Administración Pública o de la *Oficina de Registro*, aquél será introducido en el soporte en el que se generaron las *Claves* durante el proceso de Presolicitud, es decir, la *Tarjeta criptográfica* de la FNMT-RCM.

*10.3.3.7. Período de validez del Certificado de personal al servicio de la Administración Pública*

85. El periodo de validez de los *Certificados* de personal al servicio de la Administración Pública emitidos por la FNMT-RCM será de cuatro (4) años contados a partir del momento de la emisión del *Certificado*, siempre y cuando no se extinga su vigencia por las causas y procedimientos expuestos en el apartado “Extinción de la vigencia del Certificado” de la *Declaración General de Prácticas de Certificación* o lo dispuesto, en su caso, en la *Ley de Emisión* correspondiente.

*10.3.3.8. Revocación del Certificado de personal al servicio de la Administración Pública*

86. La revocación de *Certificados* implica, además de su extinción, la finalización de la relación y régimen de uso del *Certificado* con la FNMT-RCM.

87. La revocación de un *Certificado* para el personal al servicio de la Administración, dado su carácter instrumental para el desarrollo de las funciones públicas, solamente podrá ser solicitada por el responsable de la *Oficina de Registro*, correspondiente. El *Titular* podrá plantear a la *Oficina de Registro* la revocación y/o suspensión se existen causas que así lo aconsejan, en los términos recogidos en las presentes *Políticas de Certificación y Prácticas de Certificación Particulares*.

88. No obstante, la FNMT-RCM podrá revocar los *Certificados* para el personal al servicio de la Administración Pública en los supuestos recogidos en la *Declaración General de Prácticas de Certificación*.

89. La *Ley de Emisión* podrá, adicionalmente, establecer otras causas de revocación, suspensión y cancelación de la suspensión.



90. 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*.
91. Serán causas admitidas para la revocación de un *Certificado* las expuestas en el apartado “Causas de revocación de *Certificados*” de la *Declaración General de Prácticas de Certificación*, si bien, la capacidad para su realización solamente se le reconoce al responsable de la *Oficina de Registro*. Asimismo, se recuerda lo previsto en el apartado “Extinción de la vigencia del *Certificado*” de la *Declaración General de Prácticas de Certificación*, en relación con la solicitud de *Certificados* existiendo otro en vigor a favor del mismo *Titular* y mismo personal y perteneciente a la misma *Ley de Emisión*.
92. Las actuaciones necesarias para solicitar la revocación serán realizadas por la *Oficina de Registro* correspondiente a la entidad u organismo *Titular* y con la que la FNMT-RCM ha suscrito el convenio correspondiente.
93. En todo caso, FNMT-RCM recibirá de la Administración, organismos y/o entidad, aquella información relevante a efectos de la revocación de un *Certificado*, a través el modelo de solicitud de revocación del *Certificado* que se le presente, en formato papel o electrónico, por la *Oficina de Registro*.
94. La *Oficina de Registro* transmitirá 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.
95. FNMT-RCM igualmente 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 la *Oficina de Registro* correspondiente. 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*.
96. Una vez que la FNMT-RCM ha procedido a la revocación del *Certificado*, se publicará en el *Directorio* seguro la *Lista de Revocación* indicando el número de serie del *Certificado* revocado, la fecha y hora en que se ha realizado la revocación y, en su caso, la causa de la misma,

#### 10.3.3.9. *Suspensión del Certificado de personal al servicio de la Administración Pública*

97. La suspensión de *Certificados* deja sin efecto el *Certificado* durante un período de tiempo y en unas condiciones determinadas.
98. La suspensión de los *Certificados*, dada la naturaleza de estos *Certificados*, solamente podrá ser realizada por el responsable de la *Oficina de Registro* correspondiente, aunque el *Titular* podrá solicitarla a la *Oficina de Registro* en los supuestos pertinentes.
99. A continuación se describe el procedimiento a seguir por la *Oficina de Registro* por el que se le toman los datos personales, se confirma su identidad, vigencia del cargo o empleo y en su caso se formaliza la solicitud de suspensión de un *Certificado* por parte de un legítimo interesado. Serán causas admitidas para la suspensión de un *Certificado* las expuestas en el apartado “Causas de suspensión de *Certificados*” de la *Declaración General de Prácticas de Certificación*.



100. Estas actividades serán realizadas por la *Oficinas de Registro* de la entidad u organismo al que pertenece el *Titular*. La FNMT-RCM procederá a suspender el *Certificado* durante un plazo de noventa (90) días, plazo tras el cual se extinguirá el *Certificado* mediante su revocación directa por parte del *Prestador de Servicios de Certificación* de la FNMT-RCM, salvo que se hubiera levantado la suspensión por parte de la *Oficina de Registro* correspondiente. No obstante lo anterior, el plazo previsto para la suspensión del *Certificado* podrá verse alterado en función de los procedimientos judiciales o administrativos que lo pudieran afectar.
101. Si durante el plazo de suspensión del *Certificado* éste caducara o se solicitara su revocación, se producirán las mismas consecuencias que para los *Certificados* no suspendidos que se vieran afectados por supuestos de caducidad o de revocación.

1. La *Oficina de Registro* del ámbito correspondiente al órgano, organismo o entidad pública *Titular* podrá solicitar la suspensión del *Certificado* mediante la firma del modelo de solicitud de suspensión del *Certificado* que se le presente en formato papel o electrónico.

Las *Oficinas de Registro* transmitirán los registros tramitados a la FNMT-RCM para que ésta proceda a la suspensión del *Certificado*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

Una vez que la FNMT-RCM ha procedido a la suspensión del *Certificado*, se publicará en el *Directorio* la correspondiente *Lista de Revocación*, conteniendo el número de serie del *Certificado* suspendido, la fecha y hora en que se ha realizado la suspensión y como causa de revocación: “suspensión”.

En todos los supuestos anteriores de estas *Prácticas de Certificación* particulares donde sea necesaria la identificación y sea posible la identificación telemática, se tendrá en cuenta por el Prestador FNMT-RCM las funcionalidades previstas para el DNI-e, de acuerdo con la legislación específica y el uso de otro *Certificado* emitido por la FNMT-RCM o reconocido por ésta.

2. Cancelación de la suspensión del *Certificado* de personal al servicio de la Administración Pública

Podrán solicitar la Cancelación de la suspensión de los *Certificados* emitidos por la FNMT-RCM el responsable o encargado de la *Oficina de Registro* del ámbito del *Titular*, en los términos y condiciones expresados en la *Declaración General de Prácticas de Certificación*, siempre que dicha solicitud se efectúe durante los noventa (90) días siguientes a su suspensión. En este acto la *Oficina de Registro* aportará los datos que se le requieran y acreditará la identidad del personal a su servicio cuya identidad conste en el *Certificado*, siguiendo el procedimiento descrito anteriormente para la solicitud de emisión del *Certificado* del personal al servicio de la Administración Pública. FNMT-RCM aceptará el informe de acreditación que pudiera emitir la *Oficina de Registro* considerando lo establecido en el artículo 13.1, in fine, de la Ley de Firma Electrónica.

Los datos personales del personal al servicio de la Administración Pública y de la Administración Pública *Titular*, una vez validados por la *Oficina de Registro*, se enviarán a la FNMT-RCM mediante comunicaciones seguras establecidas para tal fin





entre la *Oficina de Registro* y la FNMT-RCM. Los datos personales y su tratamiento quedarán sometidos a la legislación específica

Una vez recibidos los datos validados por la *Oficina de Registro* de la petición de levantamiento de suspensión, la FNMT-RCM procederá a retirar este *Certificado* de la *Lista de Revocación*, no efectuándose acción técnica alguna sobre el *Certificado* en cuestión.

Como en supuestos anteriores a efectos de identificación, se tendrá en cuenta las funcionalidades previstas para el DNI-e, de acuerdo con la legislación específica y otras previstas en el ámbito de las Administraciones Públicas.

#### 10.3.3.10. Comprobación del estado del Certificado del personal al servicio de la Administración

102. El *Titular* del *Certificado* y las Administraciones ,organismos y entidades *usuarias* pertenecientes a la *Comunidad Electrónica* de este tipo de *Certificados* podrán realizar la comprobación del estado de un *Certificado*, bien, en la forma y condiciones que se expresan en los apartados “Procedimientos de consulta del estado de los *Certificados*” y “Servicio de validación de *Certificados* mediante *OCSP*” de la *Declaración General de Prácticas de Certificación*; bien, mediante el procedimiento específicamente establecido en la *Ley de Emisión* adoptada por la FNMT-RCM y la Administración u organismo actuante.

#### 10.3.4. Exclusiones y requisitos adicionales a ETSI TS 101 456

- De acuerdo con la norma en el apartado 8.2 b), se excluyen las cuestiones definidas en el apartado 7.5 j), k).
- De acuerdo con la norma en el apartado 8.2 c), se excluyen las cuestiones definidas en el apartado 7.3.5 f). En este tema se estará a lo señalado en el apartado “*Publicación del Certificado*” de este anexo.
- De acuerdo con la norma en el apartado 8.2 d), se excluyen las cuestiones definidas en el apartado 7.3.6 k). En este tema se estará a lo señalado en el apartado “*Comprobación del estado del Certificado*” de este anexo.

103. Respecto aquellos *Certificados* Reconocidos que usen Dispositivos Seguros de creación de firma, seguirán lo señalado en el apartado “Soporte del Certificado” de la *Declaración General de Prácticas de Certificación* de la FNMT-RCM, así como a lo expuesto en los apartados sobre “Ciclo de vida del certificado” del citado documento.

#### 10.3.5. Modelos de formulario

104. Los modelos de formularios que se deben cumplimentar para realizar las operaciones descritas para la gestión del ciclo de vida de los *Certificados* para personal al servicio de la Administración Pública se ponen a disposición en <http://www.ceres.fnmt.es> , así como en la *web* de cada *Oficina de Registro* correspondiente.



**11. CERTIFICADOS EMITIDOS PARA LA IDENTIFICACIÓN DE SEDES ELECTRÓNICAS DE LA ADMINISTRACIÓN PÚBLICA, ORGANISMOS Y ENTIDADES PÚBLICAS VINCULADAS O DEPENDIENTES**

**11.1. POLÍTICA DE CERTIFICACIÓN DE LOS CERTIFICADOS EMITIDOS PARA LA IDENTIFICACIÓN DE SEDES ELECTRÓNICAS DE LA ADMINISTRACIÓN PÚBLICA, ORGANISMOS Y ENTIDADES PÚBLICAS VINCULADAS O DEPENDIENTES**

**11.1.1. Identificación**

105. Las sedes electrónicas en el ámbito de actuación de las Administraciones Públicas, son direcciones electrónicas disponibles para los ciudadanos. El establecimiento de una sede electrónica conlleva la responsabilidad de la Administración u organismo actuante en relación con la integridad, veracidad y actualización de la información y servicios a los que pueda accederse. Las condiciones de publicidad oficial relativas a las sedes electrónicas, así como los principios aplicables a la sede electrónica será competencia de cada Administración *Titular* de la misma. La FNMT-RCM solamente prestará los servicios de seguridad y certificación electrónica necesarios atendiendo a las necesidades de cada Administración.
106. La presente *Política de Certificación Particular* de la FNMT-RCM para la expedición de *Certificados* para la identificación de sedes electrónicas de la Administración Pública, organismos y entidades públicas vinculadas o dependientes tiene la siguiente identificación:

|                  |   |
|------------------|---|
| Nombre           | <i>Política de Certificación de Certificados</i> para la identificación de sedes electrónicas de la Administración Pública, Organismos y entidades públicas vinculadas o dependientes |
| Referencia/OID   | 1.3.6.1.4.1.5734.3.12   |
| Versión          | 1.0   |
| Fecha de Emisión | de 1 de Agosto de 2007  |
| Localización     | <a href="http://www.cert.fnmt.es/dpcs">http://www.cert.fnmt.es/dpcs</a>   |
| DPC relacionada  | Declaración General de Prácticas de Certificación de la FNMT-RCM<br><br>Localización:<br><br><a href="http://www.cert.fnmt.es/dpcs">http://www.cert.fnmt.es/dpcs</a>                  |

**Tabla 7 Identificación Política Certificación – Sede Electrónica APE**



### 11.1.2. Tipología del *Certificado* para la identificación de sedes electrónicas de la Administración Pública, Organismos y entidades públicas vinculadas o dependientes

107. Los “*Certificados* de identificación de *sede electrónica*”, de conformidad con la definición de *sede electrónica* de la Ley 11/2007, LAECSP son aquellos *Certificados* expedidos por la FNMT-RCM bajo esta política de certificación y que vinculan unos *Datos de verificación de Firma* a los datos identificativos de una *sede electrónica* en la que existe una *persona física* que actúa como firmante o custodio de la clave y el *Titular* del *Certificado* que es la administración, organismo o entidad pública a la que pertenece y que es titular de la dirección electrónica y dominio a través de la que se accede a la *sede electrónica*. Esta *persona física* es la que tiene el control sobre dicho *Certificado* y los *Datos de creación y verificación de firma* y es responsable de su custodia de forma diligente.
108. Corresponderá al responsable de la *Oficina de Registro* la condición de firmante, custodio y, por tanto, el control de la clave y titularidad del *Certificado* de *sede electrónica*.
109. Por tanto, la *Clave Privada* asociada a la *Clave Pública* y los *Datos de creación y verificación de firma* estarán bajo la responsabilidad de dicho firmante o custodio y que actuará como representante de la entidad de la Administración Pública (*Persona Jurídica*) que tiene la titularidad, gestión y administración de la dirección electrónica correspondiente.
110. FNMT-RCM emitirá estos *Certificados* siempre que sea solicitado por los miembros de la *Comunidad Electrónica* sujetos a la Ley 11/2007 LAECSP para las diversas relaciones que puedan producirse en el ámbito de la *sede electrónica* y no se encuentre prohibido o limitado su utilización por la legislación aplicable.
111. FNMT-RCM emitirá, suspenderá y/o revocará estos *Certificados* siempre que sea solicitado por el responsable de la *Oficina de Registro* correspondiente, el cual se presumirá que ostenta capacidad y competencia suficientes a los efectos de este tipo de *Certificados*.
112. Lo dispuesto anteriormente se entenderá sin perjuicio de lo ordenado por resolución administrativa o judicial.
113. FNMT-RCM no será responsable, al igual que con el resto de *Certificados* emitidos de las actuaciones realizadas con este tipo de *Certificados* cuando se produzcan abuso de facultades o insuficiencia de las mismas y/o cuando se produzcan decisiones del miembro de la *Comunidad Electrónica Titular* del *Certificado* que afecten a la vigencia de las facultades de éste, produciendo en su caso supuestos de responsabilidad patrimonial, por lo que cualquier modificación, revocación o restricción en el *Certificado* y su uso no será oponible a la FNMT-RCM salvo que sea fehacientemente notificada por persona con competencia al efecto o, en su caso, por el responsable de la *Oficina de Registro* correspondiente.
114. Del mismo modo, FNMT-RCM no será responsable de las actuaciones realizadas con este tipo de *Certificados* cuando los datos identificativos de la *sede electrónica*, consignados en el *Certificado* y para la cual se ha emitido, sean diferentes de los asociados a la *sede electrónica* en la que se esté empleando, por lo que cualquier modificación, revocación o restricción en el *Certificado* y su uso no será oponible a la FNMT-RCM salvo que sea fehacientemente notificada. FNMT-RCM no es competente para acreditar o valorar la



- titularidad de las sedes electrónicas y/o dominios de las Administraciones, organismos o entidades públicas a las que pertenezca dicha sede electrónica.
115. La FNMT-RCM, como *Prestador de Servicios de Certificación* se reserva el derecho de no expedir o revocar este tipo de *Certificados* si el *firmante/custodio* del *Certificado* de *sede electrónica* en la que se emplea tal *Certificado*, no hace un uso adecuado del mismo, conculcando derechos de propiedad industrial o intelectual de terceros sobre las aplicaciones, sitios Web o *sedes electrónicas* que se desean proteger con tales *Certificados*, o su uso se presta a engaño o confusión sobre la titularidad de tales aplicaciones, sitios Web o *sedes electrónicas* y, por tanto, de sus contenidos. En especial, tal reserva de derechos se podrá ejecutar por la FNMT-RCM cuando en la utilización de tales *Certificados* se atente contra los siguientes principios:
- a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.
  - b) La protección de la salud pública o de las personas físicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.
  - c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y
  - d) La protección de la juventud y de la infancia.
116. La FNMT-RCM, se mantendrá indemne por parte de los titulares o responsables de los equipos, aplicaciones o *sedes electrónicas* que incumplan lo previsto en este apartado y que tenga relación con el *Certificado*, quedando exonerada de cualquier reclamación o reivindicación por el uso inadecuado de tales *Certificados*.
117. Este *Certificado* se emite por la FNMT-RCM por cuenta de la Administración Pública correspondiente a la que la FNMT-RCM presta los servicios técnicos, administrativos y de seguridad necesarios como *Prestador de Servicios de Certificación*.
118. El *Certificado* para la identificación de *sedes electrónicas* de la Administración Pública es desarrollado por la FNMT-RCM mediante una infraestructura PKI específica, basada en actuaciones de identificación y registro realizadas por las *Oficinas de Registro* designadas por el órgano, organismo o entidad de la Administración Pública que tiene la titularidad, gestión y administración de la dirección electrónica de la *sede electrónica*.
119. 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.
120. Este *Certificado*, es emitido con el perfil técnico correspondiente y/o equivalente a los denominados *Certificados Reconocidos*, con base en los criterios establecidos para tal en la Ley de Firma Electrónica (Ley 59/2003), en la normativa especial de la FNMT-RCM y en la normativa técnica EESSI, concretamente ETSI TS 101 456 - “Policy requirements for certification authorities issuing qualified certificates” y ETSI TS 101 862 - “Qualified Certificate Profile”, tanto en lo referente al *Prestador de Servicios de Certificación* como a la generación de los *Datos de Verificación de Firma* y al contenido del propio *Certificado*; todo ello sin perjuicio de las especialidades propias del ámbito de actuación de las Administraciones públicas.

121. Por consiguiente, el *Certificado* emitido para la identificación de *sedes electrónicas* no se registrará por lo dispuesto en la Ley 59/2003, de 19 de diciembre, de firma electrónica a efectos del *Certificado* de persona jurídica de acuerdo con lo dispuesto en el artículo 7.6 de la citada Ley, por lo que será de aplicación la normativa específica correspondiente y, en su defecto, las Declaraciones General y Particular de la FNMT-RCM, en defecto, como se ha dicho, de normativa específica derivada entre otros supuestos del esquema nacional de interoperabilidad y/o seguridad.

### 11.1.3. Gestión de la Política de Certificación

122. La FNMT-RCM dispone específicamente de una *Política de Certificación* efectiva en relación con los *Certificados* emitidos para la identificación de *sedes electrónicas* de la Administración General del Estado y, en su caso, otras Administraciones Públicas del ámbito de aplicación de la Ley 11/2007, de 22 de junio, LAECSP, y, en particular, declara que:

- La FNMT-RCM tiene capacidad para especificar, revisar, y aprobar la *Política de Certificación* de estos *Certificados* a través de su Dirección General y demás órganos directivos de la misma.
- La FNMT-RCM dispone (apartado 11.2, siguiente) de una *Declaración Particular de Prácticas de Certificación* en la que se detallan las prácticas de certificación empleadas para la expedición de *Certificados* conformes a la *Política de Certificación* aquí expuesta para este tipo de *Certificado*.
- La FNMT-RCM dispone, dentro de las competencias de la Dirección y demás órganos directivos de la misma, 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.
- La FNMT-RCM realiza análisis de riesgos para evaluar las amenazas del sistema y proponer las medidas de seguridad adecuadas (salvaguardas) para todas las áreas implicadas.
- La *Declaración Particular de Prácticas de Certificación* se pone a disposición del público mediante el URL:

<http://www.cert.fnmt.es/dpcs/>

- La *Ley de Emisión* de cada tipo o grupo de *Certificados*, caso de establecerse, podrá ser de acceso restringido total o parcialmente por razones de seguridad al tratarse de un sistema de certificación de uso en el ámbito de las Administraciones públicas y personal correspondiente.
- La *Política de Certificación* de *Certificados* emitidos para la identificación de *sedes electrónicas* se pone a disposición del público mediante el URL:

<http://www.cert.fnmt.es/dpcs/>

- Esta *Política de Certificación* recoge las obligaciones y responsabilidades generales de las partes implicadas en la emisión y uso de los *Certificados* de *sede electrónica* en



el ámbito público, los cuales están emitidos por la FNMT-RCM bajo a esta *Política de Certificación*, sin perjuicio de las especialidades que pudieran existir en el contrato o convenio correspondiente o si procede en la *Ley de Emisión*.

- Se dispone de un *OID* específico para identificar la *Política de Certificación* aquí desarrollada, siendo el *OID* asignado en el marco de la numeración de la FNMT-RCM: 1.3.6.1.4.1.5734.3.12

123. La *Política de Certificación* de la FNMT-RCM para el presente *Certificado* se define en base al documento ETSI TS 101 456, en concreto en su apartado 8, cumpliéndose los requisitos expuestos en los apartados 6 y 7 con las exclusiones señaladas en el apartado 8.2 (que se exponen en el apartado ***Exclusiones y Requisitos Adicionales a ETSI TS 101456*** de la presente *Política de Certificación*). En caso de discrepancia entre este documento y la referida norma, prevalecerá este documento.

#### 11.1.4. Comunidad y ámbito de aplicación

124. La presente *Política de Certificación* es de aplicación en la expedición de *Certificados de sede electrónica* ámbito público. Estos *Certificados* tendrán las siguientes características:

- a) Son expedidos como *Certificados Reconocidos* o con efecto equivalente a los denominados reconocidos con base en los criterios establecidos para tal en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y en la normativa técnica EESSI ETSI TS 101 862 – “Qualified Certificate Profile”.
- b) Son expedidos por la FNMT-RCM como *Prestador de Servicios de Certificación* cumpliendo con los criterios establecidos en la Ley 59/2003, de 19 de diciembre, citada, y en la normativa técnica EESSI, concretamente ETSI TS 101 456 - “Policy requirements for certification authorities issuing qualified certificates”.
- c) Los *Certificados* emitidos bajo esta *Política de Certificación* son expedidos para los órganos y entidades encuadrables en el concepto legal de Administración Pública, organismos y entidades públicas vinculadas o dependientes y que forman parte de la *Comunidad Electrónica*, tal y como se define en el apartado ***Definiciones*** de la *Declaración General de Prácticas de Certificación* de la FNMT-RCM, y con objeto exclusivo de identificar una *sede electrónica* de titularidad de cualesquiera de estos sujetos públicos.

En el marco de esta *Política de Certificación*, el *Solicitante* del *Certificado* se corresponde con personal con competencia suficiente y que presta sus servicios en la Administración Pública del Reino de España, bien sea en un órgano, organismo, entidad de la Administración general, Autonómica o Local del Estado y que tiene la titularidad, gestión y administración de la dirección electrónica a través de la que se accede a la *sede electrónica*.

- d) Los *Certificados* emitidos bajo esta *Política de Certificación* se consideran idóneos como parte integrante de sistemas de firma electrónica que requieran niveles de seguridad específicos y, en especial, para el establecimiento de comunicaciones seguras entre una dirección electrónica y el usuario que se conecte a ella, además de ser una herramienta para autenticar e identificar a la dirección electrónica para la cual han sido emitidos. Por tanto, los *Certificados* emitidos bajo esta política se consideran





adecuados para el desarrollo de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP), a los efectos de identificación de las *sedes electrónicas* en el ámbito público y para el establecimiento de comunicaciones seguras con ellas, con idoneidad para ser utilizados en la generación de firma electrónica reconocida en dicho ámbito.

125. La *Ley de Emisión* de estos *Certificados* podrá determinar, en defecto de normativa específica, las condiciones de uso y régimen específico o individualizado de estos *Certificados* que permitirán la identificación de las *sedes electrónicas* y atribución a las Administraciones, organismos y entidades titulares de tales sedes electrónicas y responsables de sus contenidos de los diferentes actos y resoluciones realizados; todo ello, sin modificación legal o variación respecto de la actuación que vienen realizando las Administraciones, organismos y entidades en los soportes tradicionales en papel y otros.

#### 11.1.5. Responsabilidad y obligaciones de las partes

126. Serán partes a los efectos de este apartado los siguientes sujetos:

- La Administración, organismos, entidades públicas representadas a través de los diferentes órganos competentes. Salvo indicación en contrario, corresponderá la representación a las *Oficinas de Registro* correspondiente a través de su responsable.

- Los *Titulares*, que serán:

los órganos, organismos y entidades de la Administración Pública que tengan la titularidad, gestión y administración de la dirección electrónica a través de la cual se accede a la *sede electrónica* o, en su caso, órgano en quién se deleguen las atribuciones o facultades. FNMT-RCM considerará como entidades u órgano delegados, salvo indicación en contrario, a las *Oficinas de Registro*.

- Los Firmantes/Custodios, que serán:

el personal al servicio de las Administraciones, organismos y entidades públicas que realiza la solicitud del Certificado y que, por tanto, toma el papel de firmante y custodio de los Datos de Creación de Firma. FNMT-RCM considerará, salvo indicación en contrario, que el responsable de la Oficina de Registro es el firmante y custodio del Certificado y de los Datos de Creación de Firma contenidos en el mismo.

- FNMT-RCM, en cuanto Prestador de Servicios de Certificación.

- En su caso, resto de *Comunidad Electrónica* y terceros.

127. El régimen de derechos y obligaciones de las Administraciones, organismos, entidades públicas y la FNMT-RCM se regirá mediante el correspondiente acuerdo o convenio regulador de los servicios de certificación. En estos acuerdos o convenios podrá establecerse la *Ley de Emisión* de estos *Certificados*; sin perjuicio, de lo dispuesto en la presente Declaración en relación con las características o requisitos comunes aplicables a la *Ley de Emisión* de cada tipo de *Certificado* que se establece, con carácter general y efecto subsidiario, a lo no previsto en los acuerdos o convenios correspondientes.

128. Con carácter general y de forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la *Declaración General de Prácticas de Certificación*, la





Administración, organismos, entidades públicas *Titulares*, representadas a través de los diferentes órganos competentes, actuando a través del responsable de la *Oficina de Registro* para la emisión de este tipo de *Certificados*, tiene la obligación de:

- No realizar registros o tramitar solicitudes de *Certificados* para la identificación de *sedes electrónicas* por personal que preste sus servicios en una entidad diferente a la que representa como *Oficina de Registro*, salvo habilitación expresa de otra entidad.
- No realizar registros o tramitar solicitudes de *Certificados* emitidos bajo esta política y cuya titularidad, referida al órgano de la administración, se corresponda con una entidad de la administración pública sobre la que no tenga potestades o no tenga competencias para actuar como *Oficina de Registro*.
- No realizar registros o tramitar solicitudes de *Certificados* emitidos bajo esta política y cuya titularidad, referida al órgano u organismo de la administración, no se corresponda con la titularidad de la dirección electrónica a través de la que se accede a la *sede electrónica* que identificará el *Certificado* objeto de la solicitud.
- No realizar registros o tramitar solicitudes de *Certificados* emitidos bajo esta política y cuya titularidad, referida al firmante y custodio de los *Datos de Creación de Firma*, se corresponda con una *persona física* que no preste sus servicios en la entidad titular del *Certificado* y/o no coincida con alguno de los contactos establecidos, en las bases de datos correspondientes, para la gestión y administración de la dirección electrónica a través de la que se accede a la *sede electrónica* que identificará el *Certificado* objeto de la solicitud.
- Comprobar fehacientemente los datos identificativos y competenciales de los *Titulares* del *Certificado* (la Administración propietaria de la *sede electrónica* y de la dirección electrónica, dominio o URL, a través del cual se accede a tal *sede*) y *Solicitantes* (la persona física con atribución suficiente para solicitar un *Certificado de sede electrónica*) del *Certificado* y verificar su correspondencia con los titulares y contactos establecidos, en las bases de datos correspondientes, para la gestión y administración de la dirección electrónica a través de la que se accede a la *sede electrónica* que identificará el *Certificado* objeto de la solicitud.
- Solicitar la revocación del *Certificado* de identificación de *sede electrónica* emitido bajo esta política cuando alguno de los datos referidos a los *Titulares* o los firmantes/custodios del *Certificado*
  - sea incorrecto, inexacto o haya variado respecto a lo consignado en el *Certificado* o
  - no se correspondan con el titular, firmante/custodio y contactos establecidos, en las bases de datos correspondientes, para la gestión y administración de la dirección electrónica consignada en el *Certificado* objeto de la revocación.
- No utilizar el *Certificado* cuando alguno de los datos referidos al cargo, puesto de trabajo o empleo o cualquier otro relativo al firmante/custodio del *Certificado* sea inexacto, incorrecto o no refleje o caracterice adecuadamente su relación con el órgano o la entidad en la que presta sus servicios; o, existan razones de seguridad que así lo aconsejen.





129. Las relaciones de la FNMT-RCM y el *Titular* quedarán determinadas principalmente, a los efectos del régimen de uso de los *Certificados* a través del documento relativo a las condiciones de utilización o en su caso, contrato de emisión del *Certificado* y atendiendo a los acuerdos, convenios o documento de relación entre la FNMT-RCM y la Administración Pública correspondiente.
130. El resto de la Comunidad Electrónica y los terceros regularán sus relaciones con la FNMT-RCM a través de la Declaración General de Prácticas de Certificación y; en su caso, a través de estas Políticas de Certificación y Prácticas de Certificación Particulares; todo ello sin perjuicio de lo dispuesto en la normativa sobre firma electrónica y demás normativa que resulte de aplicación.
131. FNMT-RCM no será responsable de la comprobación de la coincidencia entre los Titulares y la dirección electrónica consignados en el Certificado con el titular y contactos administrativos que figuran, para dicha dirección electrónica, en las bases de datos de las entidades reguladoras de la asignación y gestión de nombres direcciones electrónicas, correspondiendo esta actividad y responsabilidad a la Oficina de Registro.
132. FNMT-RCM no será responsable de la utilización de los *Certificados* emitidos bajo esta *Política* cuando el *Titular* del *Certificado* electrónico a través de su representante o firmante/custodio realice actuaciones sin facultades o extralimitándose de las mismas o no se corresponda con los titulares y contactos autorizados para la gestión de la dirección electrónica para la cual ha sido emitido el *Certificado*.

#### 11.1.6. Límites de uso de los Certificados para la identificación de sedes electrónicas

133. Constituyen límites de uso de este tipo de *Certificados* las competencias administrativas correspondientes a cada *Titular* identificado al amparo de las *sedes electrónicas* de la Administración Pública, Organismos y entidades públicas vinculadas o dependientes, de conformidad con la Ley 11/2007, LAECSP, para la identificación de *sedes electrónicas* y el establecimiento de comunicaciones seguras con éstas. La FNMT-RCM y la Administración, organismos y entidades podrán fijar en los acuerdos o convenios, o a través del documento de relación correspondiente o, si fuera procedente en la *Ley de Emisión* de estos *Certificados*, otros límites adicionales.
134. El *Certificado* de sede electrónica del ámbito público, no permitirá a sus *Titulares* emplear este tipo de *Certificados*, por persona o entidad distinta a la FNMT-RCM, para:
  - Firmar otro *Certificado*, salvo autorización previa y expresa de la FNMT-RCM.
  - Usos particulares o privados.
  - Firmar software o componentes.
  - Generar *Listas de Revocación* como prestador de servicios de certificación.
  - Cualquier uso que exceda de la finalidad de este tipo de *Certificados* sin la autorización previa de la FNMT-RCM





## 11.2. PRÁCTICAS DE CERTIFICACIÓN PARTICULARES PARA LOS CERTIFICADOS EMITIDOS PARA LA IDENTIFICACIÓN DE SEDES ELECTRÓNICAS DE LA ADMINISTRACIÓN PÚBLICA, ORGANISMOS Y ENTIDADES PÚBLICAS VINCULADAS O DEPENDIENTES

135. La FNMT-RCM en su labor como *Prestador de Servicios de Certificación* y para demostrar la necesaria fiabilidad para la prestación de dichos servicios, ha desarrollado una *Declaración de Prácticas de Certificación* cuyo objeto es la información pública sobre las condiciones generales de prestación de los servicios de certificación por parte de la FNMT-RCM en su condición de *Prestador de Servicios de Certificación*.
136. En especial deberá tenerse presente, a efectos interpretativos del presente anexo el apartado “Definiciones” del cuerpo principal de la *Declaración General de Prácticas de Certificación*.
137. El Presente documento trae causa y forma parte integrante de la *Declaración General de Prácticas de Certificación* de la FNMT-RCM y define el conjunto de prácticas particulares adoptadas por la FNMT-RCM como *Prestador de Servicios de Certificación* para la gestión del ciclo de vida de los *Certificados para la identificación de sedes electrónicas de la Administración Pública*, expedidos bajo la *Política de Certificación de Certificados para la identificación de sedes electrónicas de la Administración Pública, Organismos y entidades públicas vinculadas o dependientes* identificada con el OID 1.3.6.1.4.1.5734.3.12.

### 11.2.1. Servicios de Gestión de las Claves de los Usuarios y Titulares

138. La FNMT-RCM bajo ningún concepto genera ni almacena las *Claves Privadas* de los *Titulares*, que son generadas bajo su exclusivo control y el del responsable de la *Oficina de Registro* cuya custodia esta bajo su responsabilidad o, en su caso, bajo la responsabilidad de la persona designada por la *Oficina de Registro*.

### 11.2.2. Gestión del ciclo de vida de los Certificados

#### 11.2.2.1. Registro de los Titulares de Certificados de sede electrónica ámbito público

139. Con carácter previo al establecimiento de cualquier relación institucional con los *Titulares*, la FNMT-RCM informa a través de los medios y direcciones web citadas en estas Prácticas y, subsidiariamente, en la *Declaración General de Prácticas de Certificación*, acerca de las condiciones del servicio así como de las obligaciones, garantías y responsabilidades de las partes implicadas en la expedición y uso de los *Certificados* por ella emitidos en su labor como *Prestador de Servicios de Certificación*.
140. La FNMT-RCM en su actividad como *Prestador de Servicios de Certificación*, a través de las *Oficinas de Registro* procede a la identificación de los *solicitantes* y futuros *Titulares* que soliciten *Certificados* para la identificación de *sedes electrónicas* mediante aquellos procedimientos que así se dispongan para ello. FNMT-RCM considerará con competencia al efecto cualquier solicitud que venga realizada por el responsable de la *Oficina de Registro* correspondiente, que se considerará representante del *Titular*.
141. 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, legitimidad y competencia de los representantes, 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.

142. La FNMT-RCM, dado que en su actividad como *Prestador de Servicios de Certificación* no genera el par de *Claves* de los *Titulares*, pone todos los mecanismos necesarios durante el proceso de *Solicitud de Certificados* para posibilitar que el responsable de la *Oficina de Registro* y/o el representante del *Titular* se encuentra en posesión de la *Clave Privada* asociada a la *Clave Pública* que se certificará.

#### 11.2.2.2. Procedimiento de solicitud del Certificado para la identificación de sedes electrónicas

143. A continuación se describe el procedimiento de solicitud del *Certificado* por el que se toma la denominación oficial de la Administración, organismo o entidad pública, que serán los *Titulares* de los *Certificados*, los datos personales de los representantes de los *Titulares*, se confirma su identidad, vigencia del cargo o empleo y se formaliza, entre el *Titular* y la FNMT-RCM el documento de condiciones de utilización o el contrato tipo de emisión para la posterior emisión de un *Certificado* para la identificación de la *sede electrónica*.

144. Se hace constar que FNMT-RCM, en función de la relación de *Titulares* remitida por la Administración, organismo o entidad pública, considerará, bajo responsabilidad de las correspondientes órganos, organismos y/o entidades que actuarán a través de las *Oficinas de Registro*, que estos *Titulares* cumplen los requisitos establecidos en la presente Declaración y, por tanto, tienen la legitimidad y competencia necesarias para solicitar y obtener el *Certificado* de identificación de *sede electrónica*. La FNMT-RCM presumirá con facultades y competencia suficientes a los representantes de los *Titulares* que tengan encomendada la responsabilidad de la *Oficina de Registro*.

145. FNMT-RCM, no tendrá, en este tipo de *Certificado*, la responsabilidad de comprobar:
- La potestad y competencia de la *Oficina de Registro* para solicitar un *Certificado* de identificación de *sede electrónica* en nombre del órgano, organismo o entidad de la administración en cuestión y *Titular* del *Certificado*.
  - La titularidad del órgano, organismo o entidad de la administración sobre la dirección electrónica y/o dominio que se consignará en el *Certificado*
  - Que el *Solicitante* del *Certificado* tenga la condición de personal al servicio de la Administración pública *Titular* con legitimidad y competencia suficiente para iniciar la solicitud y actuar como firmante y/o custodio del *Certificado*.

146. Por tanto, todas las actividades de comprobación serán realizadas por las *Oficinas de Registro* implantadas por el organismo o entidad de la Administración Pública en cuestión que se corresponderá, en cada caso, con el organismo o entidad *Titular* del *Certificado* y de la dirección electrónica a través de la que se accede a su *sede electrónica*.

#### 11.2.2.3. Presolicitud

147. El representante del *Titular* que, habitualmente, será el responsable de la *Oficina de Registro* correspondiente, en el sistema de firma electrónica basado en dispositivo seguro o



- medio equivalente, genera las *Claves Pública y Privada* que serán vinculadas al *Certificado*, convirtiéndose posteriormente en datos de *verificación y creación* de firma respectivamente.
148. El representante y/o responsable de la *Oficina de Registro* compone una solicitud electrónica de *Certificado*, generalmente en formato PKCS#10, y accede al *sitio web* del *Prestador de Servicios de Certificación*, la FNMT-RCM, a través de la dirección  
<https://ape.cert.fnmt.es/PrerregistroSolicitudesComponentesAPE/index.html>
149. donde se mostrará un formulario en el que dicho representante deberá introducir los datos del órgano *Titular* a cargo de la *sede electrónica* para la cual se emitirá el *Certificado*, y los datos de la *persona física* propios en su condición de responsable de la custodia diligente de los datos de creación de firma. Adicionalmente, el responsable también deberá introducir la solicitud electrónica generada anteriormente.
150. Como respuesta al envío del formulario la FNMT-RCM asignará e indicará al responsable un código de solicitud para su utilización en la *Oficina de Registro* y en el momento de la solicitud del *Certificado*
151. Con carácter previo el representante y/o responsable de la *Oficina de Registro* y la Administración que será *Titular* deberán consultar la *Declaración General de Prácticas de Certificación* y las presentes *Políticas de Certificación y Prácticas de Certificación Particulares* en la dirección  
<http://www.cert.fnmt.es/dpcs/>
152. con las condiciones de uso y obligaciones para las partes, pudiendo realizar las consultas que estime oportunas sobre el alcance de esta Declaración; todo ello, sin perjuicio de que con posterioridad, el representante del *Titular* responsable de la *Oficina de Registro* y la FNMT-RCM, deban suscribir el documento de condiciones de utilización o si procede el contrato de emisión. En ningún caso la continuación del procedimiento de presolicitud implicará la conclusión del proceso.
153. Al realizar esta presolicitud se envía a la FNMT-RCM la *Clave Pública* generada, junto con la correspondiente prueba de posesión de la *Clave Privada*, para la posterior emisión del *Certificado*.
154. La FNMT-RCM, tras recibir esta información, comprobará mediante la *Clave Pública* del peticionario la validez de la información de la presolicitud firmada, comprobando únicamente la posesión y correspondencia de la pareja de *Claves* criptográficas por parte del representante y/o responsable de la *Oficina de Registro*.
155. Esta información no dará lugar a la generación de un *Certificado* por parte de la FNMT-RCM, en tanto que ésta no reciba firmada por el responsable de la *Oficina de Registro* la solicitud del *Certificado*.

#### 11.2.2.4. Confirmación de las identidades y requisitos de las partes

156. El responsable de la *Oficina de Registro* se identificará a través de su documento nacional de identidad o documento de identificación sustitutorio ante la FNMT-RCM, mediante la correspondiente aplicación de registro y uso de su propio *Certificado Reconocido*. FNMT-RCM presumirá que el responsable de la *Oficina de Registro* se encuentra en el ejercicio de



la competencia y con capacidad suficiente para realizar los trámites para la obtención de este tipo de *Certificados*.

*11.2.2.5. Personación del Solicitante ante las Oficinas de Registro*

157. En supuestos distintos a la intervención del responsable de la *Oficina de Registro*, a efectos de obtención del *Certificado*, se considerará *Solicitante* con legitimación y competencia suficientes a la persona designada por el *Titular del Certificado de sede electrónica*.
158. Para obtener el *Certificado*, el *Solicitante* se personará ante una *Oficina de Registro* designada a tal efecto por el organismo o entidad *Titular del Certificado*.

*11.2.2.6. Comparecencia y documentación*

159. En supuestos distintos a la intervención del responsable de la *Oficina de Registro*, a efectos de obtención del *Certificado*, el representante del *Titular Solicitante* se personará y aportará los datos que se le requieran y que acrediten, ante la *Oficina de Registro*:
- su identidad personal,
  - su condición de personal al servicio del órgano, organismo o entidad de la Administración *Titular del Certificado* y titular de la dirección electrónica a través de la que se accede a la *sede electrónica* objeto del *Certificado*
  - su condición de persona habilitada o designada para la gestión de la dirección electrónica a través de la que se accede a la *sede electrónica* objeto del *Certificado*
160. FNMT-RCM estará y admitirá, en todo caso a la función e informe que realice la *Oficina de Registro* designada por la Administración. En el caso de que no se acrediten los puntos anteriores, la *Oficina de Registro* no continuará con la tramitación de la solicitud del *Certificado*.

*11.2.2.7. Envío de información a la FNMT-RCM*

161. Una vez confirmada la identidad del *Solicitante* y vigencia de las condiciones de legitimación y competencia exigidas a éste, incluida pero no limitada, a la titularidad sobre la dirección electrónica, se suscribirá el documento de condiciones de utilización o, en su caso, contrato de solicitud por el *Solicitante* en nombre del *Titular* y/o el responsable de la *Oficina de Registro*. La información y documentos anteriores serán enviados, junto con el código de solicitud recogido en la fase de presolicitud a la FNMT-RCM. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.
162. Dicho envío sólo se producirá si la *Oficina de Registro* tiene legitimidad y competencia para actuar como tal en nombre del órgano, organismo o entidad de la Administración Pública del *Certificado* de identificación de la *sede electrónica* y si ésta administración es titular de la dirección electrónica a través de la que se accede a la *sede electrónica* objeto del *Certificado*.
163. 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.

*11.2.2.8. Extensión de la función de registro e identificación a otros Certificados emitidos por la FNMT-RCM.*

164. Los miembros de la *Comunidad Electrónica* podrán recibir la prestación de servicios de certificación y firma electrónica de la FNMT-RCM, basada en la emisión de *Certificados* electrónicos pertenecientes a diferentes *Leyes de Emisión* y en soportes distintos, mediante la aceptación de las condiciones que, específicamente, se le exhibirán a instancia de la FNMT-RCM en las diferentes webs y demás soportes de servicios de los miembros de la *Comunidad Electrónica*, de acuerdo con lo establecido en la legislación sectorial correspondiente y con las limitaciones establecidas en la legislación reguladora del tratamiento de datos de carácter personal.
165. En la prestación de los servicios señalados en el párrafo anterior, se podrán extender los efectos de las actuaciones derivadas del registro e identificación, con los límites temporales previstos en la legislación de firma electrónica, así como la reguladora del DNI-e.; todo ello sin perjuicio de las especialidades que puedan derivarse del ámbito de las Administraciones Públicas.

*11.2.2.9. Emisión del Certificado para la identificación de sede electrónica*

166. Una vez recibidos en la FNMT-RCM los datos de los *Titulares*, la información que describe la relación del representante con la Administración Pública (sin perjuicio que se remita por el responsable de la *Oficina de Registro*), así como el código de solicitud obtenido en la fase de presolicitud y, en su caso, la información que describe su titularidad y gestión de la dirección electrónica de la sede en cuestión, se procederá a la emisión del *Certificado*.
167. La emisión de *Certificados* supone la generación de documentos electrónicos que confirman la identidad y titularidad de una dirección electrónica a través de la que se accede a una *sede electrónica*, así como la gestión de ésta por parte de un órgano, organismo o entidad de la Administración Pública española, así como el vínculo con un firmante/custodio de los datos de creación de firma y responsable de las operaciones que se realicen con dicho *Certificado* en el marco de la identificación de una *sede electrónica* y el establecimiento de comunicaciones seguras con ésta.
168. La emisión de *Certificados* de la FNMT-RCM sólo puede realizarla ella misma, en su calidad de *Prestador de Servicios de Certificación*, no existiendo ninguna otra entidad u organismo con capacidad de emisión de los mismos.
169. La FNMT-RCM, por medio de su *Firma electrónica*, autentica los *Certificados* y confirma la identidad y competencia de sus *Titulares*, así como la titularidad de la dirección electrónica de la sede y contactos establecidos para la gestión de dicha dirección, de conformidad con la información recibida por parte de la *Oficina de Registro*. 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*.
170. La FNMT-RCM, en ningún caso, incluirá en un *Certificado* información distinta de la aquí mostrada, ni circunstancias, atributos específicos de los firmantes o límites distintos a los previstos en los acuerdos, convenios y, en su caso, a los previstos en la *Ley de Emisión* correspondiente.

171. En cualquier caso la FNMT-RCM actuará diligentemente para:

- Comprobar que el *Solicitante* del *Certificado* o el responsable de la *Oficina de Registro* utilice la *Clave Privada* correspondiente a la *Clave Pública* vinculada a la identidad del *Titular* del mismo. Para ello la FNMT-RCM comprobará la correspondencia entre la *Clave privada* y la *Clave pública*.
- Lograr que la información incluida en el *Certificado* se base en la información proporcionada por el *Solicitante* y/o por el responsable de la *Oficina de Registro* correspondiente.
- No ignorar hechos notorios que puedan afectar a la fiabilidad del *Certificado*.
- Lograr que el *DN* (nombre distintivo) asignado en el *Certificado* sea único en toda la *Infraestructura de Clave Pública* de la FNMT-RCM.

172. Para la emisión del Certificado se seguirán los siguientes pasos:

1. Composición del nombre distintivo (DN) del *Titular*

Con los datos de la dirección electrónica de la sede 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 de lugar a ambigüedades. No se contempla el uso de seudónimos como forma de identificación del *Titular*.

El *DN* está compuesto de los siguientes elementos:

$DN=CN, OU, OU, OU, O, C$

El conjunto de atributos OU, OU, OU, O, C representa la rama del directorio en la que se encuentra ubicada la entrada correspondiente al *Titular* y/o firmante/custodio en cuestión.

El atributo *CN* contiene la dirección electrónica a través de la cual se accede a la sede electrónica objeto del *Certificado*.

Una vez compuesto el nombre distintivo (*DN*) se crea la correspondiente entrada en el directorio, procurando que el nombre distintivo sea único en toda la *Infraestructura de Clave Pública* del *Prestador de Servicios de Certificación*.

2. Composición de la identidad alternativa del *Titular*

La identidad alternativa del *Titular*, tal como se contempla en la presente tipología de *Certificados* contiene la identidad de los titulares del *Certificado* distribuida en una serie de atributos. Se utiliza la extensión *subjectAltName* definida en X.509 versión 3 para ofrecer esta información.

Dentro de dicha extensión, se utilizará el subcampo `directoryName` para incluir un conjunto de atributos definidos por la FNMT-RCM, que incorporan información sobre el *Titular* en cuestión, siguiendo el siguiente criterio:

| Tipo Certificado | Información   | Atributo FNMT     | OID (*)               |
|------------------|---|-------------------|-----------------------|
| Sede electrónica | Descripción del componente  | fnmtDescripcion   | 1.3.6.1.4.1.5734.1.8  |
|                  | Entidad titular del certificado   | fnmtPropEnt       | 1.3.6.1.4.1.5734.1.14 |
|                  | CIF de la entidad titular del certificado   | fnmtCIF           | 1.3.6.1.4.1.5734.1.15 |
|                  | Nombre custodio de las claves   | fnmtRespNombre    | 1.3.6.1.4.1.5734.1.16 |
|                  | Primer apellido custodio de las claves  | fnmtRespApellido1 | 1.3.6.1.4.1.5734.1.17 |
|                  | Segundo apellido custodio de las claves   | fnmtRespApellido2 | 1.3.6.1.4.1.5734.1.18 |
|                  | NIF custodio de las claves  | fnmtRespNIF       | 1.3.6.1.4.1.5734.1.19 |
|                  | dNSName= Dirección electrónica<br>ó<br>iPAddress=Dirección electrónica basada en IP |                   |                       |

**Tabla 8 Composición del subcampos `directoryName`. Sede electrónica APE**

(\*) `fnmtoid: 1.3.6.1.4.1.5734`: Espacio de numeración asignado a la Fabrica Nacional de Moneda y Timbre – Real Casa de la Moneda por el IANA.

Además se incluirán las extensiones necesarias para poder realizar el proceso de identificación de la sede a través de las direcciones electrónicas de acceso consignadas en el *Certificado*

|                      |  |
|----------------------|--|
| <b>4.extKeyUsage</b> | Autenticación de servidor: 1.3.6.1.5.5.7.3.1 |
|----------------------|--|

**Tabla 9 Extensión `extKeyUsage`. Sede Electrónica APE**

3. Generación del *Certificado* conforme al Perfil del *Certificado* de identificación de *sede electrónica*

El formato del *Certificado* para la identificación de sedes electrónicas expedido por la FNMT-RCM bajo la presente política, en consonancia con la norma UIT-T X.509 versión 3 y de acuerdo con la normativa legalmente aplicable en materia de *Certificados Reconocidos*, contiene los siguientes campos:

| CAMPO                               | CONTENIDO  | OBSERVACIONES   |
|-------------------------------------|--|---|
| <b>1. Versión</b>                   | V3   |   |
| <b>2. Serial Number</b>             | Secuencial   | [RFC3280]: the serial number <b>MUST</b> be a positive integer, not longer than 20 octets ( $1 < SN < 2^{159}$ ). Processing components <b>MUST</b> be able to interpret such long numbers.   |
| <b>3. Signature Algorithm</b>       | Sha1withRsaEncryption<br>Sha256withRsaEncryption   | OID: 1.2.840.113549.1.1.5<br>OID: 1.2.840.113549.1.1.11<br><br>Norma PKCS#1 v2.1 y RFC 3447.  |
| <b>4. Issuer Distinguished Name</b> | OU= AC APE<br>O=FNMT-RCM<br>C=ES   | Todos los <i>DirectoryString</i> codificados en UTF8. El atributo "C" ( <i>countryName</i> ) se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements", en <i>PrintableString</i> .<br>[ETSI-CPN]: the issuer name <b>MUST</b> contain the <i>countryName</i> and the <i>organizationName</i> attributes.   |
| <b>5. Validez</b>                   | 48 meses   | 48 meses a partir del momento de la emisión.  |
| <b>6. Subject</b>                   | CN= XXXXXX<br>OU= "Organizacion_Entidad"<br>OU=AC APE<br>O=FNMT-RCM<br>C=ES  | Todos los <i>DirectoryString</i> codificados en UTF8. El atributo "C" ( <i>countryName</i> ) se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements", en <i>PrintableString</i> .<br><br>El atributo CN contiene el nombre del servidor. El nombre podrá ser un nombre de host o una dirección IPy debería corresponderse con la forma de invocación del servicio:<br>CN=www.nombrehost.es<br>ó<br>CN=111.222.121.212 |
| <b>7. Subject Public Key Info</b>   | Algoritmo: RSA Encryption<br>Longitud: 2048 bits   |   |
| <b>8. Subject Key Identifier</b>    | Función hash SHA-1 sobre la clave pública del sujeto.  | RFC 3280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo <i>subjectPublicKey</i> del sujeto (excluyendo etiqueta, longitud y número de bits no usados).   |
| <b>9. Authority Key Identifier</b>  | Función hash SHA-1 sobre la clave pública de la AC emisora (AC subordinada). NO SE incluye la identificación del certificado de la AC emisora (en este caso, DN de la AC Raíz, | RFC 3280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo <i>subjectPublicKey</i> de la AC emisora (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo <i>Subject Key Identifier</i> de la AC emisora (AC subordinada).  |

| CAMPO                           |                                  | CONTENIDO  | OBSERVACIONES  |
|---------------------------------|----------------------------------|--|--|
|                                 |                                  | número de serie de la AC Subordinada).   |  |
| <b>10. KeyUsage</b>             |                                  |  |  |
|                                 | <b>Digital Signature</b>         | 1  | <p>Si es necesario que tenga la misma operatividad que FNMT Clase 2 CA, tendrá La Norma ETSI TS 102 280 V1.1.1 (2004-03) – “X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons” recomienda el uso exclusivo del bit de no repudio para certificados destinados a validar el compromiso con el contenido firmado, tales como firmas electrónicas sobre transacciones o acuerdos.</p> <p>En el <i>Technical Corrigendum 3</i> de la ITU-T X509 de 04/2004, el bit de no-repudio es renombrado a <b>contentCommitment</b>. En este documento se recoge lo siguiente:</p> <p><i>“Note that it is not incorrect to refer to this keyUsage bit using the identifier nonRepudiation. However, the use of this identifier has been deprecated. Regardless of the identifier used, the semantics of this bit are as specified in this Directory Specification.”</i></p> |
|                                 | <b>Non Repudiation</b>           | 0  |  |
|                                 | <b>Key Encipherment</b>          | 1  |  |
|                                 | <b>Data Encipherment</b>         | 0  |  |
|                                 | <b>Key Agreement</b>             | 0  |  |
|                                 | <b>Key Certificate Signatura</b> | 0  |  |
|                                 | <b>CRL Signature</b>             | 0  |  |
| <b>11. extKeyUsage</b>          |                                  | Autenticación de servidor:<br>1.3.6.1.5.5.7.3.1  | <p>[RFC3280]: Certificate using applications MAY require that a particular purpose be indicated in order for the certificate to be acceptable to that application. If a CA includes extended key usages to satisfy such applications, but does not wish to restrict usages of the key, the CA can include the special keyPurposeID anyExtendedKeyUsage. If the anyExtendedKeyUsage key purpose is present, the extension SHOULD NOT be critical.</p>   |
| <b>12. Certificate Policies</b> |                                  |  |  |
|                                 | <b>Policy Identifier</b>         | OID asociado a la DPC o PC de certificado de firma de Sello electrónico.<br>(fnmtPolCertSedeElect)<br>1.3.6.1.4.1.5734.3.12                      | <p>RFC 3739 obliga la existencia de al menos un valor.</p> <p>La Ley de Firma Electrónica dice para los certificados reconocidos: “La identificación del prestador de servicios de certificación que expide el certificado y su domicilio”. Se incluirá en la DPC.</p> <p><i>In an end entity certificate, these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used.</i></p>  |
|                                 | <b>URL CPS</b>                   | http://www.cert.fnmt.es/dpcs/  |  |
|                                 | <b>Notice Reference</b>          | Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM ( C/Jorge Juan 106-28009-Madrid-España) |  |
| <b>13. qcStatements</b>         |                                  | Id-etsi-qcs-QcCompliance<br>id-etsi-qcs-QcLimitValue : 0€<br>Id-etsi-qcs-<br>QcRetentionPeriod: 15 años  | <p>ETSI TS 101 862 define la inclusión de las siguientes declaraciones para certificados cualificados:</p> <p>1.- <b>id-etsi-qcs-QcCompliance</b> – Indica que el certificado es cualificado. Solo si no</p>   |

| CAMPO                                     | CONTENIDO  | OBSERVACIONES  |                          |
|---|--|--|--------------------------|
|   |  | <p>está explícito en las políticas indicadas en la extensión correspondiente.</p> <p>2.- <b>id-etsi-qcs-QcLimitValue</b> – Opcional. Indica el valor límite para transacciones.</p> <p>3.- <b>id-etsi-qcs-QcRetentionPeriod</b> – Opcional. Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otra información relevante. En este caso la Ley obliga: <i>"Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo."</i>. Dado que la FNMT va a conservar la información de manera indefinida, y que la norma no establece un valor para indicar un periodo indefinido, no se incluirá este QC y se indicará en la DPC.</p> <p>4.- <b>id-etsi-qcs-QcSSCD</b> – Opcional. Indica que la clave privada correspondiente al certificado está almacenada en un dispositivo seguro de creación de firma de acuerdo al Anexo III de la Directiva del Parlamento Europeo 1999/93/EC, sobre un framework comunitario para firmas electrónicas.</p> |                          |
| <p><b>14. Subject Alternate Names</b></p> | <p>Dirección del directorio:<br/>OID.1.3.6.1.4.1.5734.1.8=fnmtDescripción<br/>OID.1.3.6.1.4.1.5734.1.14=fnmtPropEnt<br/>OID.1.3.6.1.4.1.5734.1.15=fnmtCIF<br/>OID.1.3.6.1.4.1.5734.1.16=fnmtRespNombre<br/>OID.1.3.6.1.4.1.5734.1.17=fnmtRespApellido1<br/>OID.1.3.6.1.4.1.5734.1.18=fnmtRespApellido2<br/>OID.1.3.6.1.4.1.5734.1.19=fnmtRespNIF</p> <p>dNSName= Nombre de Host<br/>ó<br/>iPAddress=Dirección IP</p> | <p>Descripción</p>   | <p>fnmtDescripción</p>   |
|   |  | <p>Entidad propietaria</p>   | <p>fnmtPropEnt</p>       |
|   |  | <p>CIF</p>   | <p>fnmtCIF</p>           |
|   |  | <p>Nombre Responsable</p>  | <p>fnmtRespNombre</p>    |
|   |  | <p>Apellido1 Responsable</p>   | <p>fnmtRespApellido1</p> |
|   |  | <p>Apellido2 Responsable</p>   | <p>fnmtRespApellido2</p> |
|   |  | <p>NIF Responsable</p>   | <p>fnmtRespNIF</p>       |
| <p><b>15. Basic Constraints</b></p>       |  | <p>[RFC 3280] This extension MAY appear as a critical or non-critical extension in end entity certificates.</p>  |                          |
|   | <p><b>Subject Type</b></p>   | <p>Entidad Final</p>   |                          |
| <p><b>16. CRLDistributionPoints</b></p>   | <p>LDAP:<br/>ldap://ldapape.cert.fnmt.es:<br/>puerto/CN=CRLnnn,OU= AC<br/>APE, O=FNMT, C=ES</p>  |  |                          |

| CAMPO                        | CONTENIDO  | OBSERVACIONES   |
|------------------------------|--|---|
|                              | ?certificateRevocationList; binary?base<br>?objectclass=cRLDistributionPoint<br>HTTP:<br>http://www.cert.fnmt.es/crlsape/CRLnnn.crl  |   |
| 17. Auth. Information Access | OCSP:<br><a href="http://ocspape.cert.fnmt.es/ocspape/OcspResponder">http://ocspape.cert.fnmt.es/ocspape/OcspResponder</a><br>CA:<br><a href="http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt">http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt</a> | Contendrá información de localización del OCSP Responder. URL resuelta a diferentes servidores. Ley de Firma Electrónica: " <b>Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro</b> ". |
| 18. netscapeCertType         | sSLSERVER,sMIME  | Tipo de certificado según Netscape  |
| 19. fnmtTipoCertificado      | 1.3.6.1.4.1.5734.1.33: "Sede Electrónica"  | Tipo de certificado para Sede Electrónica   |
| 20. AuthorityKeyIdentifier   | 2.5.29.35: Identificador de clave del prestador de servicios de certificación  |   |

Tabla 10 Perfil del Certificado de Sede Electrónica - APE

#### 11.2.2.10. Publicación del Certificado de identificación de sede electrónica

173. Una vez generado el *Certificado* por parte de la FNMT-RCM como *Prestador de Servicios de Certificación*, se publicará en el *Directorio*, concretamente en la entrada correspondiente al nombre distintivo de la dirección electrónica, tal como se ha definido en el apartado "*Emisión del Certificado*" de este documento.

#### 11.2.2.11. Descarga e instalación del Certificado de identificación de sede electrónica

174. Realizados los trámites anteriores y generado el *Certificado de sede electrónica*, la FNMT-RCM pondrá a disposición del responsable de la *Oficina de Registro* correspondiente un mecanismo de descarga del *Certificado*, en la dirección de titularidad de la Administración u organismo, a través del siguiente enlace:

<http://ape.cert.fnmt.es/appsUsuario/descargameh/descargaCertInicio.jsp>

175. A tal efecto se accederá a la opción "Descarga de su Certificado".

176. En este proceso guiado se le pedirá al responsable de la *Oficina de Registro* del ámbito del *Titular* que introduzca el CIF del órgano, organismo o entidad pública con el que realizó el proceso de presolicitud así como el código de solicitud devuelto por el sistema al finalizar dicho proceso. Si el *Certificado* no ha sido aún generado por cualquier motivo, se le indicará este hecho en el momento que intente su descarga.

177. Si el *Certificado* ya ha sido puesto a disposición del *Titular*, aquél será introducido directamente en el soporte en el que se generaron las *Claves* durante el proceso de Presolicitud.

*11.2.2.12. Período de validez del Certificado de identificación de sede electrónica*

178. El periodo de validez de los *Certificados* de identificación de *sede electrónica* emitidos por la FNMT-RCM será de cuatro (4) años contados a partir del momento de la emisión del *Certificado*, siempre y cuando no se extinga su vigencia por las causas y procedimientos expuestos en el apartado “Extinción de la vigencia del Certificado” de la *Declaración General de Prácticas de Certificación* o lo dispuesto, en su caso, en la *Ley de Emisión* correspondiente.

*11.2.2.13. Revocación del Certificado de identificación de sede electrónica*

179. La revocación de *Certificados* consiste en la cancelación de la garantía de identidad, autenticidad u otras propiedades del *Titular* y sus representantes y su correspondencia con la clave pública asociada. Implica, además de su extinción, la finalización de la relación y régimen de uso del *Certificado* con la FNMT-RCM.

180. Estarán legitimados para solicitar la revocación de un *Certificado* de identificación de *sede electrónica*, en base a la inexactitud de datos, variación de los mismos o cualquier otra causa a valorar por los *Titulares*:

- El órgano directivo, organismo o entidad pública *Titular* del *Certificado* o persona en quien delegue,
- La *Oficina de Registro*, —a través de su responsable— que esté designada a tal efecto, por la Administración, organismo o entidad vinculada o dependiente *Titular* del *Certificado* a revocar, cuando detecte que alguno de los datos consignados en el *Certificado*
  - es incorrecto, inexacto o haya variado respecto a lo consignado en el *Certificado* o
  - la *persona física*, firmante/custodio, del *Certificado* no se corresponda con el responsable máximo o designado para la gestión y administración de la dirección electrónica consignada en el *Certificado* objeto de la revocación

181. siempre en el marco de los términos y condiciones acerca de la Revocación de *Certificados* en la *Declaración General de Prácticas de Certificación*.

182. La revocación, también podrá llevarse a cabo en los supuestos previstos en la Declaración General de Prácticas de Certificación, respecto de la persona física responsable o designada por el *Titular*.

*11.2.2.14. Procedimiento por el que se obtienen los datos personales del Solicitante de la revocación, se confirma su identidad y la capacidad para realizar dicha solicitud y la formalización de la misma.*

183. Serán causas admitidas para la revocación de un *Certificado* las expuestas en la *Declaración General de Prácticas de Certificación* de la FNMT-RCM, si bien la *Ley de Emisión* de aplicación podrá establecer, adicionalmente, otras causas de revocación o en su caso suspensión y/o su cancelación.

184. En todo caso FNMT-RCM, presumirá la competencia y capacidad del solicitante cuando se trate del responsable de la *Oficina de Registro* correspondiente. No obstante, se señalan, para su cumplimiento en su caso, las siguientes actuaciones:

1. Personación del *Solicitante* ante las *Oficinas de Registro*

Para revocar el *Certificado*, el *Solicitante* con capacidad y competencia suficientes, se personará ante una *Oficina de Registro* designada a tal efecto por el órgano, organismo o entidad *Titular del Certificado* a revocar o se realizará directamente por el responsable de la *Oficina de Registro*.

2. Comparecencia y documentación

El *Solicitante* aportará los datos que se le requieran y que acrediten:

- su identidad personal,
- su condición de personal al servicio del órgano, organismo o entidad de la Administración pública *Titular del Certificado* y *Titular* de la dirección electrónica a través de la que se accede a la *sede electrónica* objeto del *Certificado* o su condición de responsable de la *Oficina de Registro*.
- su condición de persona designada para la gestión de la dirección electrónica a través de la que se accede a la *sede electrónica* objeto del *Certificado* a revocar o de personal adscrito a la *Oficina de Registro* designada a tal efecto por el organismo o entidad *Titular del Certificado* a revocar

FNMT-RCM estará y admitirá, en todo caso, la función e informe que realice la *Oficina de Registro* designada por la Administración. En el caso de que no se acrediten los puntos anteriores, la *Oficina de Registro* no procederá con la solicitud de revocación del *Certificado*

3. Envío de la solicitud de revocación a la FNMT-RCM y tramitación

Sin que existan causas notorias de falta de competencia del responsable de la *Oficina de Registro* y/o una vez confirmada la identidad del *Solicitante*, vigencia de las condiciones exigidas a éste y suscrito el documento de solicitud de revocación, la *Oficina de Registro* procederá a validar los datos y a enviarlos a la FNMT-RCM para la revocación efectiva del *Certificado*.

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

Dicho envío sólo se producirá si la *Oficina de Registro* tiene potestad para actuar como tal en nombre del órgano, organismo o entidad de la Administración Pública *Titular del Certificado* y si éste es titular de la dirección electrónica a través de la que se accede a la *sede electrónica* objeto del *Certificado*

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.

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

11.2.2.15. *Suspensión del Certificado de identificación de sede electrónica*

185. La suspensión de *Certificados* deja sin efectos el *Certificado* durante un período de tiempo y en unas condiciones determinadas.
186. La suspensión de los *Certificados* será considerada una revocación temporal de la vigencia del *Certificado* por lo que los procedimientos y entidades habilitadas para la solicitud y tramitación de la *revocación* del *Certificado* son de aplicación en el caso de la *suspensión*. Adicionalmente se tendrán en cuenta para la admisión de las *suspensión* las causas admitidas expuestas en el apartado “Causas de suspensión de *Certificados*” de la *Declaración General de Prácticas de Certificación*.
187. La FNMT-RCM procederá a suspender el *Certificado* de forma provisional durante un plazo de noventa (90) días, plazo tras el cual se extinguirá el *Certificado* mediante su revocación directa por parte del *Prestador de Servicios de Certificación* de la FNMT-RCM, salvo que se hubiera levantado la suspensión. No obstante lo anterior, el plazo previsto para la suspensión del *Certificado* podrá verse alterado en función de los procedimientos judiciales o administrativos que lo pudieran afectar.
188. Si durante el plazo de suspensión del *Certificado* éste caducara o se solicitara su revocación, se producirán las mismas consecuencias que para los *Certificados* no suspendidos que se vieran afectados por supuestos de caducidad o de revocación.

11.2.2.16. *Cancelación de la suspensión del Certificado de identificación de sede electrónica*

189. Podrán solicitar la Cancelación de la suspensión de los *Certificados* emitidos por la FNMT-RCM los *Titulares*, a través de sus representantes, siempre que dicha solicitud se efectúe durante los noventa (90) días siguientes a su suspensión.
190. La FNMT-RCM considerará que se actúa con capacidad bastante, a los efectos de este apartado, cuando la solicitud se realice a través del responsable de la *Oficina de Registro* correspondiente.
191. Sin perjuicio de lo señalado en el párrafo anterior, y en el caso de actuación a través de otros representantes del *Titular* del *Certificado* distintos al responsable de la *Oficina de Registro*, la comparecencia y/o acto de petición de cancelación se llevará a través y/o ante la *Oficina de Registro* designada por el organismo o entidad a la que pertenece el *Titular* y según el criterio vigente de la FNMT-RCM, al objeto de que ésta sea homogénea en todos los casos.
192. En este acto, el *solicitante representante del Titular* del *Certificado*, con competencia suficiente, objeto de la petición, aportará los datos que se le requieran y acreditará su identidad personal, siguiendo el procedimiento descrito anteriormente para la solicitud de emisión del *Certificado* de identificación de *sede electrónica*. FNMT-RCM aceptará el informe de acreditación que pudiera emitir la *Oficina de Registro* considerando lo establecido en el artículo 13.1, in fine, de la Ley 59/2003, de 19 de diciembre, de firma electrónica.
193. Los datos personales del responsable de la *Oficina de Registro* o del representante del *Titular*, una vez validados por la *Oficina de Registro*, se enviarán a la FNMT-RCM mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la



- FNMT-RCM. Los datos personales y su tratamiento quedarán sometidos a la legislación específica
194. Una vez recibidos los datos validados por la *Oficina de Registro* de la petición de levantamiento de suspensión, la FNMT-RCM procederá a retirar este *Certificado* de la *Lista de Revocación*, no efectuándose acción técnica alguna sobre el *Certificado* en cuestión.

#### 11.2.2.17. Comprobación del estado del Certificado de identificación de sede electrónica

195. El *Titular* del *Certificado* y las Administraciones, organismos y entidades *usuarias* pertenecientes a la *Comunidad Electrónica* podrán realizar la comprobación del estado de un *Certificado* en la forma y condiciones que se expresan en los apartados “Procedimientos de consulta del estado de los *Certificados*” y “Servicio de validación de *Certificados* mediante *OCSF*” de la *Declaración General de Prácticas de Certificación*, sin perjuicio de lo que pueda establecerse mediante acuerdo o convenio de la FNMT-RCM, el *Titular* del *Certificado* y, en su caso, los integrantes de la *Comunidad Electrónica*.
196. FNMT-RCM no proporciona servicio de comprobación de *Certificados* de otros *Titulares* salvo en los casos que así se establezca a través de convenios y/o contratos con el correspondiente consentimiento de los miembros integrantes de la *Comunidad Electrónica* o en los términos previstos en la *Ley de Emisión*.
197. En particular, para la difusión y confianza en los sistemas que cuenten con estos *Certificados*, la FNMT-RCM, podrá proporcionar la posibilidad de verificar, por el miembro de la *Comunidad electrónica* o un tercero, que el *Certificado* de identificación de *sede electrónica* es un *Certificado* válido emitido por la FNMT-RCM, así como otras características del mismo.

#### 11.2.3. Exclusiones y requisitos adicionales a ETSI TS 101 456

- De acuerdo con la norma en el apartado 8.2 b), se excluyen las cuestiones definidas en el apartado 7.5 j), k).
  - De acuerdo con la norma en el apartado 8.2 c), se excluyen las cuestiones definidas en el apartado 7.3.5 f). En este tema se estará a lo señalado en el apartado “*Publicación del Certificado*” de este anexo.
  - De acuerdo con la norma en el apartado 8.2 d), se excluyen las cuestiones definidas en el apartado 7.3.6 k). En este tema se estará a lo señalado en el apartado “*Comprobación del estado del Certificado*” de este anexo.
198. Respecto aquellos *Certificados Reconocidos* que usen Dispositivos Seguros de creación de firma, seguirán lo señalado en el apartado “Soporte del Certificado” del documento *Declaración General de Prácticas de Certificación* de la FNMT-RCM, así como a lo expuesto en los apartados sobre “Ciclo de vida del certificado” del citado documento. Todo ello sin perjuicio de la calificación del dispositivo como medio equivalente de conformidad con la Ley 11/2007, de 22 de junio, LAECSP.



#### **11.2.4. Modelos de formulario**

199. Los modelos de formularios que se deben cumplimentar para realizar las operaciones descritas para la gestión del ciclo de vida de los *Certificados* para personal al servicio de la Administración Pública se ponen a disposición en <http://www.ceres.fnmt.es>

**12. CERTIFICADOS EMITIDOS PARA LA ACTUACIÓN ADMINISTRATIVA AUTOMATIZADA DE LA ADMINISTRACIÓN PÚBLICA, ORGANISMOS Y ENTIDADES PÚBLICAS VINCULADAS O DEPENDIENTES**

**12.1. POLÍTICA DE CERTIFICACIÓN DE LOS CERTIFICADOS EMITIDOS PARA LA ACTUACIÓN ADMINISTRATIVA AUTOMATIZADA DE LA ADMINISTRACIÓN PÚBLICA, ORGANISMOS Y ENTIDADES PÚBLICAS VINCULADAS O DEPENDIENTES**

**12.1.1. Identificación**

200. Para la identificación y autenticación del ejercicio de competencias administrativas en procesos automatizados, FNMT-RCM desarrolla este servicio de certificación electrónica, sobre la base de su consideración del concepto legal previsto en la Ley 11/2007, de 22 de junio de Acceso Electrónico de los ciudadanos a los Servicios Públicos correspondiente al art. 18. a): Sello electrónico de la Administración Pública, y demás órganos y entidades vinculadas o dependientes, basado en un *Certificado* electrónico en los términos previstos en la Ley 59/2003, de 19 de diciembre, de firma electrónica.
201. La presente *Política de Certificación* Particular de la FNMT-RCM para la expedición de *Certificados* para la actuación administrativa automatizada de la Administración Pública, organismos y entidades públicas vinculadas o dependientes tiene la siguiente identificación:

|                  |  |
|------------------|--|
| Nombre           | <i>Política de Certificación de Certificados</i> para la actuación administrativa automatizada de la Administración Pública, organismos y entidades públicas vinculadas o dependientes |
| Referencia/OID   | 1.3.6.1.4.1.5734.3.13  |
| Versión          | 1.0  |
| Fecha de Emisión | 1 de Agosto de 2007  |
| Localización     | <a href="http://www.cert.fnmt.es/dpcs/">http://www.cert.fnmt.es/dpcs/</a>  |
| DPC relacionada  | Declaración General de Prácticas de Certificación de la FNMT-RCM<br>Localización:<br><a href="http://www.cert.fnmt.es/dpcs/">http://www.cert.fnmt.es/dpcs/</a>                         |

**Tabla 11 Identificación Política Certificación – Actuación Automatizada APE**



### 12.1.2. Tipología del Certificado para la actuación administrativa automatizada de la Administración Pública, organismos y entidades públicas vinculadas o dependientes

202. Los “*Certificados* para la actuación administrativa automatizada” con el concepto de sello electrónico, son aquellos *certificados* expedidos por la FNMT-RCM bajo esta política de certificación y que vinculan unos *Datos de verificación de Firma* a:
- los datos identificativos y de autenticación de determinada Administración, organismo o entidad y sus respectivas unidades organizativas (unidad que se realiza la actuación administrativa automatizada: área, sección, departamento y
  - la *persona física* responsable de la correspondiente *Oficina de Registro* y/o representante de la Administración, organismo o entidad *Titular* del *Certificado* y, en su caso, el personal en quien se delegue a efectos de la actuación administrativa automatizada.
203. La *persona física* actúa como firmante de las actuaciones administrativas automatizadas y custodia de la clave y, por tanto, es la que tiene el control sobre dicho *Certificado* y los *Datos de creación y verificación de firma* y es responsable de su custodia de forma diligente, sin perjuicio, de las delegaciones que puedan producirse, de acuerdo con el régimen legal correspondiente.
204. FNMT-RCM emitirá estos *Certificados* de sello electrónico siempre que sea solicitado por los miembros de la *Comunidad Electrónica* del ámbito de la Ley 11/2007, de 22 de junio, LAECSP para las diversas relaciones que puedan producirse en el ámbito de la actuación administrativa automatizada y no se encuentre prohibido o limitado su utilización por la legislación aplicable.
205. FNMT-RCM no será responsable de las actuaciones realizadas con este tipo de *Certificados* cuando se produzcan abuso de facultades o insuficiencia de las mismas y/o cuando se produzcan decisiones del miembro de la *Comunidad Electrónica Titular* del *Certificado* que afecten a la vigencia de las facultades de éste, por lo que cualquier modificación, revocación o restricción en el *Certificado* y su uso no será oponible a la FNMT-RCM salvo que sea fehacientemente notificada.
206. Del mismo modo, FNMT-RCM no será responsable de las actuaciones realizadas con este tipo de *Certificados* cuando los datos identificativos y de autenticación de la unidad organizativa de la entidad de la administración consignada en el *Certificado* no se corresponda con una unidad dependiente de dicha entidad de la administración.
207. La FNMT-RCM, como *Prestador de Servicios de Certificación* se reserva el derecho de no expedir o revocar este tipo de *Certificados*, con exoneración de responsabilidad a estos efectos, si el usuario del *Certificado* y/o el *firmante/custodio* y/o unidad organizativa (realiza la actuación administrativa automatizada) en la que se emplea tal *Certificado*, carece de competencia, no hace un uso adecuado del mismo, conculcando derechos de explotación, de propiedad industrial o intelectual de terceros sobre las aplicaciones y actuaciones realizadas o cualquier legislación vigente.
208. La FNMT-RCM, se mantendrá indemne por parte del *Titular* y las personas responsables o representantes del mismo, respecto de cuestiones de titularidad de derechos y/o los vicios o





- defectos de los equipos, aplicaciones o sistemas que incumplan lo previsto en este apartado y que tenga relación con el *Certificado*, quedando exonerada de cualquier reclamación o reivindicación por el uso inadecuado de tales *Certificados*.
209. Este *Certificado* se emite por la FNMT-RCM por cuenta de la Administración Pública correspondiente a la que la FNMT-RCM presta los servicios técnicos, administrativos y de seguridad necesarios como *Prestador de Servicios de Certificación*.
210. El *Certificado* de sello electrónico para la actuación administrativa automatizada de la Administración Pública es desarrollado por la FNMT-RCM mediante una infraestructura PKI específica, basada en actuaciones de identificación, autenticación y registro realizadas por la red de *Oficinas de Registro* designadas por el órgano, organismo o entidad de la Administración Pública de la que depende la unidad organizativa que realiza la actuación administrativa automatizada consignada en el *Certificado*.
211. 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.
212. Este *Certificado*, es emitido con el perfil técnico correspondiente a los *Certificados Reconocidos o sistemas de firma electrónica* equivalentes según lo dispuesto en la Ley 59/2003, de 19 de diciembre, de firma electrónica con base en los criterios establecidos en esta ley, así como, en la normativa especial de la FNMT-RCM y en la normativa técnica EESSI, concretamente ETSI TS 101 456 - “Policy requirements for certification authorities issuing qualified certificates” y ETSI TS 101 862 – “Qualified Certificate Profile”, tanto en lo referente al *Prestador de Servicios de Certificación* como a la generación de los *Datos de Verificación de Firma* y al contenido del propio *Certificado*.

### 12.1.3. Gestión de la Política de Certificación

213. La FNMT-RCM dispone específicamente de una *Política de Certificación* efectiva en relación con los *Certificados* emitidos para la actuación administrativa automatizada de la Administración General del Estado y, en su caso, otras Administraciones Públicas del ámbito de aplicación de la Ley 11/2007, de 22 de junio, LAECSP, y, en particular, declara que:
- La FNMT-RCM tiene capacidad para especificar, revisar, y aprobar la *Política de Certificación* de estos *Certificados Reconocidos*, a través de su Dirección General y demás órganos directivos de la misma.
  - La FNMT-RCM dispone de unas *Prácticas de Certificación Particulares* (apartado 12.2, siguiente) en la que se detallan las prácticas de certificación empleadas para la expedición de *Certificados* conformes a la *Política de Certificación* aquí expuesta para este tipo de *Certificado*.
  - La FNMT-RCM dispone, dentro de las competencias de la Dirección general y demás órganos directivos de la misma, 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*.



- La FNMT-RCM realiza análisis de riesgos para evaluar las amenazas del sistema y proponer las medidas de seguridad adecuadas (salvaguardas) para todas las áreas implicadas.
- Las *de Prácticas de Certificación Particulares* se ponen a disposición del público mediante el URL:

<http://www.cert.fnmt.es/dpcs/>

- La *Ley de Emisión* de cada tipo o grupo de *Certificados*, caso de establecerse, podrá ser de acceso restringido total o parcialmente por razones de seguridad al tratarse de un sistema de certificación de uso en el ámbito de las Administraciones públicas y personal correspondiente.
- La *Política de Certificación* de *Certificados* emitidos para la actuación administrativa automatizada se pone a disposición del público mediante el URL:

<http://www.cert.fnmt.es/dpcs/>

- Esta *Política de Certificación* recoge las obligaciones y responsabilidades generales de las partes implicadas en la emisión y uso de los *Certificados* para la actuación administrativa automatizada de la Administración y emitidos por la FNMT-RCM bajo a esta *Política de Certificación*, sin perjuicio de las especialidades que pudieran existir en el contrato o convenio correspondiente o si procede en la *Ley de Emisión*.
- Se dispone de un *OID* específico para identificar la *Política de Certificación* aquí desarrollada, siendo el *OID* asignado en el marco de la numeración de la FNMT-RCM: 1.3.6.1.4.1.5734.3.13

214. La *Política de Certificación* de la FNMT-RCM para el presente tipo de *Certificado* se define en base al documento ETSI TS 101 456, en concreto en su apartado 8, cumpliéndose los requisitos expuestos en los apartados 6 y 7 con las exclusiones señaladas en el apartado 8.2 (que se exponen en el apartado ***Exclusiones y Requisitos Adicionales a ETSI TS 101456*** de la presente *Política de Certificación*). En caso de discrepancia entre este documento y la referida norma, prevalecerá este documento.

#### 12.1.4. Comunidad y ámbito de aplicación

215. La presente *Política de Certificación* es de aplicación en la expedición de *Certificados* electrónicos idóneos para operar como sello electrónico, teniendo las siguientes características:

- a) Son expedidos como *Certificados Reconocidos* o de efecto equivalente a los denominados *Certificados* reconocidos con base en los criterios establecidos para tal en la Ley 59/2003, de 19 de diciembre, de firma electrónica y en la normativa técnica EESSI ETSI TS 101 862 – “Qualified Certificate Profile”.
- b) Son expedidos por la FNMT-RCM como *Prestador de Servicios de Certificación* cumpliendo con los criterios establecidos en la Ley 59/2003, de 19 de diciembre, de firma electrónica, normativa especial de la FNMT-RCM y en la normativa técnica

EESSI, concretamente ETSI TS 101 456 - “Policy requirements for certification authorities issuing qualified certificates”.

- c) Los *Certificados* emitidos bajo esta *Política de Certificación* son expedidos para la Administración Pública, organismos y entidades públicas vinculadas o dependientes y que forman parte de la *Comunidad Electrónica*, tal y como se define en el apartado *Definiciones* de la *Declaración General de Prácticas de Certificación de la FNMT-RCM*, y con objeto exclusivo de realizar la identificación y autenticación del ejercicio de la competencia en la actuación administrativa automatizada, mediante Sello electrónico.
- d) En el marco de esta *Política de Certificación*, el *Solicitante* del *Certificado* se corresponde con el responsable de la *Oficina de Registro* y/o el representante del *Titular* o persona en quien delegue la unidad organizativa que realiza la actuación administrativa automatizada y a consignar en el *Certificado* y que presta sus servicios en una Administración Pública del Reino de España, bien sea un órgano, organismo, entidad de la Administración general, Autonómica o Local del Estado bajo la que se enmarca dicha unidad organizativa.
- e) Los *Certificados* emitidos bajo esta *Política de Certificación* incluyen el número de identificación fiscal y la denominación correspondiente de la entidad, órgano o unidad de la Administración Pública *Titular* del *Certificado*.
- f) Los *Certificados* emitidos bajo esta *Política de Certificación* se consideran válidos como parte integrante de sistemas de firma electrónica para la actuación administrativa automatizada por parte de la Administración Pública. En concreto, estos *Certificados* reúnen los requisitos establecidos por la legislación de firma electrónica y son válidos para la creación de sellos electrónicos de Administración Pública, órgano, organismo o entidad de derecho público. Por tanto, los *Certificados* emitidos bajo esta política se consideran adecuados para el desarrollo de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP), a los efectos de identificación y autenticación de la competencia en la actuación administrativa automatizada de la Administración Pública.

216. 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 los *Titulares*. Todo ello, sin modificación legal o variación respecto de la actuación que vienen realizando estos *Titulares* en los soportes tradicionales en papel u otros.

#### 12.1.5. Responsabilidad y obligaciones de las partes

217. Serán partes a los efectos de este apartado los siguientes sujetos:

- Los *Titulares*: la Administración, organismos, entidades públicas representadas a través de los diferentes órganos competentes.
- Los firmantes/custodios de los *Certificados* y de los *Datos de Creación de Firma*: el personal al servicio de las Administraciones, organismos y entidades públicas que realizan la solicitud del *Certificado* y/o el responsable de la *Oficina de Registro*

correspondiente, consignados en el *Certificado* y que por tanto toman el papel de firmante/s y custodio/s de los Datos de Creación de Firma.

- FNMT-RCM, en cuanto Prestador de Servicios de Certificación
- En su caso, resto de *Comunidad Electrónica* y terceros

218. El régimen de derechos y obligaciones de las Administraciones, organismos, entidades públicas y la FNMT-RCM se regirá mediante el correspondiente acuerdo o convenio regulador de los servicios de certificación. En estos acuerdos o convenios podrá establecerse la *Ley de Emisión* de estos *Certificados*.

219. Con carácter general y de forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la *Declaración General de Prácticas de Certificación*, la Administración, organismos, entidades públicas *Titulares*, representadas a través de los diferentes órganos competentes y la *Oficina de Registro* que actúan para la solicitud de emisión de este tipo de *Certificados* a la FNMT-RCM tiene la obligación de:

- No realizar registros o tramitar solicitudes de *Certificados* para la actuación administrativa automatizada emitidos bajo esta política, por parte de personal que preste sus servicios en una entidad diferente a la que representa como *Oficina de Registro*.
- No realizar registros o tramitar solicitudes de *Certificados* emitidos bajo esta política y cuya titularidad, referida al órgano de la administración, se corresponda con una entidad de la administración pública sobre la que no tenga potestades o no tenga competencias para actuar como *Oficina de Registro*.
- No realizar registros o tramitar solicitudes de *Certificados*, emitidos bajo esta política, para una unidad organizativa que no sea dependiente del órgano de la administración *Titular del Certificado*
- No realizar registros o tramitar solicitudes de *Certificados* emitidos bajo esta política y cuya titularidad, referida al firmante y custodio de los *datos de creación de firma*, e identidad de la persona solicitante no se corresponda con la *persona física* que sea el máximo responsable de la unidad organizativa a consignar en el *Certificado*, salvo que se trate del responsable de la *Oficina de Registro*.
- Comprobar fehacientemente los datos identificativos del *Solicitante*, representante del *Titular del Certificado*, y verificar su pertenencia a la unidad organizativa como máximo responsable de ésta.
- Revocar el *Certificado* emitido bajo esta política cuando alguno de los datos referidos a los *Titulares* o firmantes/custodios del *Certificado*
  - sea incorrecto o inexacto o
  - la *persona física* (firmante/custodio) representante del *Titular del Certificado*, no sea un responsable con capacidad suficiente de la unidad organizativa consignada en él
  - la denominación de la unidad organizativa consignada en el *Certificado* sea inexacta o no se corresponda con una unidad operativa o

- No utilizar el *Certificado* cuando sean inexactos o incorrectos:
    - alguno de los datos referidos a su condición de responsable con capacidad suficiente de la unidad organizativa consignada en el *Certificado* o
    - los datos de pertenencia al órgano administrativo *Titular* del *Certificado* o
    - cualquier otro dato que refleje o caracterice la relación de éste con la unidad organizativa u órgano de la administración consignado en el *Certificado*
220. Las relaciones de la FNMT-RCM y el firmante/custodio quedarán determinadas principalmente a los efectos del régimen de uso de los *Certificados* a través del documento relativo a las condiciones de utilización o en su caso, contrato de emisión del *Certificado* y por como se tipifique en los acuerdos o convenios o documento de relación entre la FNMT-RCM y el órgano, organismo o entidad pública.
221. El resto de la Comunidad Electrónica y los terceros regularán sus relaciones con la FNMT-RCM a través de la Declaración General de Prácticas de Certificación, y, en su caso, a través de estas Políticas de Certificación y Prácticas de Certificación Particulares. Todo ello, sin perjuicio de lo dispuesto en la normativa sobre firma electrónica y demás normativa que resulte de aplicación.
222. FNMT-RCM no será responsable de la comprobación de la pertenencia de la unidad organizativa a consignar en el *Certificado* al órgano de la administración Titular del *Certificado* ni de la pertenencia del Solicitante a la unidad organizativa como máximo responsable de ésta, correspondiendo esta actividad y responsabilidad de comprobación a la Oficina de Registro. FNMT-RCM considerará representante del órgano, organismo o entidad de la administración Titular del *Certificado*, salvo que sea informada de lo contrario al responsable de la Oficina de Registro correspondiente.
223. FNMT-RCM no será responsable de la utilización de los *Certificados* emitidos bajo esta política cuando los representantes del *Titular* del *Certificado* electrónico realicen actuaciones sin facultades o extralimitándose de las mismas.

#### **12.1.6. Límites de uso de los Certificados para la actuación administrativa automatizada mediante sellos electrónicos**

224. Constituyen límites de uso de este tipo de *Certificados* la creación de sellos electrónicos de Administración Pública, organismo o entidad de derecho público, de conformidad con la Ley 11/2007, de 22 de junio, LAECSP para la identificación y autenticación del ejercicio de la competencia en la actuación administrativa automatizada de la unidad organizativa perteneciente a una Administración, organismo o entidad pública.
225. La FNMT-RCM y la Administración, organismos y entidades podrán fijar en los acuerdos o convenios, o a través del documento de relación correspondiente o, si fuera procedente en la *Ley de Emisión* de estos *Certificados*, otros límites adicionales.
226. Para poder usar los *Certificados* para la actuación administrativa automatizada dentro de los límites señalados y de forma diligente, se deberá previamente formar parte de la *Comunidad Electrónica*, y adquirir la condición de *Entidad Usuaría*.
227. En cualquier caso, si un tercero desea confiar en la firma electrónica realizada con uno de estos *Certificados* (sello para actuaciones automatizadas) sin acceder a los servicios de



comprobación de la vigencia 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*.

228. Además, incluso dentro del ámbito de la *Comunidad Electrónica*, no se podrán emplear este tipo de *Certificados*, por persona o entidad distinta a la FNMT-RCM, para:
- Firmar otro *Certificado* sin autorización previa y expresa de la FNMT-RCM.
  - Usos particulares o privados.
  - Firmar software o componentes.
  - Generar sellos de tiempo para procedimientos de *Fechado electrónico* sin autorización previa y expresa de la FNMT-RCM
  - Prestar servicios, sin autorización previa y expresa de la FNMT-RCM a título gratuito u oneroso, como por ejemplo serían a título enunciativo:
    - Prestar servicios de *OCSP*.
    - Generar *Listas de Revocación*.
  - Y, con carácter general, cualquier uso que se extralimite de los identificados en este apartado.

## 12.2. PRÁCTICAS DE CERTIFICACIÓN PARTICULARES PARA LOS CERTIFICADOS EMITIDOS PARA LA ACTUACIÓN ADMINISTRATIVA AUTOMATIZADA DE LA ADMINISTRACIÓN PÚBLICA, ORGANISMOS Y ENTIDADES PÚBLICAS, VINCULADAS O DEPENDIENTES

229. La FNMT-RCM en su labor como *Prestador de Servicios de Certificación* y para demostrar la necesaria fiabilidad para la prestación de dichos servicios, ha desarrollado una *Declaración de Prácticas de Certificación* cuyo objeto es la información pública sobre las condiciones generales de prestación de los servicios de certificación por parte de la FNMT-RCM en su condición de *Prestador de Servicios de Certificación*.
230. En especial deberá tenerse presente, a efectos interpretativos del presente anexo el apartado “Definiciones” del cuerpo principal de la *Declaración General de Prácticas de Certificación*.
231. El Presente documento trae causa y forma parte integrante de la *Declaración de Prácticas de Certificación* de la FNMT-RCM y define el conjunto de prácticas particulares adoptadas por la FNMT-RCM como *Prestador de Servicios de Certificación* para la gestión del ciclo de vida de los *Certificados para la actuación administrativa automatizada de la Administración Pública, Organismos y entidades públicas vinculadas o dependientes*, expedidos bajo la *Política de Certificación de Certificados para la actuación administrativa automatizada de la Administración Pública, Organismos y entidades públicas vinculadas o dependientes* identificada con el OID 1.3.6.1.4.1.5734.3.13

### 12.2.1. Servicios de Gestión de las Claves de los Usuarios y Titulares

232. La FNMT-RCM bajo ningún concepto genera ni almacena las *Claves Privadas de Titulares y/o representantes*, que son generadas bajo su exclusivo control y cuya custodia están bajo su responsabilidad.

### 12.2.2. Gestión del ciclo de vida de los Certificados

#### 12.2.2.1. Registro de los Titulares

233. Con carácter previo al establecimiento de cualquier relación institucional con los *Titulares*, la FNMT-RCM informa, a través de los medios y direcciones web citadas en estas *Prácticas de Certificación Particulares* y, subsidiariamente, en la *Declaración General de Prácticas de Certificación*, acerca de las condiciones del servicio así como de las obligaciones, garantías y responsabilidades de las partes implicadas en la expedición y uso de los *Certificados* por ella emitidos en su labor como *Prestador de Servicios de Certificación*.

234. La FNMT-RCM, en su actividad como *Prestador de Servicios de Certificación* a través de las *Oficinas de Registro* procede a la identificación de los *solicitantes* y futuros *Titulares* que soliciten *Certificados* para la actuación administrativa automatizada de la Administración Pública, Organismos y entidades públicas vinculadas o dependientes mediante aquellos procedimientos que así se dispongan para ello. FNMT-RCM considerará con competencia al efecto cualquier solicitud que venga realizada por el responsable de la *Oficina de Registro* correspondiente, que se considerará representante del *Titular*.

235. 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, legitimidad y competencia de los representantes, almacenando la información legal exigida 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.

236. La FNMT-RCM, dado que en su actividad como *Prestador de Servicios de Certificación* no genera el par de *Claves* de los *Titulares*, pone todos los mecanismos necesarios durante el proceso de *Solicitud de Certificados* para posibilitar que el responsable de la *Oficina de Registro* y/o el representante del *Titular* se encuentra en posesión de la *Clave Privada* asociada a la *Clave Pública* que se certificará.

#### 12.2.2.2. Procedimiento de solicitud del Certificado para la actuación administrativa automatizada de la Administración Pública

237. A continuación se describe el procedimiento de solicitud del *Certificado* por el que se toma la denominación oficial de las unidades administrativas pertenecientes a la Administración, organismo o entidad pública, que serán los *Titulares* de los *Certificados* para la actuación administrativa automatizada, se toman los datos personales de los representantes de los *Titulares*, que en lo referente a persona física coincide con el *Solicitante*, y tendrá legitimación y competencia suficientes para solicitar y obtener el *Certificado*, se confirma su identidad, vigencia del cargo o empleo y se formaliza, entre el representante del *Titular* y



- la FNMT-RCM el documento de condiciones de utilización o el contrato tipo de emisión, para la posterior emisión de un *Certificado* para la actuación administrativa automatizada de la Administración Pública.
238. Se hace constar que FNMT-RCM, en función de la relación de *Titulares* remitida por la Administración, organismo o entidad pública, considerará, bajo responsabilidad de las correspondientes órganos, organismos y/o entidades que actuarán a través de las *Oficinas de Registro*, que estos *Titulares* cumplen los requisitos establecidos en la presente Declaración y, por tanto, tienen la legitimidad y competencia necesarias para solicitar y obtener el *Certificado* para la actuación administrativa automatizada de la Administración Pública.
239. FNMT-RCM considerará con capacidad y competencia suficientes a los responsables de las *Oficinas de Registro* a efectos de realizar la solicitud del *Certificado*, así como para realizar los trámites que se describen.
240. FNMT-RCM, no tendrá en este tipo de *Certificado* la responsabilidad de comprobar:
- La potestad y competencia de la *Oficina de Registro* para solicitar un *Certificado* para la actuación administrativa automatizada en nombre del órgano de la administración en cuestión y *Titular* del *Certificado*
  - La pertenencia y dependencia de la unidad organizativa a consignar en el *Certificado* al órgano, organismo o entidad de la administración *Titular* del *Certificado*
  - Que el *Solicitante* del *Certificado* para la actuación administrativa automatizada, tenga la condición de personal al servicio de la unidad administrativa perteneciente a la Administración, organismo o entidad pública *Titular* del *Certificado*.
  - La condición del *Solicitante* de responsable de la unidad organizativa a consignar en el *Certificado* perteneciente a la Administración que será *Titular* con legitimidad y competencia suficientes para realizar tal solicitud.
241. Dado que la FNMT-RCM no mantiene relación jurídica funcional, administrativa o laboral con los *Titulares*, más allá del documento de condiciones de utilización o en su caso contrato de emisión, todas las actividades de comprobación serán realizadas por las *Oficinas de Registro* implantadas por el organismo o entidad de la Administración Pública en cuestión y que se corresponde, en cada caso, con el órgano, organismo o entidad *Titular* del *Certificado*.
1. Presolicitud
- El representante del *Titular* que, habitualmente, será el responsable de la *Oficina de Registro* correspondiente, genera las *Claves Pública y Privada* que serán vinculadas al *Certificado*, convirtiéndose posteriormente en datos de *verificación y creación* de firma respectivamente
- El representante y/o responsable de la *Oficina de Registro* compone una solicitud electrónica de *Certificado*, generalmente en formato PKCS#10, y accede al *sitio web* del *Prestador de Servicios de Certificación*, la FNMT-RCM, a través de la dirección
- <https://ape.cert.fnmt.es/PrerregistroSolicitudesComponentesAPE/index.html>
- donde se mostrará un formulario en el que el dicho representante deberá introducir los datos del órgano *Titular* para la cual se emitirá el *Certificado* y del que depende la

unidad organizativa y los datos de la *persona física* propios en su condición de responsable de la custodia diligente de los datos de creación de firma y que por tanto será el firmante/custodio. Adicionalmente el responsable también deberá introducir la solicitud electrónica generada anteriormente.

Como respuesta al envío del formulario la FNMT-RCM asignará e indicará al responsable código de solicitud para su utilización en la *Oficina de Registro* y en el momento de la solicitud del *Certificado*

Con carácter previo el representante y/o responsable de la *Oficina de Registro* y la Administración, que será *Titular*, deberá consultar la *Declaración General de Prácticas de Certificación*, y la presentes *Políticas de Certificación y Prácticas de Certificación Particulares* en la dirección

<http://www.cert.fnmt.es/dpcs/>

con las condiciones de uso y obligaciones para las partes, pudiendo realizar las consultas que estime oportunas sobre el alcance de esta Declaración; todo ello, sin perjuicio de que con posterioridad, el representante del, *Titular* y/o responsable de la *Oficina de Registro*, y FNMT-RCM, deban suscribir el documento de condiciones de utilización o si procede el contrato de emisión. En ningún caso la continuación del procedimiento de presolicitud implicará la conclusión del proceso.

Al realizar esta presolicitud se envía a la FNMT-RCM la *Clave Pública* generada, junto con la correspondiente prueba de posesión de la *Clave Privada*, para la posterior emisión del *Certificado*.

La FNMT-RCM, tras recibir esta información, comprobará mediante la *Clave Pública* del peticionario la posesión y correspondencia de la pareja de *Claves* criptográficas por parte del representante y/o responsable de la *Oficina de Registro*.

Esta información no dará lugar a la generación de un *Certificado* por parte de la FNMT-RCM, en tanto que ésta no reciba firmada por el responsable de la *Oficina de Registro* la solicitud del *Certificado*.

## 2. Confirmación de las identidades y requisitos de las partes

El responsable de la *Oficina de Registro* se identificará a través de su documento nacional de identidad o documento de identificación sustitutorio ante la FNMT-RCM, mediante la correspondiente aplicación de registro y uso de su propio *Certificado* personal. FNMT-RCM presumirá que el responsable de la *Oficina de Registro* se encuentra en el ejercicio de la competencia y con capacidad suficiente para realizar los trámites de obtención de este tipo de *Certificados*.

### a) Personación del Solicitante ante las Oficinas de Registro

En supuestos distintos a la intervención del responsable de la *Oficina de Registro*, a efectos de obtención del *Certificado*, se considerará *Solicitante*, con legitimación y competencia suficientes a la persona designada por el *Titular* del *Certificado*.

Para obtener el *Certificado*, el *solicitante* se personará ante una *Oficina de Registro* designada a tal efecto por el organismo o entidad *Titular* del *Certificado*.

FNMT-RCM considerará al responsable de la *Oficina de Registro* con capacidad y competencia suficiente por el hecho de su designación por parte del *Titular*.

b) Comparecencia y documentación

En supuestos distintos a la intervención del responsable de la *Oficina de Registro*, a efectos de obtención del *Certificado*, el representante del *Titular*, *Solicitante*, comparecerá y aportará los datos que se le requieran y que acrediten, ante la *Oficina de Registro*:

- i. su identidad personal,
- ii. su condición de personal al servicio del órgano, organismo o entidad de la Administración *Titular* del *Certificado* para la actuación administrativa automatizada.
- iii. su condición máximo responsable o persona habilitada o designada con legitimación y competencia suficientes en la unidad organizativa, órgano, organismo o entidad pública a consignar en el *Certificado* y desde la que se realiza la actuación administrativa automatizada.

FNMT-RCM estará y admitirá, en todo caso, a la función e informe que realice la *Oficina de Registro* designada por la Administración. En el caso de que no se acrediten los puntos anteriores, la *Oficina de Registro* no continuará con la tramitación de la solicitud del *Certificado*.

c) Envío de información a la FNMT-RCM

Una vez confirmada la identidad del *Solicitante* y vigencia de las condiciones de legitimación y competencia exigidas a éste, se suscribirá el documento de condiciones de utilización o, en su caso, contrato de solicitud por el *Solicitante*, en nombre del *Titular*, y/o el responsable de la *Oficina de Registro*. La información y documentos anteriores serán enviados, junto con el código de solicitud recogido en la fase de presolicitud a la FNMT-RCM. Los datos personales y su tratamiento quedarán sometidos a la legislación específica

Dicho envío sólo se producirá si la *Oficina de Registro* tiene potestad para actuar como tal en nombre del órgano, organismo o entidad de la Administración Pública *Titular* del *Certificado* para la actuación administrativa automatizada y si ésta posee la unidad organizativa a consignar en el *Certificado* y desde la que se realizará la actuación administrativa automatizada.

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.

12.2.2.3. *Emisión del Certificado para la actuación administrativa automatizada de la Administración Pública*

242. Una vez recibidos en la FNMT-RCM los datos de los *Titulares*, de los *Solicitantes* y firmantes/custodios, la información que describe su relación con la Administración Pública, la unidad organizativa desde la que se realizará la actuación administrativa automatizada



- objeto del *Certificado*, así como el código de solicitud obtenido en la fase de presolicitud, se procederá a la emisión del *Certificado*.
243. La emisión de *Certificados* supone la generación de documentos electrónicos que confirman la identificación y autenticación del *Titular* y del personal facultado firmante/custodio de la *Oficina de Registro* y/o unidad organizativa de la Administración actuante, organismo o entidad pública vinculada o dependiente. y al que se vincula los *datos de verificación de firma* que se corresponden unívoca e inequívocamente con unos *datos de creación de firma* bajo la custodia de dicho firmante/custodio.
244. La emisión de *Certificados* de la FNMT-RCM sólo puede realizarla ella misma, en su calidad de *Prestador de Servicios de Certificación*, no existiendo ninguna otra entidad u organismo con capacidad de emisión de los mismos. La FNMT-RCM, por medio de su *Firma electrónica*, autentica los *Certificados* y confirma la identidad y competencia de sus *Titulares*, así como su condición de *Titular* del *Certificado* para la actuación administrativa automatizada (sello electrónico) y del personal firmante/custodio encargado de la gestión de dicho *Certificado* y sello electrónico, de conformidad con la información recibida por parte de la *Oficina de Registro*. 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*.
245. La FNMT-RCM en ningún caso incluirá en un *Certificado* información distinta de la aquí mostrada, ni circunstancias, atributos específicos de los firmantes/custodios o límites distintos a los previstos en los acuerdos, convenios y, en su caso, a los previstos en la *Ley de Emisión* correspondiente.
246. En cualquier caso la FNMT-RCM actuará diligentemente para:
- Comprobar que el *Solicitante* del *Certificado* o el responsable de la *Oficina de Registro* utilice la *Clave Privada* correspondiente a la *Clave Pública* vinculada a la identidad del *Titular* del mismo. Para ello la FNMT-RCM comprobará la correspondencia entre la *Clave privada* y la *Clave pública*.
  - Lograr que la información incluida en el *Certificado* se base en la información proporcionada por el *Solicitante* y/o por el responsable de la *Oficina de Registro* correspondiente.
  - No ignorar hechos notorios que puedan afectar a la fiabilidad del *Certificado*.
  - Lograr que el *DN* (nombre distintivo) asignado en el *Certificado* sea único en toda la *Infraestructura de Clave Pública* de la FNMT-RCM.
247. Para la emisión del *Certificado* se seguirán los siguientes pasos:
1. Composición del nombre distintivo (DN) del *Titular*  
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 de lugar a ambigüedades. No se contempla el uso de seudónimos como forma de identificación del *Titular*.  
El *DN* está compuesto de los siguientes elementos:  
DN=CN, OU, OU, OU, O, C



El conjunto de atributos OU, OU, OU, O, C representa la rama del directorio en la que se encuentra ubicada la entrada correspondiente al *Titular* y/o firmante/custodio en cuestión.

El atributo *CN* contiene el nombre de la *Oficina de Registro* y/o unidad organizativa de la Administración, organismo o entidad pública que realiza la actuación administrativa automatizada de la que depende.

Una vez compuesto el nombre distintivo (*DN*) se crea la correspondiente entrada en el directorio, procurando que el nombre distintivo sea único en toda la *Infraestructura de Clave Pública* del *Prestador de Servicios de Certificación*.

2. Composición de la identidad alternativa del *Titular*

La identidad alternativa del *Titular* y/o firmante/custodio, tal como se contempla en la presente tipología de *Certificados* contiene la identidad de los *titulares* del *Certificado* y el nombre de la *Oficina de Registro* y/o unidad organizativa distribuida en una serie de atributos. Se utiliza la extensión *subjectAltName* definida en *X.509* versión 3 para ofrecer esta información.

Dentro de dicha extensión, se utilizará el subcampo *directoryName* para incluir un conjunto de atributos definidos por la FNMT-RCM, que incorporan información sobre el *Titular* en cuestión, siguiendo el siguiente criterio:

| Tipo Certificado                      | Información                       | Atributo FNMT     | OID (*)      |
|---------------------------------------|-----------------------------------|-------------------|--------------|
| Actuación administrativa automatizada | Unidad organizativa de la entidad | fnmtDescripcion   | fnmtoid.1.8  |
|                                       | Entidad titular del certificado   | fnmtPropEnt       | fnmtoid.1.14 |
|                                       | CIF de la entidad titular         | fnmtCIF           | fnmtoid.1.15 |
|                                       | Nombre del custodio               | fnmtRespNombre    | fnmtoid.1.16 |
|                                       | Primer apellido del custodio      | fnmtRespApellido1 | fnmtoid.1.17 |
|                                       | Segundo apellido del custodio     | fnmtRespApellido2 | fnmtoid.1.18 |
|                                       | NIF del custodio                  | fnmtRespNIF       | fnmtoid.1.19 |



**Tabla 12 Composición del subcampos `directoryName`. Actuación automatizada APE**

(\*) `fnmtoid: 1.3.6.1.4.1.5734`: Espacio de numeración asignado a la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda por el IANA.

3. Generación del *Certificado* conforme al Perfil del *Certificado* para la actuación administrativa automatizada

El formato del *Certificado* para la actuación administrativa automatizada expedido por la FNMT-RCM bajo la presente política, en consonancia con la norma UIT-T X.509 versión 3 y de acuerdo con la normativa legalmente aplicable en materia de *Certificados Reconocidos*, contiene los siguientes campos:

| CAMPO                        | CONTENIDO  | OBSERVACIONES  |
|------------------------------|--|--|
| 1. Versión                   | V3   |  |
| 2. Serial Number             | Secuencial   | [RFC3280]: the serial number MUST be a positive integer, not longer than 20 octets ( $1 < SN < 2^{159}$ ). Processing components MUST be able to interpret such long numbers.  |
| 3. Signature Algorithm       | Sha1withRsaEncryption<br>Sha256withRsaEncryption   | OID: 1.2.840.113549.1.1.5<br>OID: 1.2.840.113549.1.1.11<br><br>Norma PKCS#1 v2.1 y RFC 3447.   |
| 4. Issuer Distinguished Name | OU= AC APE<br>O=FNMT-RCM<br>C=ES   | Todos los <i>DirectoryString</i> codificados en UTF8. El atributo "C" ( <i>countryName</i> ) se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements", en <i>PrintableString</i> .<br>[ETSI-CPN]: the issuer name MUST contain the <i>countryName</i> and the <i>organizationName</i> attributes. |
| 5. Validez                   | 48 meses   | 48 meses a partir del momento de la emisión.   |
| 6. Subject                   | CN= DESCRIPCION d – ENTIDAD e – CIF 12345678B<br>OU= "Organizacion_Entidad"<br>OU=AC APE<br>O=FNMT-RCM<br>C=ES | Todos los <i>DirectoryString</i> codificados en UTF8. El atributo "C" ( <i>countryName</i> ) se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements", en <i>PrintableString</i> .  |
| 7. Subject Public Key Info   | Algoritmo: RSA Encryption<br>Longitud: 2048 bits   |  |
| 8. Subject Key Identifier    | Función hash SHA-1 sobre la clave pública del sujeto.  | RFC 3280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo <i>subjectPublicKey</i> del sujeto (excluyendo etiqueta, longitud y número de bits no usados).  |
| 9. Authority Key Identifier  | Función hash SHA-1 sobre la clave pública de la AC emisora (AC subordinada). NO SE incluye la                  | RFC 3280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo <i>subjectPublicKey</i> de la AC emisora (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo  |

| CAMPO                           | CONTENIDO   | OBSERVACIONES  |
|---------------------------------|---|--|
|                                 | identificación del certificado de la AC emisora (en este caso, DN de la AC Raíz, número de serie de la AC Subordinada). | <i>Subject Key Identifier</i> de la AC emisora (AC subordinada).   |
| <b>10. KeyUsage</b>             |   |  |
|                                 | <b>Digital Signature</b>  | 1  |
|                                 | <b>Non Repudiation</b>  | 1  |
|                                 | <b>Key Encipherment</b>   | 1  |
|                                 | <b>Data Encipherment</b>  | 1  |
|                                 | <b>Key Agreement</b>  | 0  |
|                                 | <b>Key Certificate Signatura</b>  | 0  |
|                                 | <b>CRL Signature</b>  | 0  |
|                                 |   | Si es necesario que tenga la misma operatividad que FNMT Clase 2 CA, tendrá La Norma ETSI TS 102 280 V1.1.1 (2004-03) – “X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons” recomienda el uso exclusivo del bit de no repudio para certificados destinados a validar el compromiso con el contenido firmado, tales como firmas electrónicas sobre transacciones o acuerdos.   |
|                                 |   | En el <i>Technical Corrigendum 3</i> de la ITU-T X509 de 04/2004, el bit de no-repudio es renombrado a <b>contentCommitment</b> . En este documento se recoge lo siguiente:  |
|                                 |   | <i>“Note that it is not incorrect to refer to this keyUsage bit using the identifier nonRepudiation. However, the use of this identifier has been deprecated. Regardless of the identifier used, the semantics of this bit are as specified in this Directory Specification.”</i>  |
| <b>11. extKeyUsage</b>          | Autenticación de cliente:<br>1.3.6.1.5.5.7.3.2<br>Protección de correo electrónico:<br>1.3.6.1.5.5.7.3.4                | <i>[RFC3280]: Certificate using applications MAY require that a particular purpose be indicated in order for the certificate to be acceptable to that application. If a CA includes extended key usages to satisfy such applications, but does not wish to restrict usages of the key, the CA can include the special keyPurposeID anyExtendedKeyUsage. If the anyExtendedKeyUsage key purpose is present, the extension SHOULD NOT be critical.</i>           |
| <b>12. Certificate Policies</b> |   |  |
|                                 | <b>Policy Identifier</b>  | OID asociado a la DPC o PC de certificado de firma de Sello electrónico.<br>(fnmtPolCertSelloElect)<br>1.3.6.1.4.1.5734.3.13   |
|                                 | <b>URL CPS</b>  | http://www.cert.fnmt.es/dpcs/  |
|                                 | <b>Notice Referente</b>   | Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM ( C/Jorge Juan 106-28009-Madrid-España)   |
|                                 |   | RFC 3739 obliga la existencia de al menos un valor.<br>La Ley de Firma Electrónica dice para los certificados reconocidos: “La identificación del prestador de servicios de certificación que expide el certificado y su domicilio”. Se incluirá en la DPC.<br><br><i>In an end entity certificate, these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used.</i> |
| <b>13. qcStatements</b>         | id-etsi-qcs-QcCompliance  | ETSI TS 101 862 define la inclusión de las siguientes declaraciones para certificados  |

| CAMPO                              | CONTENIDO  | OBSERVACIONES  |                   |
|------------------------------------|--|--|-------------------|
|                                    | id-etsi-qcs-QcLimitValue : 0€<br>Id-etsi-qcs-<br>QcRetentionPeriod: 15 años  | <p>cualificados:</p> <p>1.- <b>id-etsi-qcs-QcCompliance</b> – Indica que el certificado es cualificado. Solo si no está explícito en las políticas indicadas en la extensión correspondiente.</p> <p>2.- <b>id-etsi-qcs-QcLimitValue</b> – Opcional. Indica el valor límite para transacciones.</p> <p>3.- <b>id-etsi-qcs-QcRetentionPeriod</b> – Opcional. Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otro información relevante. En este caso la Ley obliga: <i>"Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo."</i>. Dado que la FNMT va a conservar la información de manera indefinida, y que la norma no establece un valor para indicar un período indefinido, no se incluirá este QC y se indicará en la DPC.</p> <p>4.- <b>id-etsi-qcs-QcSSCD</b> – Opcional. Indica que la clave privada correspondiente al certificado está almacenada en un dispositivo seguro de creación de firma de acuerdo al Anexo III de la Directiva del Parlamento Europeo 1999/93/EC, sobre un framework comunitario para firmas electrónicas.</p> |                   |
| <b>14. Subject Alternate Names</b> | Dirección del directorio:<br>OID.1.3.6.1.4.1.5734.1.8=fnmtDescripción<br>OID.1.3.6.1.4.1.5734.1.14=fnmtPropEnt<br>OID.1.3.6.1.4.1.5734.1.15=fnmtCIF<br>OID.1.3.6.1.4.1.5734.1.16=fnmtRespNombre (Opcional)<br>OID.1.3.6.1.4.1.5734.1.17=fnmtRespApellido1 (Opcional)<br>OID.1.3.6.1.4.1.5734.1.18=fnmtRespApellido2 (Opcional)<br>OID.1.3.6.1.4.1.5734.1.19=fnmtRespNIF (Opcional) | Descripción  | fnmtDescripción   |
|                                    |  | Entidad propietaria  | fnmtPropEnt       |
|                                    |  | CIF  | fnmtCIF           |
|                                    |  | Nombre Responsable   | fnmtRespNombre    |
|                                    |  | Apellido1 Responsable  | fnmtRespApellido1 |
|                                    |  | Apellido2 Responsable  | fnmtRespApellido2 |
|                                    |  | NIF Responsable  | fnmtRespNIF       |
|                                    |  | <b>15. Basic Constraints</b>   |                   |
| <b>Subject Type</b>                | Entidad Final  | [RFC 3280] This extension MAY appear as a critical or non-critical extension in end entity certificates.   |                   |
| <b>16. CRLDistributionPoints</b>   | LDAP:<br>ldap://ldapape.cert.fnmt.es:<br>puerto/CN=CRLnnn,OU= AC<br>APE, O=FNMT, C=ES<br>?certificateRevocationList;bin  |  |                   |

| CAMPO                           | CONTENIDO  | OBSERVACIONES   |
|---------------------------------|--|---|
|                                 | ary?base<br>?objectclass=cRLDistribution<br>Point<br>HTTP:<br>http://www.cert.fnmt.es/crls<br>ape/CRLnnn.crl   |   |
| 17. Auth. Information<br>Access | OCSP:<br><a href="http://ocspape.cert.fnmt.es/ocspape/OcspResponder">http://ocspape.cert.fnmt.es/<br/>ocspape/OcspResponder</a><br>CA:<br><a href="http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt">http://www.cert.fnmt.es/cert<br/>s/ACRAIZFNMTRCM.crt</a> | Contendrá información de localización del OCSP Responder. URL resuelta a diferentes servidores. Ley de Firma Electrónica: " <b>Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro</b> ". |
| 18. netscapeCertType            | sSLCLIENT,sMIME  | Tipo de certificado según Netscape  |
| 19. fnmtTipoCertificado         | 1.3.6.1.4.1.5734.1.33: "Sello Electrónico para Procesos Automatizados"   | Tipo de certificado para Sello Electrónico para Procesos Automatizados  |
| 20. AuthorityKeyIdentifier      | 2.5.29.35: Identificador de clave del prestador de servicios de certificación  |   |

**Tabla 13 Perfil del Certificado de Actuación Administrativa Automatizada - APE**

#### 12.2.2.4. Publicación del Certificado para la actuación administrativa automatizada

248. Una vez generado el *Certificado* por parte de la FNMT-RCM como *Prestador de Servicios de Certificación*, se publicará en el *Directorio*, concretamente en la entrada correspondiente al nombre distintivo de la dirección electrónica, tal como se ha definido en el apartado "*Emisión del Certificado*" de este documento

#### 12.2.2.5. Descarga e instalación del Certificado para la actuación administrativa automatizada

249. Una vez transcurrido el tiempo establecido desde que el *solicitante* se persona en las *Oficinas de Registro* para realizar la solicitud y una vez que el *Certificado* haya sido generado, se pone a disposición del *Titular* u *Oficina de Registro* un mecanismo de descarga de *Certificado* en la dirección

250. Realizados los trámites anteriores y generado el *Certificado* para la actuación administrativa automatizada, la FNMT-RCM pondrá a disposición del responsable de la *Oficina de Registro* correspondiente un mecanismo de descarga del *Certificado* en la dirección de titularidad de la Administración u organismo, a través del siguiente enlace:

<http://ape.cert.fnmt.es/appsUsuario/descargameh/descargaCertInicio.jsp>

251. A tal efecto, se accederá a la opción "Descarga de su Certificado".

252. En este proceso guiado se le pedirá, al responsable de la *Oficina de Registro* del ámbito del *Titular*, que introduzca el CIF del órgano, organismo o entidad pública con el que realizó el proceso de presolicitud así como el código de solicitud devuelto por el sistema al finalizar

dicho proceso. Si el *Certificado* no ha sido aún generado por cualquier motivo, se le indicará este hecho en el momento que intente su descarga.

253. Si el *Certificado* ya ha sido puesto a disposición del *Titular*, aquél será introducido directamente en el soporte en el que se generaron las *Claves* durante el proceso de Presolicitud.

#### 12.2.2.6. *Período de validez del Certificado para la actuación administrativa automatizada*

254. El periodo de validez de los *Certificados* de sello electrónico para la actuación administrativa automatizada emitidos por la FNMT-RCM bajo esta *Política de Certificación* será de cuatro (4) años contados a partir del momento de la emisión del *Certificado*, siempre y cuando no se extinga su vigencia por las causas y procedimientos expuestos en el apartado “Extinción de la vigencia del Certificado” de la *Declaración General de Prácticas de Certificación* o lo dispuesto, en su caso, en la *Ley de Emisión* correspondiente.

#### 12.2.2.7. *Revocación del Certificado para la actuación administrativa automatizada*

255. La revocación de *Certificados* consiste en la cancelación de la garantía de identidad, autenticidad u otras propiedades del *Titular* y sus representantes y su correspondencia con la clave pública asociada. Implica, además de su extinción, la finalización de la relación y régimen de uso del *Certificado* con la FNMT-RCM.

256. Estarán legitimados para solicitar la revocación de un *Certificado* para la actuación administrativa automatizada, en base a la inexactitud de los datos consignados en el *Certificado*, variación de los mismos o cualquier otra causa a valorar por los *Titulares*:

- El órgano directivo de la Administración, organismos o entidades, vinculadas o dependientes, o personas en quien deleguen. FNMT-RCM considerará a los firmantes/custodios responsables de la unidad organizativa consignada en el *Certificado* y perteneciente a la entidad de la administración *Titular* del *Certificado*, con capacidad y competencia a efectos de instar la revocación.
- la *Oficina de Registro*, —a través de su responsable— que esté designada a tal efecto, por la Administración, organismo o entidad vinculada o dependiente *Titular* del *Certificado* a revocar, cuando detecte que alguno de los datos consignados en el *Certificado*
  - es incorrecto, inexacto o haya variado o
  - la *persona física* firmante/custodio del *Certificado* no se corresponda con el responsable máximo o designado de la unidad organizativa, órgano, organismo o entidad pública consignada en el *Certificado* o
  - la unidad organizativa consignada en el *Certificado* no depende organizativamente del órgano, organismo o entidad pública de la que depende el *Titular* del *Certificado*.

La revocación se realizará siempre en el marco de los términos y condiciones del apartado Revocación de *Certificados* de la *Declaración General de Prácticas de Certificación*.

12.2.2.8. *Procedimiento por el que se obtienen los datos personales del Solicitante de la revocación, se confirma su identidad y la capacidad para realizar dicha solicitud y la formalización de la misma.*

257. Serán causas admitidas para la revocación de un *Certificado* las expuestas en el apartado correspondiente de la *Declaración General de Prácticas de Certificación* de la FNMT-RCM, si bien la *Ley de Emisión* de aplicación podrá establecer adicionalmente otras causas de revocación o en su caso suspensión y/o cancelación.

1. Personación del *Solicitante* ante las *Oficinas de Registro*

Para revocar el *Certificado*, el *Solicitante* con capacidad y competencia suficientes se personará ante una *Oficina de Registro* designada a tal efecto por el órgano, organismo o entidad *Titular del Certificado* a revocar, o se realizará directamente por el responsable de la *Oficina de Registro*.

2. Comparecencia y documentación

El *Solicitante* aportará los datos que se le requieran y que acrediten:

- su identidad personal,
- su condición de personal al servicio del órgano, organismo o entidad de la Administración pública *Titular del Certificado* o su condición de responsable de la *Oficina de Registro*.
- su condición de máximo responsable o persona designada de la unidad organizativa consignada en el *Certificado* y dependiente de la administración *Titular del Certificado* o de personal adscrito a la *Oficina de Registro* designada a tal efecto por el organismo o entidad *Titular del Certificado* a revocar

FNMT-RCM estará y admitirá, en todo caso, la función e informe que realice la *Oficina de Registro* designada por la Administración. En el caso de que no se acrediten los puntos anteriores, la *Oficina de Registro* no procederá con la solicitud de revocación del *Certificado*

3. Envío de la solicitud de revocación a la FNMT-RCM y tramitación

Sin que existan causas notorias de falta de competencia del responsable de la *Oficina de Registro* y/o una vez confirmada la identidad del *Solicitante*, vigencia de las condiciones exigidas a éste y suscrito el documento de solicitud de revocación, la *Oficina de Registro* procederá a validar los datos y a enviarlos a la FNMT-RCM para la revocación efectiva del *Certificado*.

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

Dicho envío sólo se producirá si la *Oficina de Registro* tiene potestad para actuar como tal en nombre del órgano, organismo o entidad de la Administración Pública *Titular del Certificado* y si éste tiene es responsable o tiene competencia suficiente sobre la unidad organizativa consignada en el *Certificado*

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.

Una vez que la FNMT-RCM ha procedido a la revocación del certificado, se publicará en el directorio seguro la correspondiente *Lista de Certificados Revocados* conteniendo el número de serie del *Certificado* revocado, la fecha y hora de revocación y la causa de revocación.

#### 12.2.2.9. *Suspensión del Certificado para la actuación administrativa automatizada*

258. La suspensión de *Certificados* deja sin efectos el *Certificado* durante un período de tiempo y en unas condiciones determinadas.
259. La suspensión de los *Certificados* será considerada una revocación temporal de la vigencia del *Certificado* por lo que los procedimientos y entidades habilitadas para la solicitud y tramitación de la *revocación* del *Certificado* son de aplicación en el caso de la *suspensión*. Adicionalmente se tendrán en cuenta para la admisión de las *suspensión* las causas admitidas expuestas en el apartado “Causas de suspensión de *Certificados*” de la *Declaración General de Prácticas de Certificación*.
260. La FNMT-RCM procederá a suspender el *Certificado* de forma provisional durante un plazo de noventa (90) días, plazo tras el cual se extinguirá el *Certificado* mediante su revocación directa por parte del *Prestador de Servicios de Certificación* de la FNMT-RCM, salvo que se hubiera levantado la suspensión. No obstante lo anterior, el plazo previsto para la suspensión del *Certificado* podrá verse alterado en función de los procedimientos judiciales o administrativos que lo pudieran afectar.
261. Si durante el plazo de suspensión del *Certificado* éste caducara o se solicitara su revocación, se producirán las mismas consecuencias que para los *Certificados* no suspendidos que se vieran afectados por supuestos de caducidad o de revocación.

#### 12.2.2.10. *Cancelación de la suspensión del Certificado para la actuación administrativa automatizada*

262. Podrán solicitar la Cancelación de la suspensión de los *Certificados* emitidos por la FNMT-RCM los *Titulares*, a través de sus representantes, siempre que dicha solicitud se efectúe durante los noventa (90) días siguientes a su suspensión.
263. La FNMT-RCM considerará que se actúa con capacidad bastante, a los efectos de este apartado, cuando la solicitud se realice a través del responsable de la *Oficina de Registro* correspondiente.
264. Sin perjuicio de lo señalado en el párrafo anterior, y en el caso de actuación a través de otros representantes del *Titular* del *Certificado* distintos al responsable de la *Oficina de Registro*, la comparencia y/o acto de petición de cancelación se llevará a través y/o ante la *Oficina de Registro* designada por el organismo o entidad a la que pertenece el *Titular* y según el criterio vigente de la FNMT-RCM, al objeto de que ésta sea homogénea en todos los casos.
265. En este acto, el solicitante representante del *Titular* del *Certificado* con competencia suficiente, objeto de la petición, aportará los datos que se le requieran y acreditará su



identidad personal, siguiendo el procedimiento descrito anteriormente para la solicitud de emisión del *Certificado* para la actuación administrativa automatizada. FNMT-RCM aceptará el informe de acreditación que pudiera emitir la *Oficina de Registro* considerando lo establecido en el artículo 13.1 in fine de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

266. Los datos personales del responsable de la *Oficina de Registro* o del representante del *Titular*, una vez validados por la *Oficina de Registro*, se enviarán a la FNMT-RCM mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM. Los datos personales y su tratamiento quedarán sometidos a la legislación específica
267. Una vez recibidos los datos validados por la *Oficina de Registro* de la petición de levantamiento de suspensión, la FNMT-RCM procederá a retirar este *Certificado* de la *Lista de Revocación*, no efectuándose acción técnica alguna sobre el *Certificado* en cuestión.

#### 12.2.2.11. Comprobación del estado del Certificado para la actuación administrativa automatizada

268. El *Titular* del *Certificado* y las Administraciones, organismos y entidades *usuarias* pertenecientes a la *Comunidad Electrónica* podrán realizar la comprobación del estado de un *Certificado* en la forma y condiciones que se expresan en los apartados “Procedimientos de consulta del estado de los *Certificados*” y “Servicio de validación de *Certificados* mediante OCSF” de la *Declaración General de Prácticas de Certificación*, sin perjuicio de lo que pueda establecerse mediante acuerdo o convenio de la FNMT-RCM, el *Titular* del *Certificado* y, en su caso, los integrantes de la *Comunidad Electrónica*.
269. FNMT-RCM no proporciona servicio de comprobación de *Certificados* de otros *Titulares* salvo en los casos que así se establezca a través de convenios y/o contratos con el correspondiente consentimiento de los miembros integrantes de la *Comunidad Electrónica* o en los términos previstos en la *Ley de Emisión*.
270. En particular, para la difusión y confianza en los sistemas que cuenten con estos *Certificados*, la FNMT-RCM, podrá proporcionar la posibilidad de verificar, por el miembro de la *Comunidad electrónica* o un tercero, que el *Certificado* para la actuación administrativa automatizada es un *Certificado* válido emitido por la FNMT-RCM, así como otras características del mismo.

#### 12.2.3. Exclusiones y requisitos adicionales a ETSI TS 101 456

- De acuerdo con la norma en el apartado 8.2 b), se excluyen las cuestiones definidas en el apartado 7.5 j), k).
- De acuerdo con la norma en el apartado 8.2 c), se excluyen las cuestiones definidas en el apartado 7.3.5 f). En este tema se estará a lo señalado en el apartado “*Publicación del Certificado*” de este anexo.
- De acuerdo con la norma en el apartado 8.2 d), se excluyen las cuestiones definidas en el apartado 7.3.6 k). En este tema se estará a lo señalado en el apartado “*Comprobación del estado del Certificado*” de este anexo.



271. Respecto aquellos *Certificados Reconocidos* que usen Dispositivos Seguros de creación de firma, seguirán lo señalado en el apartado “Soporte del Certificado” del documento *Declaración General de Prácticas de Certificación* de la FNMT-RCM, así como a lo expuesto en los apartados sobre “Ciclo de vida del certificado” del citado documento. Todo ello sin perjuicio de la utilización de los sistemas de firma electrónica admitidos por la Ley 11/2007, de 22 de junio, LAECSP.

#### **12.2.4. Modelos de formulario**

272. Los modelos de formularios que se deben cumplimentar para realizar las operaciones descritas para la gestión del ciclo de vida de los *Certificados* para personal al servicio de la Administración Pública se ponen a disposición en <http://www.ceres.fnmt.es>