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

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM / v1.2	01/08/2010
Revisado por:	FNMT-RCM / v1.2	01/08/2010
Aprobado por:	FNMT-RCM / v1.2	01/08/2010

HISTÓRICO DEL DOCUMENTO			
Versión	**Fecha**	**Descripción**	**Autor**
1.0	06/11/2008	Creación del documento	FNMT-RCM
1.1	05/05/2009	Ampliación de la vigencia de los certificados a cuatro años.	FNMT-RCM
1.2	01/08/2010	Eliminación del apartado aspectos organizativos por incluirse en el DGPC Obligación de reflejar la entidad para la que el firmante presta los servicios (Titular del Certificado) en el certificado de personal al servicio de las administraciones públicas en la extensión subjectAltName Modificación de los perfiles de los certificados. Inclusión de nuevos perfiles conforme a nuevas políticas de certificación.	FNMT-RCM

Referencia: DPC/PCPAA0102/SGPSC/2010

Documento clasificado como: *Público*

ÍNDICES

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

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 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**.

   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 el **personal al servicio de la Administración Pública**.

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* 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 Administración Pública 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 *Declaración General de Prácticas de Certificación*.

       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 la Administración Pública,**
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 documento y que se refieren a: **Personal al servicio de la Administración Pública**, **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. 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 Administración Pública, 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*

15. 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 la *Declaración General de Prácticas de Certificación*.

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

16. La FNMT-RCM utiliza los mecanismos necesarios para mantener su *Clave privada* confidencial y mantener su integridad en la forma que se muestra en la *Declaración General de Prácticas de Certificación*.

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

17. 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 la *Declaración General de Prácticas de Certificación*.

18. 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 el anexo (Tabla 1)

19. 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*.

20. Para dicha emisión, la FNMT emplea dos posibles conjuntos de *Datos de Creación de Firma*, correspondiéndose cada conjunto con su respectivo *Certificado* de *Autoridad de Certificación* (en cualquier caso, subordinada al *Certificado Raíz* de la FNMT-RCM identificado anteriormente). Ambos *Certificados* se encuentran definidos en el anexo a este documento (Tablas 2 y 3)

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. DIFUSIÓN DE TÉRMINOS Y CONDICIONES

29. 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.

8. CERTIFICADOS EMITIDOS PARA EL PERSONAL AL SERVICIO DE LA ADMINISTRACIÓN PÚBLICA

8.1. POLÍTICA DE CERTIFICACIÓN DE LOS CERTIFICADOS EMITIDOS PARA EL PERSONAL AL SERVICIO DE LA ADMINISTRACIÓN PÚBLICA

8.2. IDENTIFICACIÓN

30. 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: Política de Certificación de Certificados para personal al servicio de la Administración Pública de España

Referencia / OID[1]:

- 1.3.6.1.4.1.5734.3.14
- 1.3.6.1.4.1.5734.3.3.4.4.1
- 1.3.6.1.4.1.5734.3.3.4.4.2

Versión: 1.2

Fecha de emisión: 1 de agosto de 2010

Localización: http://www.cert.fnmt.es/dpcs/

DPC relacionada: Declaración General de Prácticas de Certificación de la FNMT-RCM

Localización: http://www.cert.fnmt.es/dpcs/

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

31. El *Certificado* para el personal al servicio de las Administración Pública, es la certificación electrónica emitida por la FNMT-RCM que vincula a su *Titular* (la Administración, órgano,

[1] *Nota*: El OID o identificador de política es una referencia que se incluirá en el *Certificado* al objeto de que los usuarios puedan determinar las prácticas y procedimientos de aplicación para la emisión del *Certificado* en cuestión.

Si bien en este documento se desarrolla una sola política para este tipo de *Certificados*, pueden existir tres referencias diferentes a ella para diferenciar o identificar particularidades en el soporte del *Certificado* los perfiles de *Certificados*, *Autoridad de Certificación* empleada para la emisión o procedimientos de emisión de los mismos.

Así pues, la *Política y Prácticas de Certificación* de los *Certificados* para personal al servicio de la Administración Pública se describirá de forma única, identificándose cuantas particularidades puedan existan y asociándolas a los OID o referencias que correspondan.

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.

32. 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.

33. 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.

34. 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.

35. 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*.

36. Se hace constar expresamente que el *Certificado* emitido bajo esta política, constituye un *Certificado* distinto al previsto en el Anexo II de la *Declaración de Prácticas de Certificación* de FNMT Clase 2 CA 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*.

37. El *Certificado* emitido para el personal al servicio de la Administración pública no se regirá 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.

8.2.2. Gestión de la Política de Certificación

38. 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*.
- Para identificar la *Política de Certificación* aquí desarrollada, se dispone de los OIDs específicos:
  - 1.3.6.1.4.1.5734.3.14

- 1.3.6.1.4.1.5734.3.3.4.4.1
- 1.3.6.1.4.1.5734.3.3.4.4.2

- 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 101 456*** de la presente *Política de Certificación*). En caso de discrepancia entre este documento y la referida norma, prevalecerá este documento.

8.2.3. Comunidad y ámbito de aplicación

39. 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, Autonómica 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 funcionarial, 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 está *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.

8.2.4. Responsabilidad y obligaciones de las partes

40. 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.

41. 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.

42. 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.
- En el caso de que el *Certificado* esté en un soporte tipo tarjeta, descargar el *Certificado* y sus claves directamente en la tarjeta criptográfica que se proporcione a su personal. En cualquier caso, 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*.

43. 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.

44. 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*.

45. 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.

46. 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.

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

47. 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.

48. 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.

49. 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*.

50. 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*.

51. 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 *Fechado electrónico.*
- Prestar servicios a título gratuito u oneroso, salvo supuestos expresamente autorizados previamente ,como por ejemplo serían a título enunciativo:
    - Prestar servicios de *OCSP*.
    - Generar *Listas de Revocación.*
    - Prestar servicios de notificación

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

52. 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*.

53. En especial deberá tenerse presente, a efectos interpretativos del presente anexo el apartado "Definiciones" de la *Declaración General de Practicas de Certificación*.

54. 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 los OIDs 1.3.6.1.4.1.5734.3.14, 1.3.6.1.4.1.5734.3.3.4.4.1 ó 1.3.6.1.4.1.5734.3.3.4.4.2.

8.3.1. Servicios de Gestión de las *Claves* de los *Titulares*

55. 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.

8.3.2. Preparación de los *Dispositivos Seguros de Creación de Firma*

56. En el caso de los *Certificados* generados con OID's 1.3.6.1.4.1.5734.3.14 ó 1.3.6.1.4.1.5734.3.3.4.4.1 se empleará un *Dispositivo Seguro de Creación de Firma* para la generación de claves y la posterior realización de *Firma Electrónica*.

57. En estos casos, 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*.

58. 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*.

59. 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*.

8.3.3. Gestión del ciclo de vida de los *Certificados*

60. 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.

8.3.3.1. Procedimiento de solicitud del Certificado para personal al servicio de la Administración Pública

61. 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.

62. 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 funcionarial, administrativa o laboral con tal personal, más allá del documento de condiciones de utilización o, en su caso, contrato de emisión, cuyo efecto es estrictamente instrumental para el desempeño de las funciones propias del cargo.

63. 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.

64. 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 [2]

   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 habilitar, 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 habilitación 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 Publica como usuario y custodio de tales *Certificados*, no guardándose copia de ellos por la FNMT-RCM, ni por la *Oficina de Registro*.

[2] Este paso sólo será necesario en caso de que la emisión del *Certificado* sea conforme a los OIDs 1.3.6.1.4.1.5734.3.14 ó 1.3.6.1.4.1.5734.3.3.4.4.1

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[3], 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 funcionarial o laboral. Posteriormente, se generarán las *Claves Pública* y *Privada* (en *Tarjeta criptográfica* si el *Certificado* se emite con los OID's 1.3.6.1.4.1.5734.3.14 ó 1.3.6.1.4.1.5734.3.3.4.4.1*)* 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 plasmaran 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.

[3] Para los *Certificados* emitidos bajo el OID 1.3.6.1.4.1.5734.3.3.4.4.2, esta operación se **deberá** realizar siempre desde el puesto en el que el interesado realice las funciones.

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*.

Si la generación de las claves se realiza 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

8.3.3.2. Personación ante las Oficinas de Registro

65. 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.

66. 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.

8.3.3.3. Comparecencia y documentación

67. 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.

8.3.3.4. Emisión del Certificado para personal al servicio de la Administración Pública

68. 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*.

69. 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.

70. 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*.

71. 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.

72. 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 Publica* vinculada a la identidad del *Titular* del mismo. Para ello, la FNMT-RCM comprobará la correspondencia entre la *Clave privada* y la *Clave pública*.
- Lograr que la información incluida en el *Certificado* se base en la información proporcionada por 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.

73. 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.

   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.

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*, puede consultarse en los anexos al presente documento

En ellos se describen los perfiles de los *Certificados* diferenciándose según la *Autoridad de Certificación* que los emite (siempre subordinada a la *Autoridad de Certificación Raíz* de la FNMT-RCM), así como el soporte del *Certificado*.

Adicionalmente, si es el caso, se incluirán las extensiones necesarias para poder realizar el proceso de "login" en Sistemas Operativos Windows con Tarjeta Criptográfica:

Nombre extensión: extKeyUsage

Valores: Autenticación de cliente: 1.3.6.1.5.5.7.3.2

Inicio de sesión de tarjeta inteligente: 1.3.6.1.4.1.311.20.2.2

8.3.3.5. Publicación del Certificado de personal al servicio de la Administración Pública

74. 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

75. 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.

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

76. 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

https://www.cert.fnmt.es/index.php?cha=adm&sec=23&fpage=62&lang=es

77. accediendo a la opción "Descarga de su Certificado".

78. 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.

79. 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.

8.3.3.7. Vigencia del Certificado de personal al servicio de la Administración Pública

8.3.3.7.1. Caducidad

80. Los *Certificados* de personal al servicio de la Administración Pública emitidos por la FNMT-RCM tendrán validez durante un período de cuatro (4) años contados a partir del momento de la emisión del *Certificado*, siempre y cuando no se extinga su vigencia. Transcurrido este período y si el *Certificado* sigue activo, caducará, siendo necesaria la emisión de uno nuevo en caso de que el *Titular* desee seguir utilizando los servicios del *Prestador de Servicios de Certificación.*

8.3.3.7.2. Extinción de la vigencia

81. Los *Certificados* de personal al servicio de la Administración Pública emitidos por la FNMT-RCM quedarán sin efecto en los siguientes casos:

a) Terminación del período de validez del *Certificado*

b) Cese en la actividad como *Prestador de Servicios de Certificación* de la FNMT-RCM, salvo que, previo consentimiento expreso del *Suscriptor* y *Titular*, los *Certificados* expedidos por la FNMT-RCM hayan sido transferidos a otro *Prestador de Servicios de Certificación*.

En estos dos casos [a) y b)], la perdida de eficacia de los *Certificados* tendrá lugar desde que estas circunstancias se produzcan.

c) Suspensión o revocación del *Certificado* por cualquiera de las causas recogidas en el presente documento

82. A los efectos enumerados anteriormente, se hace constar que la solicitud de emisión de un *Certificado* de personal al servicio de la Administración Pública emitidos por la FNMT-RCM cuando exista otro vigente a favor del mismo *Titular* y perteneciente a la misma *Ley de Emisión* conllevará la revocación del primero obtenido.

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

8.3.3.8. Revocación del Certificado de personal al servicio de la Administración Pública

8.3.3.8.1. Causas de revocación

84. Serán causas admitidas para la revocación de un *Certificado* las expuestas a continuación, si bien, la capacidad para su realización solamente se le reconoce al responsable de la *Oficina de Registro*.

85. Asimismo, se recuerda lo previsto en el apartado "Extinción de la vigencia del *Certificado*" 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*.

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

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

- Que la revocación se debiera haber efectuado por haberse extinguido el contrato suscrito con el *Suscriptor*
- Que la revocación le haya sido solicitada por la *Oficina de Registro* correspondiente a la entidad u organismo *Titular* siguiendo el procedimiento establecido para este tipo de *Certificados*
- Que la solicitud de revocación o la causa que la motiva, le haya sido notificada mediante resolución judicial o administrativa.
- Que en las causas c) a f) del presente apartado le sean acreditados dichos extremos fehacientemente, previa identificación del *Solicitante* de la revocación.

88. Teniendo en cuenta lo anterior, serán causas de revocación de un *Certificado* de personal al servicio de la Administración Pública:

a) La solicitud de revocación por parte de las personas autorizadas. En todo caso deberá dar lugar a esta solicitud:
   - La pérdida del soporte del Certificado.
   - La utilización por un tercero de los *Datos de Creación de Firma* del *Titular*, correspondientes a los *Datos de Verificación de Firma* contenidos en el *Certificado* y vinculados a la identidad personal del *Titular*.
   - La violación o puesta en peligro del secreto de los *Datos de Creación de Firma* del *Titular* o de los del responsable de la custodia de los *Datos de Creación de Firma*
   - La no aceptación de las nuevas condiciones que puedan suponer la emisión de nuevas *Declaraciones de Prácticas de Certificación*, durante el periodo de un mes tras su publicación

b) Resolución judicial o administrativa que así lo ordene.

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

d) Terminación de la forma de representación del Representante del *Titular* del *Certificado*

e) Incapacidad sobrevenida, total o parcial, del *Suscriptor*, *Titular* o de su representado.

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

g) Contravención de una obligación sustancial de esta *Declaración de Prácticas de Certificación* por parte del *Suscriptor*, *Titular* del *Certificado* o por parte de una *Oficina de Registro* si, en este último caso, hubiese podido afectar al procedimiento de emisión del *Certificado*.

h) Resolución del contrato suscrito entre el *Suscriptor*, *Titular* del *Certificado* o su representante, y la FNMT-RCM.

i) Violación o puesta en peligro del secreto de los *Datos de Creación de Firma* de la FNMT-RCM con los que firma los *Certificados* que emite.

89. En ningún caso se debe entender que la FNMT-RCM asume obligación alguna de comprobar los extremos mencionados en las letras c) a f) del presente apartado.

90. Las actuaciones constitutivas de delito o falta de las que no tenga conocimiento la FNMT-RCM que se realicen sobre los datos y/o *Certificado*, las inexactitudes sobre los datos o falta de diligencia en su comunicación a la FNMT-RCM, producirán la exoneración de responsabilidad de la FNMT-RCM.

8.3.3.8.2. Efectos de la revocación

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

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

8.3.3.8.3. Procedimiento para la revocación

93. La solicitud de revocación de los *Certificados* de personal al servicio de la Administración Pública podrá efectuarse durante el período de validez que consta en el *Certificado*.

94. 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*.

95. 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 de Prácticas de Certificación*.

96. 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*.

97. 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.

98. 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*.

99. 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.

100. 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*.

101. 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.

8.3.3.9. Suspensión del Certificado de personal al servicio de la Administración Pública

102. La suspensión de *Certificados* deja sin efectos el *Certificado* durante un período de tiempo y en unas condiciones determinadas.

103. 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.

8.3.3.9.1. Causas de la suspensión del Certificado

104. La FNMT-RCM podrá suspender la vigencia de los *Certificados* a solicitud del legítimo interesado o de Autoridad judicial o ante la existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los *Certificados* contempladas en el apartado "Causas de Revocación del Certificado de personal al servicio de la Administración Pública".

105. Asimismo, la solicitud de suspensión puede deberse a la existencia de una investigación o procedimiento judicial o administrativo en curso, cuya conclusión pueda determinar que el *Certificado* efectivamente está afectado por una causa de revocación. En estos casos la FNMT-RCM, a solicitud de legítimo interesado, suspenderá la vigencia del *Certificado* por el plazo requerido y, transcurrido este plazo, procederá a la revocación del *Certificado* salvo que a la FNMT-RCM se le solicite de forma fehaciente por el legítimo interesado la reactivación del mismo.

8.3.3.9.2. Efectos de la suspensión

106. La suspensión de *Certificados* deja sin efecto el *Certificado* (extingue su vigencia) durante un período de tiempo y en unas condiciones determinadas.

8.3.3.9.3. Procedimiento para la suspensión de Certificados

107. La suspensión de los *Certificados*, dada la naturaleza de éstos, 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.

108. 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.

109. Estas actividades serán realizadas por la *Oficina de Registro* de la entidad u organismo al que pertenece el *Titular*.

110. 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.

111. 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* 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.

8.3.3.10. Comprobación del estado del Certificado del personal al servicio de la Administración

112. 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 este apartado.

113. El estado del *Certificado* del personal al servicio de la Administración se podrá comprobar bien a través del acceso a las *Listas de Revocación*, bien a través del *Servicio de información y consulta del estado de los Certificados* a través de OCSP.

114. Estos servicios estarán disponible las veinticuatro (24) horas del día, todos los días del año, salvo por circunstancias ajenas a la FNMT-RCM u operaciones de mantenimiento. La FNMT-RCM notificará esta última circunstancia en la dirección http://www.ceres.fnmt.es si es posible con al menos cuarenta y ocho (48) horas de antelación y tratará de solventarla en un periodo no superior a veinticuatro (24) horas

115. La FNMT-RCM dispone de un servicio de respuesta OCSP ("OCSP responder") para ofrecer el *Servicio de información y consulta del estado de los certificados* bajo los términos suscritos en el correspondiente convenio, contrato o *Ley de Emisión*.

116. El servicio funciona de la siguiente manera: El servidor OCSP recibe la petición OCSP efectuada por un Cliente OCSP registrado en el sistema y comprueba el estado de los *Certificados* incluidos en la misma. En caso de que la petición sea válida, se emitirá una respuesta de OCSP informando acerca del estado en el que se encuentran en ese momento los Certificados incluidos en la petición.

117. Será responsabilidad de la *Entidad usuaria* obtener un *Cliente OCSP* para operar con el servidor OCSP puesto a disposición por la FNMT-RCM.

118. Es responsabilidad de la *Entidad usuaria* solicitante del servicio OCSP obtener, en su caso, el consentimiento del *Titular* del *Certificado* sobre el que se solicita el servicio OCSP, así como informar a este *Titular* de las condiciones y limitaciones correspondientes.

119. Lo anterior se entiende con el alcance y limites de la legislación sobre tratamiento automatizado de datos de carácter personal y de conformidad con los correspondientes contratos, convenios o Leyes de Emisión por los que se regula el servicio de certificación electrónica de la FNMT-RCM.

120. FNMT-RCM no proporciona *Servicio de información y consulta del estado de los 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*.

8.3.4. 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.

121. 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.

8.3.5. Modelos de formulario

122. 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.

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

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

9.1.1. Identificación

123. 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.

124. 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: *Política de Certificación* de *Certificados* para la identificación de sedes electrónicas de la Administración Pública, Organismos y entidades públicas vinculadas o dependientes

Referencia / OID[4]:

- 1.3.6.1.4.1.5734.3.12
- 1.3.6.1.4.1.5734.3.3.2.2

Versión: 1.2

Fecha de emisión: 1 de agosto de 2010

Localización: http://www.cert.fnmt.es/dpcs/

---

[4] *Nota*: El OID o identificador de política es una referencia que se incluirá en el *Certificado* al objeto de que los usuarios puedan determinar las prácticas y procedimientos de aplicación para la emisión del *Certificado* en cuestión.

Si bien en este documento se desarrolla una sola política para este tipo de *Certificados*, pueden existir dos referencias diferentes a ella para diferenciar o identificar particularidades en los perfiles de *Certificados*, *Autoridad de Certificación* empleada para su emisión o procedimientos de emisión de los mismos.

Así pues, la *Política y Prácticas de Certificación* de los *Certificados* para la identificación de sedes describirá de forma única, identificándose cuantas particularidades puedan existan y asociándolas a los OID o referencias que correspondan.

DPC relacionada: Declaración General de Prácticas de Certificación de la FNMT-RCM

Localización: http://www.cert.fnmt.es/dpcs/

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

125. 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.

126. 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*.

127. 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.

128. 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.

129. 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*.

130. Lo dispuesto anteriormente se entenderá sin perjuicio de lo ordenado por resolución administrativa o judicial.

131. 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.

132. 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.

133. 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.

134. 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*.

135. 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*.

136. 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*.

137. 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.

138. 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.

139. Por consiguiente, el *Certificado* emitido para la identificación de *sedes electrónicas* no se regirá 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 cita 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.

9.1.3. Gestión de la Política de Certificación

140. 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 está 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*.
- Para identificar la *Política de Certificación* aquí desarrollada, se dispone de los OIDs específicos:
  - 1 .3.6.1.4.1.5734.3.12
  - 1.3.6.1.4.1.5734.3.3.2.2

141. 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 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.

9.1.4. Comunidad y ámbito de aplicación

142. 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 está *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.

143. 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.

9.1.5. Responsabilidad y obligaciones de las partes

144. 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.

145. 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.

146. 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.

147. 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.

148. 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.

149. 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.

150. 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.*

9.1.6. Límites de uso de los Certificados para la identificación de sedes electrónicas

151. 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.

152. 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

9.2. 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

153. 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.*

154. En especial deberá tenerse presente, a efectos interpretativos del presente anexo el apartado "Definiciones" del cuerpo principal de la *Declaración General de Practicas de Certificación*.

155. 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 ó 1.3.6.1.4.1.5734.3.3.2.2.

9.2.1. Servicios de Gestión de las *Claves* de los Usuarios y *Titulares*

156. 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*.

9.2.2. Gestión del ciclo de vida de los Certificados

9.2.2.1. Registro de los Titulares de Certificados de sede electrónica ámbito público

157. 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*.

158. 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 C*ertificados* 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*.

159. 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.

160. 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.

9.2.2.2. Procedimiento de solicitud del Certificado para la identificación de sedes electrónicas

161. 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*.

162. 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*.

163. 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*.

164. 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.*

9.2.2.3. Presolicitud

165. 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.

166. 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

167. 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.

168. 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*

169. 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/

170. 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.

171. 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*.

172. 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*.

173. 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*.

9.2.2.4. Confirmación de las identidades y requisitos de las partes

174. 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*.

9.2.2.5. Personación del Solicitante ante las Oficinas de Registro

175. 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*.

176. 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*.

9.2.2.6. Comparecencia y documentación

177. 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*

178. 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.*

9.2.2.7. Envío de información a la FNMT-RCM

179. 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.

180. 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.*

181. 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.

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

182. 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.

183. 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.

9.2.2.9. Emisión del Certificado para la identificación de sede electrónica

184. 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*.

185. 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 vinculo 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.

186. 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.

187. 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*.

188. 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.

189. 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 Publica* vinculada a la identidad del *Titular* del mismo. Para ello la FNMT-RCM comprobará la correspondencia entre la *Clave privada* y la *Clave pública*.
- Lograr que la información incluida en el *Certificado* se base en la información proporcionada por el *Solicitante* 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.

190. 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

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*, puede consultarse en los anexos al presente documento.

   En ellos se describen los perfiles de los *Certificados* diferenciándose según la *Autoridad de Certificación* que los emite (siempre subordinada a la *Autoridad de Certificación Raíz* de la FNMT-RCM).

   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*

   Nombre extensión: extKeyUsage

   Valores: Autenticación de servidor: 1.3.6.1.5.5.7.3.1

9.2.2.10. Publicación del Certificado de identificación de sede electrónica

191. 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.

9.2.2.11. Descarga e instalación del Certificado de identificación de sede electrónica

192. 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:

https://www.cert.fnmt.es/index.php?cha=adm&sec=23&fpage=62&lang=es

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

194. 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.

195. 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.

9.2.2.12. Vigencia del Certificado de identificación de sede electrónica

9.2.2.12.1. Caducidad

196. Los *Certificados* de identificación de sede electrónica emitidos por la FNMT-RCM tendrán validez durante un período de cuatro (4) años contados a partir del momento de la emisión del *Certificado*, siempre y cuando no se extinga su vigencia. Transcurrido este período y si el *Certificado* sigue activo, caducará, siendo necesaria la emisión de uno nuevo en caso de que el *Titular* desee seguir utilizando los servicios del *Prestador de Servicios de Certificación.*

9.2.2.12.2. Extinción de la vigencia del Certificado

197. Los *Certificados* de identificación de sede electrónica emitidos por la FNMT-RCM quedarán sin efecto en los siguientes casos:

a) Terminación del período de validez del *Certificado*

b) Cese en la actividad como *Prestador de Servicios de Certificación* de la FNMT-RCM, salvo que, previo consentimiento expreso del *Suscriptor* y *Titular*, los *Certificados* expedidos por la FNMT-RCM hayan sido transferidos a otro *Prestador de Servicios de Certificación*.

En estos dos casos [a) y b)], la perdida de eficacia de los *Certificados* tendrá lugar desde que estas circunstancias se produzcan.

c) Suspensión o revocación del *Certificado* por cualquiera de las causas recogidas en el presente documento

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

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

9.2.2.13. Revocación del Certificado de identificación de sede electrónica

9.2.2.13.1. Causas de revocación

200. Serán causas admitidas para la revocación de un *Certificado* las expuestas a continuación. La *Ley de Emisión* podrá, adicionalmente, establecer otras causas de revocación, suspensión y cancelación de la suspensión.

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

- Que la revocación se debiera haber efectuado por haberse extinguido el contrato suscrito con el *Suscriptor*.

- Que la revocación le haya sido solicitada por la *Oficina de Registro* correspondiente a la entidad u organismo *Titular* siguiendo el procedimiento establecido para este tipo de *Certificados*
- Que la solicitud de revocación o la causa que la motiva, le haya sido notificada mediante resolución judicial o administrativa.
- Que en las causas c) a g) del presente apartado le sean acreditados dichos extremos fehacientemente, previa identificación del solicitante de la revocación.

202. Teniendo en cuenta lo anterior, serán causas de revocación de un *Certificado* de identificación de sede electrónica:

a) La solicitud de revocación por parte de las personas autorizadas. En todo caso deberá dar lugar a esta solicitud:
   - Pérdida del soporte del *Certificado*.
   - La utilización por un tercero de los *Datos de Creación de Firma* del *Titular*, correspondientes a los *Datos de Verificación de Firma* contenidos en el *Certificado* y vinculados a la identidad personal del *Titular*.
   - La violación o puesta en peligro del secreto de los *Datos de Creación de Firma* del *Titular* o de los del responsable de la custodia de los *Datos de Creación de Firma*.
   - La no aceptación de las nuevas condiciones que puedan suponer la emisión de nuevas *Declaraciones de Prácticas de Certificación*, durante el periodo de un mes tras su publicación.

b) Resolución judicial o administrativa que así lo ordene.

c) Extinción, disolución o cierre de la sede electrónica

d) Extinción o disolución de la personalidad jurídica del *Suscriptor* o *Titular*.

e) Terminación de la forma de representación del representante del *Titular* del *Certificado*

f) Incapacidad sobrevenida, total o parcial, del *Suscriptor*, *Titular* o de su representado.

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

h) Contravención de una obligación sustancial de esta *Declaración de Prácticas de Certificación* por parte del *Suscriptor*, *Titular* del *Certificado* o por parte de una *Oficina de Registro* si, en este último caso, hubiese podido afectar al procedimiento de emisión del *Certificado*.

i) Resolución del contrato suscrito entre el *Suscriptor*, *Titular* del *Certificado* o su representante, y la FNMT-RCM.

j) Violación o puesta en peligro del secreto de los *Datos de Creación de Firma* de la FNMT-RCM, con los que firma los *Certificados* que emite.

203. En ningún caso se debe entender que la FNMT-RCM asume obligación alguna de comprobar los extremos mencionados en las letras c) a g) del presente apartado.

204. Las actuaciones constitutivas de delito o falta de las que no tenga conocimiento la FNMT-RCM que se realicen sobre los datos o *Certificado*, las inexactitudes sobre los datos o falta de diligencia en su comunicación a la FNMT-RCM, producirán la exoneración de responsabilidad de la FNMT-RCM.

9.2.2.13.2. Efectos de la revocación

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

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

9.2.2.13.3. Procedimiento para la revocación

207. La solicitud de revocación de los *Certificados* de identificación de sede electrónica podrá efectuarse durante el período de validez que consta en el *Certificado*.

208. 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

209. 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 siempre en el marco de los términos y condiciones acerca de la revocación de *Certificados* en la *Declaración de Prácticas de Certificación*.

210. 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*. En todo caso FNMT-RCM,

presumirá la competencia y capacidad del *Solicitante* cuando se trate del responsable de la *Oficina de Registro* correspondiente

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.

211. 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.

9.2.2.14. Suspensión del Certificado de identificación de sede electrónica

212. La suspensión de *Certificados* deja sin efectos el Certificado durante un período de tiempo y en unas condiciones determinadas.

213. 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.

9.2.2.14.1. Causas de suspensión

214. La FNMT-RCM podrá suspender la vigencia de los *Certificados* a solicitud del legítimo interesado o de Autoridad judicial o ante la existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los *Certificados* contempladas en el apartado "Causas de Revocación del Certificado de identificación de sede electrónica".

215. Asimismo, la solicitud de suspensión puede deberse a la existencia de una investigación o procedimiento judicial o administrativo en curso, cuya conclusión pueda determinar que el *Certificado* efectivamente está afectado por una causa de revocación. En estos casos la FNMT-RCM, a solicitud de legítimo interesado, suspenderá la vigencia del *Certificado* por el plazo requerido, y transcurrido este plazo, procederá a la revocación del *Certificado* salvo que a la FNMT-RCM se le solicite de forma fehaciente por el legítimo interesado la reactivación del mismo.

9.2.2.14.2. Efectos de la suspensión

216. La suspensión de *Certificados* deja sin efecto el *Certificado* (extingue su vigencia) durante un período de tiempo y en unas condiciones determinadas.

9.2.2.14.3. Procedimiento para la suspensión

217. 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.

218. 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 y en su caso se formaliza la solicitud de suspensión de un *Certificado* por parte de un legítimo interesado.

219. Estas actividades serán realizadas por la *Oficinas de Registro* de la entidad u organismo al que pertenece el *Titular*.

220. 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.

221. 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 identificación de sede electrónica

   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.

   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.

   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.

   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.

   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

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.

9.2.2.15. Comprobación del estado del Certificado de identificación de sede electrónica

222. 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 este apartado.

223. El estado del *Certificado* de de identificación de sede electrónica se podrá comprobar bien a través del acceso a las *Listas de Revocación*, bien a través del *Servicio de información y consulta del estado de los certificados* a través del protocolo OCSP.

224. Estos servicios estarán disponible las veinticuatro (24) horas del día, todos los días del año, salvo por circunstancias ajenas a la FNMT-RCM u operaciones de mantenimiento. La FNMT-RCM notificará esta última circunstancia en la dirección http://www.ceres.fnmt.es si es posible con al menos cuarenta y ocho (48) horas de antelación y tratará de solventarla en un periodo no superior a veinticuatro (24) horas

225. La FNMT-RCM dispone de un servicio de respuesta OCSP ("OCSP responder") para ofrecer *Servicio de información y consulta del estado de los certificados* bajo los términos suscritos en el correspondiente convenio, contrato o *Ley de Emisión*.

226. El servicio funciona de la siguiente manera: El servidor OCSP recibe la petición OCSP efectuada por un *Cliente OCSP* registrado en el sistema y comprueba el estado de los *Certificados* incluidos en la misma. En caso de que la petición sea válida, se emitirá una respuesta de OCSP informando acerca del estado en el que se encuentran en ese momento los *Certificados* incluidos en la petición.

227. Será responsabilidad de la Entidad usuaria obtener un *Cliente OCSP* para operar con el servidor OCSP puesto a disposición por la FNMT-RCM.

228. Es responsabilidad de la entidad usuaria solicitante del servicio OCSP obtener, en su caso, el consentimiento del *Titular* del *Certificado* sobre el que se solicita el servicio OCSP, así como informar a este titular de las condiciones y limitaciones correspondientes.

229. Lo anterior se entiende con el alcance y limites de la legislación sobre tratamiento automatizado de datos de carácter personal y de conformidad con los correspondientes contratos, convenios o *Leyes de Emisión* por los que se regula el servicio de certificación electrónica de la FNMT-RCM.

230. 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*.

231. 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.

9.2.3. 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.

232. 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.

9.2.4. Modelos de formulario

233. 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

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

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

10.1.1. Identificación

234. 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.

235. 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: *Política de Certificación* de *Certificados* para la actuación administrativa automatizada de la Administración Pública, organismos y entidades públicas vinculadas o dependientes

Referencia / OID[5]:

- 1.3.6.1.4.1.5734.3.13
- 1.3.6.1.4.1.5734.3.3.3.2

Versión: 1.2

Fecha de emisión: 1 de agosto de 2010

Localización: http://www.cert.fnmt.es/dpcs/

DPC relacionada: Declaración General de Prácticas de Certificación de la FNMT-RCM

[5] *Nota*: El OID o identificador de política es una referencia que se incluirá en el *Certificado* al objeto de que los usuarios puedan determinar las prácticas y procedimientos de aplicación para la emisión del *Certificado* en cuestión.

Si bien en este documento se desarrolla una sola política para este tipo de *Certificados*, pueden existir dos referencias diferentes a ella para diferenciar o identificar particularidades en los perfiles de *Certificados*, *Autoridad de Certificación* empleada para su emisión o procedimientos de emisión de los mismos.

Así pues, la *Política y Prácticas de Certificación* de los *Certificados* para la identificación de sedes describirá de forma única, identificándose cuantas particularidades puedan existan y asociándolas a los OID o referencias que correspondan.

Localización: http://www.cert.fnmt.es/dpcs/

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

236. 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.

237. La *persona física* actúa como firmante de las actuaciones administrativas automatizas y custodio 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.

238. 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.

239. 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.

240. 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.

241. 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.

242. 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*.

243. 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*.

244. 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*.

245. 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.

246. 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*.

10.1.3. Gestión de la Política de Certificación

247. 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*.
- Para identificar la *Política de Certificación* aquí desarrollada, se dispone de los OIDs específicos:
  - 1.3.6.1.4.1.5734.3.13
  - 1.3.6.1.4.1.5734.3.3.3.2

248. 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 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.

10.1.4. Comunidad y ámbito de aplicación

249. 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 está *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 está *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

250. 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.

10.1.5. Responsabilidad y obligaciones de las partes

251. 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

252. 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*.

253. 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*

254. 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.

255. 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.

256. 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.

257. 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.

10.1.6. Límites de uso de los Certificados para la actuación administrativa automatizada mediante sellos electrónicos

258. 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.

259. 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.

260. 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 Usuaria*.

261. 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*.

262. 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.

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

263. 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.*

264. En especial deberá tenerse presente, a efectos interpretativos del presente anexo el apartado "Definiciones" del cuerpo principal de la *Declaración General de Practicas de Certificación*.

265. 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 ó 1.3.6.1.4.1.5734.3.3.3.2

10.2.1. Servicios de Gestión de las *Claves* de los Usuarios y *Titulares*

266. 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.

10.2.2. Gestión del ciclo de vida de los Certificados

10.2.2.1. Registro de los Titulares

267. 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*.

268. 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 C*ertificados* 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*.

269. 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.

270. 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.

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

271. 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.

272. 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.

273. 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.

274. 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.

275. Dado que la FNMT-RCM no mantiene relación jurídica funcionarial, 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.

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

276. 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*.

277. 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 univoca e inequívocamente con unos *datos de creación de firma* bajo la custodia de dicho firmante/custodio.

278. 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*.

279. 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.

280. 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 Publica* vinculada a la identidad del *Titular* del mismo. Para ello la FNMT-RCM comprobará la correspondencia entre la *Clave privada* y la *Clave pública*.
- Lograr que la información incluida en el *Certificado* se base en la información proporcionada por el *Solicitante* 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.

281. 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

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*, puede consultarse en los anexos al presente documento.

   En ellos se describen los perfiles de los *Certificados* diferenciándose según la *Autoridad de Certificación* que los emite (siempre subordinada a la *Autoridad de Certificación Raíz* de la FNMT-RCM).

10.2.2.4. Publicación del Certificado para la actuación administrativa automatizada

282. 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

10.2.2.5. Descarga e instalación del Certificado para la actuación administrativa automatizada

283. 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

284. 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:

https://www.cert.fnmt.es/index.php?cha=adm&sec=23&fpage=62&lang=es

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

286. En este proceso guiado se le pedirá, al responsable de la *Oficina de Registro* del ámbito del *Titular,* que introduzca el NIF 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.

287. 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.

10.2.2.6. Vigencia del Certificado para la actuación administrativa automatizada

10.2.2.6.1. Caducidad

288. Los *Certificados* para la actuación administrativa automatizada emitidos por la FNMT-RCM tendrán validez durante un período de cuatro (4) años contados a partir del momento de la emisión del *Certificado*, siempre y cuando no se extinga su vigencia. Transcurrido este período y si el *Certificado* sigue activo, caducará, siendo necesaria la emisión de uno nuevo en caso de que el *Titular* desee seguir utilizando los servicios del *Prestador de Servicios de Certificación*.

10.2.2.6.2. Extinción de la vigencia del Certificado

289. Los *Certificados* para la actuación administrativa automatizada emitidos por la FNMT-RCM quedarán sin efecto en los siguientes casos:

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

b) Cese en la actividad como *Prestador de Servicios de Certificación* de la FNMT-RCM, salvo que, previo consentimiento expreso del *Suscriptor* y *Titular*, los *Certificados* expedidos por la FNMT-RCM hayan sido transferidos a otro *Prestador de Servicios de Certificación*.

En estos dos casos [a) y b)], la perdida de eficacia de los *Certificados* tendrá lugar desde que estas circunstancias se produzcan.

c) Suspensión o revocación del *Certificado* por cualquiera de las causas recogidas en el presente documento

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

10.2.2.7. Revocación del Certificado para la actuación administrativa automatizada

10.2.2.7.1. Causas de Revocación

291. Serán causas admitidas para la revocación de un *Certificado* las expuestas a continuación. La *Ley de Emisión* podrá, adicionalmente, establecer otras causas de revocación, suspensión y cancelación de la suspensión.

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

- Que la revocación se debiera haber efectuado por haberse extinguido el contrato suscrito con el *Suscriptor*.
- Que la revocación le haya sido solicitada por la *Oficina de Registro* correspondiente a la entidad u organismo *Titular* siguiendo el procedimiento establecido para este tipo de *Certificados*
- Que la solicitud de revocación o la causa que la motiva, le haya sido notificada mediante resolución judicial o administrativa.
- Que en las causas c) a f) del presente apartado le sean acreditados dichos extremos fehacientemente, previa identificación del solicitante de la revocación.

293. Teniendo en cuenta lo anterior, serán causas de revocación de un *Certificado* para la actuación administrativa automatizada:

a) La solicitud de revocación por parte de las personas autorizadas. En todo caso deberá dar lugar a esta solicitud:
   - Pérdida del soporte del *Certificado*.
   - La utilización por un tercero de los *Datos de Creación de Firma del Titular*, correspondientes a los *Datos de Verificación de Firma* contenidos en el *Certificado* y vinculados a la identidad personal del *Titular*.
   - La violación o puesta en peligro del secreto de los *Datos de Creación de Firma* del *Titular* o de los del responsable de la custodia de los *Datos de Creación de Firma*.
   - La no aceptación de las nuevas condiciones que puedan suponer la emisión de nuevas *Declaraciones de Prácticas de Certificación*, durante el periodo de un mes tras su publicación.

b) Resolución judicial o administrativa que así lo ordene.

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

d) Terminación de la forma de representación del representante del *Titular* del *Certificado*

e) Incapacidad sobrevenida, total o parcial, del *Suscriptor*, *Titular* o de su representado.

f) Inexactitudes en los datos aportados por el *Solicitante* para la obtención del *Certificado*, o alteración de los datos aportados para la obtención del *Certificado* o modificación de las circunstancias verificadas para la expedición del *Certificado*,

como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.

g) Contravención de una obligación sustancial de esta *Declaración de Prácticas de Certificación* por parte del *Suscriptor*, *Titular* del *Certificado* o por parte de una *Oficina de Registro* si, en este último caso, hubiese podido afectar al procedimiento de emisión del *Certificado*.

h) Resolución del contrato suscrito entre el *Suscriptor*, *Titular* del *Certificado* o su representante, y la FNMT-RCM.

i) Violación o puesta en peligro del secreto de los *Datos de Creación de Firma* de la FNMT-RCM, con los que firma los *Certificados* que emite.

294. En ningún caso se debe entender que la FNMT-RCM asume obligación alguna de comprobar los extremos mencionados en las letras c) a f) del presente apartado.

295. Las actuaciones constitutivas de delito o falta de las que no tenga conocimiento la FNMT-RCM que se realicen sobre los datos y/o certificado, las inexactitudes sobre los datos o falta de diligencia en su comunicación a la FNMT-RCM, producirán la exoneración de responsabilidad de la FNMT-RCM.

10.2.2.7.2. Efectos de la revocación

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

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

10.2.2.7.3. Procedimiento para la revocación de Certificados

298. La solicitud de revocación de los *Certificados* para la actuación administrativa automatizada podrá efectuarse durante el período de validez que consta en el *Certificado*.

299. 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

300. Estarán legitimados para solicitar la revocación de un *Certificado* para la actuación administrativa automatizada, en base a la inexactitud de datos, 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 respecto a lo consignado en el *Certificado* 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*.

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

301. 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*. En todo caso FNMT-RCM, presumirá la competencia y capacidad del solicitante cuando se trate del responsable de la *Oficina de Registro* correspondiente

1. Personación del *Solicitante* ante la *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.

302. 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.

10.2.2.8. Suspensión del Certificado para la actuación administrativa automatizada

303. La suspensión de *Certificados* deja sin efectos el *Certificado* durante un período de tiempo y en unas condiciones determinadas.

304. 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.

10.2.2.8.1. Causas de la suspensión

305. La FNMT-RCM podrá suspender la vigencia de los *Certificados* a solicitud del legítimo interesado o de Autoridad judicial o ante la existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los *Certificados* contempladas en el apartado "Causas de Revocación del Certificado para la actuación administrativa automatizada".

306. Asimismo, la solicitud de suspensión puede deberse a la existencia de una investigación o procedimiento judicial o administrativo en curso, cuya conclusión pueda determinar que el *Certificado* efectivamente está afectado por una causa de revocación. En estos casos la FNMT-RCM, a solicitud de legítimo interesado suspenderá la vigencia del *Certificado* por el plazo requerido y, transcurrido este plazo, procederá a la revocación del *Certificado* salvo que a la FNMT-RCM se le solicite de forma fehaciente por el legítimo interesado la reactivación del mismo.

10.2.2.8.2. Efectos de la suspensión

307. La suspensión de *Certificados* deja sin efecto el *Certificado* (extingue su vigencia) durante un período de tiempo y en unas condiciones determinadas.

10.2.2.8.3. Procedimiento para la suspensión de Certificados

308. 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.

309. 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 y en su caso se formaliza la solicitud de suspensión de un *Certificado* por parte de un legítimo interesado.

310. Estas actividades serán realizadas por la *Oficina de Registro* de la entidad u organismo al que pertenece el *Titular*.

311. 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.

312. 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 para la actuación administrativa automatizada

   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.

   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.

   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.

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.

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

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.

10.2.2.9. Comprobación del estado del Certificado para la actuación administrativa automatizada

313. 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 este apartado.

314. El estado del *Certificado* para la actuación administrativa automatizada se podrá comprobar bien a través del acceso a las *Listas de Revocación*, bien a través del servicio de consulta del estado de los *Certificados* a través de OCSP.

315. Estos servicios estarán disponible las veinticuatro (24) horas del día, todos los días del año, salvo por circunstancias ajenas a la FNMT-RCM u operaciones de mantenimiento. La FNMT-RCM notificará esta última circunstancia en la dirección http://www.ceres.fnmt.es si es posible con al menos cuarenta y ocho (48) horas de antelación y tratará de solventarla en un periodo no superior a veinticuatro (24) horas

316. La FNMT-RCM dispone de un servicio de respuesta OCSP ("OCSP responder") para ofrecer servicio de información del estado de los *Certificados* bajo los términos suscritos en el correspondiente convenio, contrato o *Ley de Emisión*.

317. El servicio funciona de la siguiente manera: El servidor OCSP recibe la petición OCSP efectuada por un *Cliente OCSP* registrado en el sistema y comprueba el estado de los *Certificados* incluidos en la misma. En caso de que la petición sea válida, se emitirá una respuesta de OCSP informando acerca del estado en el que se encuentran en ese momento los *Certificados* incluidos en la petición.

318. Será responsabilidad de la *Entidad usuaria* obtener un *Cliente OCSP* para operar con el servidor OCSP puesto a disposición por la FNMT-RCM.

319. Es responsabilidad de la entidad usuaria solicitante del servicio OCSP obtener, en su caso, el consentimiento del *Titular* del *Certificado* sobre el que se solicita el servicio OCSP, así como informar a este titular de las condiciones y limitaciones correspondientes.

320. Lo anterior se entiende con el alcance y limites de la legislación sobre tratamiento automatizado de datos de carácter personal y de conformidad con los correspondientes contratos, convenios o Leyes de Emisión por los que se regula el servicio de certificación electrónica de la FNMT-RCM.

321. FNMT-RCM no proporciona *Servicio de información y consulta sobre el estado de los 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*.

322. 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.

10.2.3. 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.

323. 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.

10.2.4. Modelos de formulario

324. 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

ANEXO I: IDENTIFICACIÓN DE CERTIFICADOS DE AUTORIDADES DE CERTIFICACIÓN

Las Autoridades de Certificación implicadas en el servicio utilizan para la firma de certificados y CRLs los certificados identificados a continuación:

Certificado Raíz de la FNMT

- Nombre distintivo: OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
- Número de serie: 00 81 bb dd 6b 24 1f da b4 be 8f 1b da 08 55 c4
- Período de validez desde: miércoles, 29 de octubre de 2008 17:59:55
- Período de validez hasta: martes, 01 de enero de 2030 2:00:00
- Huella digital (sha1): b8 65 13 0b ed ca 38 d2 7f 69 92 94 20 77 0b ed 86 ef bc 10

Certificado de la Autoridad de Certificación "AC APE"

- Nombre distintivo: OU = AC APE, O = FNMT-RCM, C = ES
- Número de serie: 10
- Período de validez desde: miércoles, 05 de noviembre de 2008 14:18:40
- Período de validez hasta: viernes, 03 de noviembre de 2023 17:38:33
- Huella digital (sha1): 8a 8e 8d 48 bc 44 f7 9d 80 67 f8 0f 14 1e c5 a0 a9 97 99 d5

Certificado de la Autoridad de Certificación "AC Administración Pública"

- Nombre distintivo: CN = AC Administración Pública, serialNumber = Q2826004J, OU = CERES, O = FNMT-RCM, C = ES
- Número de serie: 01
- Período de validez desde: viernes, 21 de mayo de 2010 11:26:24
- Período de validez hasta: sábado, 21 de mayo de 2022 11:52:26
- Huella digital (sha1): 1c 5b fa a3 dd e8 c5 a4 a9 09 d1 10 37 a5 0a ec 0b 4b 21 ec

ANEXO II: PERFILES DE CERTIFICADOS DE AUTORIDADES DE CERTIFICACIÓN

CERTIFICADO RAÍZ DE LA FNMT-RCM

CERTIFICADO RAÍZ DE LA FNMT-RCM			
CAMPO	**CONTENIDO**	**CRÍTICA**	**OBSERVACIONES**
Campos de X509v1			
1. Versión	V3		
2. Serial Number	Aleatorio		*[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 Sha256withRsaEncryption Sha512withRsaEncryption		OID: 1.2.840.113549.1.1.5 OID: 1.2.840.113549.1.1.11 OID: 1.2.840.113549.1.1.13 Norma PKCS#1 v2.1 y RFC 3447.
4. Issuer Distinguished Name	OU=AC RAIZ FNMT -RCM O=FNMT-RCM C=ES		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*.
5. Validez	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. *[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 and expressed as Zulu time (Universal Coordinated Time).*
6. Subject	OU=AC RAIZ FNMT -RCM O=FNMT-RCM C=ES		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*. Coincidirá con el campo emisor del certificado de las AC subordinada. *[RFC3280]: The issuer name MUST be a non-empty DName. Processing components MUST be prepared to receive the following attributes: countryName,* *organizationName, organizationalUnitName, distinguishedNameQualifier, stateOrProvinceName, commonName, serialNumber, and domainComponent. Processing components SHOULD be prepared for attributes: localityName, title, surname, givenName, initials, pseudonym, and generationQualifier* *[ETSI-QC]: the issuer name MUST contain the countryName attribute. The specified country MUST be the country where the issuer CA is established.* *[ETSI-CPN]: the issuer name MUST contain the countryName and the organizationName attributes.*

CERTIFICADO RAÍZ DE LA FNMT-RCM			
CAMPO	**CONTENIDO**	**CRÍTICA**	**OBSERVACIONES**
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: 4096 bits		
Campos de X509v2			
1. issuerUniqueIdentifier	No se utilizará		
2. subjectUniqueIdentifier	No se utilizará		
Extensiones de X509v3			
1. Subject Key Identifier	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 *subjectPublicKey* del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
2. Authority Key Identifier	No procede		
3. KeyUsage		SI (RFCs 3280 y 3739)	
Digital Signature	0		
Non Repudiation	0		
Key Encipherment	0		
Data Encipherment	0		
Key Agreement	0		
Key Certificate Signature	1		
CRL Signature	1		
4.extKeyUsage	No se utilizará		
5. privateKeyUsagePeriod	No se utilizará		
6. Certificate Policies		NO	[RFC 3739] obliga la existencia de al menos un valor. 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. *[RFC3280]: PolicyInformation SHOULD only contain an OID* *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 }.* *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*

CERTIFICADO RAÍZ DE LA FNMT-RCM			
CAMPO	**CONTENIDO**	**CRÍTICA**	**OBSERVACIONES**
Policy Identifier	anyPolicy 2 5 29 32 0		
URL CPS	http://www.cert.fnmt.es/dpcs/		
Notice Reference	NO para los certificados de AC, según RFC 5280 (sustituta de RFC 3280).		
7. Policy Mappings	No se utilizará		
8. Subject Alternate Names	No se utilizará	NO	
9. Issuer Alternate Names	No se utilizará		
10. Subject Directory Attributes	No se utilizará		
11. Basic Constraints		SI (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. *[RFC3280] This extension MUST appear as a critical extension in all CA certificates that contain public keys used to validate digital signatures on certificates.*
Subject Type	CA		
Path Length Constraint	Ninguno		
12. Policy Constraints	No utilizado		
13. CRLDistributionPoints	No utilizado		La revocación del certificado Raíz se publicitará por otros mecanismos.
14. Auth. Information Access	No procede	NO (RFC 3280)	
15.netscapeCertType	No procede		
16. netscapeRevocationURL	No procede		
17. netscapeCAPolicyURL	No procede		
18. netscapeComment	No procede		

Tabla 1 - Certificado raíz de la FNMT-RCM

CERTIFICADO AUTORIDAD DE CERTIFICACIÓN "AC APE"

Certificado Autoridad de Certificación "AC APE"			
CAMPO	**CONTENIDO**	**CRÍTICA**	**OBSERVACIONES**
Campos de X509v1			
1. Versión	V3		
2. Serial Number	Aleatorio		*[RFC3280]: the serial number MUST be a positive integer, not longer than 20 octets (1 < SN < 2^{159}). Processing components MUSTbe able to interpret such long numbers.*
3. Signature Algorithm	Sha1withRsaEncryption Sha256withRsaEncryption Sha512withRsaEncryption		OID: 1.2.840.113549.1.1.5 OID: 1.2.840.113549.1.1.11 OID: 1.2.840.113549.1.1.13 Norma PKCS#1 v2.1 y RFC 3447.
4. Issuer Distinguished Name	OU= AC RAIZ FNMT-RCM O=FNMT-RCM C=ES		Coincide con el campo asunto del certificado de la AC Raíz. Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*. [ETSI-CPN]: *the issuer name MUST contain the countryName and the organizationName attributes.*
5. Validez	Hasta 03/11/2023		15 años a partir de la constitución de la AC.
6. Subject	OU=AC APE O=FNMT-RCM C=ES		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*.
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: 2048 bits		
Campos de X509v2			
1. issuerUniqueIdentifier	No se utilizará		
2. subjectUniqueIdentifier	No se utilizará		
Extensiones de X509v3			
1. Subject Key Identifier	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 *subjectPublicKey* del sujeto (excluyendo etiqueta, longitud y número de bits no usados).

Certificado Autoridad de Certificación "AC APE"			
CAMPO	**CONTENIDO**	**CRÍTICA**	**OBSERVACIONES**
2. Authority Key Identifier	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 *subjectPublicKey* de la AC emisora (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo *Subject Key Identifier* de la AC emisora (AC Raíz).
3. KeyUsage		SI (RFCs 3280 y 3739)	
Digital Signature	0		
Non Repudiation	0		
Key Encipherment	0		
Data Encipherment	0		
Key Agreement	0		
Key Certificate Signature	1		
CRL Signature	1		
4.extKeyUsage	No se utilizará		
5. privateKeyUsagePeriod	No se utilizará		
6. Certificate Policies		NO	RFC 3739 obliga la existencia de al menos un valor.
Policy Identifier	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.
URL CPS	http://www.cert.fnmt.es/dpcs/		*[RFC3280]: PolicyInformation SHOULD only contain an OID.*
Notice Reference	NO para los certificados de AC, según RFC 5280 (sustituta de RFC 3280).		*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 }.* *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*
7. Policy Mappings	No se utilizará		
8. Subject Alternate Names	No se utilizara	NO	
9. Issuer Alternate Names	No se utilizará		
10. Subject Directory Attributes	No se utilizará		

Certificado Autoridad de Certificación "AC APE"			
CAMPO	**CONTENIDO**	**CRÍTICA**	**OBSERVACIONES**
11. Basic Constraints		SI	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 dependientes de esta.
Subject Type	CA	(RFC 3280)	
Path Length Constraint	0		[RFC3280] This extension MUST appear as a critical extension in all CA certificates that contain public keys used to validate digital signatures on certificates.
12. Policy Constraints	No utilizado		
13. CRLDistributionPoints	LDAP: ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU= AC RAIZ FNMT-RCM, O=FNMT-RCM, C=ES ?authorityRevocationList;binary?base ?objectclass=cRLDistributionPoint HTTP: http://www.cert.fnmt.es/crls/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 *Auth. Information Access*.
14. Auth. Information Access	No		Contendrá información de localización del OCSP Responder de la FNMT.
15.netscapeCertType	No procede		
16. netscapeRevocationURL	No procede		
17. netscapeCAPolicyURL	No procede		
18. netscapeComment	No procede		

Tabla 2 - Certificado Autoridad de Certificación "AC APE"

CERTIFICADO AUTORIDAD DE CERTIFICACIÓN "AC ADMINISTRACIÓN PÚBLICA"

Certificado Autoridad de Certificación "AC Administración Pública"				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
1. Version		2	Sí	Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado.	Sí	Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}). El número de serie se asignará de forma creciente.
3. Signature Algorithm		Sha1withRsaEncryption	Sí	String UTF8 (40). Identificando el tipo de algoritmo (OID 1.3.14.3.2.26)
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí	
	4.1. Country	C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado (Entidad de Certificación) ou= AC RAIZ FNMT-RCM	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
5. Validity		12 años	Sí	
6. Subject		Entidad emisora del certificado (CA Subordinada)	Sí	
	6.1. Country	C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	6.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Sí	UTF8 String, tamaño máximo 128 (rfc5280)

Certificado Autoridad de Certificación "AC Administración Pública"				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
	6.4. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. serialNumber=Q2826004J	Sí	PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	6.5. Common Name	cn=AC Administración Pública	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
7. Authority Key Identifier		Identificador de la clave pública de la entidad raíz. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de esta CA Subordinada	Sí	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la AC raíz.
8. Subject Public Key Info		Clave pública de la CA Subordinada para la Administración Pública, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048
9. Subject Key Identifier		Identificador de la clave pública de la CA Subordinada. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage		Uso permitido de las claves certificadas.	Sí	Normalizado en norma X509
	10.1. Digital Signature	0	Sí	Permite realizar la operación de firma electrónica.
	10.2. Content Commitment	0	Sí	Se refiere a la cualidad de un tipo de certificado que indica al software en el que se usa que debe permitir que el usuario conozca lo que firma.
	10.3. Key Encipherment	0	Sí	Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras
	10.4. Data Encipherment	0	Sí	Se utiliza para cifrar datos que no sean claves criptográficas.
	10.5. Key Agreement	0	Sí	Para uso en el proceso de acuerdo de claves
	10.6. Key Certificate Signature	1	Sí	Se permite utilizar para firmar certificados. Este uso se realiza en los certificados de autoridades de certificación.
	10.7. CRL Signature	1	Sí	Se permite utilizar para firmar listas de revocación de certificados. Este uso se realiza en los certificados de autoridades de certificación.
11. Certificate Policies		Política de certificación	Sí	

Certificado Autoridad de Certificación "AC Administración Pública"					
Campo			**Contenido**	**Obligatoriedad**	**Especificaciones**
	11.1. Policy Identifier		2.5.29.32.0 (anyPolicy)	Sí	Atendiendo a la rfc5280: "*PolicyInformation SHOULD only contain an OID.* *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 }*"
	11.2. Policy Qualifier Id				
		11.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	IA5String String. URL de las condiciones de uso.
		11.2.2 User Notice	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)	Sí	UTF8 String. Longitud máxima 200 caracteres.
12. CRL Distribution Point				Sí	
	12.1. Distribution Point 1		Punto de distribución 1 de la CRL (ARL) ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí	UTF8String Ruta donde reside la CRL (punto de distribución 1).
	12.2. Distribution Point 2		Punto de distribución 2 de la CRL (ARL) http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl	Sí	UTF8String. Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
13. Authority Info Access					
	1.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)
	1.2. Acces Location 1		http://ocspape.cert.fnmt.es/ocspape/OcspResponder	Sí	URL del servicio OCSP (no autenticado)
	1.3. Access Method 2		Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	Emisor de la entidad emisora de certificados (CA Raíz) De la rfc 5280: "*the id-ad-calssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user.*"

Certificado Autoridad de Certificación "AC Administración Pública"				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
	1.4. Access Location 2	http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt	Sí	Ruta para descarga de certificados adiconales para la validación de la cadena de certificación. Ene este caso la ruta del certificado raíz de la FNMT-RCM.
14. Basic Constraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".		
	14.1. Subject Type	CA		Tipo de sujeto: Autoridad de Certificación.
	14.2. Path Length	0		Un pathLenConstraint de cero indica que ningún no pueden existir más certificados de CA intermedios en la ruta de certificación.

Tabla 3 - Certificado Autoridad de Certificación "AC Administración Pública"

ANEXO III: PERFILES DE CERTIFICADOS PARA EL PERSONAL DE LA ADMINISTRACIÓN PÚBLICA

"AC APE" EN SOPORTE TARJETA CRIPTOGRÁFICA

Perfil del Certificado: Personal APE emitido por la Autoridad de Certificación "AC APE" en soporte Tarjeta Criptográfica y bajo el OID 1.3.6.1.4.1.5734.3.14		
CAMPO	**CONTENIDO**	**ESPECIFICACIONES**
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 Sha256withRsaEncryption	OID: 1.2.840.113549.1.1.5 OID: 1.2.840.113549.1.1.11 Norma PKCS#1 v2.1 y RFC 3447.
4. Issuer Distinguished Name	OU= AC APE O=FNMT-RCM C=ES	Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*. [ETSI-CPN]: *the issuer name MUST contain the countryName and the organizationName attributes.*
5. Validez	48 meses	48 meses a partir del momento de la emisión.
6. Subject	CN= "Identidad del firmante" OU= "Organizacion_Entidad" OU=AC APE O=FNMT-RCM C=ES	Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*. El atributo "SN" (*serialNumber*) se codificará en *PrintableString*. 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 *DirectoryString* codificados en UTF8. La identidad del firmante (CN) seguirá la siguiente sintaxis: CN= NOMBRE a1 a2 n – NIF 12345678A Donde: [1] NOMBRE y NIF son etiquetas [2] n, a1 y a2 son los nombres, primer y segundo apellido del personal al servicio de la Administración Pública respectivamente [3] 12345678A es su correspondiente NIF. [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. Nota: La identidad del Titular del certificado vendrá reflejada (de forma obligatoria) en la extensión subjectAltName [ETSI-CPN]: *The subject field of EE certificates for natural persons SHALL include at least the commonName or the givenNamen and surname attribute.*
7. Subject Public Key Info	Algoritmo: RSA Encryption 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 *subjectPublicKey* del sujeto (excluyendo etiqueta, longitud y número de bits no usados).

Perfil del Certificado: Personal APE emitido por la Autoridad de Certificación "AC APE" en soporte Tarjeta Criptográfica y bajo el OID 1.3.6.1.4.1.5734.3.14			
CAMPO		**CONTENIDO**	**ESPECIFICACIONES**
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 *subjectPublicKey* de la AC emisora (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo *Subject Key Identifier* de la AC emisora (AC subordinada).
12. KeyUsage			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 *Technical Corrigendum 3* de la ITU-T X509 de 04/2004, el bit de no-repudio es renombrado a **contentCommitment**. En este documento se recoge lo siguiente: "*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.*"
	Digital Signature	1	
	Non Repudiation	1	
	Key Encipherment	1	
	Data Encipherment	1	
	Key Agreement	0	
	Key Certificate Signature	0	
	CRL Signature	0	
13.extKeyUsage		Autenticación de cliente: 1.3.6.1.5.5.7.3.2 Protección de correo electrónico: 1.3.6.1.5.5.7.3.4 Inicio de sesión de tarjeta inteligente: 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. 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. *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.*
	Policy Identifier	OID asociado a la DPC o PC de certificado de firma de usuario final. (fnmtPolCertPersonalAdministracion) 1.3.6.1.4.1.5734.3.14	
	URL CPS	http://www.cert.fnmt.es/dpcs/	
	Notice Reference	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)	
16. qcStatements		id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcLimitValue : 0€ Id-etsi-qcs-QcRetentionPeriod: 15 años	ETSI TS 101 862 define la inclusión de las siguientes declaraciones para certificados cualificados: 1.- **id-etsi-qcs-QcCompliance** – Indica que el certificado es qualificado. Solo si no está explicito en las políticas indicadas en la extensión correspondiente. 2.- **id-etsi-qcs-QcLimitValue** – Indica el valor límite para transacciones. (No Aplicable). 3.- **id-etsi-qcs-QcRetentionPeriod** –Indica el 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: "***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.*". 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. 4.- **id-etsi-qcs-QcSSCD** – 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.

<table>
<tr><th colspan="3">Perfil del Certificado: Personal APE emitido por la Autoridad de Certificación “AC APE” en soporte Tarjeta Criptográfica y bajo el OID 1.3.6.1.4.1.5734.3.14</th></tr>
<tr><th>CAMPO</th><th>CONTENIDO</th><th>ESPECIFICACIONES</th></tr>
<tr><td>17. Subject Alternate Names</td><td>Nombre RFC822= email
Dirección del directorio:
OID.1.3.6.1.4.1.5734.1.1=Nom
OID.1.3.6.1.4.1.5734.1.2=Ape1
OID.1.3.6.1.4.1.5734.1.3=Ape2
OID.1.3.6.1.4.1.5734.1.4=NIF
OID.1.3.6.1.4.1.5734.1.38=fnmtAPECargo
OID.1.3.6.1.4.1.5734.1.39=fnmtAPEEntidad
OID.1.3.6.1.4.1.5734.1.40=fnmtAPESituacion
OID.1.3.6.1.4.1.5734.1.44=fnmtAPENIP
OID.1.3.6.1.4.1.5734.1.45=fnmtUnidadOrganizativa
OID.1.3.6.1.4.1.5734.1.15=fnmtPropCIF

UPN:
OID.1.3.6.1.4.1.311.20.2.3=email (Cadena UTF8 codificada en ASN1)</td><td>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.

<table><tr><th>Info</th><th>Atributo FNMT</th><th>OID</th></tr><tr><td>Nombre</td><td>fnmtNombre</td><td>fnmtoid.1.1</td></tr><tr><td>Primer apellido</td><td>fnmtApellido1</td><td>fnmtoid.1.2</td></tr><tr><td>Segundo apellido</td><td>fnmtApellido2</td><td>fnmtoid.1.3</td></tr><tr><td>NIF</td><td>fnmtNif</td><td>fnmtoid.1.4</td></tr><tr><td>Cargo</td><td>fnmtAPECargo</td><td>fnmtoid.1.38</td></tr><tr><td>Entidad en la que presta servicio</td><td>fnmtAPEEntidad</td><td>fnmtoid.1.39</td></tr><tr><td>Situación laboral</td><td>fnmtAPEsituacion</td><td>fnmtoid.1.40</td></tr><tr><td>Número identificación</td><td>fnmtAPENIP</td><td>fnmtoid.1.44</td></tr><tr><td>Unidad Organizativa</td><td>fnmtAPEUnidad Organizativa</td><td>fnmtoid.1.45</td></tr></table>
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.</td></tr>
<tr><td>18. Issuer Alternate Names</td><td>No se utilizará</td><td></td></tr>
<tr><td colspan="2">19. Basic Constraints</td><td rowspan="3">[RFC 3280] This extension MAY appear as a critical or non-critical extension in end entity certificates.</td></tr>
<tr><td></td><td>Subject Type</td><td>Entidad Final</td></tr>
<tr><td></td><td>Path Length Constraint</td><td>No utilizado</td></tr>
<tr><td colspan="2">20. Policy Constraints</td><td>No utilizado</td><td></td></tr>
<tr><td>21. CRLDistributionPoints</td><td>LDAP:
ldap://ldapape.cert.fnmt.es:puerto/CN=CRLnnn,OU= AC APE, O=FNMT, C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
HTTP:
http://www.cert.fnmt.es/crlsape/CRLnnn.crl</td><td></td></tr>
<tr><td>22. Auth. Information Access</td><td>OCSP:
http://ocspape.cert.fnmt.es/ocspape/OcspResponder
CA:
http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt</td><td>Contendrá información de localización del OCSP Responder. URL resuelta a diferentes servidores. Ley de Firma Electrónica: “Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro”.</td></tr>
<tr><td>23. netscapeCertType</td><td>sSLCLIENT,sMIME</td><td>Tipo de certificado según Netscape</td></tr>
<tr><td>24. fnmtTipoCertificado</td><td>1.3.6.1.4.1.5734.1.33: “Personal adscrito a la Administración”</td><td>Tipo de certificado para Personal adscrito a la Administración</td></tr>
</table>

Tabla 4 - Perfil del Certificado de Personal APE emitido por la Autoridad de Certificación “AC APE” en soporte Tarjeta Criptográfica y bajo el OID 1.3.6.1.4.1.5734.3.14

"AC ADMINISTRACIÓN PÚBLICA" EN SOPORTE TARJETA CRIPTOGRÁFICA

Personal APE emitido por la Autoridad de Certificación "AC Administración Pública" en soporte Tarjeta Criptográfica y bajo el OID 1.3.6.1.4.1.5734.3.3.4.4.1				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
1. Version		2	Sí	Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado.	Sí	Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}). El número de serie se asignará de forma creciente.
3. Signature Algorithm		Sha1withRsaEncryption	Sí	String UTF8 (40). Identificando el tipo de algoritmo (OID 1.3.14.3.2.26)
4. Issuer Distinguish Name		Entidad emisora del certificado	Sí	
	4.1. Country	C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	4.4. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. serialNumber=Q2826004J	Sí	PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	4.5. Common Name	cn=AC Administración Pública	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
5. Validity		3 años	Sí	Validez máxima limitada por "Esquema de Identificación y Firma. Perfiles de Certificados"
6. Subject		Identificación/descripción del c ustodio/responsable de las claves certificadas	Sí	
	6.1. Country	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas. C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)

Personal APE emitido por la Autoridad de Certificación "AC Administración Pública" en soporte Tarjeta Criptográfica y bajo el OID 1.3.6.1.4.1.5734.3.3.4.4.1				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
	6.2. Organization	Denominación (nombre "oficial" de la organización) titular de los servicios de certificación	Sí	UTF8 String, tamaño máximo 128 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=certificado electrónico de empleado público	Sí	
	6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado.	Opcional	UTF8 String, tamaño máximo 128 (rfc5280). Por ejemplo: ou=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.5. Organizational Unit	Número de identificación del suscriptor del certificado (supuestamente unívoco). Identificador del empleado público.	Opcional	UTF8 String, tamaño máximo 128 (rfc5280). Por ejemplo: ou=ADM5689 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.6. Serial Number	DNI/NIE del empleado público.	Sí	Por ejemplo: serialNumber=99999999R PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	6.7. Surname	Apellidos de acuerdo con documento de identificación	Sí	UTF8String (rfc5280). Por ejemplo: sn=ESPAÑOL ESPAÑOL
	6.8. Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)	Sí	UTF8String (rfc5280). Por ejemplo: gn=JUAN
	6.9. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del DNI	Sí	UTF8String (rfc5280). Por ejemplo: cn=JUAN ESPAÑOL ESPAÑOL – DNI 99999999R
7. Authority Key Identifier		Identificador de la clave pública de la CA para la Administración Pública. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la AC emisora.
8. Subject Public Key Info		Clave pública asociada al empleado público, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048
9. Subject Key Identifier		Identificador de la clave pública del suscriptor o poseedor de claves. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).

Personal APE emitido por la Autoridad de Certificación "AC Administración Pública" en soporte Tarjeta Criptográfica y bajo el OID 1.3.6.1.4.1.5734.3.3.4.4.1				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
10. Key Usage				
	10.1. Digital Signature	1		Permite realizar la operación de firma electrónica
	10.2. Content Commitment	1		Se refiere a la cualidad de un tipo de certificado que indica al software en el que se usa que debe permitir que el usuario conozca lo que firma (firma de contratos, acuses de recibo, resguardos, etc.)
	10.3. Key Encipherment	1		Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras
	10.4. Data Encipherment	1		Se utiliza para cifrar datos que no sean claves criptográficas.
	10.5. Key Agreement	0		Para uso en el proceso de acuerdo de claves
	10.6. Key Certificate Signature	0		Se permite usar para firmar certificados. Se utiliza en los certificados de autoridades de certificación.
	10.7. CRL Signature	0		Se permite usar para firmar listas de revocación de certificados.
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	Esta extensión indica que uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, además de o en lugar de los usos básicos que se indican en la extensión KeyUsage.
	11.1. Email protection	1.3.6.1.5.5.7.3.4	Sí	Proteción de correo electrónico
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Sí	Autenticación de cliente
	11.3. Any Extended Key Usage	Otros propósitos (ver comentario de columna "Especificaciones") 2.5.29.37.0	Sí	*[RFC5280]: 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.*
	11.4. Microsoft Smart Card Logon	1.3.6.1.4.1.311.20.2.2	Sí	*Necesaria para realizar logon en Windows con tarjeta/token*
12. Qualified Certificate Statements				

Personal APE emitido por la Autoridad de Certificación "AC Administración Pública" en soporte Tarjeta Criptográfica y bajo el OID 1.3.6.1.4.1.5734.3.3.4.4.1					
Campo			**Contenido**	**Obligatoriedad**	**Especificaciones**
	12.1. QcCompliance		Certificado es qualificado. (OID: 0.4.0.1862.1.1)	Sí	Indica que el certificado es cualificado. Solo si no está explicito en las políticas indicadas en la extensión correspondiente.
	12.2. QcEuRetentionPeriod		15 años (OID: 0.4.0.1862.1.3)	Sí	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: "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.".
	12.3. QcLimitValue		0 € (OID: 0.4.0.1862.1.2)	Sí	Límite de responsabilidad
	12.4. QcSSCD		Claves generadas en un DSCF (OID: 0.4.0.1862.1.4)	No	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.
13. Certificate Policies			Política de certificación	Sí	
	13.1. Policy Identifier		Identificador unívoco de la política de certificación asociada a los certificados de tipo "empleado público". En este caso: 1.3.6.1.4.1.5734.3.3.4.4.1	Sí	Identificador de la política de certificado para Empleado público-Nivel medio (tarjeta)
	13.2. Policy Qualifier Id				
		13.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	IA5String String. URL de las condiciones de uso.
		13.2.2 User Notice	Certificado reconocido de empleado público. 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)	Sí	UTF8 String. Longitud máxima 200 caracteres.
14. Subject Alternative Names			Identificación/ descripción de Identidad Administrativa	Sí	
	14.1. rfc822 Name		Correo electrónico del empleado público	Opcional	Por ejemplo: rfc822Name=jespanol@meh.es Se establecerá el valor del e-mail contacto si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.

Personal APE emitido por la Autoridad de Certificación "AC Administración Pública" en soporte Tarjeta Criptográfica y bajo el OID 1.3.6.1.4.1.5734.3.3.4.4.1					
Campo			**Contenido**	**Obligatoriedad**	**Especificaciones**
	14.2. UPN		UPN (nombre de login de red) para smartcard logon.	Opcional	Campo destinado a incluir el smart card logon de Windows para el responsable del certificado. Se establecerá el valor del UPN si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	14.3. Directory Name		Identidad Administrativa	Sí	Campos específicos definidos por la Administración para los certificados LAECSP.
		14.3.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.3.2.1 =certificado electrónico de empleado público	Sí	UTF8 String.
		14.3.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.3.2.2=<Entidad Suscriptora>	Sí	UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.2=MINISTERIO DE ECONOMÍA Y HACIENDA
		14.3.3 NIF Entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.3.2.3 =<NIF>	Sí	UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.3.2.3=Q2826004J
		14.3.4 DNI del empleado	Identificador de identidad del suscriptor-custodio de las claves. (NIF). Id Campo/Valor: 2.16.724.1.3.5.3.2.4 =<NIF>	Sí	UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.3.2.4=99999999R
		14.3.5 Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente unívoco). Número de identificación de funcionario/empleado público Id Campo/Valor: 2.16.724.1.3.5.3.2.5 =<NRP>	Opcional	UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.5=ADM12347 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
		14.3.6 Nombre	Nombre de pila del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.3.2.6 =<Nombre de pila>	Sí	UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.6=JUAN
		14.3.7 Apellido 1	Primer apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.3.2.7 =<Apellido 1>	Sí	UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.7=ESPAÑOL

Personal APE emitido por la Autoridad de Certificación "AC Administración Pública" en soporte Tarjeta Criptográfica y bajo el OID 1.3.6.1.4.1.5734.3.3.4.4.1					
Campo			**Contenido**	**Obligatoriedad**	**Especificaciones**
		14.3.8 Apellido 2	Segundo apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.3.2.8 =<Apellido 2>	Sí	UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.8=ESPAÑOL
		14.3.9 Correo electrónico	Correo electrónico de la persona responsable del certificado. Id Campo/Valor: 2.16.724.1.3.5.3.2.9 =<email de contacto>	Opcional	UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.3.2.9=jespanol@meh.es Se establecerá el valor del e-email contacto si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
		14.3.10 Unidad organizativa	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. Id Campo/Valor: 2.16.724.1.3.5.3.2.10 =<Unidad Organizativa>	Opcional	UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.10=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
		14.3.11 Puesto / cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración. Id Campo/Valor: 2.16.724.1.3.5.3.2.11 =<Puesto/Cargo>	Opcional	UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.11=ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
15. CRL Distribution Point			Punto de distribución (localizador) de la CRL	Sí	
	15.1. Distribution Point 1		Punto de publicación de la CRL1 http://www.cert.fnmt.es/crls_acape/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	UTF8String Ruta donde reside la CRL (punto de distribución 1).
	15.2. Distribution Point 2		Punto de publicación de la CRL2. ldap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Administraci%F3n%20P%FAblica,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	UTF8String. Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
16. Authority Info Access				Sí	
	16.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	Acceso al servicio OCSP

Personal APE emitido por la Autoridad de Certificación "AC Administración Pública" en soporte Tarjeta Criptográfica y bajo el OID 1.3.6.1.4.1.5734.3.3.4.4.1				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
	16.2. Acces Location 1	http://ocspape.cert.fnmt.es/ocspape/OcspResponder	Sí	URL para acceder al servicio OCSP. No es necesario firmar las peticiones OCSP
	16.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	Emisor de la entidad emisora de certificados (CA Raíz) De la rfc 5280: "*the id-ad-calssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user.*"
	16.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt	Sí	Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado raíz de la FNMT-RCM.
17. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación". También sirve para distinguir una CA de las entidades finales	Sí	De la rf5280: " *This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	17.1. Subject Type	Entidad final (valor FALSE)		Con este certificado no se pueden emitir otros

Tabla 5 - Perfil del Certificado de Personal APE emitido por la Autoridad de Certificación "AC Administración Pública" en soporte Tarjeta Criptográfica y bajo el OID 1.3.6.1.4.1.5734.3.3.4.4.1

"AC ADMINISTRACIÓN PÚBLICA" EN SOPORTE SOFTWARE

Personal APE emitido por la Autoridad de Certificación "AC Administración Pública" en soporte Software y bajo el OID 1.3.6.1.4.1.5734.3.3.4.4.2				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
1. Version		2	Sí	Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado.	Sí	Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}). El número de serie se asignará de forma creciente.
3. Signature Algorithm		Sha1withRsaEncryption	Sí	String UTF8 (40). Identificando el tipo de algoritmo (OID 1.3.14.3.2.26)
4. Issuer Distinguish Name		Entidad emisora del certificado	Sí	
	4.1. Country	C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	4.4. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. serialNumber=Q2826004J	Sí	PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	4.5. Common Name	cn=AC Administración Pública	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
5. Validity		3 años	Sí	Validez máxima limitada por "Esquema de Identificación y Firma. Perfiles de Certificados"
6. Subject		Identificación/descripción del c ustodio/responsable de las claves certificadas	Sí	
	6.1. Country	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas. C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)

Personal APE emitido por la Autoridad de Certificación "AC Administración Pública" en soporte Software y bajo el OID 1.3.6.1.4.1.5734.3.3.4.4.2				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
	6.2. Organization	Denominación (nombre "oficial" de la organización) titular de los servicios de certificación	Sí	UTF8 String, tamaño máximo 128 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou= certificado electrónico de empleado público	Sí	
	6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado.	Opcional	UTF8 String, tamaño máximo 128 (rfc5280). Por ejemplo: ou=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.5. Organizational Unit	Número de identificación del suscriptor del certificado (supuestamente unívoco). Identificador del empleado público.	Opcional	UTF8 String, tamaño máximo 128 (rfc5280). Por ejemplo: ou=ADM5689 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.6. Serial Number	DNI/NIE del empleado público.	Sí	Por ejemplo: serialNumber=99999999R PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	6.7. Surname	Apellidos de acuerdo con documento de identificación	Sí	UTF8String (rfc5280). Por ejemplo: sn=ESPAÑOL ESPAÑOL
	6.8. Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)	Sí	UTF8String (rfc5280). Por ejemplo: gn=JUAN
	6.9. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del DNI	Sí	UTF8String (rfc5280). Por ejemplo: cn=JUAN ESPAÑOL ESPAÑOL – DNI 99999999R
7. Authority Key Identifier		Identificador de la clave pública de la CA para la Administración Pública. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la AC emisora.
8. Subject Public Key Info		Clave pública asociada al empleado público, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048
9. Subject Key Identifier		Identificador de la clave pública del suscriptor o poseedor de claves. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).

Personal APE emitido por la Autoridad de Certificación "AC Administración Pública" en soporte Software y bajo el OID 1.3.6.1.4.1.5734.3.3.4.4.2				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
10. Key Usage				
	10.1. Digital Signature	1		Permite realizar la operación de firma electrónica
	10.2. Content Commitment	1		Se refiere a la cualidad de un tipo de certificado que indica al software en el que se usa que debe permitir que el usuario conozca lo que firma (firma de contratos, acuses de recibo, resguardos, etc.)
	10.3. Key Encipherment	1		Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras
	10.4. Data Encipherment	1		Se utiliza para cifrar datos que no sean claves criptográficas.
	10.5. Key Agreement	0		Para uso en el proceso de acuerdo de claves
	10.6. Key Certificate Signature	0		Se permite usar para firmar certificados. Se utiliza en los certificados de autoridades de certificación.
	10.7. CRL Signature	0		Se permite para firmar listas de revocación de certificados.
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	Esta extensión indica que uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, además de o en lugar de los usos básicos que se indican en la extensión KeyUsage.
	11.1. Email protection	1.3.6.1.5.5.7.3.4	Sí	Proteción de correo electrónico
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Sí	Autenticación de cliente
	11.3. Any Extended Key Usage	Otros propósitos (ver comentario de columna "Especificaciones" 2.5.29.37.0	Sí	*[RFC5280]: 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.*
	11.4. Microsoft Smart Card Logon	1.3.6.1.4.1.311.20.2.2	Sí	*Necesaria para realizar logon en Windows*
12. Qualified Certificate Statements				

Personal APE emitido por la Autoridad de Certificación "AC Administración Pública" en soporte Software y bajo el OID 1.3.6.1.4.1.5734.3.3.4.4.2					
Campo			**Contenido**	**Obligatoriedad**	**Especificaciones**
	12.1. QcCompliance		Certificado es qualificado. (OID: 0.4.0.1862.1.1)	Sí	Indica que el certificado es qualificado. Solo si no está explicito en las políticas indicadas en la extensión correspondiente.
	12.2. QcEuRetentionPeriod		15 años (OID: 0.4.0.1862.1.3)	Sí	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: "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.".
	12.3. QcLimitValue		0 € (OID: 0.4.0.1862.1.2)	Sí	Límite de responsabilidad
	12.4. QcSSCD		Claves generadas en un DSCF (OID: 0.4.0.1862.1.4)	No	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. Este valor sólo se consignará cuando se pueda asegurar que las clave privada ha sido generada en un DSCF de forma fehaciente (garantizado por mecanismo técnico)
13. Certificate Policies					
	13.1. Policy Identifier		Identificador unívoco de la política de certificación asociada a los certificados de tipo "empleado público". En este caso: 1.3.6.1.4.1.5734.3.3.4.4.2	Sí	Identificador de la política de certificado para Empleado público-Nivel medio (software)
	13.2. Policy Qualifier Id				
		13.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	IA5String String. URL de las condiciones de uso.
		13.2.2 User Notice	Certificado reconocido de empleado público. 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)	Sí	UTF8 String. Longitud máxima 200 caracteres.
14. Subject Alternative Names			Identificación/ descripción de Identidad Administrativa	Sí	

Personal APE emitido por la Autoridad de Certificación "AC Administración Pública" en soporte Software y bajo el OID 1.3.6.1.4.1.5734.3.3.4.4.2					
Campo			**Contenido**	**Obligatoriedad**	**Especificaciones**
	14.1. rfc822 Name		Correo electrónico del empleado público	Opcional	Por ejemplo: rfc822Name=jespanol@meh.es Se establecerá el valor del e-email contacto si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	14.2. UPN		UPN (nombre de login de red) para smartcard logon.	Opcional	Campo destinado a incluir el smart card logon de Windows para el responsable del certificado. Se establecerá el valor del UPN si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	14.3. Directory Name		Identidad Administrativa	Sí	Campos específicos definidos por la Administración para los certificados LAECSP.
		14.3.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.3.2.1 = certificado electrónico de empleado público	Sí	UTF8 String.
		14.3.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.3.2.2=<Entidad Suscriptora>	Sí	UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.2=MINISTERIO DE ECONOMÍA Y HACIENDA
		14.3.3 NIF Entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.3.2.3 =<NIF>	Sí	UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.3.2.3=Q2826004J
		14.3.4 DNI del empleado	Identificador de identidad del suscriptor-custodio de las claves. (NIF). Id Campo/Valor: 2.16.724.1.3.5.3.2.4 =<NIF>	Sí	UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.3.2.4=99999999R
		14.3.5 Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente unívoco). Número de identificación de funcionario/empleado público Id Campo/Valor: 2.16.724.1.3.5.3.2.5 =<NRP>	Opcional	UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.5=ADM12347 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
		14.3.6 Nombre	Nombre de pila del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.3.2.6 =<Nombre de pila>	Sí	UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.6=JUAN

Personal APE emitido por la Autoridad de Certificación "AC Administración Pública" en soporte Software y bajo el OID 1.3.6.1.4.1.5734.3.3.4.4.2					
Campo			**Contenido**	**Obligatoriedad**	**Especificaciones**
		14.3.7 Apellido 1	Primer apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.3.2.7 =<Apellido 1>	Sí	UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.7=ESPAÑOL
		14.3.8 Apellido 2	Segundo apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.3.2.8 =<Apellido 2>	Sí	UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.8=ESPAÑOL
		14.3.9 Correo electrónico	Correo electrónico de la persona responsable del certificado. Id Campo/Valor: 2.16.724.1.3.5.3.2.9 =<email de contacto>	Opcional	UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.3.2.9=jespanol@meh.es Se establecerá el valor del e-email contacto si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
		14.3.10 Unidad organizativa	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. Id Campo/Valor: 2.16.724.1.3.5.3.2.10 =<Unidad Organizativa>	Opcional	UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.10=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
		14.3.11 Puesto / cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración. Id Campo/Valor: 2.16.724.1.3.5.3.2.11 =<Puesto/Cargo>	Opcional	UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.11=ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
15. CRL Distribution Point			Punto de distribución (localizador) de la CRL	Sí	
	15.1. Distribution Point 1		Punto de publicación de la CRL1 http://www.cert.fnmt.es/crls_acape/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	UTF8String Ruta donde reside la CRL (punto de distribución 1).
	15.2. Distribution Point 2		Punto de publicación de la CRL2. ldap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Administraci%F3n%20P%Fablica,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	UTF8String. Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).

Personal APE emitido por la Autoridad de Certificación "AC Administración Pública" en soporte Software y bajo el OID 1.3.6.1.4.1.5734.3.3.4.4.2				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
16. Authority Info Access			Sí	
	16.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	Acceso al servicio OCSP
	16.2. Acces Location 1	http://ocspape.cert.fnmt.es/ocspape/OcspResponder	Sí	URL para acceder al servicio OCSP. No es necesario firmar las peticiones OCSP
	16.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	Emisor de la entidad emisora de certificados (CA Raíz) De la rfc 5280: "*the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user.*"
	16.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt	Sí	Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado raíz de la FNMT-RCM.
17. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación". También sirve para distinguir una CA de las entidades finales	Sí	De la rf5280: " *This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	17.1. Subject Type	Entidad final (valor FALSE)		Con este certificado no se pueden emitir otros

Tabla 6 - Perfil del Certificado: Personal APE emitido por la Autoridad de Certificación "AC Administración Pública" en soporte Software y bajo el OID 1.3.6.1.4.1.5734.3.3.4.4.2

ANEXO IV: PERFILES DE CERTIFICADOS PARA LA IDENTIFICACIÓN DE SEDES ELECTRÓNICAS "AC APE"

Perfil del Certificado de Sede Electrónica emitido por la Autoridad de Certificación "AC APE" y bajo el OID 1.3.6.1.4.1.5734.3.12		
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 Sha256withRsaEncryption	OID: 1.2.840.113549.1.1.5 OID: 1.2.840.113549.1.1.11 Norma PKCS#1 v2.1 y RFC 3447.
4. Issuer Distinguished Name	OU= AC APE O=FNMT-RCM C=ES	Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*. [ETSI-CPN]: *the issuer name MUST contain the countryName and the organizationName attributes.*
5. Validez	48 meses	48 meses a partir del momento de la emisión.
6. Subject	CN= XXXXXX OU= "Organizacion_Entidad" OU=AC APE O=FNMT-RCM C=ES	Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*. 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: CN=www.nombrehost.es ó CN=111.222.121.212
7. Subject Public Key Info	Algoritmo: RSA Encryption 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 *subjectPublicKey* 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 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 *subjectPublicKey* de la AC emisora (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo *Subject Key Identifier* de la AC emisora (AC subordinada).
10. KeyUsage		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 *Technical Corrigendum 3* de la ITU-T X509 de 04/2004, el bit de no-repudio es renombrado a **contentCommitment**. En este documento se recoge lo siguiente: "*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.*"
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	1	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signatura	0	
CRL Signature	0	

Perfil del Certificado de Sede Electrónica emitido por la Autoridad de Certificación "AC APE" y bajo el OID 1.3.6.1.4.1.5734.3.12				
CAMPO		**CONTENIDO**		**OBSERVACIONES**
11. extKeyUsage		Autenticación de servidor: 1.3.6.1.5.5.7.3.1		*[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.*
12. Certificate Policies				RFC 3739 obliga la existencia de al menos un valor. 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. *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.*
	Policy Identifier	OID asociado a la DPC o PC de certificado de firma de Sello electrónico. (fnmtPolCertSedeElect) 1.3.6.1.4.1.5734.3.12		
	URL CPS	http://www.cert.fnmt.es/dpcs/		
	Notice Reference	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)		
13. qcStatements		Id-etsi-qcs-QcCompliance id-etsi-qcs-QcLimitValue : 0€ Id-etsi-qcs-QcRetentionPeriod: 15 años		ETSI TS 101 862 define la inclusión de las siguientes declaraciones para certificados cualificados: 1.- **id-etsi-qcs-QcCompliance** – Indica que el certificado es qualificado. Solo si no está explicito en las políticas indicadas en la extensión correspondiente. 2.- **id-etsi-qcs-QcLimitValue** – Indica el valor límite para transacciones. 3.- **id-etsi-qcs-QcRetentionPeriod** – Indica el 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: "***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.*". 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. 4.- **id-etsi-qcs-QcSSCD** – 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.
14. Subject Alternate Names		Dirección del directorio: OID.1.3.6.1.4.1.5734.1.8=fnmtDescripcion OID.1.3.6.1.4.1.5734.1.14=fnmtPropEnt OID.1.3.6.1.4.1.5734.1.15=fnmtCIF OID.1.3.6.1.4.1.5734.1.16=fnmtRespNombre OID.1.3.6.1.4.1.5734.1.17=fnmtRespApellido1 OID.1.3.6.1.4.1.5734.1.18=fnmtRespApellido2 OID.1.3.6.1.4.1.5734.1.19=fnmtRespNIF dNSName= Nombre de Host ó iPAddress=Dirección IP (*) 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.	Descripción	fnmtDescripcion
			Entidad propietaria	fnmtPropEnt
			CIF	fnmtCIF
			Nombre Responsable	fnmtRespNombre
			Apellido1 Responsable	fnmtRespApellido1
			Apellido2 Responsable	fnmtRespApellido2
			NIF Responsable	fnmtRespNIF
15. Basic Constraints				*[RFC 3280] This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	Subject Type	Entidad Final		
16. CRLDistributionPoints		LDAP: ldap://ldapape.cert.fnmt.es:*puerto*/CN=CRLnnn,OU= AC APE, O=FNMT, C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint HTTP: http://www.cert.fnmt.es/crlsape/CRLnnn.crl		

Perfil del Certificado de Sede Electrónica emitido por la Autoridad de Certificación "AC APE" y bajo el OID 1.3.6.1.4.1.5734.3.12		
CAMPO	**CONTENIDO**	**OBSERVACIONES**
17. Auth. Information Access	OCSP: http://ocspape.cert.fnmt.es/ocspape/OcspResponder CA: http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt	Contendrá información de localización del OCSP Responder. URL resuelta a diferentes servidores. Ley de Firma Electrónica: "***Garantizar la disponibilidad de un servicio de consulta*** *sobre la vigencia de los certificados rápido y seguro*".
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 7 - Perfil del Certificado de Sede Electrónica emitido por la Autoridad de Certificación "AC APE" y bajo el OID 1.3.6.1.4.1.5734.3.12

"AC ADMINISTRACIÓN PÚBLICA"

Sede Electrónica emitido por la Autoridad de Certificación "AC Administración Pública" y bajo el OID 1.3.6.1.4.1.5734.3.3.2.2				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
1. Version		2	Sí	Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado.	Sí	Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}). El número de serie se asignará de forma creciente.
3. Signature Algorithm		Sha1withRsaEncryption	Sí	String UTF8 (40). Identificando el tipo de algoritmo (OID 1.3.14.3.2.26)
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí	
	4.1. Country	C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	4.4. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. serialNumber=Q2826004J	Sí	PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	4.5. Common Name	cn=AC Administración Pública	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
5. Validity		3 años	Sí	Validez máxima limitada por "Esquema de Identificación y Firma. Perfiles de Certificados"
6. Subject		Identificación/descripción del c ustodio/responsable de las claves certificadas	Sí	
	6.1. Country	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas. C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)

Sede Electrónica emitido por la Autoridad de Certificación "AC Administración Pública" y bajo el OID 1.3.6.1.4.1.5734.3.3.2.2				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
	6.2. Organization	Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación (custodio del certificado)	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=sede electrónica	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	6.4. Organizational Unit	El nombre descriptivo de la sede.	Sí	Por ejemplo: ou=Oficina Virtual del MEH. UTF8 String, tamaño máximo 128 (rfc5280)
	6.5. Serial Number	Número único de identificación de la Entidad suscriptora de srvicios de certificación. En este caso el NIF	Sí	Por ejemplo: serialNumber=Q2826004J PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	6.6. Common Name	Denominación de nombre de dominio (DNS o IP) donde residirá el certificado y que identificara a la sede	Sí	Por ejemplo: cn=www.meh.es UTF8 String (rfc5280)
7. Authority Key Identifier		Identificador de la clave pública del PSC. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la AC emisora.
8. Subject Public Key Info		Clave pública de la sede, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048
9. Subject Key Identifier		Identificador de la clave pública del suscriptor o poseedor de claves. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage		Uso permitido de las claves certificadas.	Sí	Normalizado en norma X509
	10.1. Digital Signature	1		Permite realizar la operación de firma electrónica
	10.2. Content Commitment	0		Se refiere a la cualidad de un tipo de certificado que indica al software en el que se usa que debe permitir que el usuario conozca lo que firma.
	10.3. Key Encipherment	1		Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras
	10.4. Data Encipherment	0		Se utiliza para cifrar datos que no sean claves criptográficas.
	10.5. Key Agreement	0		Para uso en el proceso de acuerdo de claves

Sede Electrónica emitido por la Autoridad de Certificación "AC Administración Pública" y bajo el OID 1.3.6.1.4.1.5734.3.3.2.2				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
	10.6. Key Certificate Signature	0		Se permite usar para firmar certificados. Se utiliza en los certificados de autoridades de certificación.
	10.7. CRL Signature	0		Se permite usar para firmar listas de revocación de certificados.
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	Esta extensión indica que uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, además de o en lugar de los usos básicos que se indican en la extensión KeyUsage.
	11.1. Server Authentication	1.3.6.1.5.5.7.3.1	Sí	Autenticación TSL web Server
	11.2. Any Extended Key Usage	Otros propósitos (ver comentario de columna "Especificaciones" 2.5.29.37.0	Sí	*[RFC5280]: 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.*
12. Qualified Certificate Statements		Extensiones cualificadas.		ETSI TS 101 862 define la inclusión de ciertas declaraciones para certificados cualificados
	12.1. QcCompliance	Certificado es qualificado. (0.4.0.1862.1.1)	Sí	Indica que el certificado es cualificado. Solo si no está explicito en las políticas indicadas en la extensión correspondiente.
	12.2. QcEuRetentionPeriod	15 años (OID: 0.4.0.1862.1.3)	Sí	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: "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.".
	12.3. QcLimitValue	0 € (OID: 0.4.0.1862.1.2)	Sí	Límite de responsabilidad
	12.4. QcSSCD	Claves generadas en un DSCF (OID: 0.4.0.1862.1.4)	No	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.
13. Certificate Policies		Política de certificación	Sí	

Sede Electrónica emitido por la Autoridad de Certificación "AC Administración Pública" y bajo el OID 1.3.6.1.4.1.5734.3.3.2.2					
Campo			**Contenido**	**Obligatoriedad**	**Especificaciones**
	13.1. Policy Identifier		Identificador unívoco de la política de certificación asociada a los certificados de tipo "Sede electrónica". En este caso: 1.3.6.1.4.1.5734.3.3.2.2	Sí	Identificador de la política de certificado para Sede-Nivel medio
	13.2. Policy Qualifier Id			Sí	
		13.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	IA5String String. URL de las condiciones de uso.
		13.2.2 User Notice	Certificado reconocido de sede electrónica. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM (C/Jorge Juan 106-28009-Madrid-España)	Sí	UTF8 String. Longitud máxima 200 caracteres.
14. Subject Alternative Names			Identificación/ descripción de Identidad Administrativa	Sí	
	14.1. rfc822 Name		Correo electrónico de contacto de la Sede (entidad suscriptora)	Opcional	Por ejemplo: rfc822Name=webmaster@meh.es Se establecerá el valor del e-email contacto entidad suscriptora si se aporta en la solicitud de certificado.
	14.2. DNS Name		Nombre de Dominio (DNS) de la Sede	Sí	UTF8 String, tamaño máximo 128. Nombre Dominio donde se eneuntra la Sede. Por ejemplo: DNSName = www.sede.meh.gob.es
	14.3. Directory Name		Identidad Administrativa	Sí	Campos específicos definidos por la Administración para los certificados LAECSP.
		14.3.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.1.2.1 =sede electrónica	Sí	UTF8 String.
		14.3.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.1.2.2=<Entidad Suscriptora>	Sí	UTF8 String. Por ejemplo: 2.16.724.1.3.5.1.2.2=Ministerio de Economía y Hacienda
		14.3.3 NIF Entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.1.2.3 =<NIF>	Sí	UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.1.2.3=Q2826004J
		14.3.4 Nombre descriptivo	Breve descripción de la Sede. 2.16.724.1.3.5.1.2.4 =<Descripción breve de la sede>	Sí	UTF8 String, tamaño máximo 128. Por ejemplo: 2.16.724.1.3.5.1.2.4=Oficina vitual del MEH

Sede Electrónica emitido por la Autoridad de Certificación "AC Administración Pública" y bajo el OID 1.3.6.1.4.1.5734.3.3.2.2					
Campo			**Contenido**	**Obligatoriedad**	**Especificaciones**
		14.3.5 Denominación de nombre de dominio	Nombre de dominio donde se encuenta la sede 2.16.724.1.3.5.1.2.5 =Dominio de la Sede	Sí	UTF8 String, tamaño 128. Por ejemplo: 2.16.724.1.3.5.1.2.5=www.sede.meh.gob.es
15. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	
	15.1. Distribution Point 1		Punto de publicación de la CRL1ç http://www.cert.fnmt.es/crls_acape/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	UTF8String Ruta donde reside la CRL (punto de distribución 1).
	15.2. Distribution Point 2		Punto de publicación de la CRL2. ldap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Administraci%F3n%20P%FAblica,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	UTF8String. Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
16. Authority Info Access				Sí	
	16.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	
	16.2. Acces Location 1		http://ocspape.cert.fnmt.es/ocspape/OcspResponder	Sí	
	16.3. Access Method 2		Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	Emisor de la entidad emisora de certificados (CA Raíz) De la rfc 5280: "*the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user.*"
	16.4. Access Location 2		http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt	Sí	Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. Ene este caso la ruta del certificado raíz de la FNMT-RCM.
17. Basic Contraints			Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".		De la rf5280: " *This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	17.1. Subject Type		Entidad final (valor FALSE)		Con este certificado no se pueden emitir otros

Tabla 8 - Perfil del Certificado de Sede Electrónica emitido por la Autoridad de Certificación "AC Administración Pública" y bajo el OID 1.3.6.1.4.1.5734.3.3.2.2

ANEXO V: PERFILES DE CERTIFICADOS PARA LA ACTUACIÓN ADMINISTRATIVA AUTOMATIZADA

"AC APE"

Perfil del Certificado de Actuación Administrativa Automatizada emitido por la Autoridad de Certificación "AC APE" y bajo el OID 1.3.6.1.4.1.5734.3.13			
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 Sha256withRsaEncryption	OID: 1.2.840.113549.1.1.5 OID: 1.2.840.113549.1.1.11 Norma PKCS#1 v2.1 y RFC 3447.
4. Issuer Distinguished Name		OU= AC APE O=FNMT-RCM C=ES	Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*. [ETSI-CPN]: *the issuer name MUST contain the countryName and the organizationName attributes.*
5. Validez		48 meses	48 meses a partir del momento de la emisión.
6. Subject		CN= DESCRIPCION d – ENTIDAD e – CIF 12345678B OU= "Organizacion_Entidad" OU=AC APE O=FNMT-RCM C=ES	Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*.
7. Subject Public Key Info		Algoritmo: RSA Encryption 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 *subjectPublicKey* 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 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 *subjectPublicKey* de la AC emisora (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo *Subject Key Identifier* de la AC emisora (AC subordinada).
10. KeyUsage			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 *Technical Corrigendum 3* de la ITU-T X509 de 04/2004, el bit de no-repudio es renombrado a **contentCommitment**. En este documento se recoge lo siguiente: "*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.*"
	Digital Signature	1	
	Non Repudiation	1	
	Key Encipherment	1	
	Data Encipherment	1	
	Key Agreement	0	
	Key Certificate Signatura	0	
	CRL Signature	0	
11. extKeyUsage		Autenticación de cliente: 1.3.6.1.5.5.7.3.2 Protección de correo electrónico: 1.3.6.1.5.5.7.3.4	*[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.*
12. Certificate Policies			RFC 3739 obliga la existencia de al menos un valor. 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.
	Policy Identifier	OID asociado a la DPC o PC de certificado de firma de Sello electrónico. (fnmtPolCertSelloElect) 1.3.6.1.4.1.5734.3.13	

<table>
<tr><th colspan="4">Perfil del Certificado de Actuación Administrativa Automatizada emitido por la Autoridad de Certificación “AC APE” y bajo el OID 1.3.6.1.4.1.5734.3.13</th></tr>
<tr><th colspan="2">CAMPO</th><th>CONTENIDO</th><th>OBSERVACIONES</th></tr>
<tr><td></td><td>URL CPS</td><td>http://www.cert.fnmt.es/dpcs/</td><td rowspan="2">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.</td></tr>
<tr><td></td><td>Notice Referente</td><td>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)</td></tr>
<tr><td colspan="2">13. qcStatements</td><td>id-etsi-qcs-QcCompliance
id-etsi-qcs-QcLimitValue : 0€
Id-etsi-qcs-QcRetentionPeriod: 15 años</td><td>ETSI TS 101 862 define la inclusión de las siguientes declaraciones para certificados cualificados:
1.- id-etsi-qcs-QcCompliance – Indica que el certificado es qualificado. Solo si no está explicito en las políticas indicadas en la extensión correspondiente.
2.- id-etsi-qcs-QcLimitValue – Indica el valor límite para transacciones.
3.- id-etsi-qcs-QcRetentionPeriod – Indica el 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: “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.”. 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.
4.- id-etsi-qcs-QcSSCD – 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.</td></tr>
<tr><td colspan="2">14. Subject Alternate Names</td><td>Dirección del directorio:
OID.1.3.6.1.4.1.5734.1.8=fnmtDescripcion
OID.1.3.6.1.4.1.5734.1.14=fnmtPropEnt
OID.1.3.6.1.4.1.5734.1.15=fnmtCIF
OID.1.3.6.1.4.1.5734.1.16=fnmtRespNombre (Opcional)
OID.1.3.6.1.4.1.5734.1.17=fnmtRespApellido1 (Opcional)
OID.1.3.6.1.4.1.5734.1.18=fnmtRespApellido2 (Opcional)
OID.1.3.6.1.4.1.5734.1.19=fnmtRespNIF (Opcional)

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.</td><td colspan="2"><table>
<tr><td>Descripción</td><td>fnmtDescripcion</td></tr>
<tr><td>Entidad propietaria</td><td>fnmtPropEnt</td></tr>
<tr><td>CIF</td><td>fnmtCIF</td></tr>
<tr><td>Nombre Responsable</td><td>fnmtRespNombre</td></tr>
<tr><td>Apellido1 Responsable</td><td>fnmtRespApellido1</td></tr>
<tr><td>Apellido2 Responsable</td><td>fnmtRespApellido2</td></tr>
<tr><td>NIF Responsable</td><td>fnmtRespNIF</td></tr>
</table></td></tr>
<tr><td colspan="2">15. Basic Constraints</td><td></td><td rowspan="2">[RFC 3280] This extension MAY appear as a critical or non-critical extension in end entity certificates.</td></tr>
<tr><td></td><td>Subject Type</td><td>Entidad Final</td></tr>
<tr><td colspan="2">16. CRLDistributionPoints</td><td>LDAP:
ldap://ldapape.cert.fnmt.es:puerto/CN=CRLnnn,OU= AC APE, O=FNMT, C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
HTTP:
http://www.cert.fnmt.es/crlsape/CRLnnn.crl</td><td></td></tr>
<tr><td colspan="2">17. Auth. Information Access</td><td>OCSP:
http://ocspape.cert.fnmt.es/ocspape/OcspResponder
CA:
http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt</td><td>Contendrá información de localización del OCSP Responder. URL resuelta a diferentes servidores. Ley de Firma Electrónica: “Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro”.</td></tr>
<tr><td colspan="2">18.netscapeCertType</td><td>sSLCLIENT,sMIME</td><td>Tipo de certificado según Netscape</td></tr>
<tr><td colspan="2">19. fnmtTipoCertificado</td><td>1.3.6.1.4.1.5734.1.33: “Sello Electrónico para Procesos Automatizados”</td><td>Tipo de certificado para Sello Electrónico para Procesos Automatizados</td></tr>
<tr><td colspan="2">20. AuthorityKeyIdentifier</td><td>2.5.29.35: Identificador de clave del prestador de servicios de certificación</td><td></td></tr>
</table>

Tabla 9 - Perfil del Certificado de Actuación Administrativa Automatizada emitido por la Autoridad de Certificación "AC APE" y bajo el OID 1.3.6.1.4.1.5734.3.13

"AC ADMINISTRACIÓN PÚBLICA"

Actuación Administrativa Automatizada emitido por la Autoridad de Certificación "AC Administración Pública" y bajo el OID 1.3.6.1.4.1.5734.3.3.3.2				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
1. Version		2	Sí	Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado.	Sí	Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}). El número de serie se asignará de forma creciente .
3. Signature Algorithm		Sha1withRsaEncryption	Sí	String UTF8 (40). Identificando el tipo de algoritmo (OID 1.3.14.3.2.26)
4. Issuer Distinguish Name		Entidad emisora del certificado	Sí	
	4.1. Country	C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	4.4. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. serialNumber=Q2826004J	Sí	PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	4.5. Common Name	cn=AC Administración Pública	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
5. Validity		3 años	Sí	Validez máxima limitada por "Esquema de Identificación y Firma. Perfiles de Certificados"
6. Subject		Identificación/descripción del c ustodio/responsable de las claves certificadas	Sí	
	6.1. Country	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas. C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)

	6.2. Organization	Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación (custodio del certificado)	Sí	UTF8 String, tamaño máximo 128 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=sello electrónico	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	6.4. Serial Number	Número único de identificación de la Entidad suscriptora de servicios de certificación. En este caso el NIF	Sí	Por ejemplo: serialNumber=Q2826004J PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	6.5. Common Name	Denominación de sistema o aplicación de proceso automático. Se deberá asegurar que dicho nombre tenga sentido y no de lugar a ambigüedades	Sí	UTF8String (rfc5280). Por ejemplo: cn=SERVICIO DE REGISTRO DEL MEH
7. Authority Key Identifier		Identificador de la clave pública del PSC. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la AC emisora.
8. Subject Public Key Info		Clave pública de la sede, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048
9. Subject Key Identifier		Identificador de la clave pública del suscriptor o poseedor de claves. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage				
	10.1. Digital Signature	1		Permite realizar la operación de firma electrónica
	10.2. Content Commitment	1		Se refiere a la cualidad de un tipo de certificado que indica al software en el que se usa que debe permitir que el usuario conozca lo que firma (firma de contratos, acuses de recibo, resguardos, etc.)
	10.3. Key Encipherment	1		Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras
	10.4. Data Encipherment	1		Se utiliza para cifrar datos que no sean claves criptográficas.
	10.5. Key Agreement	0		Para uso en el proceso de acuerdo de claves
	10.6. Key Certificate Signature	0		Se permite usar para firmar certificados. Se utiliza en los certificados de autoridades de certificación.
	10.7. CRL Signature	0		Se permite usar para firmar listas de revocación de certificados.

11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	Esta extensión indica que uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, además de o en lugar de los usos básicos que se indican en la extensión KeyUsage.
	11.1. Email protection	1.3.6.1.5.5.7.3.4	Sí	Proteción de correo electrónico
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2		Autenticación de cliente
	11.3. Any Extended Key Usage	Otros propósitos (ver comentario de columna "Especificaciones" 2.5.29.37.0	Sí	*[RFC5280]: 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.*
12. Qualified Certificate Statements		Extensiones cualificadas.		ETSI TS 101 862 define la inclusión de ciertas declaraciones para certificados cualificados
	12.1. QcCompliance	Certificado es qualificado (OID: 0.4.0.1862.1.1)	Sí	Indica que el certificado es qualificado. Solo si no está explicito en las políticas indicadas en la extensión correspondiente.
	12.2. QcEuRetentionPeriod	15 años (OID: 0.4.0.1862.1.3)	Sí	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: "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.".
	12.3. QcLimitValue	0 € (OID: 0.4.0.1862.1.2)	Sí	Límite de responsabilidad
	12.4. QcSSCD	Claves generadas en un DSCF (OID: 0.4.0.1862.1.4)	No	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. Este valor sólo se consignará cuando se pueda asegurar que las clave privada ha sido generada en un DSCF de forma fehaciente (mecanismo técnico o proceso auditado)
13. Certificate Policies		Política de certificación	Sí	
	13.1. Policy Identifier	Identificador unívoco de la política de certificación asociada a los certificados de tipo "sello electrónico". En este caso: 1.3.6.1.4.1.5734.3.3.3.2	Sí	Identificador de la política de certificado para Sello-Nivel medio

	13.2. Policy Qualifier Id				
		13.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	IA5String String. URL de las condiciones de uso.
		13.2.2 User Notice	Certificado reconocido de sello electrónico de Admon., órgano o entidad de derecho público. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM (C/Jorge Juan 106-28009-Madrid-España)	Sí	UTF8 String. Longitud máxima 200 caracteres.
14. Subject Alternative Names			Identificación/ descripción de Identidad Administrativa	Sí	
	14.1. rfc822 Name		Correo electrónico de contacto de la Sede (entidad suscriptora)	Opcional	Por ejemplo: rfc822Name=sellomeh@meh.es Se establecerá el valor del e-email contacto entidad suscriptora si se aporta en la solicitud de certificado. En caso contrario no se rellenerá este valor
	14.2. Directory Name		Identidad Administrativa	Sí	Campos específicos definidos por la Administración para los certificados LAECSP.
		14.2.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.2.2.1 =sello electrónico	Sí	UTF8 String.
		14.2.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.2.2.2=<Entidad Suscriptora>	Sí	UTF8 String. Por ejemplo: 2.16.724.1.3.5.2.2.2=Ministerio de Economía y Hacienda
		14.2.3 NIF Entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.2.2.3 =<NIF>	Sí	UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.2.2.3=Q2826004J
		14.2.4 Denominación de Sistema o componente	Breve descripción del componente asociado al certificado de sello. 2.16.724.1.3.5.2.2.5 =<Denominación del Sistema>	Sí	UTF8 String, tamaño máximo 128. Por ejemplo: 2.16.724.1.3.5.2.2.5= SERVICIO DE REGISTRO DEL MEH
15. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	
	15.1. Distribution Point 1		Punto de publicación de la CRL1 http://www.cert.fnmt.es/crls_acape/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	UTF8String Ruta donde reside la CRL (punto de distribución 1).

	15.2. Distribution Point 2	Punto de publicación de la CRL2. ldap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Administraci%F3n%20P%Fablica,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	UTF8String. Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
16. Authority Info Access			Sí	
	16.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	Acceso al servicio OCSP
	16.2. Acces Location 1	http://ocspape.cert.fnmt.es/ocspape/OcspResponder	Sí	URL para acceder al servicio OCSP. No es necesario firmar las peticiones OCSP
	16.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	Emisor de la entidad emisora de certificados (CA Raíz) De la rfc 5280: "*the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user.*"
	16.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt	Sí	Ruta para descarga de certificados adiconales para la validación de la cadena de certificación. Ene ste caso la ruta del certificado raíz de la FNMT-RCM.
17. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	De la rf5280: " *This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	17.1. Subject Type	Entidad final (valor FALSE)		Con este certificado no se pueden emitir otros

Tabla 10 - Perfil del Certificado de Actuación Administrativa Automatizada emitido por la Autoridad de Certificación "AC Administración Pública" y bajo el OID 1.3.6.1.4.1.5734.3.3.3.2