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 LA COMISIÓN EUROPEA

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM / v1.4	12/7/2013
Revisado por:	FNMT-RCM / v1.4	12/7/2013
Aprobado por:	FNMT-RCM / v1.4	12/7/2013

HISTÓRICO DEL DOCUMENTO			
Versión	**Fecha**	**Descripción**	**Autor**
1.0	15/11/2010	Creación del documento	FNMT-RCM
1.1	22/12/2010	Inclusión de nuevas definiciones. Se incluye también el concepto de *Oficina de Registro* centralizada y *Entidades Competentes*	FNMT-RCM
1.1	21/2/2011	Se realizan modificaciones para admitir nombres de áreas o departamentos en el CN de los certificados ligeros, así como direcciones genéricas o de grupo asociadas a estas entidades.	FNMT-RCM
1.1	21/2/2011	Se elimina la información relativa a la gestión de las políticas de certificación puesto que figura en la DGPC	FNMT-RCM
1.1	21/06/2011	Actualizada la información de la extensión de AIA para los certificados para entidades finales. Nuevo valor: http://www.cert.fnmt.es/certs/ISACA.crt	FNMT-RCM
1.2	3/2/2012	Modificación de la tabla de perfiles de certificados: Los números de serie de los certificados se asignan de forma aleatoria	FNMT-RCM

HISTÓRICO DEL DOCUMENTO			
Versión	**Fecha**	**Descripción**	**Autor**
1.3	16/4/2013	Desglose de la política de certificados de servidor en dos grandes grupos: los de servidor web y los de actuación automatizada. Inclusión de dos nuevos tipos dentro de la política de certificados de servidor: - reconocido sin dispositivo seguro de creación de firma para firma de documentos - normalizado para firma o cifrado de documentos Sustitución del término titular por firmante o suscriptor.	FNMT-RCM
1.4	12/7/2013	Párrafo 233: Corregida la expresión "Titulares del Certificados" por "Suscriptoras de los Certificados". Párrafo 358: Incluido el compromiso con el contenido en las garantías que ofrece el uso de los certificados. Párrafo 423: Corregida la validez de los certificados de servidor a 1 año.	FNMT-RCM

Referencia: DPC/PCPCE0104/SGPSC/2013

Documento clasificado como: *Público*

ÍNDICES

ÍNDICE DE CONTENIDOS

Índices 3

1. Definiciones y abreviaturas 6

2. Organización de la documentación 8

3. Introducción y alcance 9

4. Referencias 10

5. Orden de prelación 11

6. Gestión del ciclo de vida de las claves del prestador de servicios de certificación 12

6.1. Gestión del ciclo de vida de las Claves 12
6.1.1. Generación de las *Claves* del *Prestador de Servicios de Certificación* 12
6.1.2. Almacenamiento, salvaguarda y recuperación de las Claves del Prestador de Servicios de Certificación 12
6.1.3. Distribución de los Datos de verificación de Firma del Prestador de Servicios de Certificación 12
6.1.4. Almacenamiento, salvaguarda y recuperación de las Claves Privadas de la Administración, Organismos y Entidades públicas usuarias 12
6.1.5. Uso de los Datos de Creación de Firma del Prestador de Servicios de Certificación 12
6.1.6. Fin del ciclo de vida de las Claves del Prestador de Servicios de Certificación 13
6.1.7. Ciclo de vida del hardware criptográfico utilizado para firmar Certificados 13

7. Operación y gestión de la Infraestructura de Claves Públicas 14

7.1. Disponibilidad de los servicios 14

7.2. Servicio de información y consulta sobre el estado de validez de los certificados 14

7.3. Gestión de la seguridad de la información y controles de seguridad 14

8. Difusión de Términos y Condiciones 16

9. Certificados Ligeros 17

9.1. Política de certificación para la emisión de Certificados Ligeros 17
9.1.1. Identificación 17
9.1.2. Tipología del Certificado Ligero 17
9.1.3. Comunidad y ámbito de aplicación 18
9.1.4. Responsabilidad y obligaciones de las partes 18
9.1.5. Límites de uso de los *Certificados Ligeros* 20

9.2. Prácticas de certificación particulares para los Certificados Ligeros 20
9.2.1. Servicios de Gestión de las *Claves* 21
9.2.2. Gestión del ciclo de vida de los *Certificados* 21
9.2.2.1. Procedimiento de solicitud y emisión del Certificado Ligero 21
9.2.2.2. Publicación del Certificado Ligero 24
9.2.2.3. Descarga e instalación del Certificado Ligero 24
9.2.2.4. Vigencia del Certificado Ligero 25
9.2.2.5. Revocación del Certificado Ligero 25
9.2.2.6. Suspensión del Certificado Ligero 27

10. Certificados Normalizados 29

10.1. Política de certificación para la emisión de Certificados Normalizados 29
10.1.1. Identificación 29
10.1.2. Tipología del Certificado Normalizado 29
10.1.3. Comunidad y ámbito de aplicación 30
10.1.4. Responsabilidad y obligaciones de las partes 30
10.1.5. Límites de uso de los *Certificados Normalizados* 32

10.2. Prácticas de certificación particulares para los Certificados Normalizados 32
10.2.1. Servicios de Gestión de las *Claves* 33
10.2.2. Gestión del ciclo de vida de los *Certificados* 33
10.2.2.1. Procedimiento de solicitud y emisión del Certificado Normalizado 33
10.2.2.2. Publicación del Certificado Normalizado 36
10.2.2.3. Descarga e instalación del Certificado Normalizado 36
10.2.2.4. Vigencia del Certificado Normalizado 36
10.2.2.5. Revocación del Certificado Normalizado 37
10.2.2.6. Suspensión del Certificado Normalizado 39

11. Certificados Reconocidos 41

11.1. Política de certificación para la emisión de Certificados Reconocidos 41
11.1.1. Identificación 41
11.1.2. Tipología del Certificado Reconocido 41
11.1.3. Comunidad y ámbito de aplicación 42
11.1.4. Responsabilidad y obligaciones de las partes 42
11.1.5. Límites de uso de los *Certificados Reconocidos* 44

11.2. Prácticas de certificación particulares para los Certificados Reconocidos 45
11.2.1. Servicios de Gestión de las *Claves* 45
11.2.2. Preparación de los *Dispositivos Seguros de Creación de Firma* 45
11.2.3. Gestión del ciclo de vida de los *Certificados* 45
11.2.3.1. Procedimiento de solicitud y emisión del Certificado Reconocido 45
11.2.3.2. Publicación del Certificado Reconocido 48
11.2.3.3. Descarga e instalación del Certificado Reconocido 48
11.2.3.4. Vigencia del Certificado Reconocido 49
11.2.3.5. Revocación del Certificado Reconocido 49
11.2.3.6. Suspensión del Certificado Reconocido 51
11.2.4. Exclusiones y requisitos adicionales a ETSI TS 101 456 52

12. Certificados de Servidor 53

12.1. Política de Certificación de los Certificados de Servidor Web 53
12.1.1. Identificación 53
12.1.2. Tipología del *Certificado de servidor web* 53
12.1.3. Comunidad y ámbito de aplicación 54
12.1.4. Responsabilidad y obligaciones de las partes 55
12.1.5. Límites de uso de los Certificados de servidor web 56

12.2. Política de Certificación de los Certificados de Servidor de Actuación Automatizada 57
12.2.1. Identificación 57
12.2.2. Tipología del *Certificado de* Actuación Automatizada 57
12.2.3. Comunidad y ámbito de aplicación 59
12.2.4. Responsabilidad y obligaciones de las partes 59
12.2.5. Limitaciones de responsabilidad adicionales para los Certificados de Actuación Automatizada del tipo Reconocido sin DSCF para firma de documentos 61
12.2.6. Límites de uso de los Certificados de Actuación Automatizada 61

12.3. Prácticas de certificación particulares para los Certificados de servidor 62
12.3.1. Servicios de Gestión de las *Claves* 62
12.3.2. Gestión del ciclo de vida de los Certificados 62
12.3.2.1. Procedimiento de solicitud y emisión del Certificado de servidor 62
12.3.2.2. Publicación del Certificado de servidor 66
12.3.2.3. Descarga e instalación del Certificado de Servidor 66
12.3.2.4. Vigencia del Certificado de Servidor 66
12.3.2.5. Revocación del Certificado de servidor 67

Anexo I: Identificación de perfiles de certificación 69

ÍNDICE DE TABLAS

Tabla 1 - *Certificado Raíz* de la FNMT-RCM para la emisión de certificados para la Comisión Europea (Jerarquía subordinada al *Certificado Raíz* de la FNMT-RCM) 69

Tabla 2 – Perfil del *Certificado Ligero* 72

Tabla 3 – Perfil del *Certificado Normalizado* 75

Tabla 4 – Perfil del *Certificado Reconocido* 78

Tabla 5 – Perfil del *Certificado de Servidor web* (tipo Common Name) 82

Tabla 6 – Perfil del *Certificado de Servidor web* (tipo Wildcard) 85

Tabla 7 – Perfil del *Certificado de Actuación Automatizada* (tipo *Reconocido sin DSCF para firma de documentos*) 88

Tabla 8 – Perfil del *Certificado de Actuación Automatizada* (tipo *Normalizado para firma o cifrado de documentos)* 91

1. DEFINICIONES Y ABREVIATURAS

En el presente documento los siguientes términos tendrán las siguientes definiciones:

- *Autoridades Competentes*: Entidades designadas por alguno de los Estados Miembros de la Unión Europea, algún país de la EFTA (European Free Trade Association) u otro país, para el intercambio de información en un determinado contexto.
- *Autoridad Local de Registro (LRA)*: La *Organización* en el ejercicio de sus responsabilidades de identificación y autenticación de los *Usuarios* en nombre de *Prestador de Servicios de Certificación*
- *Aplicación*: Aplicación basada en tecnologías cliente/servidor que requiere mecanismos de seguridad en la "capa de aplicación" para el intercambio de información entre la *Autoridad Competente* y las instituciones, agencias y entidades.
- *Certificado de Servidor*: Es el certificado empleado para ser utilizado por una máquina sin necesidad de intervención directa de una persona en cada una de sus operaciones. Contempla dos tipos según la necesidad que cubren: los *Certificados de Servidor web* y los *Certificados de Actuación Automatizada.*
- *Certificado de Actuación Automatizada:* Es aquel *Certificado* empleado en operaciones automatizadas de firma y/o de cifrado de documentos.
- *Certificado de Servidor web*: Es aquel *Certificado* que permite identificar y autenticar a un servidor web o una URL.

  Dentro de esta categoría de *Certificado* de servidor, la FNMT-RCM emite un tipo especial de ***Certificado de Servidor web,*** **denominado Wildcard**, que permite a sus *Suscriptores*, miembros de la *Comunidad Electrónica UE*, identificar y autenticar todos los subdominios asociados a un dominio determinado, sin necesidad de adquirir y gestionar múltiples *Certificados*.
- *Certificado de Servidor web tipo "Common Name"*: *Certificado de Servidor web* expedido bajo [RFC5246] y que permite a un Servidor web o URL ser identificada y autenticada.
- *Certificado de Servidor web tipo "Wildcard"*: Un *Certificado de Servidor web* que permite al Firmante identificar y autenticar todos los subdominios asociados o derivados a un cierto nombre de dominio
- *Certificado Ligero*: *Certificado* emitido bajo un *Política de Certificación* que ofrece una calidad del servicio **menos gravosa** que la *Política de Certificación* para la emisión de *Certificados Reconocidos* (QCP) definida en ETSI 101 456
- *Certificado Normalizado*: *Certificado* emitido bajo una *Política de Certificación* que ofrece una calidad del servicio **equivalente** a la *Política de Certificación* para la emisión de *Certificados Reconocidos* (QCP) definida en ETSI 101 456
- *Certificado Reconocido*: *Certificado* emitido bajo una *Política de Certificación* que **incorpora los requisitos identificados en el anexo I y II** de la Directiva 1999/93/EC
- *Cliente OCSP*: Herramienta necesaria para poder hacer peticiones de información sobre el estado de validez de los *Certificados* siguiendo el protocolo *OCSP*.
- *Comunidad Electrónica UE*: Conjunto de personas y *Entidades usuarias* que se relacionan con *Certificados* entre sí o que confían en éstos y en la *Firma Electrónica* de la FNMT-RCM, bajo el marco general de la [DGPC] y las presentes *Políticas de Certificación* y el marco particular, si lo hubiera, de los correspondientes documentos de relación (acuerdos, contratos, formularios, etc.) que se hayan suscrito. Este concepto también puede ser referido como "Grupo (cerrado) ISA"

  El concepto de *Comunidad Electrónica UE* es exclusivo de las presentes *Políticas* y es excluyente con el de *Comunidad Electrónica* definido en [DGPC]
- *DGPC*: Declaración General de Prácticas de Certificación
- *Entidad usuaria*: Aquella *Organización* que se haya adherido al Contrato Marco formalizado con la Comisión Europea y que da lugar a la prestación de servicios de certificación objeto del presente documento.

- *Firmante (Certificate holder)*: Es la persona física que posee y custodia un dispositivo de creación de firma y que actúa (realiza la firma) en nombre del *Suscriptor* del *Certificado* de conformidad con sus facultades.
- *FNMT-RCM*: Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda. En el contexto de estas *Políticas de Certificación*, es el *Prestador de Servicios de Certificación.*
- *Oficinas de Registro (LRA Office)*: Oficinas instaladas por la *Organización* que se constituyen a fin de facilitar a los *Usuarios* la presentación de solicitudes relativas a los *Certificados*, con la finalidad de realizar la confirmación de su identidad y la entrega de los correspondientes títulos acreditativos de las cualidades personales, facultades de representación y demás requisitos exigidos para el tipo de *Certificado* que se solicite.
- *Organización:* La Comisión Europea (EC) e instituciones, agencias y entidades de la Unión Europea que participan en ella, así como cualquier otra agencia ejecutiva que la Comisión Europea decida establecer en Bruselas o Luxemburgo.
- *QCP*: Política de *Certificación* para la emisión de Certificados Reconocidos de conformidad con [ETSI456]
- *Referente de la LRA*: Es la persona responsable de las operaciones de registro realizadas por la *Organización* en calidad de *Autoridad Local de Registro*
- *Registrador (LRA Officer)*: Personal adscrito a la *Oficina de Registro* expresamente designado por el *Referente de la LRA* para el desempeño de las labores de registro de *Usuarios* de *Certificados* y para gestionar las solicitudes relativas a los mismos (emisión, revocación, suspensión y cancelación de la suspensión). Las actividades desempeñadas por los *Registradores* podrán ser igualmente llevadas a cabo por el *Referente de la LRA*.
- *Representantes de la Organización*: Persona física que por razón del cargo vincula y obliga a una *Organización* con el contenido del acuerdo de prestación de servicios de certificación suscrito con la FNMT-RCM.
- *Responsable del certificado de servidor*: Persona física o jurídica que tiene a su cargo la dirección, control y custodia del *Certificado de servidor*, así como los *Datos de Creación de Firma* o los *Datos de Descifrado* asociados.
- *SGSI*: Sistema de Gestión de la Seguridad
- *Solicitante*: Persona contratante con la FNMT-RCM que suscribe los términos y condiciones del servicio en nombre del *Suscriptor* del *Certificado*
- *SSL*: *Secure Sockets Layer*
- *Suscriptor* (de un *Certificado*): Es la *Organización* o *Entidad Competente* cuya identidad queda vinculada a los *Datos de verificación de firma* (Clave Pública) del *Certificado* del que es *Suscriptor* y emitido por el *Prestador de Servicios de Certificación*. Por tanto, la identidad del *Suscriptor* se vincula a lo firmado electrónicamente utilizando los *Datos de creación de firma* (Clave privada) asociados al *Certificado*.
- *TSL*: *Transport Security Layer*
- *Usuario* de los *Servicios de información y consulta del estado de los certificados*: Persona que, sin tener la condición de *Entidad usuaria*, confía en la FNMT-RCM para proporcionar información sobre el estado de los *Certificados* y que accede a dichos servicios con tal objeto.
- *Usuario* de un *Certificado*: *Firmante*

2. ORGANIZACIÓN DE LA DOCUMENTACIÓN

1. La FNMT-RCM estructura su *Declaración de Prácticas de Certificación* en varios documentos:

   - La [DGPC], que tiene por objeto la información pública de las condiciones y características generales de los servicios de certificación por parte de la FNMT-RCM como *Prestador de Servicios de Certificación*,
   - Cuantos anexos se consideren oportunos para la información pública de las condiciones de uso, limitaciones, responsabilidades, propiedades y cualquier otra información que se considere específica de cada tipo de *Certificado*. Estos anexos tendrán la condición de *Política y Prácticas de Certificación Particulares* del tipo de *Certificado* en cuestión

2. De esta forma, se considera como *Declaración de Prácticas de Certificación* de un determinado tipo de *Certificado* emitido por la FNMT-RCM al conjunto de los documentos formados por la [DGPC] y cuantos anexos especifiquen, desarrollen o particularicen las cuestiones relativas al tipo de *Certificado* en cuestión, es decir, la *Política y Prácticas de Certificación* particulares de dicho tipo de *Certificado*

3. El objetivo del presente documento es la información pública del conjunto de prácticas, condiciones y características de los servicios de certificación que presta la FNMT-RCM como *Prestador de Servicios de Certificación* en relación al ciclo de vida de los *Certificados* electrónicos para su uso en el ámbito de competencias de las *Organizaciones* y en el marco de la *Comunidad Electrónica UE*.

4. Así pues, el presente anexo trae causa y forma parte integrante de la *Declaración de Prácticas de Certificación* de la FNMT-RCM en lo relativo a los *Certificados* para su uso en el ámbito de competencias de las *Organizaciones* y en el marco de la *Comunidad Electrónica UE*, así como las *Prácticas de Certificación* empleadas en el ciclo de vida de éstos.

5. En conclusión, estas *Políticas* y *Prácticas de Certificación Particulares* concretan lo articulado en el cuerpo principal de la [DGPC], conformando, ambos documentos la *Declaración de Prácticas de Certificación* de la FNMT-RCM para los *Certificados* para su uso en el ámbito de competencias de las *Organizaciones* y en el marco de la *Comunidad Electrónica UE*. Lo descrito en este documento, sólo es de aplicación para el conjunto de *Certificados* caracterizados e identificados en estas *Políticas y Prácticas de Certificación Particulares*.

3. INTRODUCCIÓN Y ALCANCE

6. Este documento recoge las obligaciones y procedimientos que las partes se comprometen a cumplir en relación con la prestación por parte de la FNMT-RCM de servicios propios de una *Infraestructura de Claves Públicas* en el ámbito de competencias de las *Organizaciones* y en el marco de la *Comunidad Electrónica UE*.

7. Estos servicios, entre los que se encuentra la emisión de *Certificados*, posibilitarán a las *Entidades usuarias*, *Suscriptores* y *Usuarios* de los *Certificados*, de forma directa o indirecta y en determinados contextos, la realización de las siguientes operaciones: cifrado, autenticación, *Firma Electrónica*, no repudio e identificación.

8. Al objeto de que las *Entidades Usuarias, Suscriptores y Usuarios* puedan desarrollar servicios telemáticos con las garantías de seguridad adecuadas y, por otra parte, beneficiarse de cuantos pudieran estar establecidos y disponibles, la FNMT-RCM emitirá diferentes tipos de *Certificados*, cuyos requisitos, límites de uso y responsabilidades, ámbito de aplicación y procedimientos relacionados se declararán como apartados en el presente documento y que a continuación se enumeran:

    - Política de certificación para la emisión de "*Certificados ligeros*"[1]
    - Política de certificación para la emisión de "*Certificados normalizados*"[2]
    - Política de certificación para la emisión de "*Certificados reconocidos*"[3]
    - Política de certificación para la emisión de "*Certificados de servidor*"[4]

9. En especial deberá tenerse presente, a efectos interpretativos de estas *Políticas y Prácticas de Certificación Particulares*, el apartado "Definiciones" de la [DGPC].

---

[1] *Política de Certificación* que ofrece una calidad del servicio **menos gravosa** que la *Política de Certificación* para la emisión de *Certificados Reconocidos* (QCP) definida en ETSI 101 456

[2] *Política de Certificación* que ofrece una calidad del servicio **equivalente** a la *Política de Certificación* para la emisión de *Certificados Reconocidos* (QCP) definida en ETSI 101 456

[3] *Política de Certificación* que **incorpora los requisitos identificados en el anexo I y II** de la Directiva 1999/93/EC

[4] Dentro de la denominación de "*Certificados de servidor web*" se engloban los *Certificados* de servidor para un dominio concreto o de tipo Wildcard (varios subdominios dentro de un mismo dominio)

4. REFERENCIAS

[DGPC] Declaración General de Prácticas de Certificación

[D99/93EC] Directive 1999/93/EC of the European Parliament and of the council of 13 December 1999 on a community framework for electronic signatures

[D9546EC] Directive 1995/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[CD3602] Commission Decision of 16 August 2006 C(2006) 3602 concerning the security of information systems used by the European Commission

[ETSI456] ETSI TS 101 456: Policy requirement for certification authorities issuing qualified certificates

[ETSI042] ETSI TS 102 042: Policy requirements for certification authorities issuing public key certificates

[ETSI903] ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES)

[ETSI733] ETSI TS 101 733: CMS Advanced Electronic Signatures (CAdES)

[ETSI861] ETSI TS 101 861: Time Stamping Profile

[ETSI862] ETSI TS 101 862: Qualified Certificate Profile

[ETSI158] ETSI TS 102 158: Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates

[ETSI023] ETSI TS 102 023: Policy requirements for time-stamping authorities

[ISO9594] ISO/IEC 9594-8:2005: The Directory: Public-key and attribute certificate frameworks

[RFC5280] IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[RFC3647] IETF RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

[RFC5246] IETF RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2

5. ORDEN DE PRELACIÓN

10. Las presentes *Políticas y Prácticas de Certificación Particulares* de los *Certificados* emitidos para su uso en el ámbito de competencias de las *Organizaciones* y en el marco de la *Comunidad Electrónica UE*, tendrán prelación, en lo que corresponda y con carácter particular respecto de cada tipo de *Certificado*, sobre lo dispuesto en el cuerpo principal de la [DGPC]. Por tanto, en caso de que existiera contradicción entre el presente documento y lo dispuesto en [DGPC], tendrá preferencia lo aquí articulado.

11. No obstante lo anterior, en los contratos, acuerdos, formularios y condiciones que se suscriban entre la *Organización* y la FNMT-RCM o en el ámbito de relaciones entre las partes integrantes de la *Comunidad Electrónica UE*, podrán definirse especialidades que en caso de discrepancia serán de preferente aplicación.

6. GESTIÓN DEL CICLO DE VIDA DE LAS CLAVES DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

12. 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 su uso en el ámbito de competencias de las *Organizaciones* y en el marco de la *Comunidad Electrónica UE*, declara que realizará la siguiente gestión:

6.1. GESTIÓN DEL CICLO DE VIDA DE LAS *CLAVES*

6.1.1. Generación de las *Claves* del *Prestador de Servicios de Certificación*

13. 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 [DGPC].

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

14. 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 [DGPC]

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

15. 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 [DGPC]

16. Los campos del *Certificado Raíz* correspondiente a la jerarquía de certificación de los *Certificados* para su uso en el ámbito de competencias de las *Organizaciones* y en el marco de la *Comunidad Electrónica UE*, se pueden ver en la [DGPC]

17. 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*.

Para dicha emisión, la FNMT-RCM emplea *Datos de Creación de Firma* que se corresponden con su respectivo *Certificado* de *Autoridad de Certificación* (en cualquier caso, subordinada al *Certificado Raíz* de la FNMT-RCM identificado anteriormente). Este *Certificado* se encuentra definido en el anexo a este documento (

18. **Tabla 1 - *Certificado Raíz* de la FNMT-RCM para la emisión de certificados para la Comisión Europea (Jerarquía subordinada al *Certificado Raíz* de la FNMT-RCM)**)

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

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

6.1.5. Uso de los Datos de Creación de Firma del Prestador de Servicios de Certificación

20. 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.

6.1.6. Fin del ciclo de vida de las Claves del Prestador de Servicios de Certificación

21. 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.

6.1.7. Ciclo de vida del hardware criptográfico utilizado para firmar Certificados

22. 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.

7. OPERACIÓN Y GESTIÓN DE LA INFRAESTRUCTURA DE CLAVES PÚBLICAS

7.1. DISPONIBILIDAD DE LOS SERVICIOS

23. Los servicios objeto del presente documento declarativo (solicitud de certificados, registro, revocación y renovación) son monitorizados y controlados por los correspondientes sistemas de gestión de la disponibilidad.

24. El nivel de servicio que se establece para las actividades relacionadas con la *Infraestructura de Claves Públicas* incluidos en este documento será:

- de veinticuatro (24) horas del día, todos los días del año, salvo por circunstancias ajenas a la FNMT-RCM u operaciones de mantenimiento, que serán llevadas a cabo regularmente para asegurar la continuidad del servicio para el *Servicio de información y consulta del estado de validez de los Certificados* y
- en los días laborables, en horario de 9:30 a 17:30, según el calendario y hora oficial del *Prestador de Servicios de Certificación* para el resto de servicios

25. La FNMT-RCM notificará las operaciones de mantenimiento en la infraestructura a las *Organizaciones*, acordando con éstas las fechas y horario de su realización. Asimismo, también se informará 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.

7.2. SERVICIO DE INFORMACIÓN Y CONSULTA SOBRE EL ESTADO DE VALIDEZ DE LOS CERTIFICADOS

26. La FNMT-RCM pondrá a disposición de los interesados un servicio para consultas y obtención de información sobre el estado de los *Certificados* emitidos bajo las políticas definidas en el presente documento.

27. Los integrantes de la *Comunidad Electrónica UE* podrán realizar la comprobación del estado de un *Certificado* en la forma y condiciones que se expresan en este apartado.

28. Se entiende que el *Usuario* del *Servicio de información y consulta del estado de validez los Certificados*, por el mero hecho de acceder al servicio, acepta las condiciones de la *Declaración de Prácticas de Certificación* y sus obligaciones y responsabilidades como partes confiantes en los *Certificados* emitidos por la FNMT-RCM y *Firma electrónica* de ésta. La FNMT-RCM, previo al acceso del *Usuario* al referido servicio, pondrá a su disposición las condiciones antedichas.

29. El *Servicio de información y consulta sobre el estado de los certificados* se ofrecerá a través de la puesta a disposición del interesado de las *Listas de Revocación* pertinentes y a través del protocolo *OCSP*.

30. La FNMT-RCM dispone de un servicio de respuesta conforme al mencionado protocolo *OCSP* ("OCSP responder") que funciona de la siguiente forma: El servidor OCSP recibe la petición OCSP efectuada por un *Cliente OCSP* y comprueba el estado de los *Certificados* incluidos en la misma. Con la información sobre el estado de los *Certificados* compone una respuesta conforme al protocolo y se la remite al cliente.

31. Será responsabilidad del interesado obtener un *Cliente OCSP* para operar con el servidor *OCSP* puesto a disposición por la FNMT-RCM.

7.3. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CONTROLES DE SEGURIDAD

32. 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 [DGPC].

33. 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 forma que el servicio prestado por la FNMT-RCM tenga los niveles suficientes de fiabilidad que exige el mercado. El SGSI de la FNMT-RCM 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 y expuestos en el presente documento.

34. En [DGPC] se da respuesta concreta para todos aquellos aspectos referentes a los siguientes apartados de la norma ETSI TS 101 456:

- Gestión de la Seguridad.
- Clasificación y Gestión de Activos.
- Seguridad de Personal.
- Seguridad física y del entorno.
- Gestión de las Operaciones.
- Gestión de Accesos al Sistema.
- Gestión de incidencias y sistema de continuidad de negocio.
- Terminación de la FNMT-RCM como *Prestador de Servicios de Certificación*.
- Almacenamiento de la información referente a los *Certificados Reconocidos*.

8. DIFUSIÓN DE TÉRMINOS Y CONDICIONES

35. La FNMT-RCM pone a disposición de la *Comunidad Electrónica UE* y demás interesados, tanto el presente documento como la [DGPC]:

1) Los términos y condiciones que regulan la utilización de los *Certificados* expedidos por la FNMT-RCM.
2) La *Política de Certificación* aplicable a los *Certificados* expedidos por la FNMT-RCM.
3) Los límites de uso para los *Certificados* expedidos bajo las presentes *Políticas 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 las presentes *Políticas de Certificación*.
6) Reseña legal de interés, con referencia a las normas relativas a reclamaciones y resolución de conflictos.

9. CERTIFICADOS LIGEROS

9.1. POLÍTICA DE CERTIFICACIÓN PARA LA EMISIÓN DE CERTIFICADOS LIGEROS

9.1.1. Identificación

36. La presente *Política de Certificación* de la FNMT-RCM para la expedición de *Certificados Ligeros* para su uso en el ámbito de competencias de las *Organizaciones* y en el marco de la *Comunidad Electrónica UE*.

Nombre: *Política de Certificación* para la emisión de *Certificado Ligeros*

Referencia / OID[5]:

- 1.3.6.1.4.1.5734.3.4.3

Versión: 1.0

Fecha de emisión: 15 de noviembre 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/

9.1.2. Tipología del Certificado Ligero

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

- la identidad del firmante y custodio de las *Claves* y su condición de personal al servicio de la *Organización* que realiza firmas electrónicas utilizando el *Certificado* en nombre de la entidad actuante y,
- al *Suscriptor* del *Certificado*, que es la *Organización* o *Entidad Competente*.

38. Este *Certificado* se emite por la FNMT-RCM por cuenta de la *Organización* correspondientes y a la que la FNMT-RCM presta los servicios técnicos, administrativos y de seguridad necesarios como *Prestador de Servicios de Certificación*.

39. Los procesos necesarios para la gestión de este *Certificado* (emisión, revocación, renovación, etc.) son desarrollados por la FNMT-RCM mediante una infraestructura PKI específica, basada en actuaciones de identificación y registro realizadas por la red de *Oficinas de Registro* designadas por las *Organizaciones* y que son *Suscriptores* del *Certificados*.

40. [ETSI042] identifica una serie de requisitos para las *Políticas de Certificación* que, entre otros, emitan *Certificados* que tienen la denominación de "Lightweight Certificate". Esta denominación tiene su equivalencia en el término *Certificado Ligero* que se emplea en el presente documento.

41. Por cuanto antecede, los requisitos identificados en [ETSI042] para las *Políticas de Certificación* que emiten "*Certificados Ligeros*" son satisfechos en la presente *Política*. Adicionalmente, se señala que los *Certificados* emitidos bajo la presente política son emitidos con el perfil técnico correspondiente a los *Certificados Ligeros* con base en los criterios establecidos para tales *Certificados* en la normativa [ETSI042], tanto en lo referente al *Prestador de Servicios de Certificación*, como a la generación de los *Datos de Creación y Verificación de Firma* y al contenido del propio *Certificado*.

---

[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.

42. Por otra parte, [ETIS042] define los *Certificados Ligeros* como aquellos que son emitidos por una *Política de Certificación* que ofrece una calidad del servicio **menos gravosa** que la *Política de Certificación* para la emisión de *Certificados Reconocidos* (QCP) definida en [ETSI456].

43. La FNMT-RCM ha optado por rebajar las garantías de esta *Política de Certificación* para la emisión de *Certificados Ligeros* respecto a las definidas de *Certificados Reconocidos* definidas en [ETSI046] implantando un servicio de registro basado en la autenticación, al menos telemática, del *Firmante* y custodio de los *Datos de Creación de Firma*, no requiriéndose la personación física de éste último en la *Oficina de Registro*.

44. Los detalles del servicio de registro para esta *Política de Certificación* figuran más adelante en el apartado correspondiente.

9.1.3. Comunidad y ámbito de aplicación

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

a) Son expedidos por la FNMT-RCM como *Prestador de Servicios de Certificación* cumpliendo con los criterios establecidos en la Ley española 59/2003, de 19 de diciembre, de Firma Electrónica y en la Directiva Europea de Firma Electrónica [D99/93EC]

b) Son expedidos como *Certificados Ligeros* con base en los criterios establecidos para tal en la normativa técnica EESSI, concretamente en la *Política de Certificación* para la emisión de *Certificados Ligeros* identificados en la norma [ETSI042] – LCP (Lightweight Certificate Policy)

c) Los *Certificados* emitidos bajo esta *Política de Certificación* son expedidos para las *Organizaciones* que forman parte de la *Comunidad Electrónica UE,* tal y como se define en el apartado Definiciones de este documento. En el marco de esta *Política de Certificación*, los *Usuarios* y custodios de los *Datos de Creación de Firma* se corresponden con el personal de las *Organizaciones* en el ejercicio de sus competencias y funciones públicas propias del cargo, de la relación funcionarial, de las funciones del empleado público, o de la condición de autorizado por la *Organización*, en relación con la entidad a la que pertenezcan o con la que se relacionen estos *Usuarios*.

9.1.4. Responsabilidad y obligaciones de las partes

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

- Las *Organizaciones* y *Entidades Competentes* representadas a través de los diferentes órganos competentes y que son los *Suscriptores* responsables de los *Certificados*.
- *Oficinas de Registro*, que, a través del personal designado por la *Organización*, serán responsables de comprobar los requisitos y condiciones ostentados por los *Usuarios* del *Certificado*.
- Los *Usuarios* del *Certificado* y sus *Claves*, que será el personal al servicio de las *Organizaciones*.
- FNMT-RCM, en cuanto *Prestador de Servicios de Certificación*.
- El resto de la *Comunidad Electrónica UE*.

47. El régimen de derechos y obligaciones de la *Organización* y la FNMT-RCM se regirá mediante los correspondientes acuerdos reguladores de los servicios de certificación.

48. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en este documento y en la [DGPC], la *Organización* como *Autoridad Local de Registro*, el *Referente de la LRA* y los *Registradores* tienen la obligación de:

- Cumplir con los procedimientos de registro facilitados por la FNMT-RCM.

- No realizar registros o tramitar solicitudes de personal que preste sus servicios en una *Organización* diferente a la que representa como *Oficina de Registro*, sin perjuicio de la creación, en la propia Comisión Europea, de *Oficinas de Registro* centralizadas que se hayan establecido.
- Comprobar fehacientemente los datos del personal al servicio de la *Organización* referidos a su identidad y su pertenencia a dicha *Organización* a la que presta sus servicios y, en su caso, cualquier otro dato que refleje o caracterice esta pertenencia.
- Solicitar la revocación o suspensión del *Certificado Ligero* para el personal al servicio de la *Organización* a la que representa la *Oficina de Registro*, cuando alguno de los datos consignados en el *Certificado* sea inexacto, incorrecto, haya variado o sea de necesaria revocación por razones de seguridad. También deberá solicitar la revocación o suspensión cuando se den las circunstancias previstas en la legislación aplicable.
- Solicitar a la FNMT-RCM la revocación del *Certificado* cuando las circunstancias que afecten a la condición del cargo, puesto de trabajo, empleo o cualquier otro dato que refleje o caracterice la relación del *Usuario* del *Certificado* con la *Organización* donde presta sus servicios, sean inexactas, incorrectas, hayan variado o sean de necesaria revocación por razones de seguridad.
- Solicitar a la FNMT-RCM, a través de la *Oficina de Registro*, la revocación o suspensión del *Certificado* cuando, directamente o a través de comunicación del personal al servicio de *Organización*, exista pérdida, extravío del soporte del *Certificado* o de su confidencialidad, o presunción de ello.
- Custodiar la documentación aportada por cualquiera de los intervinientes en los procesos de gestión de los *Certificados* (solicitudes de emisión, suspensión, cancelación de la suspensión, revocación y cualesquiera otros de la misma índole) así como los documentos generados en dichos procesos (justificantes, contratos de emisión, revocación, etc.)

49. Las relaciones de la FNMT-RCM con la *Organización* y los *Usuarios* de los *Certificados* quedarán determinadas, a los efectos del régimen de uso de los *Certificados*, por los siguientes documentos: condiciones de utilización o contrato de emisión del *Certificado*, y, subsidiariamente, las presentes *Políticas y Prácticas de Certificación Particulares* y por la [DGPC], atendiendo a los acuerdos o documentos de relación entre la FNMT-RCM y las *Organizaciones*.

50. Las relaciones de la *Organización* o *Entidad Competente Suscriptora* del *Certificado* y de su personal con la FNMT-RCM se realizarán siempre a través de la *Oficina de Registro* y su *Referente*. La FNMT-RCM no realizará ninguna acción solicitada por el personal al servicio de la *Organización* o *Usuario* del *Certificado* que no esté autorizada por *Referente de la LRA* o por la *Organización* o *Entidad Competente Suscriptora* del *Certificado*.

51. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la [DGPC], el *Usuario* del *Certificado* tiene la obligación de:

- No utilizar el *Certificado* cuando alguno de los datos referidos al cargo, puesto de trabajo, empleo o cualquier otro que dio lugar a la emisión del *Certificado* sea inexacto, incorrecto o no refleje o caracterice su relación con la *Organización* o *Entidad Competente Suscriptora*
- 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 la *Organización*.
- Mantener en todo momento el control exclusivo de los *Datos de Creación de Firma* y tomar las razonables precauciones para prevenir su pérdida, revelación, modificación o uso no autorizado
- Comunicar al *Referente de la LRA* correspondiente, la pérdida, extravío, o sospecha de ello, del soporte del *Certificado* o de su confidencialidad, del que es *Usuario* con el fin de iniciar, en su caso, los trámites de la revocación del *Certificado*.

52. El resto de la *Comunidad Electrónica UE* y los terceros regularán sus relaciones con la FNMT-RCM a través de la [DGPC] y estas *Políticas 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.

9.1.5. Límites de uso de los *Certificados Ligeros*

53. Constituyen límites de uso de este tipo de *Certificados* los sistemas de mensajería electrónica (correo electrónico) de las *Organizaciones* o *Entidades Competentes Suscriptoras* y las operaciones de autenticación y cifrado de datos que dentro de éstos se pudieran realizar. Fuera de la funcionalidad prevista anteriormente no se podrán emplear estos *Certificados*.

54. La FNMT-RCM y las *Organizaciones* podrán fijar en los acuerdos correspondientes otros límites adicionales.

55. FNMT-RCM no tendrá control sobre las actuaciones y usos de los *Certificados* que se realicen por parte del *Suscriptor*, *Usuario* o las *Oficinas de Registro*, por lo que la FNMT-RCM quedará exonerada de responsabilidad a efectos de tales usos y de la extralimitación en el uso establecido anteriormente, así como de las consecuencias y efectos que pudieran producirse por reclamaciones o posibles responsabilidades patrimoniales llevadas a cabo por cualquier miembro de la *Comunidad Electrónica UE* o por terceros.

56. Para que el *Usuario* utilice de forma diligente los *Certificados Ligeros* y *Claves* asociadas, la *Organización* a la que representa el usuario deberá previamente formar parte de la *Comunidad Electrónica UE* y haberse constituido como *Suscriptor* del *Certificado*.

57. En cualquier caso, si un tercero desea confiar en la *Firma electrónica* realizada con uno de estos *Certificados Ligeros* sin acceder a los *Servicios de información y consulta sobre el estado de validez de los certificados* emitidos bajo esta *Política de Certificación*, no se obtendrá cobertura de las presentes *Políticas y Prácticas de Certificación Particulares* y se carecerá de legitimidad alguna para reclamar o emprender acciones legales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado*.

58. Además, incluso dentro del ámbito de la *Comunidad Electrónica UE*, 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 *Sellado de Tiempo*
- 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
- Utilizar el *Certificado* para usos distintos a los inicialmente previstos respecto de los *Certificados Ligeros*

9.2. PRÁCTICAS DE CERTIFICACIÓN PARTICULARES PARA LOS CERTIFICADOS LIGEROS

59. 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*.

60. En especial deberá tenerse presente, a efectos interpretativos del presente anexo el apartado "Definiciones" de la [DGPC] y de este documento.

61. 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 Ligeros* expedidos bajo la *Política de Certificación* identificada con el OID 1.3.6.1.4.1.5734.3.4.3.

9.2.1. Servicios de Gestión de las *Claves*

62. La FNMT-RCM, bajo ningún concepto, genera ni almacena las *Claves Privadas* de los *Firmantes*, que son generadas bajo su exclusivo control y, en su caso, con la intervención de la *Oficina de Registro* correspondiente y cuya custodia está bajo responsabilidad del *Usuario* del *Certificado*.

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

63. Se definen aquí aquellos aspectos que, si bien algunos ya han sido apuntados en la [DGPC], revisten determinadas especialidades que necesitan un mayor nivel de detalle.

9.2.2.1. Procedimiento de solicitud y emisión del Certificado Ligero

64. A continuación se describe el procedimiento de solicitud por el que el *Registrador* toma los datos del personal al servicio de la *Organización*, confirma su identidad y se formaliza, entre el citado personal y la FNMT-RCM, el documento de condiciones de utilización o el contrato de emisión, según lo previsto en el acuerdo de la FNMT-RCM con la *Organización* para la posterior emisión de un *Certificado Ligero*.

65. Se hace constar que FNMT-RCM, en función de la relación de *Suscriptores* y personal *Usuario* dependiente remitida por la *Oficina de Registro*, considerará, bajo responsabilidad de las correspondientes *Organizaciones* o *Entidades Competentes*, que actuarán a través de las *Oficinas de Registro* como *Autoridad Local de Registro*, que este personal se encuentra con su cargo vigente, que sus datos personales son auténticos y están en vigor y, por tanto, habilitado para obtener y usar el *Certificado*.

66. La Comisión Europea podrá establecer, en el ámbito de actuación de sus competencias, *Oficinas de Registro* centrales o comunes con efectos uniformes para cualesquiera de las diferentes entidades de los Estados Miembro

67. FNMT-RCM, no tendrá, en este tipo de *Certificado*, la responsabilidad de comprobar el cargo o empleo del *Usuario*, así como que estos requisitos se mantienen durante toda la vida del *Certificado*. La FNMT-RCM no mantiene relación jurídica funcionarial, administrativa o laboral con el *Usuario*, más allá del documento de condiciones de utilización o, en su caso, contrato de emisión.

68. Las actividades de comprobación anteriores serán realizadas por el personal de la *Oficina de Registro* implantada por la *Organización*, que es la entidad donde el *Usuario* presta sus servicios. Por tanto y a estos efectos las *Oficinas de Registro* no serán autoridades delegadas o dependientes de la FNMT-RCM.

69. Este *Certificado* será solicitado por la *Organización* o *Entidad Competente Suscriptora* quien actuará como solicitante sin perjuicio de que las operaciones necesarias para la petición y obtención del *Certificado* se realicen por el *Referente* o el *Registrador* o, de manera instrumental, por los propios *Usuarios*.

70. Los tres pasos a realizar para la obtención del *Certificado* son:

9.2.2.1.1. Presolicitud (Paso 1)

71. Con carácter previo, el *Usuario* y el *Suscriptor* deberán consultar la [DGPC] y las presentes *Políticas 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 *Suscriptor*, respectivamente, del *Certificado*, que se plasmaran en el documento de condiciones de utilización o, si procede, el contrato de emisión.

72. El *Usuario* deberá acceder a la dirección electrónica https://ec.fnmt.es donde se mostrarán las instrucciones para realizar una generación de *Claves*. En esta dirección deberá introducir su nombre, primer apellido y dirección de correo electrónico en el punto de recogida de datos dispuesto para ello.

73. En el caso de que se desee un *Certificado Ligero* para una unidad organizativa dependiente del *Suscriptor* del *Certificado*, el *Usuario* podrá introducir en estos campos los datos referidos al nombre de dicha unidad. Asimismo, la dirección de correo facilitada podrá corresponderse con un buzón genérico –no personal- de dicha unidad.

74. A continuación se generarán las *Claves Pública* y *Privada* que serán vinculadas al *Certificado*, convirtiéndose en su momento en *Datos de Verificación y Creación de Firma* respectivamente.

75. 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*.

76. La FNMT-RCM, tras recibir esta información, comprobará mediante la *Clave Pública* del *Usuario* la validez de la información de la presolicitud firmada, comprobando, únicamente, la posesión y correspondencia de la pareja de *Claves* criptográficas por parte de éste.

77. Si todo es correcto, la FNMT-RCM asignará un código de solicitud a la petición realizada por el *Usuario* y se lo indicará en una página web de respuesta.

78. 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*.

9.2.2.1.2. Acreditación de la identidad y solicitud (Paso 2)

79. Una vez que el *Usuario* ha obtenido el código de solicitud en el subproceso de "Presolicitud" deberá realizar la correspondiente solicitud de emisión de *Certificado* a través de la *Oficina de Registro* que le corresponda (aquella que representa a la *Organización* ante la FNMT-RCM en las operaciones de gestión de *Certificados* y en la que el *Usuario* presta sus servicios).

80. Esta solicitud podrá realizarse bien por personación física o de forma telemática. En cualquier caso, el *Registrador* autenticará al *Usuario* mediante el requerimiento de aportación de

- datos personales (como mínimo el nombre, primer apellido, correo electrónico y número distintivo del documento oficial a aportar) y datos vinculados a la solicitud en cuestión (código de solicitud) y
- la documentación correspondiente y consistente en el documento oficial que acredite la identidad del *Usuario*.

Nota: En el caso de haberse introducido en los campos nombre, apellido y correo electrónico datos genéricos referidos a una unidad organizativa dependiente del *Suscriptor*, el *Usuario* también deberá aportar documentación acreditativa de las facultades de representación bastante para realizar dicha solicitud en nombre de la unidad organizativa en cuestión.

81. Adicionalmente, el *Registrador* requerirá al *Usuario* la aportación (presencialmente, por correo electrónico o fax) de una fotocopia del documento oficial que acredite la identidad de éste y en el que figuren los datos referidos a la identidad del *Usuario*. Estos documentos serán custodiados por la *Oficina de Registro* como parte de la solicitud.

82. El *Registrador* comprobará la condición del *Usuario* como empleado de la *Organización* o *Entidad Competente Suscriptora* del *Certificado* y con cargo vigente, así como la veracidad del correo electrónico, todo ello por los medios que tenga a su disposición y habida cuenta de que la *Oficina de Registro* actúa en representación de la *Organización* en cuestión y por tanto conoce de forma fehaciente esta información.

83. FNMT-RCM, no tendrá la responsabilidad de comprobar los datos personales, la condición de empleado, ni el correo electrónico del *Usuario*, así como que estos requisitos o

condiciones se mantienen durante toda la vida del *Certificado*, al no ostentar relación jurídica funcionarial, administrativa o laboral con el *Usuario*, 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.

84. La aportación de estos datos y documentos avalarán la identidad del *Usuario* y será condición necesaria y suficiente para el establecimiento del vínculo entre identidad y *Datos de Creación de Firma* que se crea en el momento de la emisión del *Certificado*.

85. No es necesaria la personación física del interesado en la *Oficina de Registro* puesto que esta *Política de Certificación* conlleva unas condiciones de emisión menos gravosas que las recogidas en [ETSI456] y además la *Oficina de Registro* tiene constancia previa de los datos identificativos del *Usuario* por pertenecer a la misma *Organización*. Adicionalmente este forma de acreditación está en plena sintonía con los requisitos establecidos para las *Políticas de Certificación* para la emisión de "Lightweight Certificates" (*Certificados Ligeros*) o LCP definidas en [ETSI042].

86. Una vez que el *Registrador* confirme la identidad del *Usuario*, la vigencia de su cargo o empleo en la *Organización* y habiendo aceptado el documento de condiciones de utilización o, en su caso, el contrato de solicitud por el *Usuario* y la *Oficina de Registro*, ésta procederá a validar los datos y a enviarlos a la FNMT-RCM junto con el código de solicitud recogido en la fase de presolicitud.

87. La *Oficina de Registro* recibirá un justificante con los datos de la solicitud realizada y que deberá custodiar como parte de ésta.

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

89. 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.

9.2.2.1.3. Emisión del Certificado (Paso 3)

90. Una vez recibidos en la FNMT-RCM los datos personales del *Usuario*, la información que describe su relación con la *Organización* o *Entidad Competente Suscriptora* del *Certificado*, así como el código de solicitud obtenido en la fase de presolicitud, se procederá a la emisión del *Certificado*.

91. La emisión de *Certificados* supone la generación de documentos electrónicos que confirman la identidad del *Firmante,* su relación con la *Organización* así como su correspondencia con la *Clave Pública* asociada.

92. La emisión de los *Certificados* sujetos a las presentes *Políticas* sólo puede realizarse por la FNMT-RCM en su calidad de *Prestador de Servicios de Certificación*, no existiendo ninguna otra entidad u organismo con capacidad de emisión de los mismos.

93. La FNMT-RCM, por medio de su *Firma electrónica*, autentica el *Certificado* y confirma la identidad del *Suscriptor,* así como su relación con el *Usuario*, 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 el *Certificado*, la FNMT-RCM utilizará mecanismos criptográficos que doten de autenticidad e integridad al *Certificado*.

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

- Comprobar que el *Usuario* del *Certificado* utiliza la *Clave Privada* correspondiente a la *Clave Publica* vinculada a la identidad del *Firmante* 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 Claves Públicas* de la FNMT-RCM.

95. Para la emisión del *Certificado Ligero* se seguirán los siguientes pasos:

1. Composición del nombre distintivo (DN) del *Certificado Ligero*

   Con los datos personales del *Usuario* 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 este tipo de *Certificados* está compuesto de los siguientes elementos:

   DN≡CN, O, C

   El conjunto de atributos O, C representa la rama del directorio en la que se encuentra ubicada la entrada correspondiente a los *Certificados Ligeros* emitidos al *Usuario* al servicio de la *Organización* en cuestión.

   El atributo *CN* contiene los datos de identificación del *Usuario* o, en su caso, los datos de identificación de la unidad organizativa dependiente del *Suscriptor* del *Certificado*.

   El atributo O contiene el nombre de la *Organización*.

   El atributo C contiene el código de país al que pertenece la *Organización*.

   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 *Usuario*

   La identidad alternativa del *Usuario*, tal como se contempla en la presente tipología de *Certificados*, contiene la dirección de correo electrónico de éste aportada durante los procesos de presolicitud y acreditación de la identidad. Se utiliza la extensión subjectAltName definida en *X.509* versión 3 para ofrecer esta información.

3. Generación del *Certificado* conforme al perfil del *Certificado Ligero*.

   El formato del *Certificado Ligero* estará en consonancia con la norma UIT-T X.509 versión 3 y de acuerdo con la normativa legalmente aplicable.

   En la **Tabla 2 – Perfil del *Certificado Ligero*** anexa a este documento puede consultarse el perfil de este tipo de *Certificados*

9.2.2.2. Publicación del Certificado Ligero

96. Una vez generado el *Certificado* por parte del *Prestador de Servicios de Certificación*, se publicará en el *Directorio*, concretamente en la entrada correspondiente a la *Organización*.

97. A la dirección de correo electrónico proporcionada por el *Usuario* se le enviará una comunicación de la disposición de su *Certificado* para su descarga.

9.2.2.3. Descarga e instalación del Certificado Ligero

98. Una vez generado el *Certificado*, se pone a disposición del *Usuario* un mecanismo de descarga en la dirección https://ec.fnmt.es accediendo a la opción “Descarga de su Certificado”.

99. En este proceso guiado se le pedirá al interesado que introduzca su nombre, primer apellido y correo electrónico con el que se realizó el proceso de presolicitud, así como el código de solicitud devuelto por el sistema al finalizar dicho proceso.

100. Si el *Certificado* no ha sido aún generado por cualquier motivo, se le indicará este hecho en el momento que intente su descarga. En caso contrario se pondrá a disposición del interesado, quien lo introducirá en el soporte en el que se generaron las *Claves* durante el proceso de presolicitud.

9.2.2.4. Vigencia del Certificado Ligero

9.2.2.4.1. Caducidad

101. Los *Certificados Ligeros* emitidos bajos la presente *Política de Certificación* 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 *Suscriptor* desee seguir utilizando los servicios del *Prestador de Servicios de Certificación.*

9.2.2.4.2. Extinción de la vigencia

102. Los *Certificados Ligeros* emitidos por la FNMT-RCM bajo la presente política 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*, 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 pérdida 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

103. A los efectos enumerados anteriormente, se hace constar que la solicitud de emisión de un *Certificado Ligero* cuando exista otro vigente a favor del mismo *Usuario* y *Suscriptor* y bajo la misma *Política de Certificación* conllevará la revocación del primero obtenido.

104. 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 validez de los certificados*.

9.2.2.5. Revocación del Certificado Ligero

9.2.2.5.1. Causas de revocación del Certificado Ligero

105. Serán causas de revocación de un *Certificado Ligero*:

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* o sospecha del compromiso de la confidencialidad de éste
- La utilización por un tercero de los *Datos de Creación de Firma*, correspondientes a los *Datos de Verificación de Firma* contenidos en el *Certificado* y vinculados a la identidad del *Firmante*.
- La violación o puesta en peligro del secreto de los *Datos de Creación de Firma*.
- La no aceptación de la *Organización* o *Entidad Competente* 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, así como los supuestos previstos en la legislación aplicable.

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

d) Terminación de la relación entre el *Usuario* y la *Organización* o *Entidad Competente Suscriptor* del *Certificado*

e) Incapacidad sobrevenida, total o parcial, o fallecimiento del *Usuario*.

f) Inexactitudes o alteraciones en los datos aportados por el *Usuario* para la obtención del *Certificado* o modificación de las circunstancias verificadas para su expedición, 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 *Usuario,* del *Suscriptor* del *Certificado* o del personal de la *Oficina de Registro* si hubiese podido afectar al procedimiento de emisión del *Certificado*.

h) Resolución del contrato suscrito entre la *Organización* 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.

106. 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.

107. 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, incluyendo las causas antes mencionadas, a la FNMT-RCM, producirán la exoneración de responsabilidad de la FNMT-RCM.

9.2.2.5.2. Efectos de la revocación

108. 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 validez de los certificados*.

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

9.2.2.5.3. Procedimiento para la revocación

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

111. La revocación de un *Certificado Ligero* puede ser solicitada por el *Suscriptor* a través del *Referente de la LRA* o de los *Registradores.* Asimismo, el *Usuario* podrá plantear a la *Oficina de Registro* la revocación o suspensión si existen causas que lo justifiquen, en los términos recogidos en la presente *Política y Prácticas de Certificación Particulares*.

112. Sin perjuicio de lo anterior, la FNMT-RCM podrá revocar los *Certificados Ligeros* en los supuestos recogidos en la *Declaración de Prácticas de Certificación* y en la legislación aplicable.

113. El *Usuario* o el *Suscriptor* a través de un representante con capacidad suficiente podrá solicitar la operación de revocación bien personándose en la *Oficina de Registro* correspondiente, bien vía telemática. El *Registrador* deberá comprobar la capacidad suficiente del peticionario para realizar la solicitud de revocación.

114. En cualquiera de los casos, el peticionario deberá acreditar la identidad del *Usuario* del *Certificado* a revocar mediante la aportación de los datos personales de éste (al menos nombre, primer apellido y correo electrónico).

115. El registrador formalizará la petición de revocación mediante la aplicación de registro, que generará dos impresos con el contrato de solicitud, para su posterior impresión.

116. Después de que el *Registrador* confirme la identidad del peticionario, la vigencia de su cargo o empleo en la *Organización* y habiendo firmado los impresos contractuales, el *Registrador* procederá a validar los datos y a enviarlos a la FNMT-RCM.

117. La *Oficina de Registro* deberá custodiar los impresos justificativos de la solicitud como parte de ésta.

118. La FNMT-RCM recibirá aquella información relevante a efectos de la revocación de un *Certificado* a través el modelo de solicitud de revocación que se le presente, en formato papel o electrónico, por la *Oficina de Registro*.

119. La *Oficina de Registro* transmitirá las solicitudes a la FNMT-RCM para que proceda a la revocación del *Certificado*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

120. FNMT-RCM considerará que el peticionario de la revocación de un *Certificado* de este tipo cuenta con la capacidad suficiente si la petición es realizada a través de la *Oficina de Registro* correspondiente. FNMT-RCM no valorará la conveniencia de la solicitud de revocación cuando ésta sea realizada a través de la *Oficina de Registro* antedicha.

121. 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. De forma análoga esta información también estará disponible mediante el protocolo OCSP en el correspondiente *Servicio de información sobre el estado de validez de los Certificados*.

9.2.2.6. Suspensión del Certificado Ligero

122. 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.

9.2.2.6.1. Causas de la suspensión del Certificado Ligero

123. La FNMT-RCM podrá suspender la vigencia de los *Certificados* ante una solicitud de las mismas personas autorizadas y bajo las mismas condiciones que para la solicitud de revocación.

124. 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.

9.2.2.6.2. Efectos de la suspensión

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

9.2.2.6.3. Procedimiento para la suspensión de Certificados

126. Los procedimientos y personas autorizadas para la solicitud y tramitación de la revocación del *Certificado* son de aplicación en el caso de la suspensión.

127. La *Oficina de Registro* transmitirá las solicitudes tramitados a la FNMT-RCM para que proceda a la suspensión del *Certificado*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

128. La FNMT-RCM suspenderá el *Certificado* de forma provisional durante un plazo de quince (15) días, plazo tras el cual se extinguirá el *Certificado* mediante su revocación directa por parte del *Prestador de Servicios de Certificación*, salvo que se hubiera cancelado la suspensión. No obstante lo anterior, el plazo previsto para la suspensión del *Certificado* podrá verse alterado en función de la duración de las investigaciones o los procedimientos judiciales o administrativos que lo pudieran afectar.

129. Una vez que la FNMT-RCM ha procedido a la suspensión 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. De forma análoga esta información también estará disponible mediante el

protocolo OCSP en el correspondiente *Servicio de información sobre el estado de validez de los Certificados*.

130. 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.

9.2.2.6.4. Cancelación de la suspensión del Certificado Ligero

131. Podrán solicitar la cancelación de la suspensión de los *Certificados Ligeros* las mismas personas legitimadas para la solicitud de la suspensión, en las mismas condiciones y siguiendo los mismos procedimientos.

132. La *Oficina de Registro* transmitirá las solicitudes a la FNMT-RCM para que ésta proceda a la cancelación de la suspensión del *Certificado*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

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

10. CERTIFICADOS NORMALIZADOS

10.1. POLÍTICA DE CERTIFICACIÓN PARA LA EMISIÓN DE CERTIFICADOS NORMALIZADOS

10.1.1. Identificación

134. La presente *Política de Certificación* de la FNMT-RCM para la expedición de *Certificados Normalizados* para su uso en el ámbito de competencias de las *Organizaciones* y en el marco de la *Comunidad Electrónica UE*.

Nombre: *Política de Certificación* para la emisión de *Certificados Normalizados*

Referencia / OID:

- 1.3.6.1.4.1.5734.3.4.2

Versión: 1.0

Fecha de emisión: 15 de noviembre 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/

10.1.2. Tipología del Certificado Normalizado

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

- la identidad del *Firmante* y custodio de las *Claves* y su condición de personal al servicio de la *Organización* que realiza firmas electrónicas utilizando el *Certificado* en nombre de la entidad actuante y,
- al *Suscriptor* del *Certificado*, que es la *Organización* o *Entidad Competente*.

136. Este *Certificado* se emite por la FNMT-RCM por cuenta de la *Organización* correspondientes y a la que la FNMT-RCM presta los servicios técnicos, administrativos y de seguridad necesarios como *Prestador de Servicios de Certificación*.

137. Los procesos necesarios para la gestión de este *Certificado* (emisión, revocación, renovación, etc.) son desarrollados por la FNMT-RCM mediante una infraestructura PKI específica, basada en actuaciones de identificación y registro realizadas por la red de *Oficinas de Registro* designadas por las *Organizaciones* y que son *Suscriptoras* del *Certificados*.

138. [ETSI042] identifica una serie de requisitos para las *Políticas de Certificación* que entre otros, emitan *Certificados* que tienen la denominación de "Normalized Lightweight Certificate". Esta denominación tiene su equivalencia en el término *Certificado Normalizado* que se emplea en el presente documento.

139. Por cuanto antecede, los requisitos identificados en [ETSI042] para las *Políticas de Certificación* que emiten "*Certificados Normalizados*" son satisfechos en la presente *Política*. Adicionalmente, se señala que los *Certificados* emitidos bajo la presente política son emitidos con el perfil técnico correspondiente a los *Certificados Normalizados* con base en los criterios establecidos para tales *Certificados* en la normativa [ETSI042], tanto en lo referente al *Prestador de Servicios de Certificación*, como a la generación de los *Datos de Creación y Verificación de Firma* y al contenido del propio *Certificado*.

140. Por otra parte, [ETIS042] define los *Certificados Normalizados* como aquellos que son emitidos por una *Política de Certificación* (NCP) que ofrece una calidad del servicio **equivalente** a la *Política de Certificación* para la emisión de *Certificados Reconocidos* (QCP) definida en [ETSI456]. Asimismo, [ETSI042] reconoce expresamente la validez de

la *Política de Certificación* NCP para cuestiones criptográficas al objeto de realizar operaciones de autenticación o cifrado de datos.

141. Los *Certificados Normalizados* son creados para aumentar los límites de uso y ámbito de aplicación respecto de los *Certificados Reconocidos*, facilitando de este modo la adaptación de los primeros con otras instituciones, especificaciones y estándares similares a [ETSI456].

142. En este esfuerzo de harmonización e interoperabilidad entre sistemas, el nivel de calidad dispuesto en la Directiva [D99/93EC] puede verse consagrado al estar reconocido y aceptado en un marco de trabajo mucho más amplio pero sin llegar a estar sujeto a las especificaciones propias de ésta.

10.1.3. Comunidad y ámbito de aplicación

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

a) Son expedidos por la FNMT-RCM como *Prestador de Servicios de Certificación* cumpliendo con los criterios establecidos en la Ley española 59/2003, de 19 de diciembre, de Firma Electrónica y en la Directiva Europea de Firma Electrónica [D99/93EC]

b) Son expedidos como *Certificados Normalizados* con base en los criterios establecidos para tal en la normativa técnica EESSI, concretamente en la Política de Certificación para la emisión de *Certificados Normalizados* identificados en la norma [ETSI042] – NCP (Normalized Certificate Policy)

c) Los *Certificados* emitidos bajo esta *Política de Certificación* son expedidos para las *Organizaciones* que forman parte de la *Comunidad Electrónica UE,* tal y como se define en el apartado Definiciones de este documento. En el marco de esta *Política de Certificación*, los *Usuarios* y custodios de los *Datos de Creación de Firma* se corresponden con el personal de las *Organizaciones* en el ejercicio de sus competencias y funciones públicas propias del cargo, de la relación funcionarial, de las funciones del empleado público, o de la condición de autorizado por la *Organización*, en relación con la entidad a la que pertenezcan o con la que se relacionen estos *Usuarios*.

10.1.4. Responsabilidad y obligaciones de las partes

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

- Las *Organizaciones* o *Entidades Competentes* representadas a través de los diferentes órganos competentes y que son los *Suscriptores* responsables de los *Certificados*.
- *Oficinas de Registro*, que, a través del personal designado por la *Organización*, serán responsables de comprobar los requisitos y condiciones ostentados por los *Usuarios* del *Certificado*.
- Los *Usuarios* del *Certificado* y sus *Claves*, que será el personal al servicio de las *Organizaciones*.
- FNMT-RCM, en cuanto *Prestador de Servicios de Certificación*.
- El resto de la *Comunidad Electrónica UE*.

145. El régimen de derechos y obligaciones de la *Organización* y la FNMT-RCM se regirá mediante los correspondientes acuerdos reguladores de los servicios de certificación.

146. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en este documento y en la [DGPC], la *Organización* como *Autoridad Local de Registro*, el *Referente de la LRA* y los *Registradores* tienen la obligación de:

- Cumplir con los procedimientos de registro facilitados por la FNMT-RCM.
- No realizar registros o tramitar solicitudes de personal que preste sus servicios en una *Organización* diferente a la que representa como *Oficina de Registro*, sin perjuicio de

la creación, en la propia Comisión Europea, de *Oficinas de Registro* centralizadas que se hayan establecido.

- Comprobar fehacientemente los datos del personal al servicio de la *Organización* referidos a su identidad y su pertenencia a dicha *Organización* a la que presta sus servicios y, en su caso, cualquier otro dato que refleje o caracterice esta pertenencia.
- Solicitar la revocación o suspensión del *Certificado Normalizado* para el personal al servicio de la *Organización* a la que representa la *Oficina de Registro*, cuando alguno de los datos consignados en el *Certificado* sea inexacto, incorrecto, haya variado o sea de necesaria revocación por razones de seguridad. También deberá solicitar la revocación o suspensión cuando se den las circunstancias previstas en la legislación aplicable.
- Solicitar a la FNMT-RCM la revocación del *Certificado* cuando las circunstancias que afecten a la condición del cargo, puesto de trabajo, empleo o cualquier otro dato que refleje o caracterice la relación del *Usuario* del *Certificado* con la *Organización* donde presta sus servicios, sean inexactas, incorrectas, hayan variado o sean de necesaria revocación por razones de seguridad.
- Solicitar a la FNMT-RCM, a través de la *Oficina de Registro*, la revocación o suspensión del *Certificado* cuando, directamente o a través de comunicación del personal al servicio de *Organización*, exista pérdida, extravío del soporte del *Certificado* o de su confidencialidad, o presunción de ello.
- Custodiar la documentación aportada por cualquiera de los intervinientes en los procesos de gestión de los *Certificados* (solicitudes de emisión, suspensión, cancelación de la suspensión, revocación y cualesquiera otros de la misma índole) así como los documentos generados en dichos procesos (justificantes, contratos de emisión, revocación, etc.)

147. Las relaciones de la FNMT-RCM con la *Organización* y los *Usuarios* de los *Certificados* quedarán determinadas, a los efectos del régimen de uso de los *Certificados*, por los siguientes documentos: condiciones de utilización o contrato de emisión del *Certificado*, y, subsidiariamente, las presentes *Políticas y Prácticas de Certificación Particulares* y por la [DGPC], atendiendo a los acuerdos o documentos de relación entre la FNMT-RCM y las *Organizaciones*.

148. Las relaciones de la *Organización* o *Entidad Competente Suscriptora* del *Certificado* y de su personal con la FNMT-RCM se realizarán siempre a través de la *Oficina de Registro* y su *Referente*. La FNMT-RCM no realizará ninguna acción solicitada por el personal al servicio de la *Organización* o *Usuario* del *Certificado* que no esté autorizada por *Referente de la LRA* o por la *Organización* o *Entidad Competente Suscriptora* del *Certificado*.

149. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la [DGPC], el *Usuario* del *Certificado* tiene la obligación de:

- No utilizar el *Certificado* cuando alguno de los datos referidos al cargo, puesto de trabajo, empleo o cualquier otro que dio lugar a la emisión del *Certificado* sea inexacto, incorrecto o no refleje o caracterice su relación con la *Organización* o *Entidad Competente Suscriptora*
- 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 la *Organización*.
- Mantener en todo momento el control exclusivo de los *Datos de Creación de Firma* y tomar las razonables precauciones para prevenir su pérdida, revelación, modificación o uso no autorizado
- Comunicar al *Referente de la LRA* correspondiente, la pérdida, extravío, o sospecha de ello, del soporte del *Certificado* o de su confidencialidad, del que es *Usuario* con el fin de iniciar, en su caso, los trámites de la revocación del *Certificado*.

150. El resto de la *Comunidad Electrónica UE* y los terceros regularán sus relaciones con la FNMT-RCM a través de la [DGPC] y estas *Políticas y Prácticas de Certificación Particulares*; todo ello sin perjuicio de lo dispuesto en la normativa sobre firma electrónica y demás normativa que resulte de aplicación.

10.1.5. Límites de uso de los *Certificados Normalizados*

151. Constituyen límites de uso de este tipo de *Certificados* las operaciones de autenticación que dentro de los sistemas de las *Organizaciones* o *Entidades Competentes Suscriptoras* se pudieran realizar. Asimismo, la *Organización* podrá autorizar al *Usuario* el empleo de este tipo de *Certificados* como herramienta de identificación y autenticación en sistemas ajenos a su titularidad. Fuera de la funcionalidad prevista anteriormente no se podrán emplear estos *Certificados*.

152. La FNMT-RCM y las *Organizaciones* podrán fijar en los acuerdos correspondientes otros límites adicionales.

153. FNMT-RCM no tendrá control sobre las actuaciones y usos de los *Certificados* que se realicen por parte del *Suscriptor*, *Usuario* o las *Oficinas de Registro*, por lo que la FNMT-RCM quedará exonerada de responsabilidad a efectos de tales usos y de la extralimitación en el uso establecido anteriormente, así como de las consecuencias y efectos que pudieran producirse por reclamaciones o posibles responsabilidades patrimoniales llevadas a cabo por cualquier miembro de la *Comunidad Electrónica UE* o por terceros.

154. Para que el *Usuario* utilice de forma diligente los *Certificados Normalizados* y *Claves* asociadas, la *Organización* a la que representa el usuario deberá previamente formar parte de la *Comunidad Electrónica UE* y haberse constituido como *Suscriptor* del *Certificado*.

155. En cualquier caso, si un tercero desea confiar en la *Firma electrónica* realizada con uno de estos *Certificados Normalizados* sin acceder a los *Servicios de información y consulta sobre el estado de validez de los certificados* emitidos bajo esta *Política de Certificación*, no se obtendrá cobertura de las presentes *Políticas y Prácticas de Certificación Particulares* y se carecerá de legitimidad alguna para reclamar o emprender acciones legales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado*.

156. Además, incluso dentro del ámbito de la *Comunidad Electrónica UE*, 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 *Sellado de Tiempo*
- 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
- Utilizar el *Certificado* para usos distintos a los inicialmente previstos respecto de los *Certificados Normalizados*

10.2. PRÁCTICAS DE CERTIFICACIÓN PARTICULARES PARA LOS CERTIFICADOS NORMALIZADOS

157. 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*.

158. En especial deberá tenerse presente, a efectos interpretativos del presente anexo el apartado "Definiciones" de la [DGPC] y de este documento.

159. 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 Normalizados* expedidos bajo la *Política de Certificación* identificada con el OID 1.3.6.1.4.1.5734.3.4.2

10.2.1. Servicios de Gestión de las *Claves*

160. La FNMT-RCM, bajo ningún concepto, genera ni almacena las *Claves Privadas* de los *Firmantes*, que son generadas bajo su exclusivo control y, en su caso, con la intervención de la *Oficina de Registro* correspondiente y cuya custodia está bajo responsabilidad del *Usuario* del *Certificado*.

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

161. Se definen aquí aquellos aspectos que, si bien algunos ya han sido apuntados en la [DGPC], revisten determinadas especialidades que necesitan un mayor nivel de detalle.

10.2.2.1. Procedimiento de solicitud y emisión del Certificado Normalizado

162. A continuación se describe el procedimiento de solicitud por el que el *Registrador* toma los datos del personal al servicio de la *Organización*, confirma su identidad y se formaliza, entre el citado personal y la FNMT-RCM, el documento de condiciones de utilización o el contrato de emisión, según lo previsto en el acuerdo de la FNMT-RCM con la *Organización* para la posterior emisión de un *Certificado Normalizado*.

163. Se hace constar que FNMT-RCM, en función de la relación de *Suscriptores* y personal *Usuario* dependiente remitida por la *Oficina de Registro*, considerará, bajo responsabilidad de las correspondientes *Organizaciones*, que actuarán a través de las *Oficinas de Registro* como *Autoridad Local de Registro*, que este personal se encuentra con su cargo vigente, que sus datos personales son auténticos y están en vigor y, por tanto, habilitado para obtener y usar el *Certificado*.

164. La Comisión Europea podrá establecer, en el ámbito de actuación de sus competencias, Oficinas de Registro centrales o comunes con efectos uniformes para cualesquiera de las diferentes entidades de los Estados Miembro

165. FNMT-RCM, no tendrá, en este tipo de *Certificado*, la responsabilidad de comprobar el cargo o empleo del *Usuario*, así como que estos requisitos se mantienen durante toda la vida del *Certificado*. La FNMT-RCM no mantiene relación jurídica funcionarial, administrativa o laboral con el *Usuario*, más allá del documento de condiciones de utilización o, en su caso, contrato de emisión.

166. Las actividades de comprobación anteriores serán realizadas por el personal de la *Oficinas de Registro* implantada por la *Organización*, que es la entidad donde el *Usuario* presta sus servicios. Por tanto y a estos efectos las *Oficinas de Registro* no serán autoridades delegadas o dependientes de la FNMT-RCM.

167. Este *Certificado* será solicitado por la *Organización* o *Entidad Competente Suscriptora* quien actuará como solicitante sin perjuicio de que las operaciones necesarias para la petición y obtención del *Certificado* se realicen por el *Referente* o el *Registrador* o, de manera instrumental, por los propios *Usuarios*.

168. Los tres pasos a realizar para la obtención del *Certificado* son:

10.2.2.1.1. Presolicitud (Paso 1)

169. Con carácter previo, el *Usuario* y el *Suscriptor* deberán consultar la [DGPC] y las presentes *Políticas 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 *Suscriptor*, respectivamente, del *Certificado*, que se plasmaran en el documento de condiciones de utilización o, si procede, el contrato de emisión.

170. El *Usuario* deberá acceder a la dirección electrónica https://ec.fnmt.es donde se mostrarán las instrucciones para realizar una generación de *Claves*. En esta dirección deberá introducir su nombre, primer apellido y dirección de correo electrónico en el punto de recogida de datos dispuesto para ello.

171. A continuación se generarán las *Claves Pública* y *Privada* que serán vinculadas al *Certificado*, convirtiéndose en su momento en *Datos de Verificación y Creación de Firma* respectivamente.

172. 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*.

173. La FNMT-RCM, tras recibir esta información, comprobará mediante la *Clave Pública* del *Usuario* la validez de la información de la presolicitud firmada, comprobando, únicamente, la posesión y correspondencia de la pareja de *Claves* criptográficas por parte de éste.

174. Si todo es correcto, la FNMT-RCM asignará un código de solicitud a la petición realizada por el *Usuario* y se lo indicará en una página web de respuesta.

175. 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*.

10.2.2.1.2. Acreditación de la identidad y solicitud (Paso 2)

176. Una vez que el *Usuario* ha obtenido el código de solicitud en el subproceso de "Presolicitud" deberá realizar la correspondiente solicitud de emisión de *Certificado* a través de la *Oficina de Registro* que le corresponda (aquella que representa a la *Organización* ante la FNMT-RCM en las operaciones de gestión de *Certificados* y en la que el *Usuario* presta sus servicios).

177. Esta solicitud requerirá la personación física del *Usuario* en la *Oficina de Registro* donde el *Registrador* autenticará al *Usuario* mediante el requerimiento de aportación de

- datos personales (como mínimo el nombre, primer apellido, correo electrónico y número distintivo del documento oficial a aportar) y datos vinculados a la solicitud en cuestión (código de solicitud) y
- el documento oficial que acredite la identidad del *Usuario* en el que figuren los datos identificativos de éste

178. El *Registrador* comprobará la condición del *Usuario* como empleado de la *Organización* o *Entidad Competente Suscriptora* del *Certificado* y con cargo vigente por los medios que tenga a su disposición y habida cuenta de que la *Oficina de Registro* actúa en representación de la *Organización* en cuestión y por tanto conoce de forma fehaciente esta información.

179. FNMT-RCM, no tendrá la responsabilidad de comprobar los datos personales ni la condición de empleado, así como que estos requisitos o condiciones se mantienen durante toda la vida del *Certificado*, al no ostentar relación jurídica funcionarial, administrativa o laboral con el *Usuario*, 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.

180. La personación del *Usuario* ante el *Registrador* y la presentación del documento oficial que acredita su identidad, así como los procedimientos a observar por éste último, avalarán la identidad del *Usuario* y su relación con la *Organización* o *Entidad Competente Suscriptora*, siendo condición necesaria y suficiente para el establecimiento del vínculo entre identidad y *Datos de Creación de Firma* que se crea en el momento de la emisión del *Certificado*.

181. La aplicación de registro generará dos impresos con el contrato de solicitud y las condiciones de utilización, para su posterior impresión y firma por parte del *Usuario* y *Registrador*.

182. Después de que el *Registrador* confirme la identidad del *Usuario*, la vigencia de su cargo o empleo en la *Organización* y habiendo firmado los impresos contractuales, el *Registrador* procederá a validar los datos y a enviarlos a la FNMT-RCM junto con el código de solicitud recogido en la fase de presolicitud.

183. La *Oficina de Registro* deberá custodiar los impresos contractuales firmados por ambas partes como parte de la solicitud.

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

185. 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.

10.2.2.1.3. Emisión del Certificado (Paso 3)

186. Una vez recibidos en la FNMT-RCM los datos personales del *Usuario*, la información que describe su relación con la *Organización* o *Entidad Competente Suscriptora* del *Certificado*, así como el código de solicitud obtenido en la fase de presolicitud, se procederá a la emisión del *Certificado*.

187. La emisión de *Certificados* supone la generación de documentos electrónicos que confirman la identidad del *Firmante,* su relación con la *Organización* así como su correspondencia con la *Clave Pública* asociada.

188. La emisión de los *Certificados* sujetos a las presentes *Políticas* sólo puede realizarse por la FNMT-RCM en su calidad de *Prestador de Servicios de Certificación*, no existiendo ninguna otra entidad u organismo con capacidad de emisión de los mismos.

189. La FNMT-RCM, por medio de su *Firma electrónica*, autentica el *Certificado* y confirma la identidad del *Suscriptor,* así como su relación con el *Usuario*, 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 el *Certificado*, la FNMT-RCM utilizará mecanismos criptográficos que doten de autenticidad e integridad al *Certificado*.

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

- Comprobar que el *Usuario* del *Certificado* utiliza la *Clave Privada* correspondiente a la *Clave Publica* vinculada a la identidad del *Firmante* 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 Claves Públicas* de la FNMT-RCM.

191. Para la emisión del *Certificado Ligero* se seguirán los siguientes pasos:

1. Composición del nombre distintivo (DN) del *Certificado Normalizado*

   Con los datos personales del *Usuario* 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 este tipo de *Certificados* está compuesto de los siguientes elementos:

   DN≡CN, O, C

   El conjunto de atributos O, C representa la rama del directorio en la que se encuentra ubicada la entrada correspondiente a los *Certificados Normalizados* emitidos al *Usuario* al servicio de la *Organización* en cuestión.

   El atributo *CN* contiene los datos de identificación del *Usuario*.

   El atributo O contiene el nombre de la *Organización*.

El atributo C contiene el código de país al que pertenece la *Organización*.

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 *Usuario*

   La identidad alternativa del *Usuario*, tal como se contempla en la presente tipología de *Certificados*, contiene el nombre, el primer apellido y la dirección de correo electrónico de éste aportada durante los procesos de presolicitud y acreditación de la identidad. Se utiliza la extensión subjectAltName definida en *X.509* versión 3 para ofrecer esta información.

3. Generación del *Certificado* conforme al perfil del *Certificado Normalizado*.

   El formato del *Certificado Normalizado* estará en consonancia con la norma UIT-T X.509 versión 3 y de acuerdo con la normativa legalmente aplicable.

   En la **Tabla 3 – Perfil del *Certificado Normalizado*** anexa a este documento puede consultarse el perfil de este tipo de *Certificados*

10.2.2.2. Publicación del Certificado Normalizado

192. Una vez generado el *Certificado* por parte del *Prestador de Servicios de Certificación*, se publicará en el *Directorio*, concretamente en la entrada correspondiente a la *Organización*.

193. A la dirección de correo electrónico proporcionada por el *Usuario* se le enviará una comunicación de la disposición de su *Certificado* para su descarga.

10.2.2.3. Descarga e instalación del Certificado Normalizado

194. Una vez generado el *Certificado*, se pone a disposición del *Usuario* un mecanismo de descarga en la dirección https://ec.fnmt.es accediendo a la opción "Descarga de su Certificado".

195. En este proceso guiado se le pedirá al interesado que introduzca su nombre, primer apellido y correo electrónico con el que se realizó el proceso de presolicitud, así como el código de solicitud devuelto por el sistema al finalizar dicho proceso.

196. Si el *Certificado* no ha sido aún generado por cualquier motivo, se le indicará este hecho en el momento que intente su descarga. En caso contrario se pondrá a disposición del interesado, quien lo introducirá en el soporte en el que se generaron las *Claves* durante el proceso de presolicitud.

10.2.2.4. Vigencia del Certificado Normalizado

10.2.2.4.1. Caducidad

197. Los *Certificados Normalizados* emitidos bajos la presente *Política de Certificación* 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.*

10.2.2.4.2. Extinción de la vigencia

198. Los *Certificados Normalizados* emitidos por la FNMT-RCM bajo la presente política 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 *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 pérdida 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

199. A los efectos enumerados anteriormente, se hace constar que la solicitud de emisión de un *Certificado Normalizado* para personal al servicio de las entidades de la Unión Europea cuando exista otro vigente a favor del mismo *Titular* y perteneciente a la misma *Política de Certificación* conllevará la revocación del primero obtenido.

200. 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*.

10.2.2.5. Revocación del Certificado Normalizado

10.2.2.5.1. Causas de revocación del Certificado Normalizado

201. Serán causas de revocación de un *Certificado Normalizado*:

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* o sospecha del compromiso de la confidencialidad de éste
- 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 del *Titular*.
- La violación o puesta en peligro del secreto de los *Datos de Creación de Firma* del *Titular*
- La no aceptación de la *Organización* o *Entidad Competente* 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, así como los supuestos previstos en la legislación aplicable.

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

d) Terminación de la relación entre el *Usuario* y la *Organización* o *Entidad Competente Titular* del *Certificado*

e) Incapacidad sobrevenida, total o parcial, o fallecimiento del *Usuario*.

f) Inexactitudes o alteraciones en los datos aportados por el *Usuario* para la obtención del *Certificado* o modificación de las circunstancias verificadas para su expedición, 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 *Usuario*, del *Titular* del *Certificado* o del personal de la *Oficina de Registro* si hubiese podido afectar al procedimiento de emisión del *Certificado*.

h) Resolución del contrato suscrito entre la *Organización* 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.

202. 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.

203. 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, incluyendo las causas antes mencionadas, a la FNMT-RCM, producirán la exoneración de responsabilidad de la FNMT-RCM.

10.2.2.5.2. Efectos de la revocación

204. 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 validez de los certificados*.

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

10.2.2.5.3. Procedimiento para la revocación

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

207. La revocación de un *Certificado Normalizado* puede ser solicitada por el *Titular* a través del *Referente de la LRA* o de los *Registradores.* Asimismo, el *Usuario* podrá plantear a la *Oficina de Registro* la revocación o suspensión si existen causas que lo justifiquen, en los términos recogidos en la presente *Política y Prácticas de Certificación Particulares*.

208. Sin perjuicio de lo anterior, la FNMT-RCM podrá revocar los *Certificados Normalizados* en los supuestos recogidos en la *Declaración de Prácticas de Certificación* y en la legislación aplicable.

209. El *Usuario,* o el *Titular* a través de un representante con capacidad suficiente, podrá solicitar la operación de revocación personándose en la *Oficina de Registro* correspondiente. El *Registrador* deberá comprobar la capacidad suficiente del peticionario para realizar la solicitud de revocación.

210. El peticionario deberá acreditar la identidad del *Usuario* del *Certificado* a revocar mediante la aportación de los datos personales de éste (al menos nombre, primer apellido y correo electrónico). En cualquier caso, el peticionario deberá acreditar su identidad mediante la aportación del documento oficial correspondiente.

211. El registrador formalizará la petición de revocación mediante la aplicación de registro, que generará dos impresos con el contrato de solicitud, para su posterior impresión y firma por parte del peticionario y *Registrador*

212. Después de que el *Registrador* confirme la identidad del peticionario y su capacidad suficiente y habiendo firmado los impresos contractuales, el *Registrador* procederá a validar los datos y a enviarlos a la FNMT-RCM.

213. La *Oficina de Registro* deberá custodiar los impresos contractuales firmados por ambas partes como parte de la solicitud.

214. La FNMT-RCM recibirá aquella información relevante a efectos de la revocación de un *Certificado* a través el modelo de solicitud de revocación que se le presente, en formato papel o electrónico, por la *Oficina de Registro*.

215. La *Oficina de Registro* transmitirá las solicitudes a la FNMT-RCM para que proceda a la revocación del *Certificado*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

216. FNMT-RCM considerará que el peticionario de la revocación de un *Certificado* de este tipo cuenta con la capacidad suficiente si la petición es realizada a través de la *Oficina de Registro* correspondiente. FNMT-RCM no valorará la conveniencia de la solicitud de revocación cuando ésta sea realizada a través de la *Oficina de Registro* antedicha.

217. 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. De forma análoga esta información también estará disponible mediante el

protocolo OCSP en el correspondiente *Servicio de información sobre el estado de validez de los Certificados*.

10.2.2.6. Suspensión del Certificado Normalizado

218. 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.

10.2.2.6.1. Causas de la suspensión del Certificado Normalizado

219. La FNMT-RCM podrá suspender la vigencia de los *Certificados* ante una solicitud de las mismas personas autorizadas y bajo las mismas condiciones que para la solicitud de revocación.

220. 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.

10.2.2.6.2. Efectos de la suspensión

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

10.2.2.6.3. Procedimiento para la suspensión de Certificados

222. Los procedimientos y personas autorizadas para la solicitud y tramitación de la revocación del *Certificado* son de aplicación en el caso de la suspensión.

223. La *Oficina de Registro* transmitirá las solicitudes tramitados a la FNMT-RCM para que proceda a la suspensión del *Certificado*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

224. La FNMT-RCM suspenderá el *Certificado* de forma provisional durante un plazo de quince (15) días, plazo tras el cual se extinguirá el *Certificado* mediante su revocación directa por parte del *Prestador de Servicios de Certificación*, salvo que se hubiera cancelado la suspensión. No obstante lo anterior, el plazo previsto para la suspensión del *Certificado* podrá verse alterado en función de la duración de las investigaciones o los procedimientos judiciales o administrativos que lo pudieran afectar.

225. Una vez que la FNMT-RCM ha procedido a la suspensión 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. De forma análoga esta información también estará disponible mediante el protocolo OCSP en el correspondiente *Servicio de información sobre el estado de validez de los Certificados*.

226. 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.

10.2.2.6.4. Cancelación de la suspensión del Certificado Normalizado

227. Podrán solicitar la cancelación de la suspensión de los *Certificados Normalizados* las mismas personas legitimadas para la solicitud de la suspensión, en las mismas condiciones y siguiendo los mismos procedimientos.

228. La *Oficina de Registro* transmitirá las solicitudes a la FNMT-RCM para que ésta proceda a la cancelación de la suspensión del *Certificado*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

229. Una vez recibidos los datos validados por la *Oficina de Registro* de la petición de levantamiento de suspensión, la FNMT-RCM procederá a retirar el *Certificado* en cuestión

de la *Lista de Certificados Revocados*, no efectuándose acción técnica alguna sobre el *Certificado*.

11. CERTIFICADOS RECONOCIDOS

11.1. POLÍTICA DE CERTIFICACIÓN PARA LA EMISIÓN DE CERTIFICADOS RECONOCIDOS

11.1.1. Identificación

230. La presente *Política de Certificación* de la FNMT-RCM para la expedición de *Certificados Reconocidos* para su uso en el ámbito de competencias de las *Organizaciones* y en el marco de la *Comunidad Electrónica UE*.

Nombre: *Política de Certificación* para la emisión de *Certificados Reconocidos*

Referencia / OID:

- 1.3.6.1.4.1.5734.3.4.1

Versión: 1.0

Fecha de emisión: 15 de noviembre 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/

11.1.2. Tipología del Certificado Reconocido

231. El *Certificado Reconocido* es la certificación electrónica emitida por la FNMT-RCM que vincula a su *Suscriptor* (la *Organización*) con unos *Datos de Verificación de Firma* y confirma, de forma conjunta:

- la identidad del firmante y custodio de las *Claves* y su condición de personal al servicio de la *Organización* que realiza firmas electrónicas utilizando el *Certificado* en nombre de la entidad actuante y,
- al *Suscriptor* del *Certificado*, que es la *Organización*.

232. Este *Certificado* se emite por la FNMT-RCM por cuenta de la *Organización* correspondientes y a la que la FNMT-RCM presta los servicios técnicos, administrativos y de seguridad necesarios como *Prestador de Servicios de Certificación*.

233. Los procesos necesarios para la gestión de este *Certificado* (emisión, revocación, renovación, etc.) son desarrollados por la FNMT-RCM mediante una infraestructura PKI específica, basada en actuaciones de identificación y registro realizadas por la red de *Oficinas de Registro* designadas por las *Organizaciones* y que son *Suscriptoras* de los *Certificados*.

234. [ETSI456] identifica una serie de requisitos para las *Políticas de Certificación* que entre otros, emitan *Certificados* que tienen la denominación de "Qualified Certificate". Esta denominación tiene su equivalencia en el término *Certificado Reconocido* que se emplea en el presente documento.

235. Los requisitos identificados en [ETSI456] para las *Políticas de Certificación* que emiten "*Certificados Reconocidos*" son satisfechos en la presente *Política*. Adicionalmente, se señala que los *Certificados* emitidos bajo la presente política son emitidos con el perfil técnico correspondiente a los *Certificados Reconocidos* con base en los criterios establecidos para tales *Certificados* en la normativa [ETSI456] y [ETSI862], tanto en los referente al *Prestador de Servicios de Certificación*, como a la generación de los *Datos de Creación y Verificación de Firma* y al contenido del propio *Certificado*.

236. Por otra parte, [ETIS456] define los *Certificados Reconocidos* como aquellos que cumplen con los requisitos establecidos en el anexo I de la Directiva [D99/93EC] y son emitidos por un *Prestador de Servicios de Certificación* que cumple con los requisitos establecidos en el anexo II de dicha Directiva y en lo que respecta a la gestión de estos *Certificados*.

237. Por cuanto antecede, podemos concluir que los *Certificados* emitidos bajo la presenta *Política de Certificación* incorporan los requisitos identificados en el anexo I y II de la Directiva [D99/93EC]

11.1.3. Comunidad y ámbito de aplicación

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

a) Son expedidos por la FNMT-RCM como *Prestador de Servicios de Certificación* cumpliendo con los criterios establecidos en la Ley española 59/2003, de 19 de diciembre, de Firma Electrónica y en la Directiva Europea de Firma Electrónica [D99/93EC]

b) Son expedidos como *Certificados Reconocidos* con base en los criterios establecidos para tales en la normativa técnica EESSI, concretamente en la *Política de Certificación* para la emisión de *Certificados Reconocidos* identificados en la norma [ETSI456] – QCP (Qualified Certificate Policy), y para la realización de *Firma electrónica* en *Dispositivos seguros de creación de firma*

c) Por *Dispositivo seguro de creación de Firma* se entiende la *Tarjeta criptográfica* de la FNMT-RCM que cumple técnicamente con los criterios establecidos en [D99/93EC].

d) Los *Certificados* emitidos bajo esta *Política de Certificación* son expedidos para las *Organizaciones* que forman parte de la *Comunidad Electrónica UE,* tal y como se define en el apartado Definiciones de este documento. En el marco de esta *Política de Certificación*, los *Usuarios* y custodios de los *Datos de Creación de Firma* se corresponden con el personal de las *Organizaciones* en el ejercicio de sus competencias y funciones públicas propias del cargo, de la relación funcionarial, de las funciones del empleado público, o de la condición de autorizado por la *Organización*, en relación con la entidad a la que pertenezcan o con la que se relacionen estos *Usuarios*

11.1.4. Responsabilidad y obligaciones de las partes

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

- Las *Organizaciones* representadas a través de los diferentes órganos competentes y que son los *Titulares* responsables de los *Certificados*.
- *Oficinas de Registro*, que, a través del personal designado por la *Organización*, serán responsables de comprobar los requisitos y condiciones ostentados por los *Usuarios* del *Certificado*.
- Los *Usuarios* del *Certificado* y sus *Claves*, que será el personal al servicio de las *Organizaciones*.
- FNMT-RCM, en cuanto *Prestador de Servicios de Certificación*.
- El resto de la *Comunidad Electrónica UE*.

240. El régimen de derechos y obligaciones de la *Organización* y la FNMT-RCM se regirá mediante los correspondientes acuerdos reguladores de los servicios de certificación.

241. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en este documento y en la [DGPC], la *Organización*, como *Autoridad Local de Registro*, el *Referente de la LRA* y los *Registradores* tienen la obligación de:

- Cumplir con los procedimientos de registro facilitados por la FNMT-RCM.
- No realizar registros o tramitar solicitudes de personal que preste sus servicios en una *Organización* diferente a la que representa como *Oficina de Registro*, sin perjuicio de la creación, en la propia Comisión Europea, de *Oficinas de Registro* centralizadas que se hayan establecido.

- Comprobar fehacientemente los datos del personal al servicio de la *Organización* referidos a su identidad y su pertenencia a dicha *Organización* a la que presta sus servicios y, en su caso, cualquier otro dato que refleje o caracterice esta pertenencia.
- Solicitar la revocación o suspensión del *Certificado Reconocido* para el personal al servicio de la *Organización* a la que representa la *Oficina de Registro*, cuando alguno de los datos consignados en el *Certificado* sea inexacto, incorrecto, haya variado o sea de necesaria revocación por razones de seguridad. También deberá solicitar la revocación o suspensión cuando se den las circunstancias previstas en la legislación aplicable.
- Solicitar a la FNMT-RCM la revocación del *Certificado* cuando las circunstancias que afecten a la condición del cargo, puesto de trabajo, empleo o cualquier otro dato que refleje o caracterice la relación del *Usuario* del *Certificado* con la *Organización* donde presta sus servicios, sean inexactas, incorrectas, hayan variado o sean de necesaria revocación por razones de seguridad.
- Solicitar a la FNMT-RCM, a través de la *Oficina de Registro*, la revocación o suspensión del *Certificado* cuando, directamente o a través de comunicación del personal al servicio de *Organización*, exista pérdida, extravío del soporte del *Certificado* o de su confidencialidad, o presunción de ello.
- Custodiar la documentación aportada por cualquiera de los intervinientes en los procesos de gestión de los *Certificados* (solicitudes de emisión, suspensión, cancelación de la suspensión, revocación y cualesquiera otros de la misma índole) así como los documentos generados en dichos procesos (justificantes, contratos de emisión, revocación, etc.)
- Custodiar diligentemente las *Tarjetas criptográficas* que la FNMT-RCM entrega a la *Organización* de forma que su distribución a los *Usuarios* esté controlada y no se conserve ningún dato de activación o uso de la misma (por ejemplo, el PIN, clave de desbloqueo, etc.). Cualquier incidencia relacionada con las *Tarjeta criptográficas* deberá ser puesta en conocimiento de la FNMT-RCM

242. Las relaciones de la FNMT-RCM con la *Organización* y los *Usuarios* de los *Certificados* quedarán determinadas, a los efectos del régimen de uso de los *Certificados*, por los siguientes documentos: condiciones de utilización o contrato de emisión del *Certificado*, y, subsidiariamente, las presentes *Políticas y Prácticas de Certificación Particulares* y por la [DGPC], atendiendo a los acuerdos o documentos de relación entre la FNMT-RCM y las *Organizaciones*.

243. Las relaciones de la *Organización Titular* del *Certificado* y de su personal con la FNMT-RCM se realizarán siempre a través de la *Oficina de Registro* y su *Referente*. La FNMT-RCM no realizará ninguna acción solicitada por el personal al servicio de la *Organización* o *Usuario* del *Certificado* que no esté autorizada por *Referente de la LRA* o por la *Organización Titular* del *Certificado*.

244. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la [DGPC], el *Usuario* del *Certificado* tiene la obligación de:

- No utilizar el *Certificado* cuando alguno de los datos referidos al cargo, puesto de trabajo, empleo o cualquier otro que dio lugar a la emisión del *Certificado* sea inexacto, incorrecto o no refleje o caracterice su relación con la *Organización Titular*
- 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 la *Organización*.
- Mantener en todo momento el control exclusivo de los *Datos de Creación de Firma* y tomar las razonables precauciones para prevenir su pérdida, revelación, modificación o uso no autorizado. Asimismo, el *Usuario* deberá mantener bajo su control los datos de activación o uso de la *Tarjeta criptográfica*.

- Devolver la *Tarjeta criptográfica* al *Referente de la LRA* una vez que los *Certificados* que se encuentran en su interior hayan perdido su vigencia.
- Comunicar al *Referente de la LRA* correspondiente, la pérdida, extravío, o sospecha de ello, del soporte del *Certificado* o de su confidencialidad, del que es *Usuario* con el fin de iniciar, en su caso, los trámites de la revocación del *Certificado*.

245. El resto de la *Comunidad Electrónica UE* y los terceros regularán sus relaciones con la FNMT-RCM a través de la [DGPC] y estas *Políticas 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.

11.1.5. Límites de uso de los *Certificados Reconocidos*

246. Constituyen límites de uso de este tipo de *Certificados* las operaciones de *Firma electrónica* que los *Usuarios* pudieran realizar en el ejercicio de sus competencias por cuenta de la *Organización Titular* del *Certificado*, siempre en el marco de las capacidades de representación que permita la relación que los vincula. Fuera de la funcionalidad prevista anteriormente no se podrán emplear estos *Certificados*.

247. La FNMT-RCM y las *Organizaciones* podrán fijar en los acuerdos correspondientes otros límites adicionales.

248. FNMT-RCM no tendrá control sobre las actuaciones y usos de los *Certificados* que se realicen por parte del *Titular*, *Usuario* o las *Oficinas de Registro*, por lo que la FNMT-RCM quedará exonerada de responsabilidad a efectos de tales usos y de la extralimitación en el uso establecido anteriormente, así como de las consecuencias y efectos que pudieran producirse por reclamaciones o posibles responsabilidades patrimoniales llevadas a cabo por cualquier miembro de la *Comunidad Electrónica UE* o por terceros.

249. Para que el *Usuario* utilice de forma diligente los *Certificados Reconocidos* y *Claves* asociadas, la *Organización* a la que representa el usuario deberá previamente formar parte de la *Comunidad Electrónica UE* y haberse constituido como *Titular* del *Certificado*.

250. En cualquier caso, si un tercero desea confiar en la *Firma electrónica* realizada con uno de estos *Certificados Reconocidos* sin acceder a los *Servicios de información y consulta sobre el estado de validez de los certificados* emitidos bajo esta *Política de Certificación*, no se obtendrá cobertura de las presentes *Políticas y Prácticas de Certificación Particulares* y se carecerá de legitimidad alguna para reclamar o emprender acciones legales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado*.

251. Además, incluso dentro del ámbito de la *Comunidad Electrónica UE*, 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 *Sellado de Tiempo*
- 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
- Utilizar el *Certificado* para usos distintos a los inicialmente previstos respecto de los *Certificados Reconocidos*

11.2. PRÁCTICAS DE CERTIFICACIÓN PARTICULARES PARA LOS CERTIFICADOS RECONOCIDOS

252. 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*.

253. En especial deberá tenerse presente, a efectos interpretativos del presente anexo el apartado "Definiciones" de la [DGPC] y de este documento.

254. 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 Reconocidos* expedidos bajo la *Política de Certificación* identificada con el OID 1.3.6.1.4.1.5734.3.4.1.

11.2.1. Servicios de Gestión de las *Claves*

255. La FNMT-RCM, bajo ningún concepto, genera ni almacena las *Claves Privadas* de los *Firmantes*, que son generadas bajo su exclusivo control y, en su caso, con la intervención de la *Oficina de Registro* correspondiente y cuya custodia está bajo responsabilidad del *Usuario* del *Certificado*.

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

256. La presente *Política de Certificación* obliga a emplear un *Dispositivo seguro de creación de firma* para la generación de claves y la posterior realización de *Firma Electrónica*. Al objeto de facilitar el cumplimiento de este requisito, la FNMT-RCM proporcionará a las *Organizaciones*, para su entrega a los *Usuarios*, *Tarjetas criptográficas* para la generación de sus *Claves Privadas* y el almacenamiento de los *Certificados*.

257. La *Tarjeta criptográfica* es entregada 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 introduzcan el *Certificado* en *la Tarjeta Criptográfica*.

258. La FNMT-RCM proporciona este tipo de tarjetas ya que permite a los *Firmantes* mantener el "exclusivo control" sobre los *Datos de creación de firma*.

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

259. Se definen aquí aquellos aspectos que, si bien algunos ya han sido apuntados en la [DGPC], revisten determinadas especialidades que necesitan un mayor nivel de detalle.

11.2.3.1. Procedimiento de solicitud y emisión del Certificado Reconocido

260. A continuación se describe el procedimiento de solicitud por el que el *Registrador* toma los datos del personal al servicio de la *Organización*, confirma su identidad y se formaliza, entre el citado personal y la FNMT-RCM, el documento de condiciones de utilización o el contrato de emisión, según lo previsto en el acuerdo de la FNMT-RCM con la *Organización* para la posterior emisión de un *Certificado Reconocido*.

261. Se hace constar que FNMT-RCM, en función de la relación de *Suscriptores* y personal *Usuario* dependiente remitida por la *Oficina de Registro*, considerará, bajo responsabilidad de las correspondientes *Organizaciones*, que actuarán a través de las *Oficinas de Registro* como *Autoridad Local de Registro*, que este personal se encuentra con su cargo vigente, que sus datos personales son auténticos y están en vigor y, por tanto, habilitado para obtener y usar el *Certificado*.

262. La Comisión Europea podrá establecer, en el ámbito de actuación de sus competencias, Oficinas de Registro centrales o comunes con efectos uniformes para cualesquiera de las diferentes entidades de los Estados Miembro

263. FNMT-RCM, no tendrá, en este tipo de *Certificado*, la responsabilidad de comprobar el cargo o empleo del *Usuario*, así como que estos requisitos se mantienen durante toda la vida del *Certificado*. La FNMT-RCM no mantiene relación jurídica funcionarial, administrativa o laboral con el *Usuario*, más allá del documento de condiciones de utilización o, en su caso, contrato de emisión.

264. Las actividades de comprobación anteriores serán realizadas por el personal de la *Oficinas de Registro* implantada por la *Organización*, que es la entidad donde el *Usuario* presta sus servicios. Por tanto y a estos efectos las *Oficinas de Registro* no serán autoridades delegadas o dependientes de la FNMT-RCM.

265. Este *Certificado* será solicitado por la *Organización Suscriptora* quien actuará como solicitante sin perjuicio de que las operaciones necesarias para la petición y obtención del *Certificado* se realicen por el *Referente* o el *Registrador* o, de manera instrumental, por los propios *Usuarios*.

266. Los tres pasos a realizar para la obtención del *Certificado* son:

11.2.3.1.1. Presolicitud (Paso 1)

267. Con carácter previo, el *Usuario* y el *Suscriptor* deberán consultar la [DGPC] y las presentes *Políticas 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 *Suscriptor*, respectivamente, del *Certificado*, que se plasmaran en el documento de condiciones de utilización o, si procede, el contrato de emisión.

268. Con la Tarjeta criptográfica y los complementos necesarios para su utilización debidamente instalados, el *Usuario* deberá acceder a la dirección electrónica https://ec.fnmt.es donde se mostrarán las instrucciones para que la *Tarjeta* genere las *Claves* en su interior. En esta dirección, el *Usuario* deberá introducir su nombre, primer apellido y dirección de correo electrónico en el punto de recogida de datos dispuesto para ello.

269. A continuación, en el interior de la *Tarjeta* se generarán las *Claves Pública* y *Privada* que serán vinculadas al *Certificado*, convirtiéndose en su momento en *Datos de Verificación y Creación de Firma* respectivamente.

270. 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*.

271. La FNMT-RCM, tras recibir esta información, comprobará mediante la *Clave Pública* del *Usuario* la validez de la información de la presolicitud firmada, comprobando, únicamente, la posesión y correspondencia de la pareja de *Claves* criptográficas por parte de éste.

272. Si todo es correcto, la FNMT-RCM asignará un código de solicitud a la petición realizada por el *Usuario* y se lo indicará en una página web de respuesta.

273. 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*.

11.2.3.1.2. Acreditación de la identidad y solicitud (Paso 2)

274. Una vez que el *Usuario* ha obtenido el código de solicitud en el subproceso de "Presolicitud" deberá realizar la correspondiente solicitud de emisión de *Certificado* a través de la *Oficina de Registro* que le corresponda (aquella que representa a la *Organización* ante la FNMT-RCM en las operaciones de gestión de *Certificados* y en la que el *Usuario* presta sus servicios).

275. Esta solicitud requerirá la personación física del *Usuario* en la *Oficina de Registro* donde el *Registrador* autenticará al *Usuario* mediante el requerimiento de aportación de

- datos personales (como mínimo el nombre, primer apellido, correo electrónico y número distintivo del documento oficial a aportar) y datos vinculados a la solicitud en cuestión (código de solicitud) y
- el documento oficial que acredite la identidad del *Usuario* en el que figuren los datos identificativos de éste

276. El *Registrador* comprobará la condición del *Usuario* como empleado de la *Organización Suscriptora* del *Certificado* y con cargo vigente por los medios que tenga a su disposición y habida cuenta de que la *Oficina de Registro* actúa en representación de la *Organización* en cuestión y por tanto conoce de forma fehaciente esta información.

277. FNMT-RCM, no tendrá la responsabilidad de comprobar los datos personales ni la condición de empleado, así como que estos requisitos o condiciones se mantienen durante toda la vida del *Certificado*, al no ostentar relación jurídica funcionarial, administrativa o laboral con el *Usuario*, 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.

278. La personación del *Usuario* ante el *Registrador* y la presentación del documento oficial que acredita su identidad, así como los procedimientos a observar por éste último, avalarán la identidad del *Usuario* y su relación con la *Organización Suscriptora*, siendo condición necesaria y suficiente para el establecimiento del vínculo entre identidad y *Datos de Creación de Firma* que se crea en el momento de la emisión del *Certificado*.

279. La aplicación de registro generará dos impresos con el contrato de solicitud y las condiciones de utilización, para su posterior impresión y firma por parte del *Usuario* y *Registrador*.

280. Después de que el *Registrador* confirme la identidad del *Usuario*, la vigencia de su cargo o empleo en la *Organización* y habiendo firmado los impresos contractuales, el *Registrador* procederá a validar los datos y a enviarlos a la FNMT-RCM junto con el código de solicitud recogido en la fase de presolicitud.

281. La *Oficina de Registro* deberá custodiar los impresos contractuales firmados por ambas partes como parte de la solicitud.

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

283. 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.

11.2.3.1.3. Emisión del Certificado (Paso 3)

284. Una vez recibidos en la FNMT-RCM los datos personales del *Usuario*, la información que describe su relación con la *Organización Suscriptora* del *Certificado*, así como el código de solicitud obtenido en la fase de presolicitud, se procederá a la emisión del *Certificado*.

285. La emisión de *Certificados* supone la generación de documentos electrónicos que confirman la identidad del *Firmante,* su relación con la *Organización* así como su correspondencia con la *Clave Pública* asociada.

286. La emisión de los *Certificados* sujetos a las presentes *Políticas* sólo puede realizarse por la FNMT-RCM en su calidad de *Prestador de Servicios de Certificación*, no existiendo ninguna otra entidad u organismo con capacidad de emisión de los mismos.

287. La FNMT-RCM, por medio de su *Firma electrónica*, autentica el *Certificado* y confirma la identidad del *Suscriptor,* así como su relación con el *Usuario*, 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 el *Certificado*, la FNMT-RCM utilizará mecanismos criptográficos que doten de autenticidad e integridad al *Certificado*.

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

- Comprobar que el *Usuario* del *Certificado* utiliza la *Clave Privada* correspondiente a la *Clave Publica* vinculada a la identidad del *Firmante* 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 Claves Públicas* de la FNMT-RCM.

289. Para la emisión del *Certificado Ligero* se seguirán los siguientes pasos:

1. Composición del nombre distintivo (DN) del *Certificado Reconocido*

   Con los datos personales del *Usuario* 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 este tipo de *Certificados* está compuesto de los siguientes elementos:

   DN≡CN, O, C

   El conjunto de atributos O, C representa la rama del directorio en la que se encuentra ubicada la entrada correspondiente a los *Certificados Reconocidos* emitidos al *Usuario* al servicio de la *Organización* en cuestión.

   El atributo *CN* contiene los datos de identificación del *Usuario*.

   El atributo O contiene el nombre de la *Organización*.

   El atributo C contiene el código de país al que pertenece la *Organización*.

   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 *Usuario*

   La identidad alternativa del *Usuario*, tal como se contempla en la presente tipología de *Certificados*, contiene el nombre, el primer apellido y la dirección de correo electrónico de éste aportada durante los procesos de presolicitud y acreditación de la identidad. Se utiliza la extensión subjectAltName definida en *X.509* versión 3 para ofrecer esta información.

3. Generación del *Certificado* conforme al perfil del *Certificado Reconocido*.

   El formato del *Certificado Reconocido* estará en consonancia con la norma UIT-T X.509 versión 3 y de acuerdo con la normativa legalmente aplicable.

   En la **Tabla 4 – Perfil del *Certificado Reconocido*** anexa a este documento puede consultarse el perfil de este tipo de *Certificados*

11.2.3.2. Publicación del Certificado Reconocido

290. Una vez generado el *Certificado* por parte del *Prestador de Servicios de Certificación*, se publicará en el *Directorio*, concretamente en la entrada correspondiente a la *Organización*.

291. A la dirección de correo electrónico proporcionada por el *Usuario* se le enviará una comunicación de la disposición de su *Certificado* para su descarga.

11.2.3.3. Descarga e instalación del Certificado Reconocido

292. Una vez generado el *Certificado*, se pone a disposición del *Usuario* un mecanismo de descarga en la dirección https://ec.fnmt.es accediendo a la opción “Descarga de su Certificado”.

293. En este proceso guiado se le pedirá al interesado que introduzca su nombre, primer apellido y correo electrónico con el que se realizó el proceso de presolicitud, así como el código de solicitud devuelto por el sistema al finalizar dicho proceso.

294. Si el *Certificado* no ha sido aún generado por cualquier motivo, se le indicará este hecho en el momento que intente su descarga. En caso contrario se pondrá a disposición del interesado, quien lo introducirá en la *Tarjeta* en la que se generaron las *Claves* durante el proceso de presolicitud.

11.2.3.4. Vigencia del Certificado Reconocido

11.2.3.4.1. Caducidad

295. Los *Certificados Reconocidos* emitidos bajos la presente *Política de Certificación* 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 *Suscriptor* desee seguir utilizando los servicios del *Prestador de Servicios de Certificación.*

11.2.3.4.2. Extinción de la vigencia

296. Los *Certificados Reconocidos* emitidos por la FNMT-RCM bajo la presente política 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*, 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 pérdida 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

297. A los efectos enumerados anteriormente, se hace constar que la solicitud de emisión de un *Certificado Reconocido* cuando exista otro vigente a favor del mismo *Usuario* y *Suscriptor* y bajo la misma *Política de Certificación* conllevará la revocación del primero obtenido.

298. 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 validez de los certificados*.

11.2.3.5. Revocación del Certificado Reconocido

11.2.3.5.1. Causas de revocación del Certificado Reconocido

299. Serán causas de revocación de un *Certificado Reconocido*:

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* o sospecha del compromiso de la confidencialidad de éste
- 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 del *Firmante*.
- La violación o puesta en peligro del secreto de los *Datos de Creación de Firma*.

- La no aceptación de la *Organización* 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, así como los supuestos previstos en la legislación aplicable.

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

d) Terminación de la relación entre el *Usuario* y la *Organización Suscriptora* del *Certificado*

e) Incapacidad sobrevenida, total o parcial, o fallecimiento del *Usuario*.

f) Inexactitudes o alteraciones en los datos aportados por el *Usuario* para la obtención del *Certificado* o modificación de las circunstancias verificadas para su expedición, 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 *Usuario,* del *Suscriptor* del *Certificado* o del personal de la *Oficina de Registro* si hubiese podido afectar al procedimiento de emisión del *Certificado*.

h) Resolución del contrato suscrito entre la *Organización* 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.

300. 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.

301. 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, incluyendo las causas antes mencionadas, a la FNMT-RCM, producirán la exoneración de responsabilidad de la FNMT-RCM.

11.2.3.5.2. Efectos de la revocación

302. 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 validez de los certificados*.

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

11.2.3.5.3. Procedimiento para la revocación

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

305. La revocación de un *Certificado Reconocido* puede ser solicitada por el *Suscriptor* a través del *Referente de la LRA* o de los *Registradores.* Asimismo, el *Usuario* podrá plantear a la *Oficina de Registro* la revocación o suspensión si existen causas que lo justifiquen, en los términos recogidos en la presente *Política y Prácticas de Certificación Particulares*.

306. Sin perjuicio de lo anterior, la FNMT-RCM podrá revocar los *Certificados Reconocidos* en los supuestos recogidos en la *Declaración de Prácticas de Certificación* y en la legislación aplicable.

307. El *Usuario* o el *Suscriptor* a través de un representante con capacidad suficiente podrá solicitar la operación de revocación bien personándose en la *Oficina de Registro* correspondiente, bien vía telemática. El *Registrador* deberá comprobar la capacidad suficiente del peticionario para realizar la solicitud de revocación.

308. En cualquiera de los casos, el peticionario deberá acreditar la identidad del *Usuario* del *Certificado* a revocar mediante la aportación de los datos personales de éste (al menos nombre, primer apellido y correo electrónico)

309. El registrador formalizará la petición de revocación mediante la aplicación de registro, que generará dos impresos con el contrato de solicitud, para su posterior impresión y firma por parte del peticionario y *Registrador*

310. Después de que el *Registrador* confirme la identidad del peticionario y su capacidad suficiente y habiendo firmado los impresos contractuales, el *Registrador* procederá a validar los datos y a enviarlos a la FNMT-RCM.

311. La *Oficina de Registro* deberá custodiar los impresos contractuales firmados por ambas partes como parte de la solicitud.

312. La FNMT-RCM recibirá aquella información relevante a efectos de la revocación de un *Certificado* a través el modelo de solicitud de revocación que se le presente, en formato papel o electrónico, por la *Oficina de Registro*.

313. La *Oficina de Registro* transmitirá las solicitudes a la FNMT-RCM para que proceda a la revocación del *Certificado*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

314. FNMT-RCM considerará que el peticionario de la revocación de un *Certificado* de este tipo cuenta con la capacidad suficiente si la petición es realizada a través de la *Oficina de Registro* correspondiente. FNMT-RCM no valorará la conveniencia de la solicitud de revocación cuando ésta sea realizada a través de la *Oficina de Registro* antedicha.

315. 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. De forma análoga esta información también estará disponible mediante el protocolo OCSP en el correspondiente *Servicio de información sobre el estado de validez de los Certificados*.

11.2.3.6. Suspensión del Certificado Reconocido

316. 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.

11.2.3.6.1. Causas de la suspensión del Certificado Reconocido

317. La FNMT-RCM podrá suspender la vigencia de los *Certificados* ante una solicitud de las mismas personas autorizadas y bajo las mismas condiciones que para la solicitud de revocación.

318. 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.

11.2.3.6.2. Efectos de la suspensión

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

11.2.3.6.3. Procedimiento para la suspensión de Certificados

320. Los procedimientos y personas autorizadas para la solicitud y tramitación de la revocación del *Certificado* son de aplicación en el caso de la suspensión.

321. La *Oficina de Registro* transmitirá las solicitudes tramitados a la FNMT-RCM para que proceda a la suspensión del *Certificado*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

322. La FNMT-RCM suspenderá el *Certificado* de forma provisional durante un plazo de quince (15) días, plazo tras el cual se extinguirá el *Certificado* mediante su revocación directa por

parte del *Prestador de Servicios de Certificación*, salvo que se hubiera cancelado la suspensión. No obstante lo anterior, el plazo previsto para la suspensión del *Certificado* podrá verse alterado en función de la duración de las investigaciones o los procedimientos judiciales o administrativos que lo pudieran afectar.

323. Una vez que la FNMT-RCM ha procedido a la suspensión 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. De forma análoga esta información también estará disponible mediante el protocolo OCSP en el correspondiente *Servicio de información sobre el estado de validez de los Certificados*.

324. Si durante el plazo de suspensión del *Certificado* éste caducara o se solicitara su revocación, se producirán las mismas consecuencias que para los *Certificados* no suspendidos que se vieran afectados por supuestos de caducidad o de revocación.

11.2.3.6.4. Cancelación de la suspensión del Certificado Reconocido

325. Podrán solicitar la cancelación de la suspensión de los *Certificados Reconocidos* las mismas personas legitimadas para la solicitud de la suspensión, en las mismas condiciones y siguiendo los mismos procedimientos.

326. La *Oficina de Registro* transmitirá las solicitudes a la FNMT-RCM para que ésta proceda a la cancelación de la suspensión del *Certificado*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

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

11.2.4. Exclusiones y requisitos adicionales a ETSI TS 101 456

328. 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.

12. CERTIFICADOS DE SERVIDOR

12.1. POLÍTICA DE CERTIFICACIÓN DE LOS CERTIFICADOS DE SERVIDOR WEB

12.1.1. Identificación

329. La presente *Política de Certificación* de la FNMT-RCM para la expedición de *Certificados de servidor web*, también conocidos como *Certificados* SSL/TSL, para su uso en el ámbito de competencias de las *Organizaciones* y en el marco de la *Comunidad Electrónica UE*.

Nombre: *Política de Certificación* de *Certificados de servidor web*

Referencia / OID:

- 1.3.6.1.4.1.5734.3.4.4 – Para los Certificados del tipo Common Name
- 1.3.6.1.4.1.5734.3.4.5 – Para los Certificados del tipo Wildcard

Versión: 1.0

Fecha de emisión: 15 de noviembre 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/

12.1.2. Tipología del *Certificado de servidor web*

330. Los *Certificados de servidor web* son aquellos *Certificados* expedidos por la FNMT-RCM bajo la presente *Política de Certificación* y que vinculan unos *Datos de Verificación de Firma* a un servidor o aplicación sobre la que existe una persona física o jurídica determinada que actúa como responsable, siendo ésta la que tiene el control sobre dicho servidor o aplicación.

331. Este tipo de *Certificados* se emplean por las *Organizaciones* o *Entidades Competentes Suscriptoras* al objeto de identificar y autenticar la dirección URL (nombre de dominio) o IP de un servidor web, de modo que los usuarios que accedan a él tengan las garantías suficientes de que tal acceso se está realizando a la verdadera dirección web (dominio o IP) del servidor.

332. La *Clave Privada* asociada a la *Clave Pública* estará bajo la responsabilidad y custodia del *Responsable del certificado* que actuará como representante de la persona física o jurídica titular del servidor web objeto del *Certificado*.

333. A los efectos del artículo 6 de la Ley española 59/2003, de 19 de diciembre, de Firma Electrónica, los *Certificados de servidor web* se considerarán *Certificados* electrónicos cuando exista vinculación indubitada entre el *Certificado de servidor web* y la *Organización* o *Entidad Competente Suscriptora* de éste. FNMT-RCM emitirá estos *Certificados* siempre que sea solicitado por los miembros de la *Comunidad Electrónica UE* para las diversas relaciones que puedan producirse y no se encuentre prohibido o limitado su utilización por la legislación aplicable.

334. FNMT-RCM no será responsable de las actuaciones realizadas con este tipo de *Certificados* cuando se produzca abuso de facultades o insuficiencia de las mismas y/o cuando se produzcan decisiones del *Suscriptor* del *Certificado* que afecten a la vigencia de las facultades del responsable, por lo que cualquier modificación, revocación o restricción no será oponible a la FNMT-RCM salvo que sea fehacientemente notificada.

335. Estos *Certificados de servidor web* son emitidos y firmados por la FNMT-RCM para ser instalados y utilizados por servidores con soporte SSL/TSL, con el objeto de que se herede la confianza que representa la FNMT-RCM como *Prestador de Servicios de Certificación*.

336. Sólo podrán obtener *Certificados de servidor web* aquellas entidades que hayan suscrito un acuerdo con la FNMT-RCM, en virtud del cual formen parte de la *Comunidad Electrónica*

UE tal y como se contempla en la *Declaración de Prácticas de Certificación* de la FNMT-RCM.

337. Estos *Certificados de servidor web*, no conllevan el efecto jurídico de equivalencia de firma electrónica reconocida con las actuaciones realizadas a través de firma manuscrita tradicional. No obstante, tendrán la validez y eficacia jurídica atendiendo a su respectiva naturaleza según la legislación aplicable.

338. La FNMT-RCM, como *Prestador de Servicios de Certificación* se reserva el derecho de no expedir o revocar este tipo de *Certificados* si el *Responsable* del mismo o el responsable del servidor o aplicación que se sirve de tal *Certificado*, no hace un uso adecuado del mismo vulnerando derechos de propiedad industrial o intelectual de terceros sobre las aplicaciones, sitios web o equipos 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 equipos. 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:

- La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.
- La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.
- 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
- La protección de la juventud y de la infancia.

339. La FNMT–RCM quedará exonerada y se mantendrá indemne de cualquier reclamación o reivindicación por el uso inadecuado de los *Certificados de servidor web* realizado por:

- su *Suscriptor* o su *Responsable* o
- el propietario o responsable de los equipos o aplicaciones que empleen el *Certificado*

y, en ambos casos, que incumplan lo previsto en la *Declaración de Prácticas de Certificación*.

340. La FNMT-RCM expide bajo la presente *Política de Certificación* los siguientes tipos de *Certificados de servidor web*:

- *Certificado de servidor web* para su uso en un nombre de dominio o IP (Common Name)
- *Certificado de servidor web* para su uso en varios nombres de subdominios dentro de un dominio dado (Wildcard).

341. En ambos casos, los *Certificados de servidor web* permiten identificar a un servidor web accesible a través de un nombre de dominio o IP.

12.1.3. Comunidad y ámbito de aplicación

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

a) Son expedidos por la FNMT-RCM como *Prestador de Servicios de Certificación* cumpliendo con los criterios establecidos en la Ley española 59/2003, de 19 de diciembre, de Firma Electrónica y en la Directiva Europea de Firma Electrónica [D99/93EC]

b) Los *Certificados* emitidos bajo esta *Política de Certificación* son expedidos para las *Organizaciones* que forman parte de la *Comunidad Electrónica UE,* tal y como se define en el apartado Definiciones de este documento. En el marco de esta *Política de Certificación*, los *Responsables del Certificado* y custodios de los *Datos de Creación de Firma* se corresponden con el personal de las *Organizaciones* en el ejercicio de sus competencias y funciones públicas propias del cargo, de la relación funcionarial, de

las funciones del empleado público, o de la condición de autorizado por la *Organización*, en relación con la entidad a la que pertenezcan o con la que se relacionen estos *Responsables*.

12.1.4. Responsabilidad y obligaciones de las partes

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

- Las *Organizaciones* o *Entidades Competentes* representadas a través de los diferentes órganos competentes y que son los *Suscriptores* de los *Certificados*.
- *Oficinas de Registro*, que, a través del personal designado por la *Organización*, serán responsables de comprobar los requisitos y condiciones ostentados por los *Responsables del Certificado*.
- Los *Responsables del Certificado* y sus *Claves*, que será el personal al servicio de las *Organizaciones*.
- FNMT-RCM, en cuanto *Prestador de Servicios de Certificación*.
- El resto de la *Comunidad Electrónica UE*.

344. El régimen de derechos y obligaciones de la *Organización* y la FNMT-RCM se regirá mediante los correspondientes acuerdos reguladores de los servicios de certificación.

345. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en este documento y en la [DGPC], la *Organización* como *Autoridad Local de Registro*, el *Referente de la LRA* y los *Registradores* tienen la obligación de:

- Cumplir con los procedimientos de registro facilitados por la FNMT-RCM.
- No realizar registros o tramitar solicitudes de personal que preste sus servicios en una *Organización* diferente a la que representa como *Oficina de Registro*, sin perjuicio de la creación, en la propia Comisión Europea, de *Oficinas de Registro* centralizadas que se hayan establecido.
- Solicitar la revocación o suspensión del *Certificado de servidor web* cuando alguno de los datos consignados en el *Certificado* sea inexacto, incorrecto, haya variado o sea de necesaria revocación por razones de seguridad. También deberá solicitar la revocación o suspensión cuando se den las circunstancias previstas en la legislación aplicable.
- Solicitar a la FNMT-RCM, a través de la *Oficina de Registro*, la revocación cuando, directamente o a través de comunicación del personal al servicio de *Organización*, exista pérdida, extravío del soporte del *Certificado* o de su confidencialidad, o presunción de ello.
- Custodiar la documentación aportada por cualquiera de los intervinientes en los procesos de gestión de los *Certificados* (solicitudes de emisión, revocación y cualesquiera otros de la misma índole) así como los documentos generados en dichos procesos (justificantes, contratos de emisión, revocación, etc.)
- Comprobar fehacientemente los datos del personal al servicio de la *Organización* o *Entidad Competente Suscriptora* del *Certificado* y referidos a su identidad y su pertenencia a ésta, así como la capacidad suficiente para realizar solicitudes en nombre del *Suscriptor* del *Certificado*. Del mismo modo, se deberá verificar su correspondencia con los titulares y contactos establecidos, en las bases de datos correspondientes, para la gestión y administración de la dirección electrónica o nombre de dominio que identificará al *Certificado* objeto de la solicitud y al correspondiente servidor.

346. Las relaciones de la FNMT-RCM con la *Organización* y los *Responsables de los Certificados* quedarán determinadas, a los efectos del régimen de uso de los *Certificados*, por los siguientes documentos: condiciones de utilización o contrato de emisión del *Certificado*, y, subsidiariamente, las presentes *Políticas y Prácticas de Certificación Particulares* y por la [DGPC], atendiendo a los acuerdos o documentos de relación entre la FNMT-RCM y las *Organizaciones*.

347. Las relaciones de la *Organización* o *Entidad Competente Suscriptora* del *Certificado* y de su personal con la FNMT-RCM se realizarán siempre a través de la *Oficina de Registro* y su *Referente*. La FNMT-RCM no realizará ninguna acción solicitada por el personal al servicio de la *Organización* o *Responsables del Certificado* que no esté autorizada por *Referente de la LRA* o por la *Organización* o *Entidad Competente Suscriptora* del *Certificado*.

348. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la [DGPC], el *Responsable del Certificado* tiene la obligación de:

- No utilizar el *Certificado* en servidores web cuyo contenido:
  - pueda vulnerar los derechos de propiedad industrial o intelectual de terceros, poner en peligro el orden público, la investigación penal, la seguridad pública o la defensa nacional
  - atente contra la protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores
  - menoscabe 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
  - ponga en peligro la protección de la juventud y de la infancia
- Realizar un uso adecuado del *Certificado* en base a las competencias y facultades atribuidas por la *Organización* o *Entidad Competente Suscriptora*.
- Mantener en todo momento el control exclusivo de los *Datos de Creación de Firma* y tomar las razonables precauciones para prevenir su pérdida, revelación, modificación o uso no autorizado
- Comunicar al *Referente de la LRA* correspondiente, la pérdida, extravío, o sospecha de ello, del soporte del *Certificado* o de su confidencialidad, del que es *Responsable* con el fin de iniciar, en su caso, los trámites de la revocación del *Certificado*.

349. El resto de la *Comunidad Electrónica UE* y los terceros regularán sus relaciones con la FNMT-RCM a través de la [DGPC] y estas *Políticas 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.

12.1.5. Límites de uso de los Certificados de servidor web

350. El uso de este tipo de *Certificados* queda limitado a los servidores web de las *Organizaciones* o *Entidades Competentes Suscriptoraes* al objeto de la identificación y autenticación de la dirección URL o IP de dichos servidores. Fuera de la funcionalidad prevista anteriormente no se podrán emplear estos *Certificados*.

351. La FNMT-RCM y las *Organizaciones* podrán fijar en los acuerdos correspondientes otros límites adicionales.

352. FNMT-RCM no tendrá control sobre las actuaciones y usos de los *Certificados* que se realicen por parte del *Suscriptor*, *Responsable* o las *Oficinas de Registro*, por lo que la FNMT-RCM quedará exonerada de responsabilidad a efectos de tales usos y de la extralimitación en el uso establecido anteriormente, así como de las consecuencias y efectos que pudieran producirse por reclamaciones o posibles responsabilidades patrimoniales llevadas a cabo por cualquier miembro de la *Comunidad Electrónica UE* o por terceros.

353. Para que el *Responsable* utilice de forma diligente los *Certificados de servidor web* y *Claves* asociadas, la *Organización* o *Entidad Competente* a la que representa deberá previamente formar parte de la *Comunidad Electrónica UE* y haberse constituido como *Suscriptor* del *Certificado*.

354. En cualquier caso, si un tercero desea confiar en las operaciones realizadas con uno de estos *Certificados de servidor web* sin acceder a los *Servicios de información y consulta sobre el estado de validez de los certificados* emitidos bajo esta *Política de Certificación*, no se

obtendrá cobertura de las presentes *Políticas y Prácticas de Certificación Particulares* y se carecerá de legitimidad alguna para reclamar o emprender acciones legales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado*.

355. Además, incluso dentro del ámbito de la *Comunidad Electrónica UE*, 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 *Sellado de Tiempo*
- 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
- Utilizar el *Certificado* para usos distintos a los inicialmente previstos respecto de los *Certificados de servidor web*

12.2. POLÍTICA DE CERTIFICACIÓN DE LOS CERTIFICADOS DE SERVIDOR DE ACTUACIÓN AUTOMATIZADA

12.2.1. Identificación

356. La presente *Política de Certificación* de la FNMT-RCM para la expedición de *Certificados de Actuación Automatizada* para su uso en el ámbito de competencias de las *Organizaciones* y en el marco de la *Comunidad Electrónica UE*.

Nombre: *Política de Certificación* de *Certificados de Actuación Automatizada*

Referencia / OID:

- 1.3.6.1.4.1.5734.3.4.7 – Para los *Certificados de Actuación Automatizada* del tipo *Reconocido sin DSCF para firma de documentos*
- 1.3.6.1.4.1.5734.3.4.8 – Para los *Certificados de Actuación Automatizada* del tipo *Normalizado para firma o cifrado de documentos*

Versión: 1.0

Fecha de emisión: 12 de marzo de 2013

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/

12.2.2. Tipología del *Certificado de* Actuación Automatizada

357. Los *Certificados de Actuación Automatizada* son aquellos *Certificados* expedidos por la FNMT-RCM bajo la presente *Política de Certificación* y que vinculan unos *Datos de Verificación de Firma* a un servidor o aplicación sobre la que existe una persona física o jurídica determinada que actúa como responsable, siendo ésta la que tiene el control sobre dicho servidor o aplicación.

358. Este tipo de *Certificados* se emplean por las *Organizaciones* o *Entidades Competentes Suscriptoras* al objeto de realizar tramitaciones automatizadas que ofrezcan garantías de autenticidad, confidencialidad y compromiso con el contenido.

359. La *Clave Privada* asociada a la *Clave Pública* estará bajo la responsabilidad y custodia del *Responsable del certificado* que actuará como representante de la persona física o jurídica titular del servidor objeto del *Certificado*.

360. A los efectos del artículo 6 de la Ley española 59/2003, de 19 de diciembre, de Firma Electrónica, los *Certificados de servidor* se considerarán *Certificados* electrónicos cuando exista vinculación indubitada entre el *Certificado de servidor* y la *Organización* o *Entidad Competente Suscriptora* de este. FNMT-RCM emitirá estos *Certificados* siempre que sea solicitado por los miembros de la *Comunidad Electrónica UE* para las diversas relaciones que puedan producirse y no se encuentre prohibido o limitado su utilización por la legislación aplicable.

361. FNMT-RCM no será responsable de las actuaciones realizadas con este tipo de *Certificados* cuando se produzca abuso de facultades o insuficiencia de las mismas y/o cuando se produzcan decisiones del *Suscriptor* del *Certificado* que afecten a la vigencia de las facultades del responsable, por lo que cualquier modificación, revocación o restricción no será oponible a la FNMT-RCM salvo que sea fehacientemente notificada.

362. Sólo podrán obtener *Certificados de Actuación Automatizada* aquellas entidades que hayan suscrito un acuerdo con la FNMT-RCM, en virtud del cual formen parte de la *Comunidad Electrónica UE* tal y como se contempla en la *Declaración de Prácticas de Certificación* de la FNMT-RCM.

363. Estos *Certificados de servidor*, no conllevan el efecto jurídico de equivalencia de firma electrónica reconocida con las actuaciones realizadas a través de firma manuscrita tradicional. No obstante, tendrán la validez y eficacia jurídica atendiendo a su respectiva naturaleza según la legislación aplicable.

364. La FNMT-RCM, como *Prestador de Servicios de Certificación* se reserva el derecho de no expedir o revocar este tipo de *Certificados* si el *Responsable* del mismo o el responsable del servidor o aplicación que se sirve de tal *Certificado*, no hace un uso adecuado del mismo vulnerando derechos de propiedad industrial o intelectual de terceros sobre las aplicaciones, sitios web o equipos 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 equipos. 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:

- La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.
- La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.
- 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
- La protección de la juventud y de la infancia.

365. La FNMT–RCM quedará exonerada y se mantendrá indemne de cualquier reclamación o reivindicación por el uso inadecuado de los *Certificados de Actuación Automatizada* realizado por:

- su *Suscriptor* o su *Responsable* o
- el propietario o responsable de los equipos o aplicaciones que empleen el *Certificado*

y, en ambos casos, que incumplan lo previsto en la *Declaración de Prácticas de Certificación*.

366. La FNMT-RCM expide bajo la presente *Política de Certificación* los siguientes tipos de *Certificados de servidor de Actuación Automatizada*:

- *Certificado de Actuación Automatizada* para su uso como *Reconocido sin DSCF para firma de documentos.* Al que aplican los requisitos, expuestos en este mismo documento, para la política de *Certificados Reconocidos* ([ETSI456]).

- *Certificado de Actuación Automatizada* para su uso como *Normalizado para firma o cifrado de documentos*. Al que aplican los requisitos, expuestos en este mismo documento, para la política de *Certificados Normalizados* ([ETSI042]).

12.2.3. Comunidad y ámbito de aplicación

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

c) Son expedidos por la FNMT-RCM como *Prestador de Servicios de Certificación* cumpliendo con los criterios establecidos en la Ley española 59/2003, de 19 de diciembre, de Firma Electrónica y en la Directiva Europea de Firma Electrónica [D99/93EC]

d) Los *Certificados* emitidos bajo esta *Política de Certificación* son expedidos para las *Organizaciones* que forman parte de la *Comunidad Electrónica UE,* tal y como se define en el apartado Definiciones de este documento. En el marco de esta *Política de Certificación*, los *Responsables del Certificado* y custodios de los *Datos de Creación de Firma* se corresponden con el personal de las *Organizaciones* en el ejercicio de sus competencias y funciones públicas propias del cargo, de la relación funcionarial, de las funciones del empleado público, o de la condición de autorizado por la *Organización*, en relación con la entidad a la que pertenezcan o con la que se relacionen estos *Responsables*.

12.2.4. Responsabilidad y obligaciones de las partes

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

- Las *Organizaciones* o *Entidades Competentes* representadas a través de los diferentes órganos competentes y que son los *Suscriptores* de los *Certificados*.
- *Oficinas de Registro*, que, a través del personal designado por la *Organización*, serán responsables de comprobar los requisitos y condiciones ostentados por los *Responsables del Certificado*.
- Los *Responsables del Certificado* y sus *Claves*, que será el personal al servicio de las *Organizaciones*.
- FNMT-RCM, en cuanto *Prestador de Servicios de Certificación*.
- El resto de la *Comunidad Electrónica UE*.

369. El régimen de derechos y obligaciones de la *Organización* y la FNMT-RCM se regirá mediante los correspondientes acuerdos reguladores de los servicios de certificación.

370. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en este documento y en la [DGPC], la *Organización* como *Autoridad Local de Registro*, el *Referente de la LRA* y los *Registradores* tienen la obligación de:

- Cumplir con los procedimientos de registro facilitados por la FNMT-RCM.
- No realizar registros o tramitar solicitudes de personal que preste sus servicios en una *Organización* diferente a la que representa como *Oficina de Registro*, sin perjuicio de la creación, en la propia Comisión Europea, de *Oficinas de Registro* centralizadas que se hayan establecido.
- Solicitar la revocación o suspensión del *Certificado de servidor* cuando alguno de los datos consignados en el *Certificado* sea inexacto, incorrecto, haya variado o sea de necesaria revocación por razones de seguridad. También deberá solicitar la revocación o suspensión cuando se den las circunstancias previstas en la legislación aplicable.
- Solicitar a la FNMT-RCM, a través de la *Oficina de Registro*, la revocación cuando, directamente o a través de comunicación del personal al servicio de *Organización*, exista pérdida, extravío del soporte del *Certificado* o de su confidencialidad, o presunción de ello.

- Custodiar la documentación aportada por cualquiera de los intervinientes en los procesos de gestión de los *Certificados* (solicitudes de emisión, revocación y cualesquiera otros de la misma índole) así como los documentos generados en dichos procesos (justificantes, contratos de emisión, revocación, etc.)
- Comprobar fehacientemente los datos del personal al servicio de la *Organización* o *Entidad Competente Suscriptora* del *Certificado* y referidos a su identidad y su pertenencia a ésta, así como la capacidad suficiente para realizar solicitudes en nombre del *Suscriptora* del *Certificado*. Del mismo modo, se deberá verificar su correspondencia con los titulares y contactos establecidos, en las bases de datos correspondientes, para la gestión y administración de la dirección electrónica o nombre de dominio que identificará al *Certificado* objeto de la solicitud y al correspondiente servidor.

371. Las relaciones de la FNMT-RCM con la *Organización* y los *Responsables de los Certificados* quedarán determinadas, a los efectos del régimen de uso de los *Certificados*, por los siguientes documentos: condiciones de utilización o contrato de emisión del *Certificado*, y, subsidiariamente, las presentes *Políticas y Prácticas de Certificación Particulares* y por la [DGPC], atendiendo a los acuerdos o documentos de relación entre la FNMT-RCM y las *Organizaciones*.

372. Las relaciones de la *Organización* o *Entidad Competente Suscriptor* del *Certificado* y de su personal con la FNMT-RCM se realizarán siempre a través de la *Oficina de Registro* y su *Referente*. La FNMT-RCM no realizará ninguna acción solicitada por el personal al servicio de la *Organización* o *Responsables del Certificado* que no esté autorizada por *Referente de la LRA* o por la *Organización* o *Entidad Competente Suscriptora* del *Certificado*.

373. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la [DGPC], el *Responsable del Certificado* tiene la obligación de:

- No utilizar el *Certificado* en servidores cuyo contenido:
  - pueda vulnerar los derechos de propiedad industrial o intelectual de terceros, poner en peligro el orden público, la investigación penal, la seguridad pública o la defensa nacional
  - atente contra la protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores
  - menoscabe 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
  - ponga en peligro la protección de la juventud y de la infancia
- Realizar un uso adecuado del *Certificado* en base a las competencias y facultades atribuidas por la *Organización* o *Entidad Competente Suscriptora*.
- Mantener en todo momento el control exclusivo de los *Datos de Creación de Firma* y tomar las razonables precauciones para prevenir su pérdida, revelación, modificación o uso no autorizado
- Comunicar al *Referente de la LRA* correspondiente, la pérdida, extravío, o sospecha de ello, del soporte del *Certificado* o de su confidencialidad, del que es *Responsable* con el fin de iniciar, en su caso, los trámites de la revocación del *Certificado*.

374. El resto de la *Comunidad Electrónica UE* y los terceros regularán sus relaciones con la FNMT-RCM a través de la [DGPC] y estas *Políticas 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.

12.2.5. Limitaciones de responsabilidad adicionales para los Certificados de Actuación Automatizada del tipo Reconocido sin DSCF para firma de documentos

375. La FNMT-RCM mientras emita y administre los certificados en cumplimiento con su política de certificación y su declaración de prácticas de certificación, no se hace responsable de ninguna pérdida de beneficios, oportunidades comerciales, contratos, ingresos o de ahorros previstos ni de ninguna pérdida indirecta o consecuente.

376. LA FNMT-RCM no limita el importe de las transacciones que puedan realizarse mediante el uso de este certificado electrónico. No obstante, a este respecto se observará la limitación de responsabilidad establecida tanto en la General Certification Practices Statement, como las establecidas por contrato o convenio, y las particularidades específicas del presente apartado.

377. La responsabilidad total de la FNMT-RCM , como máxima y en su conjunto, en concepto de una demanda por daños y perjuicios interpuesta por todas las partes en un acuerdo de confianza relacionada con este certificado concreto, se calculará aplicando las siguientes condiciones de contorno jerárquicas:

Criterio 1: La suma total no es menor de tres veces el precio / cantidad total de el(los) Contrato(s) Específico(s) o Pedido(s).

Criterio 2: Para todo caso, las cuantías que en concepto de daños y perjuicios debiera satisfacer por imperativo judicial la FNMT-RCM a terceros perjudicados, y/o miembros de la Comunidad electrónica se limitan a un máximo de SEIS MIL EUROS (6.000€) euros

378. Las limitaciones de responsabilidad dispuestas en la presente sub-cláusula serán siempre las mismas, independientemente del número de firmas digitales, operaciones o demandas relacionadas con dicho certificado.

12.2.6. Límites de uso de los Certificados de Actuación Automatizada

379. El uso de este tipo de *Certificados* queda limitado a los sistemas de las *Organizaciones* o *Entidades Competentes Suscriptoras* al objeto de la realización de operaciones automatizadas de firma o cifrado de documentos. Fuera de la funcionalidad prevista anteriormente no se podrán emplear estos *Certificados*.

380. La FNMT-RCM y las *Organizaciones* podrán fijar en los acuerdos correspondientes otros límites adicionales.

381. FNMT-RCM no tendrá control sobre las actuaciones y usos de los *Certificados* que se realicen por parte del *Suscriptor*, *Responsable* o las *Oficinas de Registro*, por lo que la FNMT-RCM quedará exonerada de responsabilidad a efectos de tales usos y de la extralimitación en el uso establecido anteriormente, así como de las consecuencias y efectos que pudieran producirse por reclamaciones o posibles responsabilidades patrimoniales llevadas a cabo por cualquier miembro de la *Comunidad Electrónica UE* o por terceros.

382. Para que el *Responsable* utilice de forma diligente los *Certificados de servidor* y *Claves* asociadas, la *Organización* o *Entidad Competente* a la que representa deberá previamente formar parte de la *Comunidad Electrónica UE* y haberse constituido como *Suscriptor* del *Certificado*.

383. En cualquier caso, si un tercero desea confiar en las operaciones realizadas con uno de estos *Certificados de servidor* sin acceder a los *Servicios de información y consulta sobre el estado de validez de los certificados* emitidos bajo esta *Política de Certificación*, no se obtendrá cobertura de las presentes *Políticas y Prácticas de Certificación Particulares* y se carecerá de legitimidad alguna para reclamar o emprender acciones legales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado*.

384. Además, incluso dentro del ámbito de la *Comunidad Electrónica UE*, 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 *Sellado de Tiempo*
- 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
- Utilizar el *Certificado* para usos distintos a los inicialmente previstos respecto de los *Certificados de Actuación Automatizada*

12.3. PRÁCTICAS DE CERTIFICACIÓN PARTICULARES PARA LOS CERTIFICADOS DE SERVIDOR

385. 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*.

386. En especial deberá tenerse presente, a efectos interpretativos del presente anexo el apartado "Definiciones" de la [DGPC] y de este documento.

387. 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 de servidor* expedidos bajo las *Políticas de Certificación* identificadas con los OIDs

- 1.3.6.1.4.1.5734.3.4.4 – Para los *Certificados de Servidor web* del tipo Common Name
- 1.3.6.1.4.1.5734.3.4.5 – Para los *Certificados de Servidor web* del tipo Wildcard
- 1.3.6.1.4.1.5734.3.4.7 – Para los *Certificados de Actuación Automatizada* del tipo *Reconocido sin DSCF para firma de documentos*
- 1.3.6.1.4.1.5734.3.4.8 – Para los *Certificados de Actuación Automatizada* del tipo *Normalizado para firma o cifrado de documentos*

12.3.1. Servicios de Gestión de las *Claves*

388. La FNMT-RCM, bajo ningún concepto, genera ni almacena las *Claves Privadas* de los *Firmantes*, que son generadas bajo su exclusivo control y, en su caso, con la intervención de la *Oficina de Registro* correspondiente y cuya custodia está bajo responsabilidad del *Responsable del Certificado*.

12.3.2. Gestión del ciclo de vida de los Certificados

389. Se definen aquí aquellos aspectos que, si bien algunos ya han sido apuntados en la [DGPC], revisten determinadas especialidades que necesitan un mayor nivel de detalle.

12.3.2.1. Procedimiento de solicitud y emisión del Certificado de servidor

390. A continuación se describe el procedimiento de solicitud por el que el *Registrador* toma los datos del personal al servicio de la *Organización*, confirma su identidad y su capacidad para realizar la solicitud del *Certificado* para el nombre de dominio, IP, institución o sistema –según corresponda- en cuestión y se formaliza, entre el citado personal y la FNMT-RCM, el documento de condiciones de utilización o el contrato de emisión, según lo previsto en el

acuerdo de la FNMT-RCM con la *Organización* para la posterior emisión de un *Certificado de servidor*.

391. La FNMT-RCM considera bajo responsabilidad de las *Organizaciones*, que actuarán a través de las *Oficinas de Registro* como *Autoridad Local de Registro*, que este personal se encuentra con su cargo vigente, que sus datos personales son auténticos y están en vigor y, por tanto, habilitado para obtener e instalar el *Certificado*. La FNMT-RCM no mantiene relación jurídica funcionarial, administrativa o laboral con este personal, más allá del documento de condiciones de utilización o, en su caso, contrato de emisión, por tanto, no tendrá la obligación de verificar los datos antedichos.

392. La Comisión Europea podrá establecer, en el ámbito de actuación de sus competencias, Oficinas de Registro centrales o comunes con efectos uniformes para cualesquiera de las diferentes entidades de los Estados Miembro

393. Las actividades de comprobación anteriores serán realizadas por el personal de la *Oficina de Registro* implantada por la *Organización*, que es la entidad donde el *Responsable del Certificado* presta sus servicios. Por tanto y a estos efectos las *Oficinas de Registro* no serán autoridades delegadas o dependientes de la FNMT-RCM.

394. Este *Certificado* será solicitado por la *Organización* o *Entidad Competente Suscriptora* quien actuará como solicitante sin perjuicio de que las operaciones necesarias para la petición y obtención del *Certificado* se realicen por el *Referente* o el *Registrador* o, de manera instrumental, por el propio *Responsable*.

395. Los tres pasos a realizar para la obtención del *Certificado* son:

12.3.2.1.1. Generación de Claves (Paso 1)

396. Con carácter previo, el *Responsable del Certificado* y el *Suscriptor* deberán consultar la [DGPC] y las presentes *Políticas y Prácticas de Certificación Particulares* en la dirección http://www.cert.fnmt.es/dpcs/ con las condiciones de uso y obligaciones propias como *Responsable* y *Suscriptor*, respectivamente, del *Certificado*, que se plasmaran en el documento de condiciones de utilización o, si procede, el contrato de emisión.

397. A continuación, el *Responsable del Certificado* deberá generar, en el propio servidor donde se utilizará, las *Claves Pública* y *Privada* que serán vinculadas a éste, convirtiéndose en su momento en *Datos de Verificación y Creación de Firma* o *Datos de Cifrado y Descifrado* respectivamente. Asimismo, con estas *Claves*, el *Responsable de Certificado* generará un *PKCS#10* para realizar la solicitud del *Certificado* a la FNMT-RCM

12.3.2.1.2. Acreditación de la identidad y solicitud (Paso 2)

398. A continuación el *Responsable del Certificado* deberá realizar la correspondiente solicitud de emisión a través de la *Oficina de Registro* que le corresponda (aquella que representa a la *Organización* ante la FNMT-RCM en las operaciones de gestión de *Certificados* y en la que el *Responsable* presta sus servicios).

399. Esta solicitud podrá realizarse bien por personación física o de forma telemática. En cualquier caso, el *Registrador* autenticará al *Responsable del Certificado* mediante el requerimiento de aportación de:

- datos personales (como mínimo el nombre, primer apellido, correo electrónico y número distintivo del documento oficial a aportar) y datos vinculados a la solicitud en cuestión (PKCS#10 y nombre del dominio o dirección IP o de la institución o sistema para el cual se emite el *Certificado*),
- fotocopia de la documentación correspondiente y consistente en el documento oficial que acredite la identidad del *Responsable del Certificado*.
- fotocopia de la designación de la *Organización* o *Entidad Competente Suscriptora* al *Responsable del Certificado* como autorizado para realizar la solicitud del *Certificado de servidor*

400. La documentación aportada por el *Responsable del Certificado* será custodiada por la *Oficina de Registro* como parte de la solicitud.

401. El *Registrador* comprobará la condición del *Responsable del Certificado y peticionario* como empleado de la *Organización* o *Entidad Competente Suscriptora* del *Certificado*, con cargo vigente y facultades suficientes a través de la correspondiente autorización de la *Organización*, así como la veracidad del correo electrónico, todo ello por los medios que tenga a su disposición y habida cuenta de que la *Oficina de Registro* actúa en representación de la *Organización* en cuestión y por tanto conoce de forma fehaciente esta información.

402. El *Registrador* comprobará a través del formulario de autorización o de solicitud del *Certificado*, que la *Organización* o *Entidad Competente* ha consignado el nombre de dominio, IP, institución o sistema a incluir en dicho *Certificado*, manifestándose como titular de dicha denominación.

403. La aportación de los datos y documentos requeridos en la solicitud avalarán la identidad del *Responsable del Certificado* y su condición de empleado y autorizado por la *Organización* o *Entidad Competente Suscriptora* del mismo y será condición necesaria y suficiente para el establecimiento del vínculo entre identidad y *Datos de Creación de Firma* que se crea en el momento de la emisión del *Certificado*.

404. Con los datos ya revisados, el *Registrador* accederá a la aplicación de registro para introducirlos, incluyendo el PKCS#10. Si la solicitud está completa, el *Registrador* recibirá como respuesta un código de solicitud que identificará la transacción y que será necesario posteriormente para la descarga del *Certificado*.

405. Al realizar esta solicitud se envía a la FNMT-RCM la *Clave Pública* generada, junto con las correspondientes pruebas de posesión (incluidas en la petición electrónica PKCS#10) de la *Clave Privada*, para la posterior emisión del *Certificado*.

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

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

12.3.2.1.3. Emisión del Certificado de servidor (Paso 3)

408. La petición cursada por la *Oficina de Registro* será validada por personal de la FNMT_RCM, que comprobará que esta petición ha sido cursada por un *Registrador* autorizado y que se ha recibido el documento de autorización del *Responsable* del *Certificado* para realizar la solicitud de emisión de un *Certificado de servidor*.

409. FNMT – RCM comprobará, a través de los sistemas de información que los registradores autorizados para cada caso tengan a su disposición, que el nombre de dominio, dirección IP a incluir en el *Certificado de Servidor web* es de titularidad de la *Organización* o *Entidad Competente* solicitante. En el caso de que no sea posible tal comprobación, FNMT-RCM aceptará la titularidad de la *Organización* o *Entidad Competente* sobre los citados nombres o direcciones en base a la correspondiente solicitud.

410. La FNMT-RCM validará también el PKCS#10 recibido en la solicitud comprobando, únicamente, la posesión y correspondencia de la pareja de *Claves* criptográficas por parte del *Responsable del Certificado*

411. Así pues, una vez recibidos los datos correspondientes a la petición y realizadas las validaciones oportunas, se procederá a la emisión del *Certificado*.

412. La emisión de *Certificados de Servidor web* supone la generación de documentos electrónicos que vinculan unos *Datos de Verificación de Firma* a un nombre de dominio o dirección IP para el acceso seguro a un servidor web bajo control de la *Organización*, así como su correspondencia con la *Clave Pública* asociada.

413. La emisión de los *Certificados* sujetos a las presentes *Políticas* sólo puede realizarse por la FNMT-RCM en su calidad de *Prestador de Servicios de Certificación*, no existiendo ninguna otra entidad u organismo con capacidad de emisión de los mismos.

414. La FNMT-RCM, por medio de su *Firma electrónica*, autentica el *Certificado* y confirma la identidad del *Suscriptor,* así como su relación con el nombre del dominio, dirección IP, institución o sistema para el cual se emite el *Certificado de Servidor*, 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 el *Certificado*, la FNMT-RCM utilizará mecanismos criptográficos que doten de autenticidad e integridad al *Certificado*.

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

- Comprobar que el *Responsable del Certificado* utiliza la *Clave Privada* correspondiente a la *Clave Publica* vinculada a la identidad del *Firmante* 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 Claves Públicas* de la FNMT-RCM.

416. Para la emisión del *Certificado de servidor* se seguirán los siguientes pasos:

1. Composición del nombre distintivo (DN) del *Certificado de servidor web*

   Con los datos del nombre del dominio, dirección IP, o nombre de institución o de sistema recogidos durante el proceso de solicitud del *Certificado*, se compone 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 *Suscriptor*.

   El *DN* para este tipo de *Certificados* está compuesto de los siguientes elementos:

   DN≡CN, O, C

   El conjunto de atributos O, C representa la rama del directorio en la que se encuentra ubicada la entrada correspondiente a los *Certificados de servidor web* emitidos a la *Organización* en cuestión.

   El atributo *CN* contiene el nombre de dominio, dirección IP, nombre de institución o de sistema para el que se emite el *Certificado*.

   El atributo O contiene el nombre de la *Organización*.

   El atributo C contiene el código de país al que pertenece la *Organización*.

   Ej.:

   CN=**www.eui.europa.eu**

   CN=213.170.35.210

   En el caso de los *Certificados de servidor web* tipo “Wildcard” el CN del *Certificado* será de la forma:

   CN=*.nombredominiosegundonivel.TLD

   siendo,

   [nombredominiosegundonivel] el nombre de dominio cuyo titular es la *Organización* o *Entidad Competente*

   [TLD] el nombre de dominio de primer nivel bajo el cual se encuentra registrado el nombre de dominio de segundo nivel

   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. Generación del *Certificado* conforme al perfil del *Certificado de servidor web*

   El formato del *Certificado de servidor*estará en consonancia con la norma UIT-T X.509 versión 3 y de acuerdo con la normativa legalmente aplicable.

En las tablas anexas a este documento puede consultarse el perfil de este tipo de *Certificados*.

Así mismo el *Certificado* incluirá el identificador de Política correspondiente. .

12.3.2.2. Publicación del Certificado de servidor

417. Una vez generado el *Certificado* por parte del *Prestador de Servicios de Certificación*, se publicará en el *Directorio*, concretamente en la entrada correspondiente a la *Organización*.

418. A la dirección de correo electrónico proporcionada por el *Responsable* se le enviará una comunicación de la disposición de su *Certificado* para su descarga.

12.3.2.3. Descarga e instalación del Certificado de Servidor

419. Una vez generado el *Certificado*, se pone a disposición del *Registrador* un mecanismo de descarga en la aplicación de registro.

420. En este proceso guiado se le pedirá al interesado que introduzca el CN para la cual se emitió el *Certificado*, así como el código de solicitud devuelto por el sistema al finalizar dicho proceso.

421. Si el *Certificado* no ha sido aún generado por cualquier motivo, se le indicará este hecho en el momento que intente su descarga. En caso contrario se pondrá a disposición del interesado.

422. Finalmente, el *Registrador* remitirá al *Responsable* el *Certificado* generado, quien lo instalará en el servidor donde se realizó la generación de claves correspondiente.

12.3.2.4. Vigencia del Certificado de Servidor

12.3.2.4.1. Caducidad

423. Los *Certificados* de *servidor*emitidos bajos la presente *Política de Certificación* por la FNMT-RCM tendrán validez durante un período de un (1) 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 *Suscriptor* desee seguir utilizando los servicios del *Prestador de Servicios de Certificación.*

12.3.2.4.2. Extinción de la vigencia

424. Los *Certificados de servidor*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*, 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 pérdida 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

425. 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 validez de los certificados*.

12.3.2.5. Revocación del Certificado de servidor

12.3.2.5.1. Causas de revocación del Certificado de servidor

426. Serán causas de revocación de un *Certificado de servidor*:

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* o sospecha del compromiso de la confidencialidad de éste
- La utilización por un tercero de los *Datos de Creación de Firma*, correspondientes a los *Datos de Verificación de Firma* contenidos en el *Certificado* y vinculados a la identidad del *Firmante*.
- La violación o puesta en peligro del secreto de los *Datos de Creación de Firma*.
- La no aceptación de la *Organización* o *Entidad Competente* 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, así como los supuestos previstos en la legislación aplicable.

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

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

e) Contravención de una obligación sustancial de esta *Declaración de Prácticas de Certificación* por parte del *Responsable del Certificado,* del *Suscriptor* o del personal de la *Oficina de Registro* si hubiese podido afectar al procedimiento de emisión del *Certificado*.

f) Resolución del contrato suscrito entre la *Organización* y la FNMT-RCM.

g) 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.

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

428. 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, incluyendo las causas antes mencionadas, a la FNMT-RCM, producirán la exoneración de responsabilidad de la FNMT-RCM.

12.3.2.5.2. Efectos de la revocación

429. 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 validez de los certificados*.

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

12.3.2.5.3. Procedimiento para la revocación

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

432. La revocación de un *Certificado de Servidor*puede ser solicitada por el *Suscriptor* a través del *Referente de la LRA* o de los *Registradores.* Asimismo, el *Responsable del Certificado* podrá plantear a la *Oficina de Registro* la revocación o suspensión si existen causas que lo

justifiquen, en los términos recogidos en la presente *Política y Prácticas de Certificación Particulares*.

433. Sin perjuicio de lo anterior, la FNMT-RCM podrá revocar los *Certificados de servidor web* en los supuestos recogidos en la *Declaración de Prácticas de Certificación* y en la legislación aplicable.

434. El *Responsable del Certificado* o el *Suscriptor*, a través de un representante con capacidad suficiente, podrá solicitar la operación de revocación bien personándose en la *Oficina de Registro* correspondiente, bien vía telemática. En cualquier caso, el *Registrador* deberá comprobar la capacidad suficiente del peticionario para realizar la solicitud de revocación.

435. En el proceso de solicitud de revocación, el peticionario comunicará al *Registrador* el número de serie y el CN del *Certificado* a revocar. Estos datos serán introducidos por éste último en la aplicación de registro al objeto de que se ejecute la revocación del *Certificado*.

436. De esta forma, el *Registrador* formalizará la petición de revocación mediante la aplicación de registro, que generará dos impresos con el contrato de solicitud para su posterior impresión.

437. Después de que el *Registrador* confirme la identidad del peticionario y su capacidad suficiente, el *Registrador* procederá a validar los datos y a enviarlos a la FNMT-RCM.

438. La *Oficina de Registro* deberá custodiar los impresos justificantes de la solicitud como parte de ésta.

439. La FNMT-RCM recibirá aquella información relevante a efectos de la revocación de un *Certificado* a través el modelo de solicitud de revocación que se le presente, en formato papel o electrónico, por la *Oficina de Registro*.

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

441. FNMT-RCM considerará que el peticionario de la revocación de un *Certificado* de servidor cuenta con la capacidad suficiente si la petición es realizada a través de la *Oficina de Registro* correspondiente. FNMT-RCM no valorará la conveniencia de la solicitud de revocación cuando ésta sea realizada a través de la *Oficina de Registro* antedicha.

442. 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. De forma análoga esta información también estará disponible mediante el protocolo OCSP en el correspondiente *Servicio de información sobre el estado de validez de los Certificados*.

ANEXO I: IDENTIFICACIÓN DE PERFILES DE CERTIFICACIÓN

Tabla 1 - *Certificado Raíz* de la FNMT-RCM para la emisión de certificados para la Comisión Europea (Jerarquía subordinada al *Certificado Raíz* de la FNMT-RCM)

Field		Content	Critical	Mandatory	Specifications
1. Version		2		Yes	Integer:=2 ([RFC5280] This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, version MUST be 3 (value is 2)(X509v3).
2. Serial Number		Certificate unique identifier number.		Yes	Integer. SerialNumber = ex: 111222. Automatically set by the Certification Entity. [RFC5280]. It will be a positive integer, not bigger than 20 octets (1- 2^{159}).
3. Signature Algorithm		Sha256withRsaEncryption		Yes	Identifies the type of algorithm used (OID 1.2.840.113549.1.1.11)
4. Issuer Distinguish Name		Certificate issuer entity (Root CA)		Yes	
	4.1. Country	C=ES		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	4.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o=FNMT-RCM		Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. Organization Unit	ou=AC RAIZ FNMT-RCM		Yes	UTF8 String, maximum size 128 (rfc5280)
5. Validity		15 years		Yes	
6. Subject		Certificate issuer entity (Subordinate CA)		Yes	
	6.1. Country	C=ES		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	6.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o=FNMT-RCM		Yes	UTF8 String, maximum size 128 (rfc5280)
	6.3. Common Name	cn=ISA CA		Yes	UTF8 String, maximum size 128 (rfc5280)
7. Authority Key Identifier		Root entity public key identifier. Medium to identify the public key corresponding to the private key used by the CA to sign the subordinate CA certificate.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits). Matches the field Subject Key Identifier of the Root CA.
8. Subject Public Key Info		Public key of the subordinate CA for the Public Administration, encoded accordingly the cryptographic algorithm. In this case RSA Encryption	No	Yes	Field to transport the Public Key and to identify the algorithm with which the key is used. The length is 4096.

Field			Content		Critical	Mandatory	Specifications
9. Subject Key Identifier			Subordinate CA public key identifier. Medium to identify certificates that contain a particular public key, and eases the building of certification paths.		No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
10. Key Usage			Permitted usage of the certified keys.		Yes	Yes	Normalized in X509
	10.1. Digital Signature		0			Yes	Allows electronic signature.
	10.2. Content Commitment		0			Yes	Points out to the software that uses the certificate if it must allow the user to know the signed content.
	10.3. Key Encipherment		0			Yes	It is used for management and transport of keys to establish secure sessions.
	10.4. Data Encipherment		0			Yes	It is used to encipher details which are not cryptographic keys.
	10.5. Key Agreement		0			Yes	For use in the Key Agreement process.
	10.6. Key Certificate Signature		1			Yes	Certificate signature allowed. It is used in CA Certificates.
	10.7. CRL Signature		1			Yes	CRL signature allowed. It is used in CA Certificates.
11. Certificate Policies			Certificate policy		No	Yes	
	11.1. Policy Identifier		2.5.29.32.0 (anyPolicy)			Yes	According to rfc3280: *"To promote interoperability, this profile RECOMMENDS that policy information terms consist of only 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	11.2.2 CPS Pointer	http://www.cert.fnmt.es/dpcs/		Yes	IA5String String. URL for the usage conditions.
		11.2.3	11.2.4 User Notice	Under the usage conditions asserted in the FNMT-RCM CPS (106, Jorge Juan street,28009, Madrid, Spain).		Yes	UTF8 String. maximum size 200 characters.
12. CRL Distribution Point					No	Yes	
	12.1. Distribution Point 1		CRL distribution point 1 (ARL) ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint			Yes	UTF8String Path where the CRL resides (distribution point 1)
	12.2. Distribution Point 2		CRL distribution point 2 (ARL) http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl			Yes	UTF8String. Path of LDAP service where the CRL resides. (distribution point 2)

Field		Content	Critical	Mandatory	Specifications
13. Authority Info Access			No		
	Access Method 1	Access method identification for revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)		Yes	OCSP (1.3.6.1.5.5.7.48.1)
	Acces Location 1	http://ocspISAca.cert.fnmt.es/ocspISAca/OcspResponder		Yes	OCSP service URL
	Access Method 2	Access method identification for additional information for validation proccess: 1.3.6.1.5.5.7.48.2 (ca cert)		Yes	Root CA certificate 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.*"
	Access Location 2	http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt		Yes	Root CA Certificate download URL.
14. Basic Constraints		This extension is used to identify whether the certification subject is a CA and the maximum depth level allowed for the certification path.	Yes		
	14.1. Subject Type	CA			Type of subject: Certification Authority
	14.2. Path Length	0			A zero value pathLenConstraint points out that no more intermediate CA certificates are allowed in the certification path.

Tabla 2 – Perfil del *Certificado Ligero*

Field		Content	Critical	Mandatory	Specifications
1. Version		2		Yes	Integer:=2 ([RFC5280] This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, version MUST be 3 (value is 2)(X509v3).
2. Serial Number		Certificate unique identifier number.		Yes	Integer. SerialNumber = ex: 111222. Automatically set by the Certification Entity. [RFC5280]. It will be a positive integer, not bigger than 20 octets (1- 2^{159}). The Serial Number will be assigned randomly.
3. Signature Algorithm		Sha256withRsaEncryption		Yes	Identifies the type of algorithm used (OID 1.2.840.113549.1.1.11)
4. Issuer Distinguish Name		Certificate issuer entity (Subordinate CA)		Yes	
	4.1. Country	C=ES		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	4.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o=FNMT-RCM.		Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. common Name	CN=ISA CA		Yes	UTF8 String, maximum size 128 (rfc5280).
5. Validity		4 years		Yes	Call for Tenders, DIGIT/R2/PO/2009/035, PKI SERVICES 1.2.1. Key generation/issuing certificates *The offered certificates have to have an operational period of at least one (1) year.*
6. Subject		Identification/description of the owner of / person responsible for the certified keys.		Yes	
	6.1. Country	C=XY Country which the EUI belongs to.		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	6.2. Organization	Title ("official" name of organization) of the certification service subscriber. o= EUI Description		Yes	UTF8 String, maximum size 128 (rfc5280)
	6.3.				
	6.4. Common Name	Name and surname as appears on identification document, preceded by the string "(MAIL)"		Yes	UTF8String (rfc5280). For instance : cn=(MAIL) JUAN ESPAÑOL
7. Authority Key Identifier		CSP public key identifier. Medium to identify the public key corresponding to the private key used by the CA to sign a certificate.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits). Matches the field Subject Key Identifier of the issuer CA.
8. Subject Public Key Info		Public Key Algorithm and Subject Public Key for the certificate subscriber. In this case RSA Encryption with	No	Yes	Field to transport the Public Key and to identify the algorithm with which the key is used. Call for Tenders,

Field			Content		Critical	Mandatory	Specifications
			2048 key lenght.				DIGIT/R2/PO/2009/035, PKI SERVICES 1.2.1. Key generation/issuing certificates *The key length shall be at least 1024 bits*
9. Subject Key Identifier			Subscriber or Key Owner public key identifier. Medium to identify certificates that contain a particular public key and eases the building of certification paths.		No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
10. Key Usage			Permitted usage of the certified keys.		Yes	Yes	Normalized in X509
	10.1. Digital Signature		1				Allows electronic signature.
	10.2. Content Commitment		0				Points out to the software that uses the certificate if it must allow the user to know the signed content.
	10.3. Key Encipherment		1				It is used for management and transport of keys to establish secure sessions.
	10.4. Data Encipherment		0				It is used to encipher details which are not cryptographic keys.
	10.5. Key Agreement		0				For use in the Key Agreement process.
	10.6. Key Certificate Signature		0				Certificate signature allowed. It is used in CA Certificates.
	10.7. CRL Signature		0				CRL signature allowed. It is used in CA Certificates.
11. Extended Key Usage			Extended or improved usage of the keys.			Yes	This extension points out one or more purposes for which the public key certificate may be used as well as or instead of the basic usages indicated in the Key Usage extension.
	11.1. Email protection		1.3.6.1.5.5.7.3.4		No	Yes	Email protection
12. Certificate Policies			Certificate policy		No	Yes	
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.4.3 0.4.0.2042.1.3			Yes	Policy identifiers of the lighweight certificate.
	12.2. Policy Qualifier Id					Yes	
		12.2.1	12.2.2 CPS Pointer	http://www.cert.fnmt.es/dpcs/		Yes	IA5String String. URL for the usage conditions.
		12.2.3	12.2.4 User Notice	Light weight certificate. Under the usage conditions asserted in the FNMT-RCM CPS (106, Jorge Juan street,28009, Madrid, Spain).		Yes	UTF8 String. maximum size 200 characters.
13. Subject Alternative Names			Identification/Description of the Administrative Identity		No	Yes	
	13.1. rfc822 Name		Suscriptor e-mail.			Yes	For instance : rfc822Name=jespanol@meh.es
	13.2. Suscriptor name		OID 1.3.6.1.4.1.5734.1.1 = Suscriptor name.			Yes	For instance OID 1.3.6.1.4.1.5734.1.1 = Juan

Field		Content	Critical	Mandatory	Specifications
	13.3. Suscriptor surname	OID 1.3.6.1.4.1.5734.1.2 = Suscriptor surname.		Yes	For instance OID 1.3.6.1.4.1.5734.1.2 = Espanol
14. CRL Distribution Point		Informs how information about the CRL associated to the certificate is obtained.	No	Yes	
	14.1. Distribution Point 1	CRL distribution point 1 http://www.cert.fnmt.es/crls_ISAca/CRL<xxx*>.crl *xxx: integer number identifier of the CRL(Partitioning CRL)		Yes	UTF8String Path where the CRL resides (distribution point 1)
	14.2. Distribution Point 2	CRL distribution point 2 ldap://ldapISAca.cert.fnmt.es/CN=CRL<xxx*>,cn=ISA%20CA,ou=European%20Commission,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: integer number identifier of the CRL(Partitioning CRL)		Yes	UTF8String. Path of LDAP service where the CRL resides. (distribution point 2)
15. Authority Info Access			No	Yes	
	15.1. Access Method 1	Identifier of the access method to the revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)		Yes	
	15.2. Acces Location 1	http://ocspISAca.cert.fnmt.es/ocspISAca/OcspResponder		Yes	
	15.3. Access Method 2	Identifier of the method of access to the information of the additional certificates needed for validation: 1.3.6.1.5.5.7.48.2 (ca cert)		Yes	Issuer of the certificates issuer entity (Root CA) 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.*"
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ISACA.crt		Yes	URL for the download of additional certificates to validate the certification path. In this case the certificate path is the certificate of FNMT-RCM used for the issuance of this type of certificates
16. Basic Constraints		This extension is used to identify whether the certification subject is a CA and the maximum depth level allowed for the certification path.			De la rf5280: " *This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	Subject Type	Final entity (valor FALSE)		Yes	Other certificates can not be issued with this certificate.

Tabla 3 – Perfil del *Certificado Normalizado*

Field		Content	Critical	Mandatory	Specifications
1. Version		2		Yes	Integer:=2 ([RFC5280] This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, version MUST be 3 (value is 2)(X509v3).
2. Serial Number		Certificate unique identifier number.		Yes	Integer. SerialNumber = ex: 111222. Automatically set by the Certification Entity. [RFC5280]. It will be a positive integer, not bigger than 20 octets (1- 2^{159}). The Serial Number will be assigned randomly.
3. Signature Algorithm		Sha256withRsaEncryption		Yes	Identifies the type of algorithm used (OID 1.2.840.113549.1.1.11)
4. Issuer Distinguish Name		Certificate issuer entity (Subordinate CA)		Yes	
	4.1. Country	C=ES		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	4.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o=FNMT-RCM		Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. common Name	CN=ISA CA		Yes	UTF8 String, maximum size 128 (rfc5280).
5. Validity		4 years		Yes	Call for Tenders, DIGIT/R2/PO/2009/035, PKI SERVICES 1.2.1. Key generation/issuing certificates *The offered certificates have to have an operational period of at least one (1) year.*
6. Subject		Identification/description of the owner of/person responsible for the certified keys.		Yes	
	6.1. Country	C=XY Country which the EUI belongs to.		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	6.2. Organization	Title ("official" name of organization) of the certification service subscriber. o= EUI Description		Yes	UTF8 String, maximum size 128 (rfc5280)
	6.3.				
	6.4. Common Name	Name and surname as appears on identification document, preceded by the string "(AUTH)"		Yes	UTF8String (rfc5280). For instance : cn=(AUTH) JUAN ESPAÑOL
7. Authority Key Identifier		CSP public key identifier. Medium to identify the public key corresponding to the private key used by the CA to sign a certificate.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits). Matches the field Subject Key Identifier of the issuer CA.
8. Subject Public Key Info		Public Key Algorithm and Subject Public Key for the certificate subscriber. In this case RSA Encryption with	No	Yes	Field to transport the Public Key and to identify the algorithm with which the key is used. Call for Tenders,

Field			Content		Critical	Mandatory	Specifications
			2048 key lenght.				DIGIT/R2/PO/2009/035, PKI SERVICES 1.2.1. Key generation/issuing certificates *The key length shall be at least 1024 bits*
9. Subject Key Identifier			Subscriber or Key Owner public key identifier. Medium to identify certificates that contain a particular public key and eases the building of certification paths.		No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
10. Key Usage			Permitted usage of the certified keys.		Yes	Yes	Normalized in X509
	10.1. Digital Signature		1				Allows electronic signature.
	10.2. Content Commitment		0				Points out to the software that uses the certificate if it must allow the user to know the signed content.
	10.3. Key Encipherment		0				It is used for management and transport of keys to establish secure sessions.
	10.4. Data Encipherment		0				It is used to encipher details which are not cryptographic keys.
	10.5. Key Agreement		0				For use in the Key Agreement process.
	10.6. Key Certificate Signature		0				Certificate signature allowed. It is used in CA Certificates.
	10.7. CRL Signature		0				CRL signature allowed. It is used in CA Certificates.
11. Extended Key Usage			Extended or improved usage of the keys.			Yes	This extension points out one or more purposes for which the public key certificate may be used as well as or instead of the basic usages indicated in the Key Usage extension.
	11.1. Client Authentication		1.3.6.1.5.5.7.3.2		No	Yes	Client Authentication
	11.2. Any Extended Key Usage		Other purposes (see comment in "Specifications" column") 2.5.29.37.0		No	Yes	*[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. Certificate Policies			Certificate policy		No	Yes	
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.4.2 0.4.0.2042.1.1			Yes	Policy identifiers of the normalized certificate.
	12.2. Policy Qualifier Id					Yes	
		12.2.1	12.2.2 CPS Pointer	http://www.cert.fnmt.es/dpcs/		Yes	IA5String String. URL for the usage conditions.
		12.2.3	12.2.4 User Notice	Normalized certificate. Under the usage conditions asserted in the FNMT-RCM CPS (106, Jorge Juan street,28009,		Yes	UTF8 String. maximum size 200 characters.

Field		Content	Critical	Mandatory	Specifications
		Madrid, Spain).			
13. Subject Alternative Names		Identification/Description of the Administrative Identity	No	Yes	
	13.1. rfc822 Name	Suscriptor e-mail.		Yes	For instance : rfc822Name=jespanol@meh.es
	13.2. Suscriptor name	OID 1.3.6.1.4.1.5734.1.1 = Suscriptor name.		Yes	For instance OID 1.3.6.1.4.1.5734.1.1 = Juan
	13.3. Suscriptor surname	OID 1.3.6.1.4.1.5734.1.2 = Suscriptor surname.		Yes	For instance OID 1.3.6.1.4.1.5734.1.2 = Espanol
14. CRL Distribution Point		Informs how information about the CRL associated to the certificate is obtained.	No	Yes	
	14.1. Distribution Point 1	CRL distribution point 1 http://www.cert.fnmt.es/crls_ISAca/CRL<xxx*>.crl *xxx: integer number identifier of the CRL(Partitioning CRL)		Yes	UTF8String Path where the CRL resides (distribution point 1)
	14.2. Distribution Point 2	CRL distribution point 2 ldap://ldapISAca.cert.fnmt.es/CN=CRL<xxx*>,cn=ISA%20CA,ou=European%20Commission,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: integer number identifier of the CRL(Partitioning CRL)		Yes	UTF8String. Path of LDAP service where the CRL resides. (distribution point 2)
15. Authority Info Access			No	Yes	
	15.1. Access Method 1	Identifier of the access method to the revocation information: : 1.3.6.1.5.5.7.48.1 (ocsp)		Yes	
	15.2. Acces Location 1	http://ocspISAca.cert.fnmt.es/ocspISAca/OcspResponder		Yes	
	15.3. Access Method 2	Identifier of the method of access to the information of the additional certificates needed for validation: 1.3.6.1.5.5.7.48.2 (ca cert)		Yes	Issuer of the certificates issuer entity (Root CA) 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.*"
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ISACA.crt		Yes	URL for the download of additional certificates to validate the certification path. In this case the certificate path is the certificate of FNMT-RCM used for the issuance of this type of certificates
16. Basic Constraints		This extension is used to identify whether the certification subject is a CA and the maximum depth level allowed for the certification path.			De la rf5280: *" This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	16.1. Subject Type	Final entity (valor FALSE)		Yes	Other certificates can not be issued with this certificate.

Tabla 4 – Perfil del *Certificado Reconocido*

Field		Content	Critical	Mandatory	Specifications
1. Version		2		Yes	Integer:=2 ([RFC5280] This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, version MUST be 3 (value is 2)(X509v3).
2. Serial Number		Certificate unique identifier number		Yes	Integer. SerialNumber = ex: 111222. Automatically set by the Certification Entity. [RFC5280]. It will be a positive integer, not bigger than 20 octets (1- 2^{159}). The Serial Number will be assigned randomly.
3. Signature Algorithm		Sha256withRsaEncryption		Yes	Identifies the type of algorithm used (OID 1.2.840.113549.1.1.11)
4. Issuer Distinguish Name		Certificate issuer entity (Subordinate CA)		Yes	
	4.1. Country	C=ES		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	4.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o= FNMT-RCM		Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. common Name	CN=ISA CA		Yes	UTF8 String, maximum size 128 (rfc5280).
5. Validity		4 years		Yes	Call for Tenders, DIGIT/R2/PO/2009/035, PKI SERVICES 1.2.1. Key generation/issuing certificates *The offered certificates have to have an operational period of at least one (1) year.*
6. Subject		Identification/description of the owner of / person responsible for the certified keys.		Yes	
	6.1. Country	C=XY Country which the EUI belongs to.		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280))
	6.2. Organization	Title ("official" name of organization) of the certification service subscriber . o=EUI Description		Yes	UTF8 String, maximum size 128 (rfc5280)
	6.3.				
	6.4. Common Name	Name and surname as appears on identification document, preceded by the string "(SIGN)"		Yes	UTF8String (rfc5280). For instance : cn=(SIGN) JUAN ESPAÑOL
7. Authority Key Identifier		CSP public key identifier. Medium to identify the public key corresponding to the private key used by the CA to sign a certificate.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits). Matches the field Subject Key Identifier of the issuer CA.
8. Subject Public Key Info		Public Key Algorithm and Subject Public Key for the certificate subscriber. In this case RSA Encryption with	No	Yes	Field to transport the Public Key and to identify the algorithm with which the key is used. Call for Tenders,

Field		Content	Critical	Mandatory	Specifications
		2048 key lenght.			DIGIT/R2/PO/2009/035, PKI SERVICES 1.2.1. Key generation/issuing certificates *The key length shall be at least 1024 bits*
9. Subject Key Identifier		Subscriber or key owner public key identifier. Medium to identify certificates that contain a particular public key, and eases the building of certification paths.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
10. Key Usage		Permitted usage of the certified keys.	Yes	Yes	Normalized in X509
	10.1. Digital Signature	0			Allows electronic signature.
	10.2. Content Commitment	1			Points out to the software that uses the certificate if it must allow the user to know the signed content.
	10.3. Key Encipherment	0			It is used for management and transport of keys to establish secure sessions.
	10.4. Data Encipherment	0			It is used to encipher details which are not cryptographic keys.
	10.5. Key Agreement	0			For use in the Key Agreement process.
	10.6. Key Certificate Signature	0			Certificate signature allowed. It is used in CA Certificates.
	10.7. CRL Signature	0			CRL signature allowed. It is used in CA Certificates.
11. Qualified Certificate Statements		Qualified extensions.	No		ETSI TS 101 862 Defines the inclusion of certain declarations for qualified certificates.
	11.1. QcCompliance	Certificate issued as a Qualified Certificate		Yes	Indicates whether the certificate is acknowledged only if it is not explicit in the indicated policies in the corresponding extension.
	11.2. QcRetentionPeriod	15 years		Yes	Number of years from certificate expiry date which registered details and other relevant information are available. In this case the law states "To conserve registered in a secure way all the information and documentation related to a qualified certificate and the CPD´s in vigor in each moment, for at least 15 years counted from the moment of its issue, so that the signatures done with it might be verified…"
	11.3. QcLimitValue	200 €		Yes	Limits of responsibility
	11.4. QcSSCD	Keys generated in a SSCD		Yes	Points out that the private key of the certificate is stored in a Secure Signature Creation Device in compliance with Annex III of the European Parliament directive 1999/91/EC regarding a communitary framework for electronic signatures. This value will only be filled when it can be assured irrefutably (technical mechanism or audited process) that the private key has been generated in a SSCD.
12. Certificate Policies		Certificate policy	No	Yes	

Field			Content		Critical	Mandatory	Specifications
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.4.1 0.4.0.1456.1.1			Yes	Policy identifiers of the qualified certificate.
	12.2. Policy Qualifier Id					Yes	
		12.2.1	12.2.2 CPS Pointer	http://www.cert.fnmt.es/dpcs/		Yes	IA5String String. URL for the usage conditions.
		12.2.3	12.2.4 User Notice	Qualified certificate. Under the usage conditions asserted in the FNMT-RCM CPS (106, Jorge Juan street,28009, Madrid, Spain).		Yes	UTF8 String. maximum size 200 characters.
13. Subject Alternative Names					No	Yes	
	13.1. rfc822 Name		Suscriptor e-mail.			Yes	For instance : rfc822Name=jespanol@meh.es
	13.2. Suscriptor name		OID 1.3.6.1.4.1.5734.1.1 = Suscriptor name.			Yes	For instance OID 1.3.6.1.4.1.5734.1.1 = Juan
	13.3. Suscriptor surname		OID 1.3.6.1.4.1.5734.1.2 = Suscriptor surname.			Yes	For instance OID 1.3.6.1.4.1.5734.1.2 = Espanol
14. CRL Distribution Point			Informs how information about the CRL associated to the certificate is obtained.		No	Yes	
	14.1. Distribution Point 1		CRL distribution point 1 http://www.cert.fnmt.es/crls_ISAca/CRL<xxx*>.crl *xxx: integer number identifier of the CRL(Partitioning CRL)			Yes	UTF8String Path where the CRL resides (distribution point 1)
	14.2. Distribution Point 2		CRL distribution point 2. ldap://ldapISAca.cert.fnmt.es/CN=CRL<xxx*>,cn=ISA%20CA,ou=European%20Commission,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: integer number identifier of the CRL(Partitioning CRL)			Yes	UTF8String. Path of LDAP service where the CRL resides. (distribution point 2)
15. Authority Info Access					No	Yes	
	15.1. Access Method 1		Identifier of the access method to the revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)			Yes	
	15.2. Acces Location 1		http://ocspISAca.cert.fnmt.es/ocspISAca/OcspResponder			Yes	
	15.3. Access Method 2		Identifier of the method of access to the information of the additional certificates needed for validation: 1.3.6.1.5.5.7.48.2 (ca cert)			Yes	Issuer of the certificates issuer entity (Root CA) 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.*"
	15.4. Access Location 2		http://www.cert.fnmt.es/certs/ISACA.crt			Yes	URL for the download of additional certificates to validate the certification path. In this case the certificate path is the certificate of FNMT-RCM used for the issuance of this type of

Field		Content	Critical	Mandatory	Specifications
					certificates
16. Basic Constraints		This extension is used to identify whether the certification subject is a CA and the maximum depth level allowed for the certification path.			De la rf5280: *" This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	16.1. Subject Type	Final entity (valor FALSE)		Yes	Other certificates can not be issued with this certificate.

Tabla 5 – Perfil del *Certificado de Servidor web* (tipo Common Name)

Field		Content	Critical	Mandatory	Specifications
1. Version		2		Yes	Integer:=2 ([RFC5280] This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, version MUST be 3 (value is 2)(X509v3).
2. Serial Number		Certificate unique identifier number.		Yes	Integer. SerialNumber = ex: 111222. Automatically set by the Certification Entity. [RFC5280]. It will be a positive integer, not bigger than 20 octets (1- 2^{159}). The Serial Number will be assigned randomly.
3. Signature Algorithm		Sha256withRsaEncryption		Yes	Identifies the type of algorithm used (OID 1.2.840.113549.1.1.11)
4. Issuer Distinguish Name		Certificate issuer entity (Subordinate CA)		Yes	
	4.1. Country	C=ES		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	4.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o=FNMT-RCM		Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. common Name	CN=ISA CA		Yes	UTF8 String, maximum size 128 (rfc5280).
5. Validity		4 years		Yes	Maximum validity limited by "Esquema de Identificación y Firma. Perfiles de Certificados"
6. Subject		Identification/description of the owner of / person responsible for the certified keys.		Yes	
	6.1. Country	C=XY Country which the EUI belongs to.		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	6.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o= EUI Description		Yes	UTF8 String, maximum size 128 (rfc5280)
	6.3.				
	6.4. Common Name	Domain on which this certificate is valid Cn=www.domain.com		Yes	UTF8String (rfc5280).
7. Authority Key Identifier		CSP public key identifier. Medium to identify the public key corresponding to the private key used by the CA to sign a certificate.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits). Matches the field Subject Key Identifier of the issuer CA.
8. Subject Public Key Info		Public key of the site, encoded accordingly the cryptographic algorithm. In this case RSA Encryption.	No	Yes	Field to transport the Public Key and to identify the algorithm with which the key is used. The length is 2048.
9. Subject Key Identifier		Subscriber or Key Owner public key identifier. Medium to identify certificates that contain a particular public key and eases the building of	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING

Field			Content		Critical	Mandatory	Specifications
			certification paths.				subjectPublicKey (excluding the tag, length, and number of unused bits).
10. Key Usage			Permitted usage of the certified keys.		Yes	Yes	Normalized in X509
	10.1. Digital Signature		1				Allows electronic signature.
	10.2. Content Commitment		0				Points out to the software that uses the certificate if it must allow the user to know the signed content.
	10.3. Key Encipherment		1				It is used for management and transport of keys to establish secure sessions.
	10.4. Data Encipherment		0				It is used to encipher details which are not cryptographic keys.
	10.5. Key Agreement		0				For use in the Key Agreement process.
	10.6. Key Certificate Signature		0				Certificate signature allowed. It is used in CA Certificates.
	10.7. CRL Signature		0				CRL signature allowed. It is used in CA Certificates.
11. Extended Key Usage			Extended or improved usage of the keys.			Yes	This extension points out one or more purposes for which the public key certificate may be used as well as or instead of the basic usages indicated in the Key Usage extension.
	11.1. Server Authentication		1.3.6.1.5.5.7.3.1		No	Yes	Server Authentication
	11.2. Email protection		1.3.6.1.5.5.7.3.4		No	Yes	Email protection
12. Certificate Policies			Certificate policy		No	Yes	
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.4.4			Yes	Certificate policy identifier for SSL/TLS Server.
	12.2. Policy Qualifier Id					Yes	
		12.2.1	12.2.2 CPS Pointer	http://www.cert.fnmt.es/dpcs/		Yes	IA5String String. URL for the usage conditions.
		12.2.3	12.2.4 User Notice	TLS Server certificate. Under the usage conditions asserted in the FNMT-RCM CPS (106, Jorge Juan street,28009, Madrid, Spain).		Yes	UTF8 String. maximum size 200 characters.
13. Subject Alternative Names			Identification/Description of the Administrative Identity		No	Yes	
	13.1. dns Name		www.domain.com			Yes	
14. CRL Distribution Point			Informs how information about the CRL associated to the certificate is obtained.		No	Yes	

Field		Content	Critical	Mandatory	Specifications
	14.1. Distribution Point 1	CRL distribution point 1 http://www.cert.fnmt.es/crls_ISAca/CRL<xxx*>.crl *xxx: integer number identifier of the CRL(Partitioning CRL)		Yes	UTF8String Path where the CRL resides (distribution point 1)
	14.2. Distribution Point 2	CRL distribution point 2 ldap://ldapISAca.cert.fnmt.es/CN=CRL<xxx*>,cn=ISA%20CA,ou=European Commission,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: integer number identifier of the CRL(Partitioning CRL)		Yes	UTF8String. Path of LDAP service where the CRL resides. (distribution point 2)
15. Authority Info Access			No	Yes	
	15.1. Access Method 1	Identifier of the access method to the revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)		Yes	
	15.2. Acces Location 1	http://ocspISAca.cert.fnmt.es/ocspISAca/OcspResponder		Yes	
	15.3. Access Method 2	Identifier of the method of access to the information of the additional certificates needed for validation: 1.3.6.1.5.5.7.48.2 (ca cert)		Yes	Issuer of the certificates issuer entity (Root CA) 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.*"
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ISACA.crt		Yes	URL for the download of additional certificates to validate the certification path. In this case the certificate path is the certificate of FNMT-RCM used for the issuance of this type of certificates
16. Basic Constraints		This extension is used to identify whether the certification subject is a CA and the maximum depth level allowed for the certification path.			De la rf5280: *" This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	Subject Type	Final entity (valor FALSE)		Yes	Other certificates can not be issued with this certificate.

Tabla 6 – Perfil del *Certificado de Servidor web* (tipo Wildcard)

Field		Content	Critical	Mandatory	Specifications
1. Version		2		Yes	Integer:=2 ([RFC5280] This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, version MUST be 3 (value is 2)(X509v3).
2. Serial Number		Certificate unique identifier number.		Yes	Integer. SerialNumber = ex: 111222. Automatically set by the Certification Entity. [RFC5280]. It will be a positive integer, not bigger than 20 octets (1- 2^{159}). The Serial Number will be assigned randomly.
3. Signature Algorithm		Sha256withRsaEncryption		Yes	Identifies the type of algorithm used (OID 1.2.840.113549.1.1.11)
4. Issuer Distinguish Name		Certificate issuer entity (Subordinate CA)		Yes	
	4.1. Country	C=ES		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	4.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o=FNMT-RCM		Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. common Name	CN=ISA CA		Yes	UTF8 String, maximum size 128 (rfc5280).
5. Validity		4 years		Yes	Call for Tenders, DIGIT/R2/PO/2009/035, PKI SERVICES 1.2.1. Key generation/issuing certificates *The offered certificates have to have an operational period of at least one (1) year.*
6. Subject		Identification/description of the owner of / person responsible for the certified keys.		Yes	
	6.1. Country	C=XY Country which the EUI belongs to.		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	6.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o= EUI Description		Yes	UTF8 String, maximum size 128 (rfc5280)
	6.3.				
	6.4. Common Name	Domain on which this certificate is valid CN=*.domain.com		Yes	UTF8String (rfc5280). For instance : CN=*.domain.com
7. Authority Key Identifier		CSP public key identifier. Medium to identify the public key corresponding to the private key used by the CA to sign a certificate.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits). Matches the field Subject Key Identifier of the issuer CA.
8. Subject Public Key Info		Public key of the site, encoded accordingly the cryptographic algorithm.	No	Yes	Field to transport the Public Key and to identify the algorithm with which the key is used.

Field			Content		Critical	Mandatory	Specifications
			In this case RSA Encryption.				The length is 2048.
9. Subject Key Identifier			Subscriber or Key Owner public key identifier. Medium to identify certificates that contain a particular public key and eases the building of certification paths.		No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
10. Key Usage			Permitted usage of the certified keys.		Yes	Yes	Normalized in X509
	10.1. Digital Signature		1				Allows electronic signature.
	10.2. Content Commitment		0				Points out to the software that uses the certificate if it must allow the user to know the signed content.
	10.3. Key Encipherment		1				It is used for management and transport of keys to establish secure sessions.
	10.4. Data Encipherment		0				It is used to encipher details which are not cryptographic keys.
	10.5. Key Agreement		0				For use in the Key Agreement process.
	10.6. Key Certificate Signature		0				Certificate signature allowed. It is used in CA Certificates.
	10.7. CRL Signature		0				CRL signature allowed. It is used in CA Certificates.
11. Extended Key Usage			Extended or improved usage of the keys.			Yes	This extension points out one or more purposes for which the public key certificate may be used as well as or instead of the basic usages indicated in the Key Usage extension.
	1.1. Server Authentication		1.3.6.1.5.5.7.3.1		No	Yes	Server authentication.
	1.2. Email protection		1.3.6.1.5.5.7.3.4		No	Yes	Email protection
12. Certificate Policies			Certificate policy		No	Yes	
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.4.4			Yes	Policy identifier of the SSL/TLS Server certificate.
	12.2. Policy Qualifier Id					Yes	
		12.2.1	12.2.2 CPS Pointer	http://www.cert.fnmt.es/dpcs/		Yes	IA5String String. URL for the usage conditions.
		12.2.3	12.2.4 User Notice	Certificate issued under wildcard policy. Under the usage conditions asserted in the FNMT-RCM CPS (106, Jorge Juan street,28009, Madrid, Spain).		Yes	UTF8 String. maximum size 200 characters.
13. Subject Alternative Names			Identification/Description of the Administrative Identity		No	Yes	
	13.1. dns Name		*.domain.com			Yes	
14. CRL Distribution Point			Informs how information about the CRL associated to the certificate is obtained.		No	Yes	
	14.1. Distribution Point 1		CRL distribution point 1 http://www.cert.fnmt.es/crls_ISAca/CRL<xxx*>.crl			Yes	UTF8String Path where the CRL resides (distribution point 1)

Field		Content	Critical	Mandatory	Specifications
		*xxx: integer number identifier of the CRL(Partitioning CRL)			
	14.2. Distribution Point 2	CRL distribution point 2 ldap://ldapISAca.cert.fnmt.es/CN=CRL<xxx*>,cn=ISA%20CA,ou=European Commission,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: integer number identifier of the CRL(Partitioning CRL)		Yes	UTF8String. Path of LDAP service where the CRL resides. (distribution point 2)
15. Authority Info Access			No	Yes	
	15.1. Access Method 1	Identifier of the access method to the revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)		Yes	
	15.2. Acces Location 1	http://ocspISAca.cert.fnmt.es/ocspISAca/OcspResponder		Yes	
	15.3. Access Method 2	Identifier of the method of access to the information of the additional certificates needed for validation: 1.3.6.1.5.5.7.48.2 (ca cert)		Yes	Issuer of the certificates issuer entity (Root CA) 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.*"
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ISACA.crt		Yes	URL for the download of additional certificates to validate the certification path. In this case the certificate path is the certificate of FNMT-RCM used for the issuance of this type of certificates
16. Basic Constraints		This extension is used to identify whether the certification subject is a CA and the maximum depth level allowed for the certification path.	Yes		De la rf5280: *" This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	Subject Type	Final entity (valor FALSE)		Yes	Other certificates can not be issued with this certificate.

Tabla 7 – Perfil del *Certificado de Actuación Automatizada* (tipo *Reconocido sin DSCF para firma de documentos*)

Field		Content	Critical	Mandatory	Specifications
1. Version		2		Yes	Integer:=2 ([RFC5280] This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, version MUST be 3 (value is 2)(X509v3).
2. Serial Number		Certificate unique identifier number		Yes	Integer. SerialNumber = ex: 111222. Automatically set by the Certification Entity. [RFC5280]. It will be a positive integer, not bigger than 20 octets (1- 2^{159}). The Serial Number will be assigned randomly.
3. Signature Algorithm		Sha256withRsaEncryption		Yes	Identifies the type of algorithm used (OID 1.2.840.113549.1.1.11)
4. Issuer Distinguish Name		Certificate issuer entity (Subordinate CA)		Yes	
	4.1. Country	C=ES		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	4.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o= FNMT-RCM		Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. common Name	CN=ISA CA		Yes	UTF8 String, maximum size 128 (rfc5280).
5. Validity		1 year		Yes	
6. Subject		Identification of an EU Institution, Agency or Body or Member State Administrations responsible for the certified keys.		Yes	
	6.1. Country	C=XY Country which the Entity belongs to.		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280))
	6.2. Organization	Title ("official" name of organization) of the certification service subscriber.		Yes	UTF8 String, maximum size 128 (rfc5280) For instance: o= EUROPEAN COMMISSION
	6.3. Common Name	Common Name as defined in the request form.		Yes	UTF8String (rfc5280). Note: The common name may be used for the EUI, MS institution and/or IT System identification.
7. Authority Key Identifier		CSP public key identifier. Medium to identify the public key corresponding to the private key used by the CA to sign a certificate.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits). Matches the field Subject Key Identifier of the issuer CA.
8. Subject Public Key Info		Public Key Algorithm and Subject Public Key for the certificate subscriber. In this case RSA Encryption with 2048 key lenght.	No	Yes	Field to transport the Public Key and to identify the algorithm with which the key is used. Call for Tenders, DIGIT/R2/PO/2009/035, PKI SERVICES 1.2.1. Key generation/issuing certificates *The key length shall be at least 1024 bits*

Field			Content		Critical	Mandatory	Specifications
9. Subject Key Identifier			Subscriber or key owner public key identifier. Medium to identify certificates that contain a particular public key, and eases the building of certification paths.		No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
10. Key Usage			Permitted usage of the certified keys.		Yes	Yes	Normalized in X509
	10.1. Digital Signature		0				Allows electronic signature.
	10.2. Content Commitment		1				Points out to the software that uses the certificate if it must allow the user to know the signed content.
	10.3. Key Encipherment		0				It is used for management and transport of keys to establish secure sessions.
	10.4. Data Encipherment		0				It is used to encipher details which are not cryptographic keys.
	10.5. Key Agreement		0				For use in the Key Agreement process.
	10.6. Key Certificate Signature		0				Certificate signature allowed. It is used in CA Certificates.
	10.7. CRL Signature		0				CRL signature allowed. It is used in CA Certificates.
11. Extended Key Usage			Extended or improved usage of the keys.			No	This extension points out one or more purposes for which the public key certificate may be used as well as or instead of the basic usages indicated in the Key Usage extension.
12. Qualified Certificate Statements			Qualified extensions.		No		ETSI TS 101 862 Defines the inclusion of certain declarations for qualified certificates.
	12.1. QcCompliance		Certificate issued as a Qualified Certificate			Yes	Indicates whether the certificate is acknowledged only if it is not explicit in the indicated policies in the corresponding extension.
	12.2. QcRetentionPeriod		15 years			Yes	Number of years from certificate expiry date which registered details and other relevant information are available. In this case the law states "To conserve registered in a secure way all the information and documentation related to a qualified certificate and the CPD´s in vigor in each moment, for at least 15 years counted from the moment of its issue, so that the signatures done with it might be verified…"
13. Certificate Policies			Certificate policy		No	Yes	
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.4.7 0.4.0.1456.1.2			Yes	Policy identifiers of the qualified certificate. TS 101 456, clause 5.2, OID claiming conformance to the certificate policy for qualified certificates issued to the public
	13.2. Policy Qualifier Id					Yes	
		13.2.1	13.2.2 CPS Pointer	http://www.cert.fnmt.es/dpcs/		Yes	IA5String String. URL for the usage conditions.

Field			Content		Critical	Mandatory	Specifications
		13.2.3	13.2.4 User Notice	Qualified certificate. Under the usage conditions asserted in the FNMT-RCM CPS (106, Jorge Juan street,28009, Madrid, Spain).		Yes	UTF8 String. maximum size 200 characters.
14. CRL Distribution Point			Informs how information about the CRL associated to the certificate is obtained.		No	Yes	
	14.1. Distribution Point 1		CRL distribution point 1 http://www.cert.fnmt.es/crls_ISAca/CRL<xxx*>.crl *xxx: integer number identifier of the CRL(Partitioning CRL)			Yes	UTF8String Path where the CRL resides (distribution point 1)
	14.2. Distribution Point 2		CRL distribution point 2. ldap://ldapISAca.cert.fnmt.es/CN=CRL<xxx*>,cn=ISA %20CA, o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: integer number identifier of the CRL(Partitioning CRL)			Yes	UTF8String. Path of LDAP service where the CRL resides. (distribution point 2)
15. Authority Info Access					No	Yes	
	15.1. Access Method 1		Identifier of the access method to the revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)			Yes	
	15.2. Acces Location 1		http://ocspISAca.cert.fnmt.es/ocspISAca/OcspResponder			Yes	
	15.3. Access Method 2		Identifier of the method of access to the information of the additional certificates needed for validation: 1.3.6.1.5.5.7.48.2 (ca cert)			Yes	Issuer of the certificates issuer entity (Root CA) 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.*"
	15.4. Access Location 2		http://www.cert.fnmt.es/certs/ISACA.crt			Yes	URL for the download of additional certificates to validate the certification path. In this case the certificate path is the root certificate of FNMT-RCM
16. Basic Constraints			This extension is used to identify whether the certification subject is a CA and the maximum depth level allowed for the certification path.				De la rf5280: *" This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	16.1. Subject Type		Final entity (valor FALSE)		Yes	Yes	Other certificates can not be issued with this certificate.

Tabla 8 – Perfil del *Certificado de Actuación Automatizada* (tipo *Normalizado para firma o cifrado de documentos)*

Field		Content	Critical	Mandatory	Specifications
1. Version		2		Yes	Integer:=2 ([RFC5280] This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, version MUST be 3 (value is 2)(X509v3).
2. Serial Number		Certificate unique identifier number		Yes	Integer. SerialNumber = ex: 111222. Automatically set by the Certification Entity. [RFC5280]. It will be a positive integer, not bigger than 20 octets (1- 2^{159}). The Serial Number will be assigned randomly.
3. Signature Algorithm		Sha256withRsaEncryption		Yes	Identifies the type of algorithm used (OID 1.2.840.113549.1.1.11)
4. Issuer Distinguish Name		Certificate issuer entity (Subordinate CA)		Yes	
	4.1. Country	C=ES		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	4.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o= FNMT-RCM		Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. common Name	CN=ISA CA		Yes	UTF8 String, maximum size 128 (rfc5280).
5. Validity		1 year		Yes	
6. Subject		Identification of an EUIs, MS institution or IT System		Yes	
	6.1. Country	C=XY Country which the Entity belongs to.		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280))
	6.2. Organization	Title ("official" name of organization) of the certification service subscriber.		Yes	UTF8 String, maximum size 128 (rfc5280) For instance: o= EUROPEAN COMMISSION
	6.3. Common Name	Common Name as defined in the request form.		Yes	UTF8String (rfc5280). Note: The common name may be used for the EUI, MS institution and/or IT System identification.
7. Authority Key Identifier		CSP public key identifier. Medium to identify the public key corresponding to the private key used by the CA to sign a certificate.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits). Matches the field Subject Key Identifier of the issuer CA.
8. Subject Public Key Info		Public Key Algorithm and Subject Public Key for the certificate subscriber. In this case RSA Encryption with 2048 key lenght.	No	Yes	Field to transport the Public Key and to identify the algorithm with which the key is used. Call for Tenders, DIGIT/R2/PO/2009/035, PKI SERVICES 1.2.1. Key generation/issuing certificates *The key length shall be at least 1024 bits*

Field			Content		Critical	Mandatory	Specifications
9. Subject Key Identifier			Subscriber or key owner public key identifier. Medium to identify certificates that contain a particular public key, and eases the building of certification paths.		No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
10. Key Usage			Permitted usage of the certified keys.		Yes	Yes	Normalized in X509
	10.1. Digital Signature		(?)				Allows electronic signature.
	10.2. Content Commitment		(?)				Points out to the software that uses the certificate if it must allow the user to know the signed content.
	10.3. Key Encipherment		(?)				It is used for management and transport of keys to establish secure sessions.
	10.4. Data Encipherment		(?)				It is used to encipher details which are not cryptographic keys.
	10.5. Key Agreement		(?)				For use in the Key Agreement process.
	10.6. Key Certificate Signature		0				Certificate signature allowed. It is used in CA Certificates.
	10.7. CRL Signature		0				CRL signature allowed. It is used in CA Certificates.
11. Extended Key Usage			Extended or improved usage of the keys.			No	This extension points out one or more purposes for which the public key certificate may be used as well as or instead of the basic usages indicated in the Key Usage extension.
(!)	16.1. AnyExtendedKeyUsage		1.3.6.1.5.5.7.3.0		No	(?)	AnyExtendedKeyUsage
(!)	16.2. Client Authentication		1.3.6.1.5.5.7.3.2		No	(?)	Client Authentication
(!)	16.3. Email protection		1.3.6.1.5.5.7.3.4		No	(?)	Email protection
12. Certificate Policies			Certificate policy		No	Yes	
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.4.8 0.4.0.2042.1.1			Yes	Policy identifiers of the normalized certificate. ETSI 102 042, clause 5.2, OID claiming conformance to the certificate policy for normalized certificates issued to the public
	12.2. Policy Qualifier Id					Yes	
		12.2.1	12.2.2 CPS Pointer	http://www.cert.fnmt.es/dpcs/		Yes	IA5String String. URL for the usage conditions.
		12.2.3	12.2.4 User Notice	Normalized certificate. Under the usage conditions asserted in the FNMT-RCM CPS (106, Jorge Juan street,28009, Madrid, Spain).		Yes	UTF8 String. maximum size 200 characters.
13. CRL Distribution Point			Informs how information about the CRL associated to the certificate is obtained.		No	Yes	
	13.1. Distribution Point 1		CRL distribution point 1 http://www.cert.fnmt.es/crls_ISAca/CRL<xxx*>.crl *xxx: integer number identifier of			Yes	UTF8String Path where the CRL resides (distribution point 1)

Field		Content	Critical	Mandatory	Specifications
		the CRL(Partitioning CRL)			
	13.2. Distribution Point 2	CRL distribution point 2. ldap://ldapISAca.cert.fnmt.es/CN=CRL<xxx*>,cn=ISA %20CA, o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: integer number identifier of the CRL(Partitioning CRL)		Yes	UTF8String. Path of LDAP service where the CRL resides. (distribution point 2)
14. Authority Info Access			No	Yes	
	14.1. Access Method 1	Identifier of the access method to the revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)		Yes	
	14.2. Acces Location 1	http://ocspISAca.cert.fnmt.es/ocspISAca/OcspResponder		Yes	
	14.3. Access Method 2	Identifier of the method of access to the information of the additional certificates needed for validation: 1.3.6.1.5.5.7.48.2 (ca cert)		Yes	Issuer of the certificates issuer entity (Root CA) 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.*"
	14.4. Access Location 2	http://www.cert.fnmt.es/certs/ISACA.crt		Yes	URL for the download of additional certificates to validate the certification path. In this case the certificate path is the root certificate of FNMT-RCM
15. Basic Constraints		This extension is used to identify whether the certification subject is a CA and the maximum depth level allowed for the certification path.			De la rf5280: " *This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	15.1. Subject Type	Final entity (valor FALSE)	Yes	Yes	Other certificates can not be issued with this certificate.

(?) Key Usage to be defined 0/1 by the Commission to cover the needs of the most users.
(!) Extended Keyusage to be included or not.