FABRICA NACIONAL DE MONEDA Y TIMBRE

REAL CASA DE LA MONEDA

(FNMT-RCM)

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

15 de Noviembre de 2004

INDICE

1 DEFINICIONES

Para informarse sobre los conceptos básicos relacionados con la Criptografía, los Prestadores de Servicios de Certificación y las Infraestructuras de Clave Pública, puede hacerlo a través de la dirección http://www.ceres.fnmt.es/ceres.htm.

No obstante, a los efectos de lo dispuesto en el presente documento y su addenda, y únicamente cuando los términos comiencen con letra mayúscula y estén en cursiva, se entenderá por:

- *Agentes de Fechado*: Prestador del servicio de Fechado electrónico.
- *Agentes de OCSP:* Prestador del servicio de OCSP.
- *APD:* "Agencia de Protección de Datos". Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Su finalidad principal es velar por el cumplimiento de la legislación sobre protección de datos personales y controlar su aplicación.
- *BOE:* (o Diario Oficial "BOE") Diario Oficial impreso y distribuido por el Boletín Oficial del Estado; Organismo público, adscrito al Ministerio de la Presidencia, encargado además, de imprimir y distribuir el Boletín Oficial del Registro Mercantil, de publicar repertorios, compilaciones de textos jurídicos, y de la ejecución de los trabajos de imprenta de carácter oficial solicitados por Ministerios, organismos y otras entidades públicas.
- *C:* En el ámbito del presente documento, es una abreviatura del vocablo inglés "Country" cuyo significado en español es "País". El "País" es un atributo que forma parte del Nombre Distintivo (*DN*) de un objeto dentro de la estructura de directorio *X.500* utilizado para nombrar la entrada correspondiente al objeto.
- *Cadena de certificación*: Una lista ordenada de *Certificados* que contiene al menos un *Certificado* y el *Certificado raíz* de la FNMT-RCM, sirviendo los *Datos de verificación de Firma* contenidos en éste último para posibilitar la autenticación del *Certificado*.
- *Certificado*: Por defecto deberá entenderse toda certificación electrónica para la que el *Solicitante* haya acreditado necesariamente la identidad del *Suscriptor*, que vincula a este unos *Datos de verificación de Firma* y confirma por lo menos su identidad.

  Todos los *Certificados*, con la excepción de los *Certificados de Persona jurídica emitidos para el ámbito tributario* y de los *Certificados de Entidades sin personalidad jurídica para el ámbito tributario*, que la FNMT-RCM emita para ser utilizados en la *Comunidad Electrónica* cuya actividad esté relacionada con servicios técnicos y administrativos de seguridad de las comunicaciones *EIT*, se emitirán mediante los procedimientos y con las garantías que le otorguen la cualidad de *reconocidos* según la legislación vigente. Asimismo, todos los *Certificados*, para ser tales, deberán contener la *Firma electrónica reconocida* de los mismos, generada por la FNMT-RCM con sus *Datos de creación de Firma* en su calidad de *Prestador de Servicios de Certificación*.

  - **Quedan excluidos del concepto de *Certificado* de esta *Declaración de Prácticas de Certificación*:**, los denominados "certificados de componentes" por no adecuarse al concepto legal de "certificado electrónico" definido por la Ley de firma electrónica 59/2003, de 19 de diciembre. No obstante, son productos de gran

utilidad que forman parte del Catálogo de Servicios y Productos de la FNMT-RCM.

- La FNMT-RCM expide los "certificados de componentes" bajo la "*Política de Certificación de certificados de componentes*" de la FNMT-RCM identificada por el OID: 1.3.6.1.4.1.5734.3.6.

  A efectos meramente informativos, recogemos los principales tipos de "certificado de componentes" que se pueden encontrar en el mencionado catálogo:

  - *Certificado de servidor [también denominado certificado de la FNMT-RCM Clase 2 CA para Servidores Web]:* Es aquel certificado que permite identificar a un servidor *web* o una URL.
  - *Certificado de firma de código [también denominado certificado de la FNMT-RCM Clase 2 CA para firma de código]:* Es aquel certificado que permite firmar código ejecutable como *applets de Java*.
  - *Certificados de Cliente de Servicios Avanzados*: Son *Certificados* emitidos y firmados por la FNMT-RCM para ser utilizados por los miembros de la Comunidad electrónica en *Servicios de Fechado Digital* y de *OCSP* o cualquier otro servicio avanzado que la FNMT-RCM pudiera poner a disposición de la *Comunidad Electrónica,* con el objeto de que se herede la confianza que representa la FNMT-RCM como *Prestador de Servicios de Certificación*.
  - *Certificado de otros componentes informáticos:* Certificado distinto de los anteriores, utilizado para identificar unas aplicaciones frente a otras, y establecer sesiones seguras.

  Se deberá entender así mismo por *Responsable del componente*, la persona responsable del sistema o dispositivo para el cual se solicita un *Certificado de componente*, que tiene capacidad suficiente para solicitar dicho *Certificado*.

- *Certificado de identidad de persona física [(también conocido como certificado de usuario de la FNMT-RCM (Clase 2)]*: La certificación electrónica expedida por la FNMT-RCM que vincula a su *Suscriptor* unos *Datos de verificación de Firma,* y confirma su identidad. La FNMT-RCM expide *Certificados de Identidad de persona física* bajo la *Política de Certificación de Certificados Reconocidos de la FNMT-RCM* identificada por el OID: 1.3.6.1.4.1.5734.3.5.
- *Certificado de Entidad sin personalidad jurídica para el ámbito tributario:* es la certificación electrónica expedida por la FNMT-RCM que vincula a su *Titular* o *Suscriptor* (siempre *Entidad sin personalidad jurídica a las que se refiere el articulo 35.4 de la Ley General Tributaria*) unos *Datos de verificación de Firma* y confirma su identidad a los solos efectos de su empleo en el ámbito tributario. Estos certificados se expiden según los términos expuestos en la ORDEN EHA/3256/2004, de 30 de septiembre, publicada en el B.O.E Nº 246 de 12 de octubre. La FNMT-RCM expide *Certificados de Entidad sin personalidad jurídica para el ámbito tributario* bajo la *Política de Certificación de Certificados de Clave Pública de la FNMT-RCM* identificada por el OID: 1.3.6.1.4.1.5734.3.7
- *Certificado de Persona jurídica para el ámbito tributario:* es la certificación electrónica expedida por la FNMT-RCM que vincula a su *Suscriptor* (siempre *Sujeto pasivo tributario*) unos *Datos de verificación de Firma* y confirma su identidad. Este certificado se corresponde con el certificado tradicional utilizado por el Ministerio de Hacienda o el

Gobierno de Navarra para el ámbito tributario. La FNMT-RCM expide *Certificados de Persona Jurídica para el ámbito tributario* bajo la *Política de Certificación de Certificados de Clave Pública de la FNMT-RCM* identificada por el OID: 1.3.6.1.4.1.5734.3.7

- *Certificado raíz* (de la FNMT-RCM): Certificado cuyo *Suscriptor* es la FNMT-RCM como *Prestador de Servicios de Certificación* y que contiene los *Datos de verificación de Firma* de la FNMT-RCM firmados con los *Datos de creación de Firma* de la FNMT-RCM como *Prestador de Servicios de Certificación*.
- *Certificado reconocido*: Certificado expedido por un *Prestador de Servicios de Certificación*, cumpliendo los requisitos establecidos respecto de la cualidad de *reconocido* por la normativa española específica sobre firma electrónica, o que adquiere esta cualidad de *reconocido* por disposición legal expresa. A día de hoy no tienen la consideración de *Certificados Reconocidos* los *Certificados de Persona jurídica para ámbito tributario*, los *Certificados de Entidades sin Personalidad Jurídica*, ni los certificados de componentes. La FNMT-RCM expide *Certificados Reconocidos* bajo la *Política de Certificación de Certificados Reconocidos de la FNMT-RCM* identificada por el OID: 1.3.6.1.4.1.5734.3.5.
- *Cifrado asimétrico*: Trascripción en símbolos, de acuerdo con una *Clave* de cifrado, de un mensaje cuyo contenido se quiere ocultar conforme a un algoritmo tal que, el conocimiento de la *Clave* de cifrado no es suficiente para descifrar la trascripción, siendo necesario el conocimiento de la correspondiente *Clave* de descifrado. El conocimiento de la *Clave* de cifrado no implica el conocimiento de la *Clave* de descifrado, ni viceversa.
- *Clave*: Secuencia de símbolos que controlan las operaciones de cifrado y descifrado.
- *Clave Privada*: Del par de *Claves* criptográficas correspondientes a un *Cifrado asimétrico*, aquella destinada a permanecer en secreto. Las *Claves Privadas* pueden constituir, en función de su generación y utilización, *Datos de creación de Firma*.
- *Clave Pública*: Del par de *Claves* criptográficas correspondientes a un *Cifrado asimétrico*, aquella destinada a ser divulgada. Las *Claves Públicas* pueden constituir, en función de su generación y utilización, *Datos de verificación de Firma*.
- *Cliente OCSP*: Herramienta necesaria para que las *Entidades usuarias* de Derecho Privado, puedan hacer peticiones *OCSP*. La FNMT-RCM facilitará una relación de productos de libre distribución, pero no suministrará *Cliente OCSP* dada su amplia disponibilidad en el Mercado.
- *CN:* Contracción de los vocablos ingleses “Common Name” cuyo significado en español es “Nombre Común”. El “Nombre Común” es un atributo que forma parte del Nombre Distintivo (*DN*) de un objeto dentro de la estructura de directorio *X.500* utilizado para nombrar la entrada correspondiente al objeto.
- *Comunidad Electrónica*: Conjunto de *Entidades usuarias* que se relacionan con *Certificados* entre sí, bajo el marco general de la presente *Declaración de Prácticas de Certificación*, y particular de los correspondientes convenios y/o contratos que hayan suscrito, directamente o a través de representantes, con la FNMT-RCM.
- *Confidencialidad*: Cualidad que supone que la información no está disponible o no ha sido revelada a personas, entidades o procesos no autorizados.
- *CPD*: Centro de Proceso de Datos.
- *Criptografía*: Disciplina que abarca los principios, significados y métodos para la transformación de datos para, de esta manera, ocultar el contenido-información, impidiendo su modificación no detectada y/o prevenir su uso no autorizado.

- *Datos de creación de Firma*: Son los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear firmas electrónicas. A efectos prácticos de esta *Declaración de Prácticas de Certificación* siempre coincidirá, desde un punto de vista técnico, con una *Clave* criptográfica asimétrica *Privada*.
- *Datos de verificación de Firma*: Son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar firmas electrónicas. A efectos prácticos de esta *Declaración de Prácticas de Certificación* siempre coincidirán, desde un punto de vista técnico, con una *Clave* criptográfica asimétrica *Pública.*
- *Declaración de Prácticas de Certificación*: Declaración puesta a disposición del público por vía electrónica y de forma gratuita, que la FNMT-RCM realiza en calidad de *Prestador de Servicios de Certificación* y en cumplimiento de lo dispuesto por la Ley, detallando: las obligaciones que se compromete a cumplir en relación con la gestión de los *Datos de creación y verificación de Firma* y de los *Certificados*; las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los *Certificados* y, en su caso, la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los *Certificados* y que deban figurar preceptivamente inscritos en dichos registros. Además en el presente documento se recogen: los detalles del régimen de responsabilidad aplicable a la FNMT-RCM como *Prestador de Servicios de Certificación*, a las *Oficinas de Registro*, a los *Solicitantes*, a los *Suscriptores*, y a las *Entidades usuarias*, los controles de seguridad aplicados a sus procedimientos e instalaciones en aquello que pueda ser publicado sin perjudicar la eficacia de los mismos y las normas de secreto y confidencialidad; así como condiciones relativas a la propiedad de bienes y activos, a la protección de datos de carácter personal, y demás cuestiones de tipo informativo que la FNMT-RCM considere interesante poner a disposición del público.
- *Dirección electrónica*: Dirección de buzón web de uso restringido bajo las condiciones establecidas para los *Servicios de Dirección electrónica* y *de Notificación* en los apartados "9.1 *Servicio de Dirección Electrónica*" y "9.2 *Servicio de Notificación* de la FNMT-RCM", que la FNMT-RCM automáticamente asigna a todo miembro de la *Comunidad Electrónica*, para constituir, por lo menos, el canal de notificación principal con la FNMT-RCM.
- *Directorio*: Repositorio de información que sigue el estándar X.500 del ITU-T.
- *Disponibilidad*: Cualidad de los datos o de la información, que implica su condición de disponible, esto es; la posibilidad de disponer de ella o la posibilidad de utilizarla o usarla.
- *Dispositivo seguro de creación de Firma*: Elemento que sirve para aplicar los *Datos de creación de Firma*, que cumple con los requisitos establecidos en las normas específicas de aplicación en España, así como las recogidas en el Anexo III de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco común para la Firma electrónica.
- *DN*: Contracción de los vocablos ingleses "Distinguished Name" cuyo significado en español es "Nombre Distintivo". El "Nombre Distintivo" es la identificación univoca de una entrada dentro de la estructura de directorio *X.500*. El DN está compuesto por el nombre común (*CN*) de la entrada más una serie de atributos que identifican la ruta seguida dentro de la estructura del directorio *X.500* para llegar a dicha entrada.
- *Documento Electrónico*: Conjunto de registros lógicos almacenado en soporte susceptible de ser leído por equipos electrónicos de procesamiento de datos, que contiene información que ilustra sobre algún hecho.

- *Documento de Seguridad LOPD*: Documento cuyo objetivo es establecer las medidas de seguridad a implantar por la FNMT-RCM en el entorno del *Prestador de Servicios de Certificación*, para la protección de los datos de carácter personal contenidos en el Fichero de Usuarios de Sistemas Electrónicos, Informáticos y Telemáticos (EIT), que fue registrado en la *APD* el día 6 de agosto de 1999.
    - Conceptos relacionados:
        - *Administrador de la Aplicación*: Personal encargado de implementar las políticas definidas por el *Responsable del Fichero* en la aplicación que contiene el Fichero de Usuarios de Sistemas EIT. Tendrá los accesos necesarios para conceder, alterar o anular el acceso autorizado sobre los datos o recursos, previa autorización de los mismos por el *Responsable de Seguridad*. Se encargará de comunicar las incidencias de seguridad que ocurran al *Responsable de Seguridad*.
        - *Auditor de Seguridad*: Personal encargado de revisar y evaluar los controles propuestos en este documento o cualquier otro referenciado. Elabora informes con el grado de cumplimiento y las discrepancias encontradas.
        - *Cesión* (de datos): toda obtención de datos resultante de la consulta de un fichero, la publicación de toda o parte de la información contenida en un fichero, su interconexión con otros ficheros, y toda comunicación de datos realizada por una persona distinta del afectado.
        - *Consentimiento* (del interesado): toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
        - *Encargado del Tratamiento*: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento.
        - *Personal de Seguridad Informática*: Personal encargado de coordinar y controlar las medidas definidas en este manual de seguridad en cuanto a *LOPD*. También se encarga tanto de mantener y revisar las incidencias que ocurran y realizar los informes sobre estas incidencias para remitirlos al *Responsable del Fichero*, a través del *Responsable de Seguridad*. Además por instrucción del *Responsable del Fichero*, facilitan las autorizaciones para que se lleven a cabo las solicitudes de altas, modificaciones o bajas de accesos a la aplicación donde están los datos del Fichero de Usuarios de Sistemas EIT y en caso de no estar de acuerdo con la solicitud la contrasta con el *Responsable de Seguridad* y el *Responsable del Fichero*.
        - *Operador de backup*: Personal responsable de la realización de las copias de seguridad y su posterior etiquetado y almacenamiento de forma segura, que depende del Área de Explotación, del *Prestador de Servicios de Certificación* de la FNMT-RCM.
        - *Responsable del Fichero (o del Tratamiento)*: Persona que decide sobre la finalidad, contenido y uso del tratamiento. Es el encargado de autorizar los accesos necesarios y definir la política que crea conveniente para la seguridad de los datos. También se encarga de revisar los informes periódicos de incidencias. Todo ello sin perjuicio de la consideración de la FNMT-RCM como responsable del fichero a los efectos de lo dispuesto en

la normativa vigente en materia de protección de datos de carácter personal.

- *Responsable de Seguridad*: Encargado de coordinar y controlar las medidas que impone el *Documento de seguridad LOPD* en cuanto al Fichero de Usuarios EIT según *LOPD*. Dicha función recae en el Director de Sistemas de Información de la FNMT-RCM.
- *Usuarios de la Aplicación*: Personal que requiere los datos del Fichero de Usuarios de Sistemas EIT para desarrollar sus funciones. Los tipos de acceso serán diferentes en relación con el trabajo que se lleva a cabo. Los usuarios son empleados del *Prestador de Servicios de Certificación* de la FNMT-RCM y tienen acceso a la información dependiendo del nivel de autorización otorgado por el *Responsable del Fichero*.

- *EIT*: Técnicas y medios electrónicos, informáticos y telemáticos.
- *Entidad usuaria*: Aquella entidad pública o privada que ha firmado un contrato o convenio con la FNMT-RCM para actuar en la *Comunidad Electrónica*.
- *Fechado electrónico:* Consignación de la fecha y hora en un documento electrónico mediante procedimientos criptográficos indelebles, basándose en las especificaciones *Request For Comments*: 3161 – "*Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"*, que logra fechar el documento de forma objetiva. También se refiere como sellado de tiempo.
- *Firma electrónica reconocida*: Es aquella *Firma electrónica avanzada* basada en un *Certificado reconocido* y generada mediante un *Dispositivo seguro de creación de Firma*.
  - *Firma electrónica avanzada*: Es aquella *Firma electrónica* que permite establecer la identidad personal del *Suscriptor* respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al *Suscriptor*, como a los datos a que se refiere, y por haber sido creada por medios que éste puede mantener bajo su exclusivo control.
  - *Firma electrónica*: Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación personal.
- *Función hash*: Una *Función hash* es una operación que se realiza sobre un conjunto de datos de cualquier tamaño de tal forma que se obtiene como resultado otro conjunto de datos, en ocasiones denominado "resumen" o "Hash" de los datos originales, de tamaño fijo e independiente del tamaño original que, además, tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es prácticamente imposible encontrar dos mensajes distintos que tengan un resumen *Hash* idéntico.
- *Hash*: Resultado de tamaño fijo que se obtiene tras aplicar una *Función hash* a un mensaje, con independencia del tamaño de este, y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.
- *Hashing*: Aplicación de una *Función hash* a un conjunto de datos.
- *Hoster informático*: Prestador de servicios informáticos de alojamiento de aplicaciones y/o de datos de terceros, que permite la conectividad del destinatario del servicio con los mismos y el acceso a ellos por los usuarios.

- *Infraestructura de Claves Públicas* (PKI, *public key infrastucture*): Infraestructura capaz de soportar la gestión de *Claves Públicas* para los servicios de autenticación, cifrado, integridad, y no repudio.
- *Integridad*: Cualidad que implica que el conjunto de datos que configura el mensaje no carece de ninguna de sus partes. Desde el punto de vista de la información que esos datos pudieran implicar, supone una inalterabilidad tanto de contenido como estructural.
- *Listas de Revocación (CRL; Certificate Revocation List)*: Lista de acceso restringido donde figuran exclusivamente las relaciones de *Certificados* revocados o suspendidos (no así, por ejemplo, los caducados).
- *LOPD:* Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, que tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar.
- *MD5:* Message Digest (algoritmo de resumen de mensajes) en su versión 5. Desarrollado por el R. Rivest en 1991 y publicada su descripción en la RFC 1321. El algoritmo consiste en tomar mensajes de longitud arbitraria y generar un resumen de 128 bits de longitud. La probabilidad de encontrar dos mensajes distintos que produzcan un mismo resumen es prácticamente nula. Por este motivo se usa para dotar de *Integridad* los documentos durante el proceso de firma electrónica.
- *Malware (Malicious software o Software malicioso):* Véase *Software malicioso*.
- *Manual del Sistema de Gestión de la Seguridad de la Información de la FNMT-RCM como Prestador de Servicios de Certificación*: También referido como *Manual de Seguridad de CERES o Manual de Seguridad*. Este manual contempla la gestión del Sistema de Gestión de la Seguridad de la Información del Departamento CERES de la FNMT-RCM al amparo de la norma *ISO 17799: Código de buenas prácticas para la Gestión de la Seguridad de la Información*, encontrándose la FNMT-RCM en proceso de adecuación e implantación para su certificación.
- *Navegador (navegador Web, browser)*: Programa que permite visualizar los contenidos de las *páginas Web* en Internet. También se conoce con el nombre de *browser*. Algunos ejemplos de *navegadores Web* o *browsers* son: Internet Explorer y Netscape Navigator.
- *Número de serie de Certificado*: Valor entero, único dentro de la FNMT-RCM, que está asociado inequívocamente con un *Certificado* expedido por ella. En presencia de dos certificados distintos pero asociados a la misma identidad, y sin confirmación de revocación para ninguno, permite identificar el más reciente gracias al número de serie y revocar de oficio el anterior.
- *OCSP (Online Certificate Status Protocol):* Protocolo informático que permite comprobar de forma rápida y sencilla la vigencia de un certificado electrónico. La FNMT-RCM pondrá este servicio a disposición de las *Entidades usuarias*, bajo las condiciones que estipule el convenio o contrato por el que se rija su *Comunidad Electrónica*.
- *Oficinas de Registro*: Oficinas instaladas por la FNMT-RCM, o por otra Entidad siempre que medie convenio con la FNMT-RCM suscrito por dicha entidad o por su superior jerárquico administrativo, que se constituye a fin de facilitar a los ciudadanos la presentación de solicitudes relativas a los *Certificados*, la confirmación de su identidad y la entrega de los correspondientes títulos acreditativos de las cualidades personales exigidas para el tipo de *Certificado* que se solicite.

- *OID (Object Identifier)*: Valor, de naturaleza jerárquica y comprensivo de una secuencia de componentes variables aunque siempre constituidos por enteros no negativos separados por un punto, que pueden ser asignados a objetos registrados y que tienen la propiedad de ser únicos entre el resto de *OID*.
- *Operación Manual a Explotación*: Secuencia de operaciones que encontrándose documentadas, son realizadas de forma manual por un operador de la FNMT-RCM.
- *OU*: Contracción de los vocablos ingleses "Organizational Unit" cuyo significado en español es "Unidad Organizativa". La unidad organizativa es un atributo que forma parte del Nombre Distintivo de un objeto dentro de la estructura de directorio *X.500*.
- *O:* En el ámbito del presente documento, es una abreviatura del vocablo inglés "Organization" cuyo significado en español es "Organización". La "Organización" es un atributo que forma parte del Nombre Distintivo (*DN*) de un objeto dentro de la estructura de directorio *X.500* utilizado para nombrar la entrada correspondiente al objeto.
- *PC/SC:* Contracción de los vocablos ingleses "Personal Computer/Smart Card" cuyo significado en español es "Computadores Personales/Tarjetas Inteligentes". Es una especificación desarrollada por el Grupo de Trabajo PC/SC para facilitar la interoperatividad necesaria para permitir que la tecnología de Tarjetas de Circuitos Integrados también conocida como Tarjetas Inteligentes puedan ser eficientemente utilizadas en entornos de computadores personales.
- *Persona jurídica:* Conjunto de personas agrupadas que constituye una unidad con finalidad propia, la cual adquiere, como entidad, capacidad jurídica y de obrar distinta de la de los miembros que la componen.
- *PIN*: Contracción de los vocablos ingleses "Personal Identification Number" cuyo significado en español es "Número de Identificación Personal". Es un número especifico para ser únicamente conocido por la persona que tiene que acceder a un recurso que se encuentra protegido por este mecanismo.
- *PKCS (Public-Key Cryptography Standards)*: Estándares criptográficos de *Clave Pública* producida por RSA Laboratorios, y aceptados internacionalmente como estándares.
- *PKCS#7* (Cryptographic Message Syntax Standard): Estándar criptográfico de *Clave Pública* producido por RSA Laboratorios, y aceptado internacionalmente como estándar, que define una sintaxis genérica para mensajes que incluyan mejoras criptográficas, tales como firma digital y/o cifrado.
- *PKCS#10* (Certification Request Syntax Standard): Estándar criptográfico de *Clave Pública* producido por RSA Laboratorios, y aceptado internacionalmente como estándar, que define la sintaxis de una petición de certificado.
- *PKCS#11* (*Cryptographic Token Interface Standard*): Estándar Criptográfico de Clave Pública producido por RSA Laboratorios, y aceptado internacionalmente como estándar, que define un interfaz de programación independiente de la tecnología de base, para utilizar tokens criptográficos (por ejemplo, tarjetas inteligentes criptográficas) como medio de autentificación.
- *Política de Certificación:* Documento integrante de la *Declaración de Prácticas de Certificación*, que establece el conjunto de reglas que indica la aplicabilidad de un *Certificado* a la *Comunidad Electrónica* y/o clase de aplicación con requisitos de seguridad comunes. Las políticas bajo las que la FNMT-RCM emite *Certificados*, se exponen en el anexo I.

  - La denominada como *Política de Certificación para certificados de componentes* sin embargo, es un documento que no forma parte de la *Declaración de Prácticas de Certificación* de la FNMT-RCM, que no obstante se adjunta provisionalmente a la misma por su carácter informativo sobre estas utilidades del Catálogo de Productos de la FNMT-RCM. Establece el conjunto de reglas de aplicación con requisitos de seguridad comunes a estos certificados. Estas Políticas se exponen en el apartado I.2 del anexo I adjunto a la *Declaración de Prácticas de Certificación de la FNMT-RCM*.

- *Práctica de Certificación:* Documento integrante de la *Declaración de Prácticas de Certificación* en el que se recogen los procedimientos específicos seguidos por la FNMT-RCM para la gestión del ciclo de vida de un *Certificado*.

  - Las *Prácticas de certificación particulares de los certificados de componentes* sin embargo, son un documento adjunto a la *Declaración de Prácticas de Certificación* a efectos meramente informativos pero sin formar parte de ella, en el que se recogen los procedimientos específicos seguidos por la FNMT-RCM para la gestión del ciclo de vida de los *certificado de componentes*. Estas prácticas se exponen en el anexo V adjunto a la *Declaración de Prácticas de Certificación* de la FNMT-RCM.

- *Prestador de Servicios de Certificación*: Es aquella persona física o jurídica que, de conformidad con la legislación sobre firma electrónica expide Certificados electrónicos, pudiendo prestar además otros servicios en relación con la *Firma electrónica*. En la presente *Declaración de Prácticas de Certificación*, se corresponderá con la Autoridad de Certificación de la FNMT-RCM, desarrollada a través de su departamento CERES.

- *RSA*: Acrónimo de Ronald Rivest, Adi Shamir y Leonard Adleman inventores del sistema criptográfico de clave asimétrica referido (1977). Criptosistema de clave pública que permite el cifrado y la firma digital.

- *Servicio de Dirección electrónica*: Servicio de buzón web para consulta (distinto del correo electrónico), restringido bajo las condiciones establecidas en el apartado "9.1 *Servicio de Dirección Electrónica*", que la FNMT-RCM a efectos de la actividad de emisión de certificados, pone a disposición de los *Suscriptores*, y del *Solicitante* de *Certificado de Persona jurídica para el ámbito tributario* para poder ser notificados.

- *Servicio de Fechado*: Servicio prestado bajo demanda por la FNMT-RCM a los interesados que lo soliciten, que basándose en las especificaciones *Request For Comments*: RFC 3161 – *"Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"* y ETSI 101861 *"Time stamping profile"*, data los documentos de forma objetiva logrando que, de forma indubitada se pueda atribuir un momento temporal a un documento electrónico.

- *Servicio de Notificación*: Servicio restringido bajo las condiciones establecidas en el apartado "9.2 *Servicio de Notificación* de la FNMT-RCM", del que todo miembro de la *Comunidad electrónica* pasa automáticamente a formar parte con la suscripción de la presente *Declaración de Prácticas de Certificación*.

- *SHA-1*: Secure Hash Algorithm (algoritmo seguro de resumen –hash–). Desarrollado por el NIST y revisado en 1994 (SHA-1). El algoritmo consiste en tomar mensajes de menos de 2^{64} bits y generar un resumen de 160 bits de longitud. La probabilidad de encontrar dos mensajes distintos que produzcan un mismo resumen es prácticamente nula. Por este motivo se usa para dotar de *Integridad* a los documentos durante el proceso de firma electrónica.

- *Sistema criptográfico*: Colección de transformaciones de texto claro en *texto cifrado* y viceversa, en la que la transformación o transformaciones que se han de utilizar son seleccionadas por *Claves*. Las transformaciones son definidas normalmente por un algoritmo matemático.
- *Software malicioso* (del inglés Malware: Malicious software)*:* Cualquier programa, documento o mensaje, susceptible de causar daños y/o perjuicios a los usuarios.
- *Solicitante*: Persona física mayor de 18 años o que ostente la cualidad de emancipado, que previa identificación, solicita la emisión de un *Certificado*. En el caso de tratarse de un *Solicitante* de *Certificado de Persona jurídica para el ámbito tributario* o de *Certificado de Entidad sin Personalidad Jurídica para el ámbito tributario*, esta persona física sólo podrá ser un administrador o un representante, legal o voluntario con poder bastante a estos efectos, de la *Persona jurídica* o *Entidad sin personalidad jurídica* que vaya a ser el *Suscriptor* del *Certificado.*
- *Sujeto pasivo tributario*: Abarcará en su conjunto tanto a las *Personas jurídicas*, como a las entidades carentes de personalidad jurídica a las que, sin embargo, la normativa tributaria considera "sujetos pasivos" a efectos fiscales. Quedarán excluidas de este concepto por lo tanto, las personas físicas.
- *SSCD (Secure Signature-creation Device):* Véase *Dispositivo seguro de creación de firma.*
- *Suscriptor (o SUBJECT)*: En el caso de *Certificados de Identidad de Personas Físicas*, es la persona cuya identidad personal queda vinculada a los datos firmados electrónicamente, a través de una *Clave Pública* certificada por el *Prestador de Servicios de Certificación*. En el caso de *Certificados de Personas Jurídicas para el ámbito tributario* y *Certificados de Entidad sin personalidad jurídica*, serán la *Persona Jurídica* y la *Entidad sin personalidad jurídica* respectivamente cuya identidad quedarán vinculadas a los datos firmados electrónicamente a través de una *Clave Pública* certificada por el *Prestador de Servicios de Certificación*. El concepto de *Suscriptor*, será referido en los *Certificados* y en las aplicaciones informáticas relacionadas con su emisión como "SUBJECT", por estrictas razones de estandarización internacional.
- *Tarjeta criptográfica*: "Tarjeta CERES" descrita en el apartado "7. *Soporte del Certificado*".
- *Texto en cifra ("texto cifrado")*: Conjunto de signos, guarismos o letras convencionales, y que solo puede comprenderse conociendo la *Clave*, es decir, la secuencia de símbolos que controlan las operaciones de cifrado y descifrado.
- *Titular* (de un *Certificado*): Véase *Suscriptor*.
- *Triple-DES*: Sistema de cifrado simétrico que surge como una evolución del DES (Data Encryption Standard – estándar de cifrado de datos) descrito en el FIPS 46-3 (Federal Information Processing Standard) que desarrolla el DEA (data encryption algorithm – algoritmo de cifrado de datos) también definido en el estándar ANSI X9.32.
- *UIT (Unión Internacional de Telecomunicaciones)*: Organización internacional del sistema de las Naciones Unidas en la cual los gobiernos y el sector privado coordinan los servicios y redes mundiales de telecomunicaciones.
- *Usuario destinatario*: Miembro de la *Comunidad Electrónica* al que se da de alta en los Servicios de *Dirección electrónica* y de *Notificación* de la FNMT-RCM. Esta condición la tendrán por defecto todos los miembros de la *Comunidad Electrónica*. La principal e inmediata consecuencia de estar dado de alta en este servicio es la asignación de una *Dirección electrónica* y la posibilidad de recibir notificaciones de la FNMT-RCM a través

de la misma. En este sentido, el miembro de la *Comunidad Electrónica*, autoriza como válida esta dirección para recibir comunicaciones, en el momento de suscribir el correspondiente contrato o convenio que le ligue con la FNMT-RCM.

- *Usuario remitente*: *Entidad usuaria* que mediante el correspondiente contrato o convenio con la FNMT-RCM, podrá utilizar el *Servicio de Notificación* de la FNMT-RCM para efectuar notificaciones electrónicas en las correspondientes *Direcciones electrónicas* de los miembros de la *Comunidad Electrónica* que hayan aceptado expresamente y con carácter previo recibirlas. En todo caso, la FNMT-RCM tendrá la condición de *Usuario remitente.*
- *X.500*: Estándar desarrollado por la UIT que define las recomendaciones del Directorio. Se corresponde con el estándar ISO/IEC 9594-1: 1993. Da lugar a la serie de recomendaciones siguientes: X.501, *X.509*, X.511, X.518, X.519, X.520, X.521 y X.525.
- *X*.509: Estándar desarrollado por la UIT Para las *Infraestructuras de Clave Pública* y los llamados "certificados de atributos".

2 PRESENTACIÓN

La FNMT-RCM, a través del Departamento CERES, con el fin de proporcionar transacciones electrónicas seguras a través de la Red, ha construido desde 1996 la infraestructura necesaria para prestar servicios de certificación electrónica con las máximas garantías. Esta infraestructura se encuentra en la actualidad plenamente operativa y experimentada. No en vano, el Departamento CERES ha obtenido como *Prestador de Servicios de Certificación*, autoridad de sellado de tiempo (Entidad de Fechado), así como desarrollador de un sistema operativo para tarjetas criptográficas, la Certificación de Calidad ISO 9001: 2000, siendo el primer *Prestador de Servicios de Certificación* español en conseguirlo.

Asimismo es de destacar la implicación en proyectos de adecuación a ISO 17799 y a la normativa de la European Electronic Signature Standardisation Initiative[1] (en adelante "EESSI") en colaboración con el Centro de Evaluación de las Tecnologías de la Información – Instituto Nacional de Técnica Aerospacial.

El objetivo de la FNMT-RCM, a través de su Departamento CERES, es proporcionar a sus clientes la *Infraestructura de Clave Pública*, así como todo un catálogo de servicios, sobre las cuales puedan apoyarse los servicios de los distintos organismos o empresas públicas o privadas, para dotarlas de seguridad y validez legal de manera sencilla y cómoda para el ciudadano. La FNMT-RCM procurará estos objetivos utilizando principalmente técnicas de cifrado (para lograr la confidencialidad de la información) y de firma electrónica, que garantizan la identidad del firmante y la integridad de la información intercambiada, siendo el esquema de firma electrónica adoptado, coherente con la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco común para la Firma electrónica, y con la legislación nacional de trasposición correspondiente, que garantizan, bajo cumplimiento de una serie de requisitos tasados, la equivalencia de la *Firma electrónica* con la firma manuscrita respecto de los efectos jurídicos presumidos.

[1] Iniciativa desarrollada por el mandato dado por la Comisión Europea al Information & Communications Technologies Standard Board, quien ha puesto en marcha a través del Information Society Standardisation System del European Committee for Standardisation y el European Telecommunication Standards Institute.

La FNMT-RCM lleva más de un siglo fabricando productos de alta seguridad y de especial sensibilidad como monedas y billetes. Pero también fabrica otros productos de seguridad como el DNI, pasaportes, sellos, papel para contratos oficiales, libros de registro, tarjetas inteligentes, etiquetas seguras, etc. tanto para el mercado nacional como para el internacional.

De esta forma, la FNMT-RCM continúa con su papel tradicional ofreciendo garantías públicas de seguridad a la sociedad española, aunque ahora también desde la perspectiva de Internet y las nuevas tecnologías, adaptándose a los nuevos tiempos y dando el salto cualitativo desde el documento físico al *Documento Electrónico*.

3 OBJETO DE LA PRESENTE *DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN*

El presente documento tiene por objeto la regulación de la prestación de los servicios de certificación por parte de la FNMT-RCM en su condición de *Prestador de Servicios de Certificación*, recogiendo en concreto las obligaciones que se compromete a cumplir en relación con la gestión de los *Datos de creación* y *verificación de Firma* y de los *Certificados*, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los *Certificados* y, en su caso, la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata y confidencial sobre la vigencia de los poderes indicados en los *Certificados* y que deban figurar preceptivamente inscritos en dichos registros. Además, en el presente documento se recogen los detalles del régimen de responsabilidad aplicable a los miembros de la *Comunidad Electrónica*, los controles de seguridad aplicados a sus procedimientos e instalaciones en aquello que pueda ser publicado sin perjudicar la eficacia de los mismos, y las normas de secreto y confidencialidad, así como cuestiones relativas a la propiedad de sus bienes y activos, a la protección de datos de carácter personal, y demás cuestiones de tipo informativo que considere interesante poner a disposición del público.

Los servicios de Suspensión de Certificados y Cancelación de la Suspensión de Certificados expuestos en la presente *Declaración de Prácticas de Certificación*, no estarán disponibles por el momento.

No forman parte de esta *Declaración de Prácticas de Certificación*, ni se pueden considerar "Certificados" los denominados "Certificados de Componentes" por no adecuarse al concepto legal de "certificado electrónico" definido por la Ley de firma electrónica 59/2003, de 19 de diciembre. No obstante, se adjuntan provisionalmente como anexo exclusivamente informativo, por ser productos de gran utilidad que forman parte del Catálogo de Servicios de la FNMT-RCM.

4 IDENTIFICACIÓN DE LA PRESENTE *DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN* Y ESTÁNDARES SEGUIDOS PARA SU ELABORACIÓN

El presente documento se denomina "*Declaración de Prácticas de Certificación de la FNMT-RCM*" e internamente será citado como "*Declaración de Prácticas de Certificación*", debiéndose entender que abarca las Prácticas de Certificación Particulares para las distintas clases de *Certificados* (anexos II a V) que se adjuntan como addenda al mismo, con excepción del anexo IV "Prácticas de Certificación particulares de los certificados de componentes", y del apartado I.2 "Políticas de Certificación para certificado de componentes de la FNMT-RCM" del Anexo I.

Esta DPC se encuentra referenciada por el *OID* 1.3.6.1.4.1.5734.4 pudiendo ser localizada en la dirección http://www.cert.fnmt.es/convenio/dpc.pdf su última versión en vigor.

Estos procedimientos se basan principalmente en las normas del *European Telecommunications Standards Institute* (ETSI): ETSI TS 102 042, ETSI TS 101 456, ETSI TS 102 023, ETSI TS 101 733, ETSI TS 101 862 y ETSI TS 101 861.

5 DISPONIBILIDAD DE LA INFORMACIÓN Y COMUNICACIONES

La FNMT-RCM interpretará, registrará, mantendrá, y publicará los procedimientos referidos en el apartado anterior "4. Identificación de la presente *Declaración de Prácticas de Certificación* y estándares seguidos para su elaboración", pudiendo además recibir comunicaciones de los interesados sobre estos asuntos, a través de la siguiente dirección de correo electrónico: ceres@fnmt.es, y en el teléfono de atención al interesado: 902 181 696.

Para cuestiones organizativas o administrativas, la dirección de contacto de la FNMT-RCM como *Prestador de Servicios de Certificación* es la siguiente:

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

Departamento CERES

C/ Jorge Juan, 106

28009 – MADRID

E-mail: ceres@fnmt.es

6 CONTROLES DE SEGURIDAD, REGISTRO DE EVENTOS Y AUDITORÍAS

La FNMT-RCM dispone de procedimientos de control físico, lógico, de personal, y de operación, destinados a garantizar la seguridad necesaria en la gestión de los *Certificados*. Asimismo, la FNMT-RCM registrará todos aquellos eventos relacionados con sus servicios que puedan ser relevantes, con el fin de verificar que todos los procedimientos internos necesarios para el desarrollo de la actividad se desarrollan de conformidad con la normativa aplicable para poder determinar las causas de una anomalía detectada.

A continuación y tomando como modelo de trabajo los documentos: *RFC 2527 Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Framework y ETSI 101 456 Policy requirements for certification authorities issuing qualified certificates*, se muestran todos los controles implementados por la FNMT-RCM como *Prestador de Servicios de Certificación*.

6.1. Registro de Eventos

6.1.1. Tipos de eventos registrados

La FNMT-RCM registrará todos aquellos eventos significativos, con el fin de verificar que todos los procedimientos internos necesarios para el desarrollo de la actividad, se ejecutan de acuerdo a este documento, a la normativa legal aplicable, y a lo establecido en el Plan de Seguridad Interna y en los Procedimientos de Calidad, y permitan detectar las causas de una anomalía detectada.

Los eventos registrados serán todas aquellas operaciones que se realicen en la gestión de claves, gestión de certificados, publicación, archivo, recuperación, directorio, registro de eventos, registro de usuarios y fabricación de tarjetas. La FNMT-RCM mantendrá archivados todos los eventos registrados más importantes, manteniendo su accesibilidad, durante un periodo nunca inferior a 15 años.

Todos los eventos registrados son susceptibles de auditarse.

Adicionalmente a los eventos expuestos, se guardarán todos los registros que especifica la norma ISO 9001: 2000 en la forma expuesta en los procedimientos generales de Calidad de la FNMT-RCM, por un periodo no inferior a 3 años. Estos registros son, fundamentalmente:

- Registros de seguimiento de la Dirección.
- Registros de diseño, desarrollo y sus revisiones.
- Registro de Acciones Correctivas.
- Registro de satisfacción de clientes.
- Registro de las revisiones del sistema.
- Otros registros.

6.1.2. Protección de un registro de actividad

Una vez registrada la actividad de los sistemas los registros no podrán ser modificados, ni borrados, permaneciendo archivados en las condiciones originales.

Este registro tendrá sólo acceso de lectura, estando restringido a las personas autorizadas por la FNMT-RCM.

La grabación del registro, con el fin de que no pueda ser manipulado ningún dato por nadie, se realizará automáticamente por un software específico que a tal efecto la FNMT-RCM estime oportuno.

El registro auditado, además de las medidas de seguridad establecidas en su grabación y posterior verificación, estará protegido de cualquier contingencia, modificación, pérdida y revelación de sus datos, durante su grabación en soportes externos, cambio de este soporte y almacenamiento de los mismos.

6.1.3. Procedimientos de copias de seguridad de los registros auditados

La FNMT-RCM, en su actividad de *Prestador de Servicios de Certificación*, por ser un sistema de alta seguridad, garantiza la existencia de copias de seguridad de todos los registros auditados.

6.1.4. Sistemas de archivo de registros

Los sistemas de archivos utilizados por la FNMT-RCM para conservar estos registros auditados, serán los internos propios de la infraestructura, y además se utilizarán soportes externos con capacidad de almacenamiento durante largos periodos de tiempo. Estos soportes tendrán las garantías suficientes para impedir que los registros sufran cualquier tipo de alteración.

La FNMT-RCM realizará varias copias que se almacenarán en diferentes lugares, que dispondrán de todas las medidas de seguridad física y lógica que eviten, en lo que razonablemente sea posible, una alteración del soporte almacenado y de los datos que contengan estos soportes. Cada copia será almacenada en un lugar diferente, con el objeto de prevenir posibles desastres en alguno de ellos.

Este archivo está provisto de un alto nivel de integridad, confidencialidad y disponibilidad para evitar intentos de manipulación de los certificados y eventos almacenados.

6.1.5. Datos relevantes que serán registrados

Serán registrados:

- La emisión y revocación, y demás eventos relevantes relacionados con los *Certificados*.
- Las firmas, y demás eventos relevantes relacionados con las *Listas de Revocación* (CRL's).
- Todas las operaciones de acceso al archivo de *Certificados*.
- Eventos relevantes de la generación de pares de números aleatorios y pseudo-aleatorios para la generación de *Claves*.
- Eventos relevantes de la generación de pares de *Claves* propias o de soporte de autenticidad. En ningún caso se incluirán los propios números ni ningún dato que facilite su predicción.
- Todas las operaciones del servicio de archivo de *Claves* y del acceso al archivo de *Claves* propias expiradas.
- Todas las operaciones relacionadas con la actividad como tercera parte confiable.

6.1.6. Protección de archivos

La FNMT-RCM garantiza que el archivo de eventos registrados cumple los siguientes requisitos:

- No podrá ser modificado por medios no autorizados.
- Ha de disponer un alto grado de disponibilidad y fiabilidad.
- Se guardará traza de los accesos realizados.

6.1.7. Realización de copias de seguridad de los archivos

En todo momento existirá una copia de seguridad de todos los archivos existentes en la FNMT-RCM, en su actividad como *Prestador de Servicios de Certificación*.

6.1.8. Obtención y verificación de la información archivada

El acceso al registro de archivos estará limitado al personal autorizado por la FNMT-RCM.

El acceso a datos cifrados por parte de terceras partes mediante el servicio de recuperación de datos sin autorización del usuario, deberá realizarse siempre bajo las condiciones que establezca la Ley.

6.2. Controles de seguridad física, de procedimientos y de personal

En este apartado se describirán todos los controles no técnicos utilizados por la FNMT-RCM como *Prestador de Servicios de Certificación* para ejecutar de forma segura las funciones asociadas a la gestión de *Certificados*.

6.2.1. Controles de Seguridad Física

La FNMT-RCM garantiza que cumple la normativa aplicable en todos los aspectos de seguridad física y las describe a lo largo del presente capítulo.

Se han establecido diferentes perímetros de seguridad, donde se llevan a cabo las actividades críticas o sensibles, con barreras de seguridad y con controles de entrada apropiados dotados de mecanismos de control de seguridad para reducir el riesgo de accesos no autorizados o de daños a los recursos informáticos.

6.2.1.1. Ubicación de las instalaciones

El edificio donde se encuentra ubicada la infraestructura del *Prestador de Servicios de Certificación*, dispone de medidas de seguridad de control de acceso al edificio, de forma que el desarrollo de la actividad y prestación de los servicios, se realicen con las suficientes garantías de *Confidencialidad* y seguridad.

Todas las operaciones críticas del *Prestador de Servicios de Certificación* se realizan dentro de un recinto físicamente seguro con diversos niveles de seguridad para acceder a las máquinas y aplicaciones críticas.

Estos sistemas estarán físicamente separados de otros sistemas de la FNMT-RCM, de forma que exclusivamente el personal autorizado del Departamento pueda acceder a ellos, y se garantice la independencia de otras redes de propósito general.

6.2.1.2. Situación del Centro de Proceso de Datos

El CPD del *Prestador de Servicios de Certificación* ha sido construido atendiendo los siguientes requerimientos físicos:

a) Situación alejada de sótanos para prevenir posibles inundaciones.

b) En un piso intermedio y alejado de salidas de humos para evitar el posible daño que éste podría causar ante un posible incendio en las plantas superiores.

c) Ausencia de ventanas al exterior del edificio.

d) Detectores de intrusión y cámaras de vigilancia en las áreas de acceso restringido para los períodos de tiempo en que los sistemas se encuentren desatendidos.

e) Control de acceso basado en tarjeta y contraseña.

f) Sistemas de protección y prevención de fuegos: campanas detectoras, extintores, formación de los operadores en la extinción de incendios, etc.

g) Existencia de mamparas transparentes, limitando las distintas zonas, que permitan observar las salas desde pasillos de acceso, para detectar intrusiones o actividades ilícitas en el interior del CPD.

h) Todo el cableado estará protegido contra daños o interceptación electromagnética o interceptación de la transmisión tanto de datos como de telefonía.

6.2.1.3. Acceso Físico

Perímetro de seguridad física

Una vez marcadas las áreas de seguridad de CERES se han establecido medidas físicas de control de accesos oportunas, sin olvidar que el recinto de la FNMT-RCM goza de un potente sistema perimetral de seguridad física compuesto por diversos anillos con avanzados medios técnicos y humanos.

Además de los diversos controles de acceso se dispone de diversos medios de control interior de las salas e instalaciones como son los controles de accesos basado en lectores de tarjetas, cámaras de videovigilancia, detectores de intrusismo, detectores de incendios, etc, además de los medios humanos dedicados a su atención tanto en el exterior como en el interior del recinto.

Controles físicos de entrada

Se dispone de un exhaustivo sistema de controles físicos de personas a la entrada y a la salida que conforman diversos anillos de seguridad.

Todas las operaciones críticas del *Prestador de Servicios de Certificación* se realizan dentro de un recinto físicamente seguro con diversos niveles de seguridad para acceder a las máquinas y aplicaciones críticas.

Estos sistemas estarán físicamente separados de otros sistemas de la FNMT-RCM, de forma que exclusivamente el personal autorizado del Departamento pueda acceder a ellos, y se garantice la independencia de otras redes de propósito general.

El trabajo en áreas seguras

El trabajo en áreas seguras se encuentra protegido por el control de acceso, y cuando el área así lo exige, monitorizado por el Departamento de Seguridad de la FNMT-RCM. No se permitirá, salvo autorización expresa de la Dirección, la presencia de equipos de fotografía, video, audio u otras formas de registro.

Áreas aisladas de carga y descarga

Las áreas de carga y descarga están aisladas y permanentemente vigiladas por medios técnicos y humanos.

Electricidad y Aire Acondicionado

Las salas donde se ubican las máquinas de la infraestructura del *Prestador de Servicios de Certificación*, disponen de suministro de electricidad y aire acondicionado suficiente para crear un entorno operativo fiable. Esta infraestructura productiva está protegida contra caídas de corriente o cualquier anomalía en el suministro eléctrico mediante una línea auxiliar independiente del centro de suministro principal, además de un grupo de suministro eléctrico autónomo.

Igualmente se han instalado mecanismos que mantienen controlados el calor y la humedad a sus niveles adecuados con el fin de conseguir una operación correcta del sistema del *Prestador de Servicios de Certificación*.

Aquellos sistemas que así lo requieren, disponen de unidades de alimentación ininterrumpida así como suministro eléctrico de doble proveedor y grupo electrógeno.

Seguridad del cableado

El cableado se encuentra en falso suelo o falso techo y se dispone de los medios adecuados (detectores en suelo y techo) para la protección del mismo ante incendios.

6.2.1.4. Exposición al agua

Se han tomado las medidas adecuadas para prevenir la exposición al agua de los equipos y el cableado.

6.2.1.5. Prevención y Protección contra incendios

Las salas disponen de los medios adecuados (detectores) para la protección de su contenido ante incendios.

El cableado se encuentra en falso suelo o falso techo y se dispone de los medios adecuados (detectores en suelo y techo) para la protección del mismo ante incendios.

6.2.1.6. Almacenamiento de Soportes

La FNMT-RCM-CERES, como *Prestador de Servicios de Certificación*, establece los procedimientos necesarios para disponer de copias de respaldo de toda la información de su infraestructura productiva.

Recuperación de la información

Existe en la FNMT-RCM-CERES planes de copia de seguridad de toda la información sensible y de aquella considerada como necesaria para la continuidad del negocio del Departamento. Existen diversos procedimientos de elaboración y recuperación en función de la sensibilidad de la información y de los medios instalados.

6.2.1.7. Eliminación de Residuos

Se dispone de una política de gestión de residuos que garantiza la destrucción de cualquier material que pudiera contener información, así como una política de gestión de los soportes removibles.

6.2.1.8. Copias de Seguridad fuera de las instalaciones

No aplicable.

6.2.2. Controles de Procedimiento

La FNMT-RCM procura que toda la gestión, tanto de procedimientos de operación, como administrativa, se lleve a cabo de forma confiable y conforme a lo establecido en este documento, realizando auditorías para evitar cualquier defecto que pueda conllevar pérdidas de confianza (A este respecto, puede consultarse el apartado 6.4. *Auditorías*).

- Se realizan auditorías, con el fin de comprobar el cumplimiento de las medidas de seguridad y de los requisitos técnicos y administrativos.
- Se realiza una segregación de funciones para evitar que una sola persona pueda conseguir el control total de la infraestructura. Para lograr que sea imposible evitar el conjunto de

medidas de salvaguarda existentes, se definen múltiples perfiles asignados al personal de la infraestructura, entre los que se distribuyen las distintas tareas y responsabilidades.

6.2.3. Controles de Seguridad de Personal

6.2.3.1 Seguridad en la definición del trabajo y los recursos

La definición de los puestos de trabajo y sus responsabilidades, incluidas las de seguridad, se integran en el Convenio que regula las relaciones de trabajo entre la FNMT-RCM y su personal laboral.

6.2.3.2 Inclusión de la seguridad en las responsabilidades laborales

La seguridad está incluida en las responsabilidades laborales sin que precise mención adicional por ser la FNMT-RCM una entidad cuyo principal objetivo es la seguridad y por ende el objetivo y la responsabilidad de todos los miembros que la integran.

En cualquier caso, se encuentra específicamente incluida en capítulo XVII "Régimen disciplinario", artículo 63, Faltas y Sanciones del referido Convenio:

> *"Serán faltas graves:*
>
> *...*
>
> *13. La utilización o difusión indebida de datos o asuntos de los que se tenga conocimiento por razón del trabajo en el Organismo.*
>
> *...*
>
> *Serán faltas muy graves:*
>
> *...*
>
> *9. La utilización de información interna de la FNMT-RCM en beneficio propio o de empresas que entren en concurrencia con la FNMT-RCM.*
>
> *..."*

La sanción puede llegar al despido, con independencia de la conculcación que se haga de los preceptos del marco general legislativo y su correspondiente sanción o pena que instruyera la Autoridad judicial.

Adicionalmente, en casos excepcionales, podrán existir acuerdos de confidencialidad personales a petición de terceras partes.

6.2.3.3 Selección y política de personal

La selección y política de personal se integran en el Convenio que regula las relaciones de trabajo entre la FNMT-RCM y su personal laboral, así como en la diversa normativa que le es de aplicación en virtud de su estatuto (Real Decreto 1114/1999, de 25 de junio, por el que se adapta la Fábrica Nacional de Moneda y Timbre a la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, se aprueba su Estatuto y se acuerda su denominación como Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (versión digital puesta a disposición en la dirección http://www.cert.fnmt.es/legsoporte/rdec1114.PDF) y su condición de Entidad Pública Empresarial dependiente del Ministerio de Economía.

6.2.3.4 Conocimientos, cualificación, experiencia y requerimientos acreditativos

Los procedimientos para la gestión del personal de la infraestructura promoverán la competencia y el saber hacer de sus empleados, así como el cumplimiento de sus obligaciones.

Serán considerados puestos de confianza dentro del ámbito de este documento, aquellos que implican el acceso o el control de componentes que puedan afectar directamente a la emisión, uso o revocación de los *Certificados*.

6.2.3.5 Acuerdos de confidencialidad

Todos los empleados, propios o contratados, que tienen acceso o control sobre estas operaciones criptográficas, incluyendo el acceso restringido al *Directorio*, son considerados como empleados de confianza. Este personal incluye, pero no está limitado, a personal de servicio al cliente, personal administrador del sistema, personal de ingeniería, y ejecutivos que fueron nombrados para verificar la infraestructura de los sistemas de seguridad del *Prestador de Servicios de Certificación*.

El personal designado permanentemente o de forma temporal para estos puestos, será debidamente acreditado e identificado por la FNMT-RCM. Periódicamente se realizará un aseguramiento de que estas personas siguen teniendo la confianza de la FNMT-RCM para la realización de estos trabajos de confidencialidad.

Las relaciones entre terceras partes y la FNMT-RCM están protegidas por el correspondiente acuerdo de confidencialidad si en el transcurso de esta relación fuera necesario el intercambio de información sensible.

El personal de la FNMT-RCM, en virtud de su convenio colectivo, no requiere la existencia de acuerdos de confidencialidad personales, según se describe en este punto, en el apartado "*Inclusión de la responsabilidad en las relaciones laborales*", sin perjuicio de que en casos excepcionales puedan existir acuerdos de confidencialidad personales, normalmente a petición de terceras partes.

6.2.3.6 Términos y condiciones de la relación laboral

Los términos y condiciones de la relación laboral se integran en el Convenio Laboral que regula las relaciones de trabajo entre la FNMT-RCM y su personal laboral, así como en la diversa normativa que le es de aplicación en virtud de su estatuto (Real Decreto 1114/1999, de 25 de junio, por el que se adapta la Fábrica Nacional de Moneda y Timbre a la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, se aprueba su Estatuto y se acuerda su denominación como Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda; versión digital del documento puesto a disposición en la dirección http://www.cert.fnmt.es/legsoporte/rdec1114.PDF) y su condición de Entidad Pública Empresarial dependiente del Ministerio de Economía.

6.2.3.7 Comunicación de las incidencias de seguridad

Las incidencias son puestas en conocimiento de la Dirección con independencia de que se activen las oportunas acciones correctivas a través del Sistema de Incidencias establecido en el Departamento para conducir a su solución de la forma más rápida posible según se describe en el *Procedimiento de Comunicación de Incidencias* y en el *Procedimiento de Gestión de Incidencias*.

6.2.3.8 Comunicación de las debilidades de seguridad

Las debilidades de seguridad son clasificadas como incidencias, y como tales se resuelven, dando lugar a las oportunas acciones correctivas, según se describe en los procedimientos anteriormente mencionados.

6.2.3.9 Comunicación de los fallos del software

Los fallos del software son clasificados como incidencias y, como tales, se resuelven dando lugar a las oportunas acciones correctivas, según se describe en el *Procedimiento de Comunicación de Incidencias* y en el *Procedimiento de Gestión de Incidencias.*

6.2.3.10 Aprendiendo de las incidencias

El *Procedimiento de Comunicación de Incidencias* y el *Procedimiento de Gestión de Incidencias* recogen también la agrupación y clasificación de las mismas para dar lugar a las correspondientes acciones correctivas o correctoras.

6.2.3.11 Procedimiento disciplinario

En el desarrollo de su actividad laboral para la FNMT-RCM-CERES, o siempre que usen medios y/o materiales de la FNMT-RCM, sus empleados ceden exclusivamente, en toda su extensión, por toda la duración máxima prevista en la Ley y para el ámbito mundial a la FNMT-RCM-CERES todos los derechos de explotación que pudieran corresponderles y en especial, y sin que esta enumeración se entienda con carácter limitativo, lo derechos de reproducción, distribución, transformación y comunicación pública relativos a propiedad intelectual, así como demás derechos de propiedad industrial, o relativos a topografía de semiconductores, sobre los trabajo, obras, invenciones y creaciones que originen y/o desarrollen. El trabajador, como consecuencia de la cesión en exclusiva de los mencionados derechos sobre los trabajos, obras, invenciones y creaciones elaboradas o creadas como consecuencia de la relación laboral que les une con la FNMT-RCM-CERES o como consecuencia del uso de los medios materiales y/o técnicos de la FNMT-RCM, no gozará del derecho de explotar las citadas obras y/o creaciones de forma alguna, aunque ello no perjudicara a la explotación o uso de las mismas por parte de la FNMT-RCM.

Con el fin de lograr cumplir la normativa interna de la FNMT-RCM-CERES, las leyes y regulaciones aplicables y la seguridad de sus empleados, la FNMT-RCM-CERES se reserva el derecho a inspeccionar en cualquier momento y llevar un seguimiento de todos los sistemas informáticos de la FNMT-RCM-CERES.

Los sistemas informáticos sujetos a inspección incluyen, pero no se limitan, a los archivos de sistema de correo electrónico, archivos del disco duro de ordenadores personales, archivos de buzón de voz, colas de impresión, documentación obtenida del fax, cajones del escritorio y áreas de almacenado. Estas inspecciones se llevarán a cabo tras haber sido aprobadas por los Departamentos de Seguridad y Asuntos Legales, con los procedimientos establecidos en la normativa legal aplicable. La FNMT-RCM-CERES además se reserva el derecho de eliminar de sus sistemas informáticos cualquier material que considere ofensivo o potencialmente ilegal.

6.2.3.12 Conductas inadecuadas

La dirección de la FNMT-RCM-CERES se reserva el derecho a revocar los privilegios de sistema de cualquier usuario en cualquier momento. No se permitirá conducta alguna que interfiera con el ritmo habitual y adecuado de los sistemas informáticos de la FNMT-RCM-CERES, que impida a otros utilizar estos sistemas o bien que sea peligroso u ofensivo.

6.2.3.13 Aplicaciones que comprometen la seguridad

Salvo concesión de la correspondiente autorización por parte de la Dirección de Sistemas de Información de la FNMT-RCM, los empleados de la FNMT-RCM-CERES no deberán adquirir, poseer, negociar o utilizar herramientas de hardware o software que pudieran ser empleadas para evaluar o comprometer los sistemas de seguridad informática. Algunos ejemplos de estas herramientas son: aquellas que ignoren la protección software contra copia no autorizada, detecten

contraseñas secretas, identifiquen puntos de seguridad vulnerables y descifren archivos. Asimismo, sin el permiso adecuado, se prohíbe a los empleados utilizar rastreadores u otro tipo de hardware o software que detecte el tráfico de un sistema en red o la actividad de un ordenador, salvo en aquellos casos que su uso sea necesario para la realización de pruebas del sistema y previa comunicación al responsable del área.

6.2.3.14 Actividades no permitidas

Los usuarios no deben comprobar o intentar comprometer las medidas de seguridad de un ordenador o sistema de comunicación a no ser que tal acción haya sido previamente aprobada, por escrito, por la Dirección de Sistemas de Información de la FNMT-RCM. Los incidentes relacionados con la "piratería informática", descubrimiento de contraseñas, descifrado de archivos, copia no autorizada de software y otras actividades que supongan una amenaza para las medidas de seguridad, o sean ilegales, se considerarán violaciones graves de la normativa interna de la FNMT-RCM-CERES. También está terminantemente prohibido el uso de sistemas de *bypass*, cuyo objetivo es evitar las medidas de protección, y otros archivos que puedan comprometer los sistemas de protección o los recursos.

6.2.3.15 Denuncia obligatoria

Todas las supuestas violaciones de la normativa, intrusiones en el Sistema, afecciones por software malicioso y otras condiciones que supongan un riesgo para la información o los sistemas informáticos de la FNMT-RCM-CERES, deberán ser inmediatamente notificadas a la Dirección de Sistemas de Información de la FNMT-RCM.

6.3. Controles de seguridad técnica

6.3.1. Gestión del ciclo de vida de las *Claves* del *Prestador de Servicios de Certificación*

6.3.1.1. Generación e instalación de las Claves del Prestador de Servicios de Certificación

Por motivos de seguridad y calidad las *Claves* que la FNMT-RCM necesita para el desarrollo de su actividad como *Prestador de Servicios de Certificación*, serán generadas por ella misma dentro de su propia infraestructura en un entorno físico seguro y al menos por dos personas autorizadas para ello.

La generación de las *Claves* y la protección de la *Clave Privada*, se realiza guardando las necesarias medidas de confidencialidad, usando sistemas de hardware y software seguros y de confianza conforme a las normas EESSI CWA14167-1 y CWA14167-2, además de tomar las precauciones necesarias para prevenir su pérdida, revelación, modificación o su uso sin autorización, de acuerdo con los requisitos de seguridad especificados en las normas EESSI (en particular ETSI TS 101 456) aplicables a los *Prestadores de Servicios de Certificación*.

Los algoritmos y longitudes de *Clave* utilizados están basados en estándares ampliamente reconocidos para el propósito para el que son generadas.

Los componentes técnicos necesarios para la creación de *Claves* están diseñados para que una *Clave* sólo se genere una vez, y para que una C*lave Privada* no pueda ser calculada desde su *Clave Pública*.

6.3.1.2. Almacenamiento, salvaguarda y recuperación de los Datos de creación y verificación de Firma del Prestador de Servicios de Certificación

Los *Datos de creación de Firma* del *Prestador de Servicios de Certificación* se encuentra protegida por un dispositivo criptográfico que cumple con los requisitos de seguridad FIPS PUB 140-1 Nivel 3. Las operaciones de firma de *Certificados* y de *Listas de Revocación* son llevadas a cabo dentro del dispositivo criptográfico, que dota de cifrado a los *Datos de creación de Firma* del *Prestador de Servicios de Certificación* en el módulo.

Cuando los *Datos de creación de Firma* se encuentran fuera del dispositivo criptográfico, se encuentran asimismo protegidos por los mecanismos criptográficos necesarios para procurar su *Confidencialidad* ante ataques basados en criptoanálisis.

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

6.3.1.3. Distribución de la clave pública de la Autoridad de Certificación

Los *Datos de verificación de Firma* del *Prestador de Servicios de Certificación* se distribuyen en forma de "certificado electrónico autofirmado", pudiéndose consultar en la dirección www.cert.fnmt.es. Para la comprobación de la autenticidad del "certificado autofirmado" se puede comprobar en formato *MD5* y *SHA-1* la huella digital que se publicó a estos efectos en el BOE nº 235 (pág. 35194) de 1 de Octubre de 1999.

6.3.1.4. Período de uso de los Datos de creación y de verificación de Firma

Los *Datos de creación y de verificación de Firma* del *Prestador de Servicios de Certificación* y de los *Suscriptores*, podrán utilizarse durante toda la vigencia del *Certificado (*sobre la vigencia de los *Certificados*, puede consultarse el apartado "9.12 Vigencia de los Certificados" de la presente *Declaración de Prácticas de Certificación).*

6.3.1.5. Usos de los Datos de creación y de verificación de Firma del Prestador de Servicios de Certificación

Los *Datos de creación y de verificación de Firma* de la FNMT-RCM en su actividad como *Prestador de Servicios de Certificación* serán utilizadas única y exclusivamente para los propósitos de:

- Firma de *Certificados*.
- Firma de las *Listas de Revocación*.

Los algoritmos y parámetros de firma utilizados por la Autoridad de Certificación de la FNMT-RCM para la firma de certificados electrónicos y listas de certificados revocados son los siguientes:

Algoritmo de firma: RSA

Parámetros del algoritmo de firma: Longitud del Módulo=1024

Algoritmo de generación de claves: rsagen1

Método de relleno: emsa-pkcs1-v1_5

Función criptográfica de Resumen: SHA-1

Este conjunto de algoritmos y parámetros se corresponden con la entrada 001 en la tabla de "suites" de firma aprobadas en ETSI SR 002 176 "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures".

La identificación del algoritmo de firma utilizado por la FNMT-RCM tanto para los certificados expedidos como para las listas de revocación viene indicado en el campo básico "signature" del certificado y de las listas de certificados revocados con la siguiente estructura ASN-1:

```
signature          AlgorithmIdentifier
AlgorithmIdentifier  ::=  SEQUENCE  {
      algorithm             OBJECT IDENTIFIER,
      parameters            ANY DEFINED BY algorithm OPTIONAL  }
algorithm = sha-1WithRSAEncryption OBJECT IDENTIFIER  ::=  {
        iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5  }
parameters = NULL
```

6.3.1.6. Cambio de los Datos de creación y de verificación de Firma del Prestador de Servicios de Certificación

La FNMT-RCM, en función de los avances ocurridos en materia criptográfica, estudiará el cambio de sus *Datos de verificación de Firma*, cuando las circunstancias lo aconsejen y minimizando el impacto en su *Comunidad Electrónica*. En caso de optar por dicho cambio, la FNMT-RCM comunicará a los miembros de su *Comunidad Electrónica*, el cambio de sus propios *Datos de creación y de verificación de Firma* y pondrá a su disposición los nuevos *Datos de verificación de Firma* en el sitio www.cert.fnmt.es.

6.3.1.7. Fin del ciclo de vida de las Claves criptográficas del Prestador de Servicios de Certificación

La FNMT-RCM destruirá o almacenará de forma apropiada las *Claves* del *Prestador de Servicios de Certificación* una vez finalizado el período de validez de las mismas, con la finalidad de evitar su uso inapropiado.

6.3.2. Gestión del ciclo de vida de las *Claves* de *Suscriptor*

6.3.2.1. Generación y almacenamiento de Claves de Suscriptor

La FNMT-RCM no almacena las *Claves Privadas* de los *Sucriptores* que utilizan su infraestructura de certificación. Las *Claves Privadas* de los *Suscriptores* son de uso y control exclusivo del propio *Suscriptor* y generadas por éste, bien a través de *Tarjetas criptográficas* o de los *navegadores*.

La FNMT-RCM conserva la *Clave Pública* del Suscriptor y la prueba de posesión de la *Clave Privada* (*Clave Pública* o mensaje, cifrado con la *Clave Privada*) según el ordenamiento legal vigente, durante un periodo no menor a 15 años.

6.3.2.2. Usos de las claves de usuario

El uso de las *Claves* de los usuarios se detalla en cada uno de los anexos II a V en los que se muestran las diferentes Prácticas de Certificación Particulares cubiertas por la FNMT-RCM como *Prestador de Servicios de Certificación*.

6.3.2.3. Periodo de utilización de las claves de usuario

Los *Datos de creación de Firma y los Datos de verificación de Firma* de los miembros de la *Comunidad Electrónica*, podrán utilizarse durante todo el periodo de vida del *Certificado*. Véase a este respecto el apartado "9.12 Vigencia de los Certificados" de la presente *Declaración de Prácticas de Certificación.*

6.3.3. Controles de seguridad de los componentes técnicos

La seguridad de todos los componentes técnicos que la FNMT-RCM utiliza en el desarrollo de su actividad como *Prestador de Servicios de Certificación*, así como en su estructura y procedimientos, se tienen presente en todo lo relativo a la certificación de la seguridad de los Sistemas de Información, de acuerdo al Esquema Nacional de Certificación de la Seguridad de los Sistemas de Información, que se aprueben en España, en particular los relativos a EESSI que sean publicados en el Diario Oficial de la Comunidades Europeas o en los correspondientes Diarios Oficiales españoles. Además se tendrán en cuenta los criterios de evaluación de la seguridad de tecnologías de información ISO 15408 (Common Criteria), en el diseño, desarrollo, evaluación y adquisición de productos y sistemas de las Tecnologías de la Información, que vayan a formar parte del *Prestador de Servicios de Certificación*, así como la normativa EESSI.

Los procesos de gestión de la seguridad de la infraestructura serán evaluados periódicamente.

6.3.4. Controles de seguridad de la red

Los medios de comunicación mediante redes publicas, que la FNMT-RCM utiliza en el desarrollo de sus actividades, utilizan suficientes mecanismos de seguridad, para evitar cualquier agresión externa a través de estas redes. Este sistema es auditado periódicamente con el fin de verificar su buen funcionamiento.

Del mismo modo, la infraestructura de la red que presta los servicios de certificación está dotada de todos los mecanismos de seguridad necesarios para garantizar un servicio fiable e íntegro. Esta red también es auditada periódicamente.

6.3.5. Controles de ingeniería del módulo criptográfico

Entre los componentes técnicos suministrados a sus usuarios, y con objeto de incrementar la confianza de la opinión pública en sus métodos criptográficos, la FNMT-RCM realiza evaluaciones de la seguridad de los productos y servicios que ofrece, utilizando para ello criterios abiertos y aceptados por el mercado.

6.3.6. Niveles de seguridad

Los niveles de seguridad que tienen los distintos componentes de la Infraestructura, así como los procedimientos y componentes que integran la actividad del Prestador de Servicios de Certificación, serán evaluados según "Criterios de Evaluación de la Seguridad de los Productos y Sistemas de las Tecnologías de la Información" (ITSEC/ITSEM) y/o Criterios Comunes (ISO15408) y, en particular, según la iniciativa EESSI.

Asimismo, respecto de la gestión de la seguridad de la información, se sigue el esquema previsto en UNE-ISO 17799 *Código de Buenas Prácticas para la Seguridad de la Información.*

Respecto de los datos personales se estará a lo especificado la normativa legal vigente y en concreto a lo dispuesto por la LOPD y por el Real Decreto 994/1999, de 11 de Junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.

6.3.7. Restablecimiento de los servicios en caso de fallo o desastre

El *Prestador de Servicios de Certificación* pondrá en marcha un Plan de Recuperación ante Desastres, que contemple:

- La redundancia de los componentes más críticos.
- La puesta en marcha de un centro de respaldo alternativo.
- El chequeo completo y periódico de los servicios de copia de respaldo.
- Compromiso de los *Datos de verificación de Firma* del *Prestador de Servicios de Certificación*. En este caso la FNMT-RCM informará a todos los miembros de la *Comunidad Electrónica* indicando que todos los *Certificados* y *Listas de Revocación* firmadas con estos datos ya no son válidos, y procederá al restablecimiento del servicio, tan pronto como sea posible y en las nuevas condiciones aplicables.

6.3.8. Terminación de la actividad de la FNMT-RCM como Prestador de Servicios de Certificación

Esta contingencia y sus consecuencias se describen en esta *Declaración de Prácticas de Certificación* en el apartado "9.18 Cese de la actividad del *Prestador de Servicios de Certificación*: Transferencia de la prestación del servicio".

6.4. Auditorías

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

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

6.4.1. Protección de las herramientas de auditoría

Todas las herramientas, informes, registros, ficheros y fuentes relacionados con la elaboración o registro de una auditoría, son considerados como información sensible y, como tal, son tratados en todos los aspectos, estando su acceso restringido a personas autorizadas.

6.4.2. Identidad del auditor

El auditor que verifique y compruebe la correcta operativa del *Prestador de Servicios de Certificación* de la FNMT-RCM, deberá ser una persona o profesional con la suficiente titulación oficial y la adecuada experiencia sobre la materia a auditar de acuerdo con la legislación que se encuentre en vigor en cada momento.

La realización de estas auditorías podrá ser encargada a Empresas Auditoras externas o a personal interno cualificado para ello (según la legislación vigente al respecto), dependiendo del grado de criticidad del área a auditar, el grado de independencia del personal implicado y su nivel de experiencia.

En los casos en los que las auditorías se elaboran por personal externo a la FNMT-RCM, se establecen las medidas y controles necesarios para regular los requisitos de auditoría, el alcance, el acceso a información sensible y demás acuerdos de *Confidencialidad* y responsabilidad sobre los activos.

En las auditorías externas, el auditor y la empresa auditora no tendrán nunca ningún tipo de vinculación laboral, comercial o de cualquier otra índole con la FNMT-RCM, ni con la parte que solicite la auditoría, siendo siempre un profesional independiente quien realiza la auditoría solicitada.

Junto con el informe obtenido de la auditoría, figurará la identificación de los auditores. El informe resultado de la auditoría estará firmado por los auditores y por el responsable del ente auditado.

6.4.3. Resultados de la auditoría y acciones correctivas

Todas las disconformidades detectadas en la auditoría serán tratadas con las correspondientes acciones correctivas. El plan de acción de puesta en marcha de las acciones correctivas será elaborado en el plazo más breve posible y será conservado junto con el informe de la auditoría para su inspección y seguimiento en posteriores auditorías.

En el caso de que la deficiencia encontrada supusiera un grave riesgo para la seguridad del Sistema, de los *Certificados*, de los *Datos de creación o verificación de Firma*, o de cualquier documento o dato considerado *Confidencial* en este documento, bien de los *Suscriptores*, o del propio *Prestador de Servicios de Certificación*, la FNMT-RCM actuará según lo descrito en el *Plan de Contingencias*, con el fin de salvaguardar la seguridad de toda la infraestructura.

De igual manera la FNMT-RCM actuará diligentemente para subsanar el error o defecto detectado en el menor espacio de tiempo posible.

6.4.4. Comunicación de los resultados

Las Autoridades Administrativas o Judiciales competentes podrán solicitar los informes de auditorías para verificar el buen funcionamiento del *Prestadores de Servicios de Certificación*.

6.4.5. Plan de auditorías

Se realizarán las siguientes auditorías:

- Seguridad: ISO 17799: Una parcial anual externa y una total cada tres (3) años para mantenimiento de la certificación (A concretar cuando se establezca el esquema de certificación correspondiente).
- Seguridad: UNE 71502: Una parcial anual externa (se puede agrupar con la anterior) y una total externa cada tres (3) años para mantenimiento de la certificación. (A concretar cuando se establezca el esquema de certificación correspondiente).
- Calidad: ISO 9001: 2000: Una parcial anual externa más una auditoría anual interna preparatoria y una total externa cada tres (3) años, para mantenimiento de la certificación.
- Protección de datos: Una cada dos (2) años interna a realizar por el Departamento de Sistemas de Información.
- Prestadores de servicios de certificación: ETSI TS 101456: Una parcial anual y una total cada tres (3) años. (A concretar cuando se establezca el esquema de certificación correspondiente).

Se realizarán los siguientes controles:

- Controles internos de seguridad de red.
- Controles y pruebas internas del plan de contingencia.
- Controles internos de Calidad y Seguridad.

- Extraordinarios: Cuando así lo exijan las circunstancias a criterio de la FNMT-RCM.

7 SOPORTE DEL CERTIFICADO

La FNMT-RCM expedirá el *Certificado* en dos soportes alternativos:

a) ***Tarjeta criptográfica*:** con método de generación de *Claves* en la propia *Tarjeta criptográfica* para imposibilitar el uso o exportación de los *Datos de creación de Firma* fuera de la Tarjeta.

La posibilidad de usar tarjetas inteligentes con criptoprocesador como soporte físico de los servicios de certificación a los *Suscriptores*, facilita su interacción con la FNMT-RCM e incrementa considerablemente el nivel de seguridad de sus aplicaciones.

En cumplimiento de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco común para la Firma electrónica y la correspondiente legislación nacional de trasposición, y, atendiendo a lo dispuesto por la "Decisión de la Comisión de 14 de julio de 2003 relativa a la publicación de los números de referencia de las normas que gozan de reconocimiento general para productos de firma electrónica, de conformidad con lo dispuesto en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo", esta *Tarjeta* constituye un *Dispositivo seguro de creación de Firma*.

Este Dispositivo permite la generación interna de *Claves* criptográficas, e impide el acceso desde al exterior a las mismas, siendo realizadas todas las operaciones criptográficas con manejo de *Claves* o, en su caso, *Datos de creación de Firma*, en el interior de la propia Tarjeta. Las *Claves* o, en su caso, *Datos de creación de Firma*, no pueden ser usados ni copiados desde el exterior.

Esta *Tarjeta criptográfica* es la recomendada por el Centro Nacional de Inteligencia (CNI, antiguo CESID) a través del Centro Criptológico Nacional, siendo el CNI el organismo con competencias exclusivas en materias criptográficas según Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

La Tarjeta ofrece *Claves RSA* de hasta 2048 bits como algoritmo de *Clave Pública*, *SHA-1* para el *Hasing*, y *Triple-DES* para el cifrado simétrico.

El sistema operativo de la tarjeta, diseñado por la FNMT-RCM, sigue las especificaciones *PC/SC* y ofrece a las aplicaciones interfaz *PKCS#11* y el interfaz Microsoft CryptoAPI.

La Tarjeta viene dotada de protección de acceso mediante PIN, y admite más de 15 *Certificados* estándar *X.509*.v3 de tamaño de *Clave* de 1024 bits, con independencia del *Prestador de Servicios de Certificación* que emita los *Certificados*.

Para una descripción detallada de las características y posibilidades de la Tarjeta, puede consultar la información puesta a disposición a través de la dirección www.cert.fnmt.es/clase2/tarjeta/main.htm en el epígrafe <<"Información técnica sobre la *Tarjeta criptográfica*">>.

b) **Soporte convencional (disco duro, disquete, etc.) de almacenamiento de software.** La generación de los *Datos de creación de Firma* y de los *Datos de verificación de Firma* se harán en el *Navegador* del *Suscriptor*, mediante procedimientos alternativos al *SSCD* para dotar de seguridad al proceso. Tanto los *Certificados*, como la *Clave Privada*, serán custodiados por el *Navegador* y su sistema operativo, y almacenados en memoria no volátil.

Habrá posibilidad en este caso de exportar los *Datos de creación de Firma* a otros soportes, cuya protección vendrá conferida por la utilización de palabras de acceso ("passwords").

La FNMT-RCM recomienda el uso de *Tarjeta criptográfica* como *Dispositivo Seguro de Creación de Firma*.

8 TIPOS DE *CERTIFICADOS* EMITIDOS POR LA FNMT-RCM, Y LÍMITES PARA SU UTILIZACIÓN

La FNMT-RCM transmite todos los derechos necesarios para el USO típico del *Certificado* a *Suscriptores* y *Entidades usuarias*, para el ámbito de la *Comunidad electrónica* a la que se han incorporado mediante la suscripción de la presente *Declaración de Prácticas de Certificación* y el correspondiente contrato o convenio particular.

Los *Certificados* nunca podrán utilizarse fuera de la *Comunidad Electrónica*, ni para usos distintos de los comprendidos en esta *Declaración de Prácticas de Certificación* y en el contrato o convenio particular correspondiente.

La FNMT-RCM emite los siguientes *Certificados* con las limitaciones de uso específicas que se recogen en su correspondientes Prácticas de Certificación Particulares que a continuación se referencian:

- *Certificado de identidad de persona física*: También denominado *Certificado de usuario de la FNMT-RCM (Clase 2 CA)*, es la certificación electrónica expedida por la FNMT-RCM que vincula a su *Suscriptor* unos *Datos de verificación de Firma* y confirma su identidad. En estos *Certificados*, el *Suscriptor* sólo lo podrá ser una persona física.

  Sus *Prácticas de Certificación* Particulares se detallan en el Anexo II.

- *Certificado de Persona jurídica para el ámbito tributario:* es la certificación electrónica expedida por la FNMT-RCM que vincula a su *Suscriptor* unos *Datos de verificación de Firma* y confirma su identidad. Sin embargo, al contrario del *Certificado de identidad de personas físicas*, el *Suscriptor* sólo lo podrá ser una *Persona jurídica* (siempre *Sujeto pasivo tributario)*. Este *Certificado* se corresponde con el certificado tradicional utilizado por el Ministerio de Hacienda o el Gobierno de Navarra para el ámbito tributario.

  Sus *Prácticas de Certificación* Particulares se detallan en el Anexo III.

- *Certificado de Entidad sin personalidad jurídica para el ámbito tributario: es la* certificación electrónica expedida por la FNMT-RCM que vincula a su *Titular* o *Suscriptor* (siempre *Entidad sin personalidad jurídica a las que se refiere el articulo 35.4 de la Ley General Tributaria*) unos *Datos de verificación de Firma* y confirma su identidad a los solos efectos de su empleo en el ámbito tributario. Estos certificados se expiden según los términos expuestos en la ORDEN EHA/3256/2004, de 30 de septiembre, publicada en el B.O.E Nº 246 de 12 de octubre.

  Sus *Prácticas de Certificación* Particulares se detallan en el Anexo IV.

NO FORMAN PARTE DE ESTA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN, ni se pueden considerar "Certificados" los denominados "CERTIFICADOS DE COMPONENTES" por no adecuarse al concepto legal de "certificado electrónico" definido por la Ley de firma electrónica 59/2003, de 19 de diciembre. No

obstante, se adjuntan provisionalmente como anexo exclusivamente informativo, por ser productos de gran utilidad que forman parte del Catálogo de Servicios de la FNMT-RCM.

9 CONDICIONES GENERALES DEL SERVICIO

La FNMT-RCM está constituida como *Prestador de Servicios de Certificación* raíz, independiente, que no forma parte de estructuras de confianza externas.

Tanto el registro inicial como la solicitud de revocación o cualquier otra operación del ciclo de vida del *Certificado* que requiera la acreditación del interesado, será realizada a través de una *Oficina de Registro*, con la excepción del procedimiento de solicitud de suspensión de *Certificados* (descrita en el apartado 9.12.4.3), las operaciones telemáticas que se realizan a través de la página web de la FNMT-RCM cuando se disponga del *Certificado* y de la *Clave Privada*, como por ejemplo la solicitud telemática de revocación de *Certificados* (descrita en el apartado 9.12.3.3), el cambio de datos personales del *Suscriptor* de las bases de datos de la FNMT-RCM (descrito en el apartado 9.2.2), o la solicitud de renovación de *Certificados* (descrita en el apartado 9.16).

Los interesados pueden consultar qué *Oficina de Registro* es la más cercana a su domicilio, a través de la dirección http://www.cert.fnmt.es/clase2/iniciomain.htm

La FNMT-RCM como *Prestador de Servicios de Certificación*, emitirá *Certificados* para todo aquel interesado que lo solicite en las condiciones previstas en esta *Declaración de Prácticas de Certificación*. Estos *Certificados* permitirán al *Suscriptor* del mismo comunicarse e identificarse con sus interlocutores de forma segura.

El formato de los *Certificados* utilizados por la FNMT-RCM se basa en el definido por la Unión Internacional de Telecomunicaciones, sector de normalización de las telecomunicaciones, en la Recomendación UIT-T X.509, de fecha Junio de 1997 o superiores (ISO/IEC 9594-8 de 1997). El formato será el especificado en la Versión 3 del mencionado formato *X.509* y será válido para el uso con protocolos de comunicación estándares tipo SSL, TLS, etc.

Asimismo, el formato de las *Listas de Revocación* publicadas por la FNMT-RCM sigue el perfil propuesto en la recomendación UIT-T X.509, en su Versión 2 en lo que se refiere a *Listas de Revocación*.

9.1 Servicio de Dirección Electrónica

La FNMT-RCM pondrá a disposición de todo *Suscriptor* una dirección en Internet que permitirá a su titular recibir en todo caso las notificaciones de la FNMT-RCM, así como la posibilidad de recibir también las reguladas por la siguiente legislación:

- Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social.
- Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.
- Orden PRE/1551/2003, de 10 de junio, por la que se desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

El servicio será conforme con los criterios recogidos en dicha legislación así como en el marco de los criterios de seguridad, normalización y conservación, a los que se refiere el Real Decreto 263/1996, de 16 de febrero, a los requisitos de autenticidad, integridad, disponibilidad y confidencialidad de los dispositivos y aplicaciones de registro y notificación, así como a los protocolos y criterios técnicos a los que deben sujetarse.

Dichos criterios de seguridad, normalización y conservación han sido objeto de informe favorable del "Consejo Superior de Informática y para el impulso de la Administración Electrónica".

9.1.1 Acceso a la dirección electrónica

La *Dirección electrónica* será accesible a través de Internet por su titular siempre que esté en posesión de los *Datos de creación de Firma* asociados al *Certificado*, lo que permitirá su autenticación.

El acceso a los servicios contará con las debidas medidas de *Confidencialidad* de modo que solo el titular sea capaz de ver la información disponible en su *Dirección electrónica*. Dichas medidas de confidencialidad podrán al menos cifrar la información mediante el uso de alguno de los protocolos de comunicación estándares SSL, TLS o similares, con una *Clave* simétrica de intercambio de datos, de por lo menos 128 bits, mediante el uso de los algoritmos de cifrado más habituales.

Las especificaciones del *Servicio de Fechado* están basadas en las especificaciones del *Request for Comments*: 3161 – "*Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).*

La FNMT-RCM guardará prueba firmada datada de cada acceso realizado a la *Dirección electrónica* y pondrá dicha información a disposición de los usuarios del servicio, así como de las autoridades competentes de acuerdo con la legislación aplicable.

La FNMT-RCM como *Prestador de Servicios de Certificación*, y a los únicos efectos de dar fe de lo acontecido, tendrá un acceso limitado a los contenidos de la *Dirección electrónica*. Dicho acceso limitado no permitirá en ningún caso a ningún empleado o colaborador externo de la FNMT-RCM el acceso a la *Dirección electrónica*. El procedimiento de acceso a la *Dirección electrónica* se regulará en los protocolos de seguridad establecidos por la FNMT-RCM. Todo acceso será anotado en un libro de control de accesos donde se hará constar al menos la fecha, la hora, el motivo justificado del acceso así como los intervinientes y su cualificación.

El titular podrá acceder a su *Dirección electrónica* mediante el uso de los *Navegadores* que cumplan la especificación W3C HTML.4.01 o superior u otros medios generalmente aceptados.

9.1.2 Contenido de la dirección de electrónica

La FNMT-RCM pondrá las medidas electrónicas, informáticas y telemáticas que resulten razonables, para permitir salvaguardar el contenido de la *Dirección electrónica*, así como evitar su eliminación o manipulación por entidades ajenas.

La FNMT-RCM autenticará (mediante prueba de posesión de los *Datos de creación de Firma*) a cualquier entidad que desee depositar información de cualquier tipo en la *Dirección electrónica*. Dicha información permitirá en caso de necesidad, identificar y suspender el acceso a la entidad que haga uso incorrecto de la *Dirección electrónica*.

La FNMT-RCM avisará electrónicamente al titular de la *Dirección electrónica* de que se ha introducido información en la misma. Dicho aviso se realizará mediante el envío de correo electrónico, mensajería SMS u otros medios generalmente aceptados, que el titular haya declarado como validos.

El acceso a los contenidos de la *Dirección electrónica* deberá ser realizado previa firma electrónica cuando el *Usuario remitente* del contenido así lo requiera. En este caso, la FNMT-RCM guardará prueba del acceso al contenido con las mismas características explicadas para el acceso a la dirección electrónica.

El contenido estará disponible para su titular, por lo menos el tiempo que el *Usuario remitente* haya definido. El titular podrá acceder y descargar la información durante ese tiempo. Pasado ese plazo la FNMT-RCM se reserva el derecho a almacenar dicha información en soportes electrónicos que no estén disponibles en línea.

Los contenidos vertidos en esta dirección electrónica no pueden ser vinculados en modo alguno a la FNMT-RCM, dado que se trata de un mero custodio que desconoce el contenido textual de los mismos, y que se limita a autenticar a las partes (imputabilidad de los documentos firmados por las partes y verificación de la integridad del documento firmado). De tal forma que si dichos contenidos pudieran ser considerados ilegales la imputación del contenido se realizará contra el firmante de los mismos.

9.1.3 Actualización tecnológica

La FNMT-RCM someterá el *Servicio de Dirección electrónica* a la actualización tecnológica constante que permita que la disponibilidad de este *Servicio* y el acceso al mismo cumpla en todo momento los criterios técnicos iniciales, así como aquellos que, fruto de los avances tecnológicos o del desarrollo normativo, le sean de aplicación.

Dicha actualización se realizará tratando de evitar en la medida de lo posible el cambio en los procedimientos seguidos por los *Usuarios destinatarios* hasta la fecha de la actualización.

La FNMT-RCM notificará a las *Usuarios destinatarios* con 2 meses de antelación, las actualizaciones que pudieran causar modificaciones en los procedimientos de acceso a la *Dirección electrónica* o de consulta del contenido depositado.

9.1.4 Prácticas del Servicio de *Dirección electrónica*

La declaración detallada de prácticas del *Servicio de Dirección electrónica* se publicará en la página *Web* de la FNMT-RCM y podrá ser variada sin previo aviso. La variación no menoscabara los derechos de los usuarios, no incumplirá los criterios legalmente aplicables, ni limitará técnicamente este *Servicio*.

9.2 Servicio de Notificación de la FNMT-RCM

La FNMT-RCM como prestador de servicios de notificación electrónica dispone de un *Servicio de Notificación* regulado por la siguiente legislación:

- Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social.
- Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.
- Orden PRE/1551/2003, de 10 de junio, por la que se desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

El servicio se adecua a los criterios recogidos en dicha legislación, así como en el marco de los criterios de seguridad, normalización y conservación a los que se refiere el Real Decreto 263/1996, de 16 de febrero, a los requisitos de autenticidad, integridad, disponibilidad y confidencialidad de los dispositivos y aplicaciones de registro y notificación, así como los protocolos y criterios técnicos a los que deben sujetarse.

Dichos criterios de seguridad, normalización y conservación han sido objeto de informe favorable del Consejo Superior de Informática y para el impulso de la Administración Electrónica.

Este servicio de notificación será empleado como método de notificación preferente por la FNMT-RCM, en su actividad como *Prestador de Servicios de Certificación,* a los miembros de la *Comunidad Electrónica*.

En este sentido y habida cuenta que la legislación sobre firma electrónica establece la obligación de notificar la revocación o suspensión de los *Certificados* a sus *Suscriptores* la FNMT-RCM recaba la dirección de correo electrónico, el número de teléfono móvil donde recibir mensajes de texto y del domicilio de los *Suscriptores* en los contratos que presente a la firma de los *Solicitantes*, antes de emitir un *Certificado*.

Estas direcciones se recogen con la finalidad general de utilizar la primera como canal principal de comunicación, dejando la segunda y tercera como canal subsidiario, para cubrir cualquier contingencia de desastre que pudiera imposibilitar a la FNMT-RCM notificar mediante el primer medio, y con la finalidad específica de notificar tanto las revocaciones y suspensiones de los *Certificados*, como la resolución de los contratos que la FNMT-RCM haya celebrado con los *Suscriptores*.

Será obligación del *Solicitante* y posteriormente del *Suscriptor*, mantener la actualidad y verdad de las mencionadas direcciones.

9.2.1 Descripción del servicio

El *Servicio de Notificación* es un servicio de "*web mail*" con acuse de recibo, cuyo acceso se realizará mediante identificación por procedimientos de *Firma electrónica reconocida*. Este *Servicio* va provisto de un sistema que logra el no repudio en destino.

Las notificaciones practicadas serán datadas y custodiadas electrónicamente.

La declaración detallada de prácticas del *Servicio* se publicará en la página *Web* de la FNMT-RCM y podrá ser variada sin previo aviso. La variación no menoscabara los derechos de los usuarios, no incumplirá los criterios legalmente aplicables, ni limitará técnicamente el *Servicio*.

El *Servicio de Notificación* electrónica se podrá complementar adicionalmente con un servicio de notificación tradicional para completar una solución de correo mixto.

9.2.2 Prestación del Servicio en relación con la presente Declaración de Prácticas de Certificación

Todos los miembros de la *Comunidad Electrónica* pasarán a ser *Usuarios destinatarios* de este servicio mediante la firma del correspondiente contrato de solicitud de *Certificado* de la FNMT, o del correspondiente contrato o convenio de incorporación a la *Comunidad electrónica*. El alta en este servicio tiene por objeto, en conjunción con la *Dirección electrónica* asignada a los *Usuarios destinatarios,* posibilitar la comunicación de la FNMT-RCM con los miembros de la *Comunidad Electrónica*. En este sentido y teniendo en cuenta lo establecido en el apartado "9.14 Datos de Carácter Personal", el *Usuario destinatario* que suscribe la presente *Declaración de Prácticas de Certificación* reconoce como medio válido de comunicación, el *Servicio de Notificación*, y autoriza

a que la FNMT-RCM utilice el mencionado *Servicio* para notificar cualquier circunstancia relativa a productos o servicios de la FNMT-RCM.

La FNMT-RCM, a los solos efectos de poder optimizar el *Servicio de Notificación* pone a disposición de los *Usuarios destinatarios* a través del apartado "Modificación de datos personales" de la página http://www.cert.fnmt.es/clase2/main.htm la "Aplicación de cambio de datos personales", para que informen a la FNMT-RCM de cualquier circunstancia relativa a sus datos personales en la forma prevista en la normativa vigente en materia de Protección de Datos Personales.

De acuerdo con la disposición transitoria primera de la ley de firma electrónica 59/2003, los certificados que hayan sido expedidos en el marco del Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica, mantendrán su validez. No obstante, será de aplicación a los mismos, esta Declaración de Prácticas de Certificación y sus modificaciones subsiguientes, si bien aquellos suscriptores que así lo deseen podrán solicitar la revocación de su certificado por no admitir las variaciones que esta *Declaración de Prácticas de Certificación* suponga, entendiéndose que, de no recibir contestación a la comunicación que la FNMT-RCM efectuará a tal efecto en el plazo de un mes desde su envío a la *Dirección electrónica*, se produce una aceptación tácita de las nuevas condiciones de contratación.

9.2.3 Acceso al servicio

El servicio será accesible a través de Internet por el miembro de la *Comunidad Electrónica*, siempre que esté en posesión de un *Certificado* válido y no revocado, así como de sus correspondientes *Datos de creación de Firma*, lo que le permitirá identificarse mediante el uso de *Firma electrónica reconocida*.

El acceso al *Servicio de Notificación* contará con las debidas medidas de *Confidencialidad* de modo que solo la FNMT-RCM y los miembros de la *Comunidad Electrónica* que cada *Usuario destinatario* acepte, sean capaces de practicar notificaciones a sus correspondientes *Direcciones electrónicas*. Dichas medidas de confidencialidad podrán al menos cifrar la información mediante el uso de alguno de los protocolos de comunicación estándares SSL, TLS o similares, con una *Clave* simétrica de intercambio de datos de al menos 128 bits mediante el uso de los algoritmos de cifrado más habituales.

La solicitud de acceso a los servicios se realizará por medios electrónicos y mediante *Firma electrónica reconocida*. La FNMT-RCM guardará la firma generada, la prueba sellada de tiempo que permita confirmar la identidad del peticionario así como su solicitud y el momento de la realización. De igual manera, la solicitud de baja en el *Servicio de Notificación* se realizará mediante los mismos procedimientos de firma y fechado.

La FNMT-RCM guardará prueba firmada y datada de cada notificación practicada y pondrá dicha información en los casos que corresponda, a disposición de la *Entidad remitente*, de la *Entidad usuaria*, así como de las autoridades competentes de acuerdo a la legislación aplicable.

9.2.4 Prácticas del Servicio de Notificación

La declaración detallada de prácticas del Servicio se publicará en la página *Web* de la FNMT-RCM y podrá ser variada sin previo aviso, si bien la FNMT-RCM enviará a la *Dirección electrónica* de los *Usuarios destinatarios* un aviso de modificación de las prácticas del Servicio. La variación no menoscabará los derechos de los *Usuarios remitentes*, no incumplirá los criterios legalmente aplicables, ni limitará técnicamente el Servicio.

9.3 Certificados electrónicos

La emisión de *Certificados* supone la generación de *Documentos Electrónicos* que acrediten la identidad y, en su caso, otras cualidades o facultades del *Suscriptor*.

Todos los *Certificados*, para ser tales, y con el fin de evitar su alteración o falsificación, deberán contener la *Firma electrónica reconocida* de los mismos, generada por la FNMT-RCM con sus *Datos de creación de Firma* en su calidad de *Prestador de Servicios de Certificación*.

La facultad de emitir *Certificados* de la FNMT-RCM reside únicamente en esta entidad, no siendo en ningún caso delegable.

No obstante, para un mayor abundamiento en las prácticas y procedimientos seguidos en la emisión por la FNMT-RCM de los distintos tipos de *Certificados* específicos, nos remitimos en cada caso al procedimiento particular descrito en los anexos II a V.

9.4 Ciclo de vida del *Certificado*

En función del tipo de *Certificado* solicitado (apartado "8. Tipos de Certificados emitidos por la FNMT-RCM, y límites para su utilización") y del soporte en que se desee alojar (apartado "7. Soporte del *Certificado*") los procedimientos implícitos en el ciclo de vida del *certificado* podrán variar. No obstante, a continuación se describen con carácter general las distintas fases del ciclo, que se complementarán según cada caso, con las *Prácticas de Certificación* Particulares que correspondan de las adjuntadas como anexos II a V.

9.5 Presolicitud

En función del tipo de certificado solicitado (apartado "8. Tipos de Certificados emitidos por la FNMT-RCM, y límites para su utilización") y del soporte en que se desee alojar (apartado "7. Soporte del *Certificado*") esa fase podrá tener mayor o menor número de trámites.

Estos trámites abarcan la primera comunicación entre el interesado y la FNMT-RCM, que podrá ser telemática a través de la página web de la FNMT-RCM, postal, o personal para adquirir según los casos el correspondiente código de solicitud, la *Tarjeta criptográfica, etc.*

La FNMT-RCM solo aceptará peticiones de certificado en los formatos PKCS#10 y SPKAC (Signed Public Key And Challenge) cuyo algoritmo de clave pública sea rsaEncryption (OID 1.2.840.113549.1.1.1), con longitud de clave mínima de 512 bits y cuyo algoritmo de firma sea sha1WithRSAEncryption (OID 1.2.840.113549.1.1.5).

Estas cuestiones y actuaciones se determinan en las *Prácticas de Certificación* Particulares adjuntas como anexos II a V.

9.6 Solicitud del *Certificado*

La fase de solicitud del *Certificado* comprende con carácter general la personación y, en todo caso, la confirmación de la identidad personal del *Solicitante*, así como la aportación de la documentación que corresponda, la cumplimentación de formularios, y la firma de los contratos que se establezcan. Estas cuestiones y actuaciones se determinan en las *Prácticas de Certificación* Particulares adjuntas como anexos II a V.

9.7 Emisión de *Certificados*

Los tramites comprendidos en el procedimiento de emisión del *Certificado* pueden a su vez ser distintos en función del *Certificado* solicitado. Cada uno de estos procedimientos se especifica en las *Prácticas de Certificación* Particulares adjuntas como anexos II a V.

9.8 Archivo de los *Datos de verificación de Firma*

Los *Datos de verificación de Firma* de los *Suscriptores* permanecerán archivados por si fuera necesaria su recuperación, en archivos y soportes seguros tanto física como lógicamente, durante el período legalmente establecido de quince (15) años.

9.9 Uso y Aceptación de *Certificados*

Para poder usar los *Certificados* o confiar en documentos firmados electrónicamente con base en los mismos, se deberá previamente formar parte de la *Comunidad Electrónica*, y adquirir la condición de *Entidad usuaria*. Fuera de la *Comunidad Electrónica* no se debe confiar en un *Certificado* o en una firma electrónica que se base en un *Certificado* emitido bajo la *Política de Certificación de Certificados Reconocidos de la FNMT-RCM*. En cualquier caso, de producirse esta confianza por parte de un tercero, no se obtendrá cobertura de la presente *Declaración de Prácticas de Certificación*, y se carecerá de legitimidad alguna para reclamar o emprender acciones judiciales contra la FNMT-RCM por daños, perjuicios, o conflictos provenientes del uso o confianza en un *Certificado*.

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

- Firmar otro certificado.
- Firmar software o componentes.
- Generar sellos de tiempo para procedimientos de *Fechado electrónico.*
- Prestar servicios a título gratuito u oneroso, como por ejemplo serían a título enunciativo:
  - Prestar servicios de OCSP.
  - Generar *Listas de Revocación.*
  - Prestar servicios de notificación.
- Realizar transacciones económicas superiores a 100€, salvo que:
  - Uno de los intervinientes sea una Entidad usuaria de Derecho Público; o
  - Medie autorización expresa y escrita de la FNMT-RCM para hacerlo y, en ese caso, en las condiciones que se establezcan en dicha autorización.

En las *Prácticas de certificación* particulares, también incluidas en esta *Declaración de Prácticas de Certificación*, se expresan de forma más detallada las limitaciones específicas para el uso de cada uno de los certificados de que se trate, que en caso de discrepancia con las aquí expuestas, serán de aplicación las citadas condiciones particulares.

La aceptación de los *Certificados* por parte del *Suscriptor* se entenderá tácitamente producida si tras haber descargado el *Certificado* el *Suscriptor* lo usa o pone a disposición de terceros y no solicita su revocación.

Al aceptar el *Certificado* el *Suscriptor* también acepta además: las normas de uso y las condiciones contenidas en la presente *Declaración de Prácticas de Certificación*, entendiendo por tal no solo el cuerpo principal de la misma sino también su addenda.

En todo caso, al aceptar un *Certificado* emitido por la FNMT-RCM, el *Suscriptor* y, en su caso, el *Solicitante* del mismo declaran:

a) Que toda la información entregada durante el procedimiento de solicitud del *Certificado* es verdadera.

b) Que el *Certificado* será usado exclusivamente para fines legales y autorizados por la FNMT-RCM de acuerdo a la presente *Declaración de Prácticas de Certificación* y siempre dentro del ámbito de la *Comunidad Electrónica*.

c) Que asegura su exclusivo control sobre los *Datos de creación de Firma* que se correspondan con los *Datos de verificación de Firma* incluidos en su *Certificado* emitido por la FNMT-RCM y vinculados a su identidad personal, lo que, en todo caso y a título meramente enunciativo, incluirá las acciones y medidas necesarias para prevenir su pérdida, revelación, modificación, o uso por tercero distinto del *Suscriptor*.

d) Que custodiará diligentemente su *Certificado*, con independencia del soporte en el que se encuentre, así como cualquier otra *Clave*, contraseña, o *PIN* de acceso relacionados con los servicios prestados por la FNMT-RCM.

e) Que comunicará inmediatamente a la FNMT-RCM cualquier circunstancia que pueda comprometer el exclusivo control, integridad o seguridad del *Certificado*, del soporte, de las *Claves*, de las contraseñas, del *PIN*, etc.

La FNMT-RCM considerará válido todo *Certificado* aceptado por el *Suscriptor* y publicado en su *Directorio* seguro correspondiente, siempre que no haya caducado y que no conozca ninguna causa de revocación que le afecte.

9.10 Publicación de los *Certificados* en *Directorio Seguro*

La FNMT-RCM publicará en un *Directorio* seguro propio y restringido, tanto los *Certificados*, como las *Listas de Revocación*.

Los operadores y administradores de la infraestructura y los módulos internos tendrán acceso, previa autenticación, a toda la información existente en el *Directorio*, pudiendo realizar todo tipo de operaciones en función del perfil definido. Las *Entidades usuarias* de Derecho Público tendrán acceso a las *Listas de Revocación*, de conformidad con lo dispuesto en el apartado "9.14 Procedimientos de consulta del estado de los *Certificados*".

Las *Entidades usuarias* de Derecho Privado, con carácter general, no tendrán acceso a las *Listas de Revocación*, realizando la validación a través del servicio OCSP descrito en el apartado "9.15 Servicio de validación de *Certificados* mediante *OCSP*", salvo autorización expresa y escrita de la FNMT-RCM.

9.11 Renovación de los *Datos de creación de Firma y de los Datos de verificación de Firma*

La solicitud de la emisión de unos nuevos *Datos de creación de Firma*, llevará aparejada la emisión de un nuevo *Certificado*. De igual forma, cada vez que se renueve un *Certificado*, se generarán nuevos *Datos de creación y de verificación de Firma*.

9.12 Vigencia de los *Certificados*

9.12.1 Caducidad

Todos los *Certificados* emitidos por el *Prestador de Servicios de Certificación* tendrán validez durante un período nunca superior a cuatro (4) años, con la excepción de los *Certificados raíz*.

Este período se contará a partir de la fecha de emisión del *Certificado*. 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*.

Cada *Certificado*, según su tipología, dispondrá de una duración específica, según las *Prácticas de Certificación* Particulares aplicables.

9.12.2 Extinción de la vigencia del *Certificado*

Los *Certificados* emitidos por la FNMT-RCM exceptuando los *Certificados raíz*, quedarán sin efecto en los siguientes casos:

a) Terminación del período de validez del *Certificado* dependiendo de la *Práctica de Certificación* Particular aplicable.

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 perdida de eficacia de los *Certificados* tendrá lugar desde que estas circunstancias se produzcan.

c) Revocación o Suspensión del *Certificado* por cualquiera de las causas recogidas en la presente *Declaración de Prácticas de Certificación*.

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 la *Lista de Revocación* de su servicio de consulta sobre la vigencia de los *Certificados*.

9.12.3 Revocación de *Certificados*

La solicitud de revocación de los *Certificados* podrá efectuarse durante el período de validez que consta en el *Certificado*. Cada tipo de *Certificado* tiene una duración específica según se recoge en las *Prácticas de Certificación Particulares* adjuntas como anexos II a V.

Estarán legitimados para solicitar la revocación de un *Certificado* directamente o a través de tercero con poder suficiente:

- *Certificado de identidad de personas físicas*: El *Suscriptor*
- *Certificado de Persona jurídica para el ámbito tributario y Certificado de Entidad Sin Personalidad Jurídica para el ámbito tributario*: El *Suscriptor* y el *Solicitante*

9.12.3.1 Causas de Revocación de *Certificados*

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

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

2) Que la revocación le haya sido solicitada por el *Suscriptor* siguiendo el procedimiento referido en el apartado "9.12.3.3 Procedimiento para la revocación de *Certificados*".

3) Que la solicitud de revocación o la causa que la motiva, le haya sido notificada mediante resolución judicial o administrativa.

4) Que en las causas c) a h) del presente apartado le sean acreditados dichos extremos fehacientemente, previa identificación del solicitante de la revocación.

Teniendo en cuenta lo anterior, serán causas de revocación de un *Certificado*:

a) La solicitud de revocación por el *Suscriptor*, su representante, la persona física o jurídica representada por el *Suscriptor*, un tercero debidamente autorizado, o la persona física solicitante de un *Certificado de Persona jurídica para el ámbito tributario* o de un *Certificado de Entidad sin personalidad jurídica para el ámbito tributario*.

   En todo caso deberá dar lugar a esta solicitud:-

   a. Pérdida del soporte del *Certificado.*

   b. La utilización por un tercero de los *Datos de creación de Firma* del *Suscriptor*, correspondientes a los *Datos de verificación de Firma* contenidos en el *Certificado* y vinculados a la identidad personal del *Suscriptor*.

   c. La violación o puesta en peligro del secreto de los *Datos de creación de Firma* del *Suscriptor o* de los del responsable de la custodia de los *Datos de creación de Firma*.

   d. La alteración de las condiciones de custodia o uso de los *Datos de creación de Firma* que estén reflejadas en los *Certificados* expedidos a una persona jurídica para el ámbito tributario o a una entidad sin personalidad jurídica.

   e. La no aceptación de las nuevas condiciones que puedan suponer la emisión de nuevas *Declaraciones de Prácticas de Certificación*, durante el periodo de un mes tras su publicación.

b) Resolución judicial o administrativa que así lo ordene.

c) Fallecimiento o extinción de la personalidad jurídica del *Suscriptor*.

d) Fallecimiento o extinción de la personalidad jurídica del representado.

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

f) Terminación de la representación.

g) Disolución de la persona jurídica representada.

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

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

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

k) 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.

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

9.12.3.2 Efectos de la revocación

Los efectos de la revocación 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 la *Lista de Revocación.*

9.12.3.3 Procedimiento para la revocación de *Certificados*

El legítimo solicitante de la revocación deberá efectuar las actuaciones pertinentes de conformidad con el procedimiento que le corresponda, según las *Prácticas de Certificación* Particulares adjuntas como anexos II a V de la presente *Declaración de Prácticas de Certificación*.

9.12.4 Suspensión de *Certificados*

La solicitud de suspensión de los *Certificados* podrá realizarse durante el período de validez de los mismos.

Estarán legitimados para solicitar la suspensión de un *Certificado* directamente o a través de tercero con poder suficiente:

- *Certificado de identidad de personas físicas*: El *Suscriptor*
- *Certificado de Persona jurídica para el ámbito tributario y Certificado de Entidad sin Personalidad Jurídica para el ámbito tributario*: El *Suscriptor* y el *Solicitante*

9.12.4.1 Causas de suspensión

La FNMT-RCM podrá suspender la vigencia de los *Certificados* a solicitud del legítimo interesado particular, o de Autoridad judicial o ante la existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los *Certificados* contempladas en el apartado "9.12.3.1 Causas de Revocación de *Certificados*". 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 mediante el procedimiento establecido en la dirección http://www.ceres.fnmt.es/, 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.

9.12.4.2 Efectos de la suspensión

Los efectos de la 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 la *Lista de Revocación.*

9.12.4.3 Procedimiento para la suspensión de *Certificados*

El legítimo solicitante de la suspensión deberá efectuar las actuaciones pertinentes de conformidad con el procedimiento que le corresponda, según las *Prácticas de Certificación* Particulares adjuntas como anexos II a V de la presente *Declaración de Prácticas de Certificación*.

9.12.4.4 Procedimiento para cancelar la suspensión de *Certificados*

El legítimo solicitante de la suspensión podrá proceder a cancelar la suspensión de los certificados, según las *Prácticas de Certificación* Particulares adjuntas como anexos II a V de la presente *Declaración de Prácticas de Certificación*.

9.13 Generación y publicación de las *Listas de Revocación*

La FNMT-RCM mantendrá en *Listas de Revocación* los *Certificados* revocados y suspendidos, por un plazo equivalente al de validez teórica del *Certificado* en el momento de su emisión. Al expirar el período originario de validez de un *Certificado*, éste dejará de estar listado en las *Listas de Revocación*.

Estas *Listas de Revocación* se publican con una periodicidad máxima de (24) veinticuatro horas y tienen una validez asimismo de (24) veinticuatro horas. Podrán emitirse nuevas *Listas de Revocación* cada vez que un *Certificado* sea revocado o suspendido.

Las *Listas de Revocación* irán en todo caso autenticadas por la FNMT-RCM, mediante la generación de *Firma electrónica reconocida* utilizando sus *Datos de creación de Firma*.

La FNMT-RCM podrá publicar la información anteriormente mencionada no sólo directamente por sus propio medios, sino a través de directorios públicos ofrecidos por otras entidades u organismos con los que tenga suscritos acuerdos de réplica, siempre que se mantenga igual garantía y seguridad.

El perfil de las *Listas de Revocación* emitidas por la FNMT-RCM son conformes a la Recomendación UTI-T X.509 versión 2.

9.14 Procedimientos de consulta del estado de los *Certificados*

El *Suscriptor* del *Certificado* no tendrá acceso a las *Listas de Revocación*. No obstante, dispone de una aplicación en la dirección http://www.cert.fnmt.es/clase2/datoscert.htm a través de la cual y previa autenticación con sus *Datos de creación de Firma*, se le informará acerca del estado de su *Certificado*.

Únicamente las *Entidades usuarias* de Derecho Público tendrán acceso a las *Listas de Revocación* (originaria o replicada), y en las condiciones establecidas en el correspondiente convenio de incorporación a la *Comunidad Electrónica*.

Las *Entidades usuarias* de Derecho Privado, dispondrán de un *Cliente OCSP* para comprobar el estado de los *Certificados* mediante consultas vía OCSP, según se refiere en el apartado "9.15 Servicio de validación de Certificados mediante *OCSP*" de la presente *Declaración de Prácticas de Certificación*.

9.15 Servicio de validación de *Certificados* mediante *OCSP*

La FNMT-RCM dispone de un servidor de *OCSP* ("OCSP responder") para ofrecer servicio de *OCSP* a las *Entidades usuarias* de Derecho privado, en los términos de esta *Declaración de Prácticas de Certificación* y bajo los términos suscritos en el correspondiente convenio de incorporación a la *Comunidad Electrónica* que se firme con la *Entidad usuaria*. Este Servicio es el único servicio de comprobación del estado del *Certificado* que se pone a disposición de este tipo de *Entidades usuarias*, con carácter general.

El servicio funciona de la siguiente manera: El servidor OCSP verifica la firma de la petición OCSP efectuada por un *Cliente OCSP* registrado en el sistema, y comprueba el estado de los *Certificados* incluidos en la misma. En caso de que la *Firma electrónica* de la solicitud sea inválida, la petición se rechaza y se retorna al cliente una respuesta negativa. En caso de que la petición sea válida, se emitirá una respuesta de OCSP informando acerca del estado en el que se encuentran en ese momento los *Certificados* incluidos en la petición.

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

9.16 Renovación de *Certificados*

Podrán solicitar la renovación de los *Certificados* emitidos por la FNMT-RCM, los *Suscriptores* y sus representantes. El procedimiento para la renovación y los efectos de dicha operación son descritos en las *Prácticas de Certificación* Particulares adjuntas como anexos II a V de la presente *Declaración de Prácticas de Certificación,*si bien, como se recoge en el apartado "9.20.1.2. Identificación del suscriptor" se indica que la renovación telemática del *Certificado* sólo se podrá realizar cuando no se haya superado el plazo máximo de 5 años desde la personación e identificación física del Suscriptor que establece la Ley de firma electrónica 59/2003, de 19 de diciembre, en su artículo 13.4.

9.17 Notificación de la emisión, renovación, revocación y suspensión de *Certificados*

Sin perjuicio de los servicios de consulta del estado del *Certificado* que la FNMT-RCM pone a disposición de los interesados legitimados, como son el servicio de atención telefónica al cliente (902 181 696), el procedimiento de consulta de las *Listas de Revocación* recogido en el apartado "9.14 Procedimiento de consulta del estado de los *Certificados*", o el Servicio de peticiones *OCSP* descrito en el apartado "9.15 Servicio de validación de *Certificados* mediante *OCSP*", la FNMT-RCM notificará a la dirección de correo electrónica (que no a la *Dirección electrónica*) de los *Suscriptores* la emisión, renovación, revocación o suspensión efectiva de su *Certificado*.

9.18 Cese de la actividad del Prestador de Servicios de Certificación: Transferencia de la prestación del servicio.

En caso de terminación de la actividad del *Prestador de Servicios de Certificación*, la FNMT-RCM se regirá por lo dispuesto en la normativa vigente sobre firma electrónica.

En todo caso, la FNMT-RCM:

a) Informará a los *Suscriptores* de los *Certificados* sobre sus intenciones de terminar su actividad como *Prestador de Servicios de Certificación* al menos con dos (2) meses de antelación al cese de esta actividad.

b) Transferirá, con el consentimiento expreso de los *Suscriptores*, aquellos *Certificados* que sigan siendo válidos en la fecha efectiva de cese de actividad a otro *Prestador de Servicios de Certificación* que los asuma. De no ser posible esta transferencia los *Certificados* se extinguirán.

c) Comunicará al Ministerio que en ese momento tenga las competencias en la materia, el cese de su actividad y el destino que vaya a dar a los *Certificados*, especificando en su caso: si los va a *transferir*, a quién, o si los dejará sin efecto. La notificación a dicho organismo se realizará con al menos dos (2) meses de antelación, en documento firmado manuscrita o electrónicamente. Además se remitirá a dicho organismo la información relativa a los *Certificados* cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a los efectos pertinentes.

9.19 Cambio de los Datos de creación de Firma de la FNMT-RCM

Esta contingencia y sus consecuencias, se describen en el apartado "6.3.1 Gestión del ciclo de vida de las *Claves* del *Prestador de Servicios de Certificación*" de esta *Declaración de Prácticas de Certificación*.

9.20 Obligaciones y Garantías de las Partes

NO FORMAN PARTE DE ESTA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN, ni se pueden considerar "Certificados" los denominados "CERTIFICADOS DE COMPONENTES" por no adecuarse al concepto legal de "certificado electrónico" definido por la Ley de firma electrónica 59/2003, de 19 de diciembre. No obstante, se adjuntan provisionalmente como anexo exclusivamente informativo, por ser productos de gran utilidad que forman parte del Catálogo de Servicios de la FNMT-RCM.

9.20.1 Obligaciones y Garantías del Prestador de Servicios de Certificación

La FNMT-RCM no estará sujeta a otras garantías ni otras obligaciones que las establecidas en la normativa sectorial de aplicación y en la presente *Declaración de Prácticas de Certificación.*

Sin perjuicio de lo dispuesto en la legislación sobre firma electrónica, y su normativa de desarrollo, el *Prestador de Servicios de Certificación* se obliga a:

9.20.1.1 Con carácter previo a la emisión del *Certificado*

a) Comprobar la identidad y circunstancias personales de los *Suscriptores* de *Certificados* con arreglo a lo dispuesto en la presente *Declaración de Prácticas de Certificación* (a este respecto puede consultarse el correspondiente procedimiento de registro de los adjuntos como anexos II a V). En ningún caso se emitirán *Certificados* para menores de edad salvo que ostenten la cualidad de emancipados.

b) Verificar que toda la información contenida en la solicitud del *Certificado* se corresponde con la aportada por el *Solicitante*.

c) Comprobar que el interesado en solicitar la emisión de un *Certificado* está en posesión de la *Clave Privada* que constituirá, una vez emitido el *Certificado*, los *Datos de creación de Firma* correspondientes a los de *Datos de verificación de Firma* que constarán en el *Certificado*, y comprobar su complementariedad.

9.20.1.2 Identificación del *Suscriptor*

a) Identificar a la persona física que solicite un *Certificado*, con carácter general exigiendo su personación y estar en posesión de número de Documento Nacional de Identidad o Número de Identificación de Extranjeros (8 dígitos + letra). Para la

identificación se procederá a presentar documentación en vigor como: el Documento Nacional de Identidad. No obstante, cabrá exceptuar el mencionado requisito de personación cuando la firma del *Suscriptor* haya sido legitimada en presencia notarial, o la solicitud verse sobre la renovación telemática del *Certificado*, siempre que no se haya superado el plazo máximo de 5 años desde la personación e identificación física del Suscriptor que establece la Ley de firma electrónica 59/2003, de 19 de diciembre, en su artículo 13.4.

b) Comprobar en el proceso de solicitud de *Certificados de Persona jurídica para el ámbito tributario* y de *Certificados de Entidades sin personalidad jurídica para el ámbito tributario*, además de lo establecido en el apartado a), los datos relativos a la constitución de la personalidad jurídica o de la entidad y a la extensión y vigencia de las facultades de representación del solicitante, bien mediante consulta en el Registro público en el que estén inscritos los documentos de constitución y de apoderamiento, bien mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente, cuando aquellos no sean de inscripción obligatoria.

c) Exigir, si los *Certificados* admitieren otros supuestos de representación, la acreditación de las circunstancias en las que se fundamenten, en la misma forma prevista anteriormente.

En cualquier caso, respecto de los requisitos que se establecen respecto de la identificación del *Suscriptor*, y del proceso de emisión de *Certificados* en general, se estará a lo dispuesto tanto en los apartados anteriores, como a lo dispuesto en las *Prácticas de Certificación* Particulares que correspondan a cada tipo de *Certificado*, que constituyen parte del Addenda de la presente *Declaración de Prácticas de Certificación*.

9.20.1.3 Generación y entrega de *Datos de creación de Firma* e información adicional*:*

a) Garantizar que los procedimientos seguidos aseguran que las *Claves privadas* que constituyan los *Datos de creación de Firma* son generados sin que se realicen copias ni se produzca el almacenamiento de los mismos por parte de la FNMT-RCM.

b) Realizar la comunicación de información al interesado o *Solicitante* de tal forma que se procure su *Confidencialidad*.

c) Poner a disposición del Solicitante (http://www.ceres.fnmt.es) la siguiente información:

a. Instrucciones para el *Suscriptor*, en especial:

La forma en que han de custodiarse los *Datos de creación de Firma*.

Los mecanismos generales que garanticen la fiabilidad de la *Firma electrónica* de un documento a lo largo del tiempo.

El procedimiento para comunicar la pérdida o utilización indebida de dichos *Datos*.

Un listado de *Dispositivos de creación y verificación de Firma* electrónica compatibles con los *Datos de creación y verificación de Firma* generados, y con el *Certificado* expedido.

Las condiciones precisas de utilización del *Certificado*, sus límites de uso y la forma en que garantiza su responsabilidad patrimonial.

b. Una descripción del método utilizado por la FNMT-RCM para comprobar la identidad del *Suscriptor* y aquellos otros datos que figuren en el *Certificado*.

c. Las certificaciones que haya obtenido la FNMT-RCM.

d. El procedimiento aplicable para la resolución de conflictos.

e. Un ejemplar de las presente *Declaración de Prácticas de Certificación*.

9.20.1.4 Conservación de la información por la FNMT-RCM

a) Conservar toda la información y documentación relativa a cada *Certificado*, en las debidas condiciones de seguridad, durante quince (15) años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.

b) Mantener un *Directorio* seguro y actualizado de *Certificados* en el que se identifican los *Certificados* expedidos, así como su vigencia, incluyendo en forma de *Listas de Revocación* la identificación de los *Certificados* que hayan sido revocados o suspendidos. La integridad de este *Directorio* se protegerá mediante la utilización de sistemas conformes con las disposiciones reglamentarias específicas que al respecto se dicten en España, y su acceso, podrá efectuarse según se dispone en el apartado 9.14 y siguientes.

c) Mantener un servicio de consulta sobre la vigencia de los *Certificados*. Este servicio se describe en el apartado "9.14 Procedimiento de consulta del estado de los *Certificados*" del presente documento.

d) Establecer un mecanismo de fechado que permitan determinar con exactitud la fecha y la hora en las que se expidió un *Certificado*, o se extinguió o suspendió su vigencia.

e) Conservar las *DPCs* durante 15 años desde su derogación por publicación de una nueva DPC, en las debidas condiciones de seguridad.

9.20.1.5 Protección de los Datos de Carácter Personal*:*

La FNMT-RCM se compromete a conocer y cumplir la legislación vigente en materia de *Protección de Datos Personales*, fundamentalmente la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. A tal efecto y con carácter enunciativo, se compromete a cumplir con las obligaciones que tal normativa establece en materia de información a los afectados, declaración de ficheros ante la Agencia de Protección de Datos, conservación y acceso a la información, así como con las medidas de seguridad establecidas en el Real Decreto 994/1999. Asimismo, garantiza que la utilización de los datos personales recabados se limitará a aquellas finalidades para las cuales éstos fueron recogidos.

Para informarse sobre la política de protección de datos seguida por la FNMT-RCM, y acerca del uso que de los datos se realiza, se puede consultar el apartado "9.22 Datos de carácter personal" de la presente *Declaración de Prácticas de Certificación.*

9.20.1.6 Suspensión y Revocación de *Certificados:*

Acerca de la suspensión y revocación de *Certificados* y de las obligaciones que la FNMT-RCM se compromete a asumir al respecto, se pueden consultar además de los anexos II a V, los apartados 9.12.3 y 9.12.4 de la presente *Declaración de Prácticas de Certificación.*

9.20.1.7 Cese de la actividad de la FNMT-RCM como *Prestador de Servicios de Certificación:*

A este respecto se puede consultar el apartado "9.18 Cese de la actividad del *Prestador de Servicios de Certificación*": Transferencia de la prestación del servicio de la presente *Declaración de Prácticas de Certificación*.

9.20.2 Obligaciones de la *Oficina de Registro*

i) Con carácter general, seguir los procedimientos establecidos por la FNMT-RCM en la *Declaración de Prácticas de Certificación* y en las *Políticas de Certificación*, en el desempeño de sus funciones de gestión, emisión, renovación y revocación de *Certificados* y no salirse de dicho marco de actuación.

ii) En particular, comprobar la identidad y cualesquiera circunstancias personales de los *Solicitantes* de los *Certificados* relevantes para el fin propio de éstos, utilizando cualquiera de los medios admitidos en Derecho, y conforme a lo previsto con carácter general en la *Declaración de Prácticas de Certificación* y con carácter particular en las correspondientes *Prácticas de Certificación* Particulares adjuntas como Addendum a la misma.

iii) Conservar toda la información y documentación relativa a los *Certificados*, cuya solicitud, renovación, suspensión o revocación gestiona durante quince (15) años.

iv) Permitir a la FNMT-RCM el acceso a los archivos y la auditoría de sus procedimientos en relación con los datos obtenidos en calidad de *Oficina de Registro*.

v) Informar a la FNMT-RCM de cualquier aspecto que afecte a los *Certificados* emitidos por la FNMT-RCM (ej.: solicitudes de emisión, renovación)

vi) Tramitar la formalización de los contratos de emisión de *Certificados* con el *Suscriptor* de los mismos, en los términos y condiciones que establezca la FNMT-RCM.

vii) Comunicar a la FNMT-RCM de forma diligente las solicitudes de emisión de *Certificados*.

viii) Respecto de la extinción de validez de los certificados.

1. Comprobar diligentemente las causas de revocación y suspensión que pudieran afectar a la vigencia de los *Certificados*.
2. Comunicar a la FNMT-RCM de forma diligente las solicitudes de revocación y suspensión de los *Certificados*.

ix) Respecto de la Protección de Datos de Carácter Personal, será de aplicación lo dispuesto en el apartado "9.22 Datos de carácter personal".

9.20.3 Obligaciones del Suscriptor

i) No usar el *Certificado* fuera de la *Comunidad electrónica*, ni de los límites especificados en las *Prácticas de certificación* particulares contenidas en los correspondiente anexos de esta *Declaración de Prácticas de Certificación*.

ii) Aportar información verdadera en la solicitud de los *Certificados*, y mantenerla actualizada.

iii) Actuar con diligencia respecto de la custodia y conservación de los *Datos de creación de Firma* o cualquier otra información sensible como *Claves*, códigos de activación del

Certificado, palabras de acceso, números de identificación personal, etc., así como de los soportes de los *Certificados*, lo que comprende en todo caso, la no revelación de ninguno de los datos mencionados.

iv) Conocer y cumplir las condiciones de utilización de los *Certificados* previstos en la *Declaración de Prácticas de Certificación* y en particular, las limitaciones de uso de los *Certificados*

v) Conocer y cumplir las modificaciones que se produzcan en la *Declaración de Prácticas de Certificación.*

vi) Notificar diligentemente a la FNMT-RCM o a cualquier otra *Oficina de Registro*, las circunstancias o sospecha de pérdida de la *Confidencialidad*, la divulgación, modificación o uso no autorizado de los *Datos de creación de Firma*, solicitando además la revocación del correspondiente *Certificado*.

vii) Revisar la información contenida en el *Certificado*, y notificar a la *Oficina de Registro* cualquier error o inexactitud.

viii) Verificar con carácter previo a confiar en los *Certificados*, la *Firma electrónica reconocida* del *Prestador de Servicios de Certificación* emisor del *Certificado.*

ix) Notificar diligentemente a la FNMT-RCM o a cualquier otra *Oficina de Registro* cualquier modificación de los datos aportados en la solicitud del *Certificado*, solicitando cuando consecuentemente fuere pertinente la revocación del mismo.

x) Devolver o destruir el *Certificado* cuando así lo exija la FNMT-RCM o la *Oficina de Registro*, cuando el *Certificado* caduque, o cuando sea revocado.

9.20.4 Obligaciones del representado

El representado en un *Certificado de Persona jurídica para el ámbito tributario*, o de un *Certificado de Entidad sin Personalidad Jurídica para el ámbito tributario*, independientemente de las obligaciones que correspondan al *Suscriptor* del *Certificado*, deberá solicitar al Departamento CERES de la FNMT-RCM, la revocación del *Certificado*, inmediatamente después a revocar el poder otorgado al representante, o si acuciara cualquier otra causa de revocación al *Certificado.*

9.20.5 Obligaciones de la Entidad usuaria

i) Verificar con carácter previo a confiar en los *Certificados*, la *Firma electrónica reconocida* del *Prestador de Servicios de Certificación* emisor del *Certificado.*

ii) Verificar el estado de los *Certificados* en la cadena de certificación, mediante consulta a las *Listas de Revocación* de *Certificados* o consultar (según se trate respectivamente de una Entidad de Derecho Público o de Derecho Privado) a través del servicio *OCSP* de la FNMT-RCM.

iii) Comprobar las limitaciones de uso del *Certificado* que se verifica.

iv) Conocer las condiciones de utilización del *Certificado* conforme a la presente *Declaración de Prácticas de Certificación.*

v) Notificar a la FNMT-RCM o a cualquier *Oficina de Registro*, cualquier anomalía relativa al *Certificado* y que pueda ser considerada como causa de revocación del mismo, aportando todos los elementos probatorios de los que disponga.

9.21 Responsabilidad de las Partes

NO FORMAN PARTE DE ESTA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN, ni se pueden considerar "Certificados" los denominados "CERTIFICADOS DE COMPONENTES" por no adecuarse al concepto legal de "certificado electrónico" definido por la Ley de firma electrónica 59/2003, de 19 de diciembre. No obstante, se adjuntan provisionalmente como anexo exclusivamente informativo, por ser productos de gran utilidad que forman parte del Catálogo de Servicios de la FNMT-RCM.

Para poder usar *Certificados* emitidos por la FNMT-RCM se deberá previamente formar parte de la *Comunidad Electrónica*, y adquirir la condición de *Entidad usuaria*. Fuera de la *Comunidad Electrónica* no se debe confiar en un certificado o en una firma electrónica que se base en un *Certificado*. En cualquier caso, de producirse esta confianza por parte de un tercero, no se obtendrá cobertura de la presente *Declaración de Prácticas de Certificación*, y se carecerá de legitimidad alguna para reclamar o emprender acciones judiciales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado*.

9.21.1 Responsabilidad del Prestador de Servicios de Certificación

La FNMT-RCM únicamente responde de la correcta identificación personal del *Solicitante*, más no de sus cualidades o cualquier otra información contenida en el *Certificado*. Respecto de esta información, la FNMT-RCM se limita únicamente a expresarla en un *Certificado* para el que se le ha acreditado la identidad de su *Suscriptor* mediante documento público.

Es condición sine qua non para la aplicación de las garantías, obligaciones y responsabilidades, que el daño o el hecho se haya producido en el ámbito de la *Comunidad Electrónica* según se define dicho concepto en esta *Declaración de Prácticas de Certificación*.

La FNMT-RCM únicamente responderá por deficiencias en los procedimientos propios de su actividad como *Prestador de Servicios de Certificación*, y conforme a lo dispuesto en estas *Políticas de Certificación* o en la Ley, mas en ningún otro caso será responsable de las acciones o de las pérdidas en las que incurran los *Suscriptores*, *Entidades usuarias*, o terceros involucrados, que no se deban a errores imputables a la FNMT-RCM en los mencionados procedimientos de expedición y/o de gestión de los *Certificados*.

La FNMT-RCM no responderá ante personas cuyo comportamiento en la utilización de los *Certificados* haya sido negligente, debiendo considerarse a estos efectos y en todo caso como negligencia la falta de observancia de lo dispuesto en la *Declaración de Prácticas de Certificación*, y en especial lo dispuesto en los apartados referidos a las obligaciones y a la responsabilidad de las partes.

La FNMT-RCM no responderá por ningún software que no haya proporcionado directamente.

No obstante, y en concreto respecto del servicio de *Dirección electrónica*, la FNMT-RCM pondrá las medidas de protección generalmente aceptadas para la protección del contenido de la *Dirección electrónica* frente a *Software Malicioso (Malware)* y las mantendrá diligentemente actualizadas para colaborar con los *Usuarios destinatarios* en evitar los daños que este tipo de software puede causar.

La FNMT-RCM no garantiza los algoritmos criptográficos ni responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si guardó la diligencia debida de acuerdo al estado actual de la técnica, y procedió conforme a lo dispuesto en esta *Declaración de Prácticas de Certificación* y en la Ley.

Para todo caso, las cuantías que en concepto de daños y perjuicios debiera satisfacer por imperativo judicial la FNMT-RCM a perjudicados, se limitan a un máximo de SEIS MIL EUROS (6.000€) euros.

9.21.2 Responsabilidad de la Oficina de Registro

En todo caso la FNMT-RCM podrá repetir contra *Oficina de Registro* que hubiera realizado el procedimiento de identificación, si la causa del daño tuviera su origen en la actuación dolosa o culposa de ésta.

9.21.3 Responsabilidad del Solicitante

El *Solicitante* responderá de que la información presentada durante la solicitud del *Certificado*, es verdadera.

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

9.21.4 Responsabilidad del Suscriptor

Será en todo caso obligación del *Suscriptor* y consecuentemente responsabilidad suya, el informar a la FNMT-RCM acerca de cualquier variación de estado o información respecto de lo reflejado en el *Certificado*, para su revocación y nueva expedición.

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

9.21.5 Responsabilidad de la Entidad usuaria

Será responsabilidad de la *Entidad usuaria* la verificación de las *Firmas electrónicas reconocidas* de los documentos, así como de los *Certificados*, no cabiendo en ningún caso presumir la autenticidad de los documentos o *Certificados* sin dicha verificación.

No podrá considerarse que la *Entidad usuaria* ha actuado con la mínima diligencia debida si confía en una firma electrónica basada en un *Certificado* emitido por la FNMT-RCM sin haber observado lo dispuesto en las presente *Declaración de Prácticas de Certificación* y comprobado que dicha firma electrónica puede ser verificada por referencia a una *Cadena de certificación* válida.

Si las circunstancias indican necesidad de garantías adicionales, la *Entidad usuaria* deberá obtener garantías adicionales para que dicha confianza resulte razonable.

Asimismo, será responsabilidad de la *Entidad usuaria* observar lo dispuesto en la presente *Declaración de Prácticas de Certificación* y sus posibles modificaciones futuras, con especial atención a los límites de uso establecidos para los *Certificados* en sus correspondientes *Políticas de Certificación*.

9.22 Datos de Carácter Personal

El régimen de protección de datos de carácter personal derivado de la aplicación de la presente *Declaración de Prácticas de Certificación* y en su caso de la actuación conjunta con cualquier

Administración, será el previsto en la Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en su normativa de desarrollo. Los ficheros serán de titularidad pública y su creación, modificación o supresión se realizará por disposición general publicada en el Boletín Oficial del Estado.

Como consecuencia de la prestación de servicios EIT, las *Oficinas de Registro* podrán acceder al fichero de usuarios de Sistemas Electrónicos, Informáticos y Telemáticos. En cualquier caso, será la FNMT-RCM en su condición de *Responsable del Fichero* la que decida sobre la finalidad, contenido y uso del tratamiento de los datos, limitándose las *Oficinas de Registro*, como *Encargadas del Tratamiento*, a utilizar los datos de carácter personal contenidos en dicho fichero, única y exclusivamente para los fines que figuran en su *Declaración de Prácticas de Certificación*. La *Oficina de Registro* en cumplimiento con lo establecido en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal se compromete a:

- Tratar los datos siguiendo estrictamente las instrucciones de la FNMT-RCM;
- No aplicar o utilizar los datos personales obtenidos, para fines distintos a los que figuren en la presente *Declaración de Prácticas de Certificación*;
- No comunicarlos a terceros, ni siquiera para su conservación;
- Guardar secreto profesional respecto de los mismos, aun después de finalizar sus relaciones con la FNMT-RCM y trasladar las obligaciones citadas en los párrafos anteriores al personal que dediquen al cumplimiento de la presente *Declaración de Prácticas de Certificación.*
- Adoptar las medidas de seguridad de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, tratamiento o acceso no autorizado, de conformidad con lo dispuesto en el Real Decreto núm. 994/1999.
- Destruir o devolver todos los datos de carácter personal objeto de tratamiento una vez finalice por cualquier causa la relación con la FNMT-RCM, salvo aquellos datos que la legislación obliga a conservarlos por un mínimo de quince (15) años.

Sin perjuicio de otras obligaciones, la *Oficina de Registro* verificará que el *Suscriptor* es informado y presta su *Consentimiento* para el tratamiento de sus datos, con las finalidades y comunicaciones previstas en los documentos de *Consentimiento* correspondiente. Asimismo comprobará que se han cumplimentado correctamente todos los campos de datos personales necesarios para la prestación del servicio.

Las *Oficinas de Registro* informarán de esta obligación a todo su personal y responderán de cualquier perjuicio que se le produzca a la FNMT-RCM como consecuencia del incumplimiento de estas obligaciones en la recogida de datos, debiendo asimismo y en este sentido, mantenerla a salvo de reclamaciones de terceros o de sanciones administrativas.

Los datos personales del *Solicitante* una vez validados y su código de solicitud recogido en el paso de Presolicitud, se enviarán a la FNMT-RCM mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM.

La FNMT-RCM no admitirá como *Suscriptor* del *Certificado*, alias, seudónimos o nombres interpuestos distintos de la identidad personal del *Suscriptor* que se recoge en el Documento nacional de Identidad, o Documento de Identificación de Extranjeros.

9.22.1 Información al Suscriptor

De conformidad con lo establecido en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa al *Suscriptor* que los datos de

carácter personal que se incluyan en los formularios o contratos que se le presenten durante su personación a la hora de solicitar la emisión de un *Certificado* se registrarán en el fichero de usuarios de Sistemas Electrónicos, Informáticos y Telemáticos (EIT), creado por la Orden de 26 de Julio de 1999 por la que se regulan las bases de datos y ficheros automatizados de carácter personal existentes en la FNMT-RCM (B.O.E. 05-08-1999) modificada por la Orden de 11 de diciembre de 2001 por la que se regulan los ficheros de datos de carácter personal de la FNMT-RCM (B.O.E. 28-12-2001), y del que será responsable la FNMT-RCM.

La prestación de los servicios EIT solamente podrá realizarse si se cumplimenta y responde en su totalidad y con datos e información verdadera a los formularios. Dichos datos son recogidos con la finalidad de prestar los servicios de certificación en los términos establecidos en la normativa vigente y en la presente *Declaración de Prácticas de Certificación*. Mediante su cumplimentación, el solicitante consiente el tratamiento de sus datos para los usos y finalidades previstas.

Los datos de carácter personal podrán ser comunicados a otras Administraciones Públicas, sus organismos autónomos y demás entidades vinculadas o dependientes dentro del ámbito del artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y de Orden Social, y normativa de desarrollo a los efectos de garantizar la prestación de los servicios de certificación y con la finalidad de comprobar la vigencia de los *Certificados* otorgados a los *Suscriptores*. Asimismo, los datos de carácter personal podrán ser cedidos de acuerdo con el artículo 11.2.c de la *LOPD* en el ámbito privado cuando sean necesarios para el desarrollo, cumplimiento y control de los servicios contratados a la FNMT-RCM y exclusivamente para cumplir con el fin propio para el que ha sido emitido el *Certificado* de acuerdo con la normativa sectorial sobre firma electrónica.

El titular de los datos podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición, dirigiéndose para ello a la Secretaría General de la FNMT-RCM sita en la calle Jorge Juan, numero 106, 28071 de Madrid o bien a través de http://www.ceres.fnmt.es/clase2/iniciomain.htm (modificación de datos personales), sin perjuicio de la obligaciones de conservación que establezca la Ley.

La FNMT-RCM adopta los niveles de seguridad requeridos por el Reglamento de Medidas de Seguridad aprobado por el Real Decreto 994/1999 de 6 de junio.

9.22.2 Información a la Entidad usuaria

Los datos contenidos en el *Directorio* seguro de *Certificados* tienen la consideración de datos de carácter personal a efectos de lo dispuesto en la *LOPD* y demás normativa complementaria, y por este motivo, la FNMT-RCM no permite que sean accedidos.

No obstante, la FNMT-RCM pone a disposición de las *Entidades usuarias* las listas de certificados revocados (que no contiene datos personales) para el cumplimiento diligente de los servicios de certificación de acuerdo con la Orden Ministerial de 11 de diciembre de 2001 por la que se regulan los ficheros de datos de carácter personal de la FNMT-RCM. El usuario como cesionario de esta información únicamente podrá utilizarla de acuerdo con esas finalidades.

No obstante, y con carácter general, cualquier registro o utilización para otros fines distintos de los anteriores o no autorizados requiere del *Consentimiento* previo de los titulares de los datos así como de otras previsiones contempladas en la Ley. Su incumplimiento está sancionado en la *LOPD* con multas que pueden alcanzar los 600.000 euros por cada una de las infracciones cometidas y sin perjuicio de la incoación de acciones penales de acuerdo con el Capitulo I del Título X del Código Penal así como de reclamaciones privadas de los afectados.

9.22.3 *Documento de seguridad LOPD*

A) Objetivo y presentación del Documento de Seguridad LOPD.

El objetivo de este documento es establecer las medidas de seguridad a implantar por la FNMT-RCM en el entorno del *Prestador de Servicios de Certificación*, para la protección de los datos de carácter personal, contenidos en el Fichero de Usuarios de Sistemas Electrónicos, Informáticos y Telemáticos (EIT), que fue registrado en la *APD* el día 6 de agosto de 1999.

La FNMT-RCM como *Prestador de Servicios de Certificación*, precisa disponer de datos de carácter personal de sus usuarios registrados, con el fin de poder identificarlos y proporcionar los *Datos de creación y verificación de Firma* indispensables para relacionarse a través de medios electrónicos, informáticos y telemáticos. Dada la naturaleza de este tipo de datos, según indica el Real Decreto 994/1999 del *Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal*, se deben adoptar medidas de seguridad de nivel medio.

La presente Normativa de Seguridad tiene por objeto preservar los datos personales procesados dentro del *Prestador de Servicios de Certificación* de la FNMT-RCM, por lo que afectará a todos aquellos recursos (personal, máquinas, aplicativos, métodos) que estén implicados en el procesamiento de estos datos. Desde el Sistema de Información que desempeña las funciones de registro de los usuarios, donde se recaban los datos, hasta el almacenamiento y archivo de los mismos en sistemas de Directorio Seguro, incluyendo los interfaces y medios de comunicación entre los diferentes sistemas, ya sean redes telemáticas privadas o públicas.

Este documento es de obligado cumplimiento para todo el personal perteneciente al *Prestador de Servicios de Certificación* de la FNMT-RCM, así como para todas las personas relacionadas con la misma, que requieran acceso a los datos de carácter personal.

La responsabilidad de todos los ficheros que contienen datos de carácter personal declarados por la FNMT-RCM corresponde a dicha entidad, ya que es la persona jurídica que decide sobre la finalidad, usos y contenido de los ficheros. No obstante, en lo que respecta al Fichero de "Usuarios de Sistemas EIT", el Director de Sistemas de Información de la FNMT-RCM es la persona facultada para decidir y autorizar sobre el uso y tratamiento de éste en representación de la FNMT-RCM.

Dentro del ámbito se incluyen las *Oficinas de Registro* como entidades colaboradoras de la FNMT-RCM como *Prestador de Servicios de Certificación*, que tienen la misión de llevar a cabo la identificación y autenticación del ciudadano, registrando sus datos personales con destino al *Prestador de Servicios de Certificación* de la FNMT-RCM.

B) Normas y estándares

Las leyes, normas y estándares que han sido considerados para la elaboración de este documento, son:

Directivas Europeas

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de esos datos.
- Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

Legislación Española

- Real Decreto 1736/1998, de 31 de julio, que desarrolla el Título III de la Ley General de Telecomunicaciones (Reglamento de Servicio Público).
- Ley Orgánica 13/1995, de 21 de abril, de regulación del uso de informática en el tratamiento de datos personales de la Comunidad de Madrid.
- Real Decreto 994 / 1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

C) Principios y normas de obligado cumplimiento

Este apartado recoge todos aquellos aspectos necesarios de obligado cumplimiento que dan respuesta a los apartados establecidos en el *artículo 8 del Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.*

Funciones y obligaciones del personal

Este Documento así como cualquier nueva versión del mismo, es conocido por todas las personas pertenecientes al *Prestador de Servicios de Certificación* de la FNMT-RCM o que tienen obligación de tratar con dichos datos de carácter personal.

Existen una serie de funciones claramente diferenciadas en lo que respecta al personal implicado en el uso y tratamiento de los datos de carácter personal del Fichero de Usuarios de Sistemas EIT, como son: El *Responsable del Fichero*, el *Responsable de Seguridad*, el *Personal de Seguridad Informática*, *Administrador de la Aplicación*, *Usuarios de la Aplicación*, *Operador de backup*, *Auditor de Seguridad*. Estas funciones y, en su caso las personas que las asumen, se definen en el punto "*Documento de Seguridad LOPD*" del apartado "1. Definiciones" de la presente *Declaración de Prácticas de Certificación*.

D) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan

La estructura de los ficheros de carácter personal utilizados por el *Prestador de Servicios de Certificación* de la FNMT-RCM, es la que se recoge en el Fichero de Usuarios de Sistemas EIT, que ha sido declarado a la *Agencia de Protección de Datos* con fecha de 6 de agosto de 1999. Esta estructura es la siguiente:

- Datos de carácter identificativo:
  - D.N.I./N.I.F.,
  - Nombre y apellidos,
  - Teléfono,
  - Dirección,
  - Dirección de correo electrónico,
  - Razón social.
- Datos de características personales:
  - *Datos de verificación de firma* y número de serie del *Certificado*.
- Datos de circunstancias sociales:
  - Atributos relativos a la capacidad y poder de representación.

- Datos de información comercial:
  - Dirección electrónica (URL).

En la Política de backup / recuperación del *Prestador de Servicios de Certificación* se han definido seis tipos diferentes de datos, atendiendo a sus requerimientos de copia y respaldo. Todos los datos tratados por la *Infraestructura de Clave Pública* han sido clasificados en alguno de estos "Tipos".

Los Tipos que se refieren a datos personales son los siguientes:

TIPO 3. **Información de auditoría**: Muestran el funcionamiento de los sistemas y entornos de aplicación a lo largo del tiempo, y constituyen evidencias y rastros de las acciones que se están realizando y las aplicaciones que se ejecutan. Por lo tanto puede contener información relativa a datos personales de sus clientes.

TIPO 5. **Datos personales**: Datos asociados a personas físicas identificadas o identificables, ya sean considerados privados o públicos.

TIPO 6. **Claves**: Básicamente, se engloban en esta categoría las claves maestras de acceso a los sistemas y entornos de aplicación, claves críticas de los sistemas, claves de administración y usuarios de emergencia. Su uso es ocasional.

Los subsistemas que tiene algún tipo de implicación en el tratamiento de los datos de carácter personal, se relacionan y describen de forma resumida a continuación:

Subsistema de Gestión de *Certificados*

Cuya misión es la creación de los *Certificados* de acuerdo al estándar *X.509*, donde se introducen las *Claves* creadas por el subsistema de generación de *Claves* y otros datos identificativos.

Subsistema de *Oficina de Registro*

Tiene como objetivo la identificación y autenticación del *Suscriptor*, donde son registrados sus datos personales para proceder a su envío, de forma cifrada, al *Prestador de Servicios de Certificación* de la FNMT-RCM.

Subsistema de Publicación

Tiene como misión la gestión de la publicación del *Directorio* del *Prestador de Servicios de Certificación* de la FNMT-RCM y las *Listas de Revocación.*

E) Procedimiento de notificación, gestión y respuesta ante las incidencias

Los datos de carácter personal subyacen en *Certificados*, estructurados de acuerdo al estándar *X.509*, siendo algunos de estos datos de uso público.

El procedimiento de alta, baja y rectificación de los datos de carácter personal está formalizado. Puede ser ejercido en la Secretaría General de la FNMT-RCM o en la página web del *Prestador de Servicios de Certificación* de la FNMT-RCM.

Las incidencias de destrucción accidental de información de los datos de carácter personal se solucionan con copias de seguridad dotadas de *Disponibilidad*, almacenadas y gestionadas de forma adecuada y debidamente protocolizada.

Existe una base de datos de incidencias con la que se abren y se gestionan las incidencias. Cada persona puede realizar diferentes gestiones en función del rol que desempeñen. De modo resumido, cualquier persona perteneciente al PSC puede abrir una incidencia, éstas son tratadas por personal del área correspondiente y una vez resuelta se cierra con la descripción de las acciones realizadas.

En caso de que la incidencia conlleve modificaciones se abre una acción correctiva que es ejecutada por el personal al que compete la acción.

Los principales campos de una incidencia son:

- Nombre de la incidencia (breve descripción)
- Persona que abre la incidencia, fecha de apertura
- Área a la que, en principio, compete la incidencia
- Prioridad
- Tipo (en general se corresponde con el Hardware/Software afectado)
- Descripción (descripción detallada de la incidencia)
- Acciones (acciones realizadas para solucionar la incidencia
- Registro de personas que manejan la incidencia

F) Procedimientos de copias de seguridad y recuperación de datos

Las características que se han definido para la realización de copias de seguridad, tienen en cuenta los siguientes factores:

- Periodicidad de la copia de seguridad (frecuencia con la que deben realizarse)
- Duración de las copias de seguridad (tiempo que deberán mantenerse las copias)
- Tipo *de copia de seguridad* (total o incremental)
- Almacenamiento (destino de las copias de seguridad)
- Cifrado (dota de *Confidencialidad*)
- Firmado (dota de *Integridad* y autenticidad)

Concretamente para los datos de Tipo 5, es decir, datos de carácter personal, se han definido las siguientes características:

- *Periodicidad de la copia de seguridad:* Se realizará como mínimo, una copia diaria de seguridad y respaldo de estos datos, cumpliendo lo exigido por el Reglamento de Medidas de Seguridad.
- *Duración de las copias de seguridad:* Las copias de seguridad se almacenarán un período de siete días laborables.
- *Tipo de copia de seguridad:* Las copias de backup se realizarán siempre completas.
- *Almacenamiento:* Las copias de seguridad y respaldo se almacenarán en el archivo ignífugo de alta seguridad del *Prestador de Servicios de Certificación* de la FNMT-RCM.
- *Cifrado:* La información no irá cifrada
- *Firmado:* La información no irá firmada.

La información detallada sobre estas clasificaciones se encuentra en el Plan de Seguridad del *Prestador de Servicios de Certificación* de la FNMT-RCM. En el *Manual de Seguridad* se definen

los responsables de las copias, quienes pueden acceder a ellas y a quién deben comunicárselo en caso de incidencia.

Mayor nivel de detalle sobre este proceso se encuentra descrito en el documento sobre la política de copias seguridad, respaldo y recuperación de la infraestructura denominado "Política de backup / recuperación".

G) Control de acceso

Sólo se tiene acceso a los datos de acuerdo al perfil asignado y siempre que dicho acceso sea necesario para el desempeño de las distintas funciones.

Por ejemplo, la *Oficina de Registro* debe proporcionar los requerimientos de control de acceso al sistema de información del *Prestador de Servicios de Certificación* de la FNMT-RCM a los registradores, proporcionándoles el nivel de acceso para llevar a cabo la función de registro.

- Control de acceso basado en perfiles: usando la identidad o el perfil del usuario del sistema, que solicita un acceso, junto con el modo de acceso solicitado.
- Se permitirá el acceso siempre que el usuario identificado solicite un modo de acceso que haya sido autorizado previamente; de lo contrario, se denegará.

El *Responsable del Fichero* ha establecido mecanismos para evitar que un usuario pueda acceder a datos de carácter personal con derechos distintos al permitido y para impedir el intento reiterado de acceso no autorizado al sistema de información.

H) Régimen de trabajo fuera de los locales de la ubicación del fichero

Todos los trabajos sobre los datos personales se llevan a cabo en el centro de trabajo de la FNMT-RCM como *Prestador de Servicios de Certificación.*

Tal como se ha comentado en el apartado anterior la función de registro se lleva a cabo en las *Oficinas de Registro* por personas debidamente autorizadas.

I) Ficheros temporales

El software disponible para el tratamiento de datos de carácter de personal necesarios para crear un certificado electrónico de acuerdo al estándar *X.509* genera ficheros temporales (ficheros de logs) que son debidamente custodiados ante la necesidad de trazabilidad de la instalación por la actividad de prestador de servicios de certificación en cumplimiento de la Ley de firma electrónica 59/2003, de 19 de diciembre.

En cualquier caso, estos ficheros tienen el mismo nivel de seguridad que el fichero declarado y por tanto se les aplica los mismos controles de seguridad.

J) Gestión de soportes

Los soportes informáticos que contienen datos de carácter personal están diligentemente identificados, pudiéndose identificar el tipo de información que contienen. Asimismo son almacenados en un lugar de acceso restringido al personal autorizado y custodiado por el personal de seguridad.

En el caso de que se produjese una salida de un soporte informático que contenga datos de carácter personal fuera del centro de trabajo del a *Prestador de Servicios de Certificación* de la FNMT-RCM, únicamente podrá ser autorizada por el *Responsable del Fichero*.

La destrucción de soportes se realiza previa baja de dicho soporte de la "aplicación de backup" (aplicación de copia de seguridad y respaldo) (que actúa como inventario de soportes) y consiste en

la destrucción física del soporte (extracción de la cinta magnética de su contenedor y triturado de la misma).

Existe un sistema de registro de entrada de soportes, que permite directa o indirectamente conocer:

- El tipo de soporte.
- La fecha y hora de entrada.
- El emisor.
- El número de soportes.
- El tipo de información que contiene.
- La forma de envío.
- La persona responsable de recibir la información, que en todo caso está debidamente autorizada por el Responsable del Fichero

Asimismo, existe un sistema de registro de salida de soportes, que permite directa o indirectamente conocer:

- El tipo de soporte.
- La fecha y hora de salida.
- El destinatario.
- El número de soportes.
- El tipo de información que contiene.
- La forma de envío.
- La persona responsable de la entrega, que en todo caso está debidamente autorizada por el *Responsable del Fichero*

Cuando un soporte vaya a ser desechado o reutilizado se seguirá el procedimiento previsto para impedir cualquier recuperación posterior de la información almacenada en él. Este procedimiento se seguirá previamente a que se proceda a la baja del soporte en el Inventario.

Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

K) Auditoría

Para el cumplimiento de todos los aspectos señalado en la *LOPD* se llevará a cabo una auditoría que verifique el cumplimiento de las normas e instrucciones indicadas en este documento. Esta auditoría se llevará a cabo al menos una vez cada dos (2) años.

Este informe de auditoría, hace referencia a la adecuación de las normas e instrucciones indicadas en este documento, identificando las debilidades y proponiendo las acciones correctoras pertinentes. Asimismo, en el informe, se incluyen los datos, hechos y observaciones en que se base el informe realizado, así como las recomendaciones propuestas.

L) Acceso Lógico

Existen varios tipos de acceso lógico al fichero:

- Acceso con usuario y contraseñas (paswords): acceso en el que un usuario de la aplicación busca la *Clave Pública* de un *Suscriptor* partiendo de los datos de identificación del mismo (*"serial number"* del *Certificado*, *"common name"*, etc.).
- Acceso privilegiado al *Directorio* o base de datos, donde se encuentran almacenados todos los datos de carácter personal. Para realizar este tipo de acceso, es necesario realizar un alta en la aplicación, de acuerdo a lo dispuesto en la normativa de seguridad del *Prestador de Servicios de Certificación* de la FNMT-RCM.

Los parámetros que están configurados y que incluyen lo exigido por el Reglamento de la *LOPD* son los que ha continuación se describen:

- Cada usuario se identifica ante la aplicación con un nombre de usuario, que es único para cada persona.
- Todo usuario para autenticarse debe introducir una contraseña, que únicamente debe conocer el usuario que pretende autenticarse. Cada usuario es responsable de su contraseña y no debe compartirla con ningún otro.
- No se han creado grupos de personas que puedan acceder con un mismo usuario y contraseña, y tampoco existen usuarios genéricos. Las cuentas genéricas que se creen para pruebas o similares se eliminan inmediatamente después de realizar dichas pruebas.
- Cada usuario es libre de cambiar su contraseña si cree que esta puede estar comprometida, pero para ello debe haberla utilizado al menos durante un día. Sin perjuicio de lo anterior, el usuario tiene la obligación de no usar la misma contraseña durante un periodo superior a tres (3) años.
- Cuando un usuario se identifica y auténtica mas de tres veces de forma errónea el sistema bloquea la cuenta de dicho usuario.
- Existe un mecanismo de control: el Registro de Eventos, encargado de almacenar, entre otra información, todos los accesos a los distintos componentes de la infraestructura

M) Acceso Físico

Solo el personal debidamente autorizado tiene acceso físico a los locales donde se encuentran ubicados los sistemas de información con datos de carácter personal, esto es, al CPD del *Prestador de Servicios de Certificación* de la FNMT-RCM.

Para acceder a estas instalaciones, se dispone de un sistema de control de acceso mediante lectores de tarjeta y teclados.

Periódicamente, se lleva a cabo un control de los registros de eventos generados por el Sistema de control de acceso, que permitirá detectar cualquier tipo de anomalía en la operativa diaria.

N) Pruebas con datos reales

Las pruebas en el desarrollo de las aplicaciones que tratan el Fichero EIT, no se hacen con datos reales.

Los distintos aplicativos que requieren acceso a dicho fichero se realizan con carga de datos de prueba.

M) Proceso de revisión

El apartado "9.22.3 Documento de Seguridad *LOPD*" ha sido confeccionado para cumplir con el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

El Documento se mantendrá actualizado. Todas las modificaciones que se produzcan como consecuencia de mejoras o adaptación por normativa legal se incorporarán al Documento.

9.23 Propiedad Intelectual e Industrial

La FNMT-RCM es titular en exclusiva de todos los derechos, incluidos los derechos de explotación, sobre el *Directorio* seguro de *Certificados* y *Listas de Revocación* en los términos señalados en el Texto Refundido de la Ley de Propiedad Intelectual aprobado mediante Real Decreto Legislativo 1/1996, de 12 de abril (Ley de Propiedad Intelectual), incluido el derecho *sui generis* reconocido en el artículo 133 de la citada Ley. En consecuencia, el acceso a los *Directorios* seguros de *Certificados* queda permitido a los miembros de la *Comunidad Electrónica* legitimados para ello, quedando prohibida cualquier reproducción, comunicación pública, distribución, transformación o reordenación salvo cuando esté expresamente autorizada por la FNMT-RCM o por la Ley. Queda asimismo prohibida la extracción y/o reutilización de la totalidad o de una parte sustancial del contenido, ya sea considerada como tal desde una perspectiva cuantitativa o cualitativa, así como su realización de forma repetida o sistemática.

La FNMT-RCM mantiene todo derecho, título y participación sobre todos los derechos de propiedad intelectual e industrial relativos a la presente *Declaración de Prácticas de Certificación*, los servicios que preste, y los programas de ordenador o hardware que utilice en dicha prestación de servicios.

Asimismo, tanto la *Tarjeta criptográfica* utilizada como soporte para almacenar los *Certificados* y *Claves* criptográficas, como la información generada mediante la prestación de los servicios por la FNMT-RCM será en todo momento propiedad exclusiva de la FNMT-RCM.

Respecto de la *Tarjeta criptográfica*, la FNMT-RCM otorga únicamente un derecho de uso a los *Suscriptores* de los *Certificados*, para que la utilicen como soporte para almacenar y utilizar los *Certificados* y *Claves* criptográficas emitidos por la FNMT-RCM o por otro *Prestador de Servicios de Certificación*.

Los *OID* utilizados tanto en los *Certificados* como para el almacenamiento de ciertos objetos en el *Directorio*, son propiedad de la FNMT-RCM y han sido registrados en el IANA (Internet Assigned Number Authority) bajo la rama iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 - IANA-Registered Private Enterprises), habiéndose asignado el número 1.3.6.1.4.1.5734 (FABRICA NACIONAL DE MONEDA Y TIMBRE - REAL CASA DE LA MONEDA). Esto puede ser consultado y comprobado en:

http://www.iana.org/assignments/enterprise-numbers

Queda prohibido, de no mediar un acuerdo expreso y firmado con la FNMT-RCM, el uso total o parcial de cualquiera de los *OID* asignados a la FNMT-RCM salvo para los menesteres específicos para los que se incluyeron en el *Certificado* o en el Directorio.

Queda prohibida la reproducción o copia incluso para uso privado de la información que pueda ser considerada como Software o Base de Datos de conformidad con la legislación vigente en materia de Propiedad intelectual, así como su comunicación pública o puesta a disposición de terceros.

Queda prohibida cualquier extracción y/o reutilización de la totalidad o de una parte sustancial de los contenidos o de las bases de datos que la FNMT-RCM ponga a disposición de los *Suscriptores* o *Entidades usuarias*.

10 ORDEN DE PRELACIÓN

Las distintas *Prácticas de Certificación* Particulares que forman parte del Addenda de la presente *Declaración de Prácticas de Certificación*, tendrán prevalencia en lo que corresponda con carácter particular y referido a sus tipos de *Certificados*, sobre lo dispuesto en el cuerpo principal de la presente *Declaración de Prácticas de Certificación*.

El anexo V "Prácticas de Certificación particulares de los certificados de componentes", el apartado I.2 "I.2 Política de Certificación para certificado de componentes de la FNMT-RCM" del anexo I, se exponen a título informativo, no siendo parte integrante de esta *Declaración de Prácticas de Certificación.*

11 LEY APLICABLE , INTERPRETACIÓN Y JURISDICCIÓN COMPETENTE

La *Declaración de Prácticas de Certificación*, se regirá por lo dispuesto por la Ley del Reino de España.

Las partes intervinientes acuerdan que todo litigio, discrepancia, cuestión o reclamación resultante de la ejecución o interpretación de la presente *Declaración de Prácticas de Certificación* o relacionada con él, directa o indirectamente, se resolverá de la siguiente manera dependiendo del producto o servicio de que se trate:

Certificado de identidad de persona física:

Se resolverá definitivamente mediante arbitraje de Derecho, en el marco de la Corte de Arbitraje de la Cámara Oficial de Comercio e Industria de Madrid, a la que se encomienda la administración del arbitraje y la designación de los árbitros de acuerdo con su Reglamento y Estatutos. Igualmente las partes hacen constar expresamente su compromiso de cumplir el laudo arbitral que se dicte, de conformidad Real Decreto 292/2004, de 20 de febrero.

Resto de productos y servicios:

La Ley del Reino de España será la que rija el cumplimiento, interpretación, integración y validez de la presente *Declaración de Prácticas de Certificación*. Esta elección de Derecho aplicable se realiza para asegurar los procedimientos y una interpretación uniforme para todos los *Suscriptores* y *Entidades Usuarias* en general, con independencia de su lugar de residencia o de donde sea utilizado el *Certificado*.

12 MODIFICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Los procedimientos contenidos en la presente *Declaración de Prácticas de Certificación* podrán ser modificados unilateralmente por la FNMT-RCM. Será obligación de la *Entidad usuaria* de Derecho Privado y del *Suscriptor*, comprobar regularmente la publicación de esta *Declaración de Prácticas de Certificación* de la FNMT-RCM, para detectar las posibles variaciones.

No obstante, de cara a facilitar a los *Usuarios destinatarios* (*Entidad usuaria* y *Suscriptor*) el conocimiento de la existencia de novedades, cuando las modificaciones practicadas en la *Declaración de Prácticas de Certificación* afecten directamente a los derechos y obligaciones de las partes integrantes de la *Comunidad Electrónica*, o bien restrinjan el ámbito de aplicación de los *Certificados*, la FNMT-RCM notificará en la *Dirección electrónica* de los interesados con una antelación mínima de treinta (30) días a la entrada en vigor de los cambios. (A este respecto, ténganse en cuenta los apartados "9.1 *Servicio de dirección electrónica*" y "9.2 *Servicio de notificación* de la FNMT-RCM" de la presente *Declaración de Prácticas de Certificación*)

Pasados quince (15) días desde el envío de la notificación sin que la FNMT-RCM obtenga respuesta del titular de la *Dirección electrónica*, se considerará que la modificación ha sido aceptada.

En caso contrario, de obtenerse una notificación no aceptando las modificaciones, se entenderá que el titular de la *Dirección electrónica* desiste unilateralmente del contrato que le vincula con la FNMT-RCM, así como con la *Comunidad Electrónica*, sin que quepa reclamación alguna por parte de los suscriptores u obligación de indemnizar por daños y perjuicios por estas causas. A este respecto, recordamos que la extinción de este contrato es uno de los supuestos comprendidos en el apartado "9.12.3.1 Causas de Revocación de *Certificados*" como causa de revocación del *Certificado* por parte de la FNMT-RCM.

ANEXO I. POLÍTICAS DE CERTIFICACIÓN DE LA FNMT-RCM

I.1 POLÍTICA DE CERTIFICACIÓN PARA CERTIFICADOS RECONOCIDOS DE LA FNMT-RCM

I.1.1 TIPOLOGIA DE LOS CERTIFICADOS RECONOCIDOS DE LA FNMT-RCM

Los *Certificados* expedidos por la FNMT-RCM bajo esta *Política de Certificación* vinculan a su *Suscriptor* unos *Datos de verificación de Firma* y confirman su identidad.

Estos *Certificados*, son expedidos como *Certificados Reconocidos* con base en los criterios establecidos para tal en la Ley de Firma Electrónica (Ley 59/2003) y en la normativa técnica EESSI, concretamente ETSI TS 101 456 - "Policy requirements for certification authorities issuing qualified certificates" en su apartado 8 "Framework for definition of other qualified certificate policies" y ETSI TS 101 862 – "Qualified Certificate Profile", tanto en lo referente al *Prestador de Servicios de Certificación* como a la generación de los *Datos de creación de Firma* y al contenido de los propios *Certificados*.

La FNMT-RCM expide bajo esta *Política de Certificación* los siguientes tipos de *Certificados*:

- *Certificado de identidad de persona física*: También denominado *Certificado de usuario de la FNMT-RCM (Clase 2 CA)*, es la certificación electrónica expedida por la FNMT-RCM que vincula a su *Suscriptor* unos *Datos de verificación de Firma* y confirma su identidad. En estos *Certificados*, el *Suscriptor* sólo lo podrá ser una persona física.

I.1.2 IDENTIFICACIÓN

La presente *Política de Certificación* de la FNMT-RCM para la expedición de *Certificados Reconocidos* tiene la siguiente identificación:

Nombre	Política de Certificación de Certificados Reconocidos de la FNMT-RCM
Referencia/OID	1.3.6.1.4.1.5734.3.5
Versión	1.0
Fecha de Emisión	1 de Enero de 2004
DPC relacionada	Declaración de Prácticas de Certificación de la FNMT-RCM OID: 1.3.6.1.4.1.5734.4 Localización: http://www.cert.fnmt.es/convenio/dpc .pdf
Localización	http://www.cert.fnmt.es/convenio/dpc.pdf

I.1.3 GESTIÓN DE LA POLÍTICA DEL CERTIFICADO

La FNMT-RCM dispone de una *Política de Certificación* efectiva y, en particular, declara que:

- La FNMT-RCM tiene capacidad para especificar, revisar, y aprobar la *Política de Certificación* de los *Certificados Reconocidos*, a través de su Dirección General.
- La FNMT-RCM dispone de una *Declaración de Prácticas de Certificación* en la que se detallan las prácticas de certificación empleadas para la expedición de Certificados Reconocidos conformes a la Política de Certificación aquí expuesta.
- La FNMT-RCM dispone, dentro de las competencias de la Dirección, de capacidad, para especificar, revisar y aprobar los procedimientos de revisión y mantenimiento tanto para la *Declaración de Prácticas de Certificación* como para la *Política de Certificación*.
- La FNMT-RCM realiza análisis de riesgos para evaluar las amenazas del sistema y proponer las medidas de seguridad adecuadas (salvaguardas) para todas las áreas implicadas.
- La *Declaración de Prácticas de Certificación* se pone a disposición del público mediante el URL: http://www.cert.fnmt.es/convenio/dpc.pdf
- La *Política de Certificación* de *Certificados reconocidos* se pone a disposición del público mediante el URL: http://www.cert.fnmt.es/convenio/dpc.pdf
- Esta *Política de Certificación* recoge las obligaciones y responsabilidades de las partes implicadas en la emisión y uso de los *Certificados Reconocidos* emitidos por la FNMT-RCM bajo a esta *Política de Certificación.*
- Se dispone de un *OID* específico para identificar la *Política de Certificación* aquí desarrollada, siendo el *OID* asignado en el marco de la numeración de la FNMT-RCM: 1.3.6.1.4.1.5734.3.5.
- La *Política de Certificación* de la FNMT-RCM para el presente certificado reconocido se define en ETSI TS 101456, apartado 8 cumpliéndose los requisitos expuestos en los apartado 6 y 7 con las exclusiones señaladas en el apartado 8.2 (que se exponen en el apartado ***Exclusiones y Requisitos Adicionales a ETSI TS 101456*** de la presente *Política de Certificación*). En caso de discrepancia entre este documento y la referida norma, prevalecerá este documento.

I.1.4 COMUNIDAD Y ÁMBITO DE APLICACIÓN

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

a) Son expedidos como *Certificados Reconocidos* con base en los criterios establecidos para tal en la Ley de Firma Electrónica (Ley 59/2003) y en la normativa técnica EESSI ETSI TS 101 862 – "Qualified Certificate Profile".

b) Son expedidos por la FNMT-RCM como *Prestador de Servicios de Certificación* cumpliendo con los criterios establecidos en la Ley de Firma Electrónica (Ley 59/2003) y en la normativa técnica EESSI, concretamente ETSI TS 101 456 - "Policy requirements for certification authorities issuing qualified certificates".

c) La *Tarjeta criptográfica* CERES utilizada como *Dispositivo seguro de creación de Firma*, cumple con los criterios establecidos en la Ley de Firma Electrónica (Ley 59/2003) para tales dispositivos.

d) Los *Certificados* emitidos bajo esta *Política de Certificación* son expedidos para *Entidades usuarias* que forma parte de la *Comunidad Electrónica* tal y como se define en el apartado ***Definiciones*** de la *Declaración de Prácticas de Certificación de la FNMT-RCM.*

I.1.5 RESPONSABILIDAD Y OBLIGACIONES DE LAS PARTES

Esta *Política de Certificación* recoge las obligaciones y responsabilidades de las partes implicadas en la emisión y uso de los *Certificados*, emitidos bajo esta *Política de Certificación.*

Por otro lado, los límites de uso quedan descritos en el apartado "Límites de uso del *Certificado*" de las distintas *Prácticas de Certificación* particulares (anexo I a IV) de los distintos tipos de *Certificados* que la FNMT-RCM expide bajo la presente *Política de Certificación.*

I.1.5.1 Obligaciones de la FNMT-RCM como Prestador de Servicios de Certificación

Las obligaciones propias de la FNMT–RCM como *Prestador de Servicios de Certificación* quedan expuestas en el apartado "9.20 "Obligaciones y garantías de las partes" de la *Declaración de Prácticas de Certificación de la FNMT-RCM.*

I.1.5.2 Obligaciones del Suscriptor y de las Entidades usuarias

Las obligaciones propias de los Suscriptores de Certificados emitidos por la FNMT–RCM bajo la presente Política de Certificación quedan expuestas en el apartado "9.20 Obligaciones y garantías de las partes" de la *Declaración de Prácticas de Certificación de la FNMT-RCM.*

I.1.5.3 Responsabilidades

Las responsabilidades de las partes implicadas en la expedición y uso de los *Certificados* emitidos bajo la presente *Política de Certificación* quedan expuestas en el apartado "9.21 Responsabilidad de las partes" de la *Declaración de Prácticas de Certificación* de la FNMT-RCM.

I.1.6 REQUERIMIENTOS DE LAS PRÁCTICAS DE LA FNMT-RCM COMO AUTORIDAD DE CERTIFICACIÓN

I.1.6.1 Declaración de Prácticas de Certificación

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 regulación de la prestación de los servicios de certificación por parte de la FNMT-RCM en su condición de *Prestador de Servicios de Certificación*, recogiendo en concreto la siguiente información:

- Las obligaciones que se compromete a cumplir en relación con la gestión de los *Datos de creación* y *verificación de Firma* y de los *Certificados.*
- Las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los *Certificados* y, en su caso, la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata y confidencial sobre la vigencia de los poderes indicados en los *Certificados* y que deban figurar preceptivamente inscritos en dichos registros.
- Detalles del régimen de responsabilidad aplicable a los miembros de la *Comunidad Electrónica.*
- Los controles de seguridad aplicados a sus procedimientos e instalaciones en aquello que pueda ser publicado, sin perjudicar la eficacia de los mismos, y las normas de secreto y confidencialidad, así como cuestiones relativas a la propiedad de sus bienes y activos, a la protección de datos de carácter personal, y demás cuestiones de tipo informativo que considere interesante poner a disposición del público.
- Definición de los procedimientos de revisión de dicha *Declaración de Prácticas de Certificación.*

I.1.6.2 Infraestructura de Clave Pública. Gestión del ciclo de vida de las *Claves*

I.1.6.2.1 Generación de las *Claves* de los *Prestadores de Servicios de Certificación*

Las *Claves* de la FNMT-RCM como *Prestador de Servicios de Certificación*, son generadas en circunstancias completamente controladas, en un entorno físicamente seguro y al menos por dos personas autorizadas para ello, utilizando sistemas hardware y software que cumplen con la normativa actual en materia de protección criptográfica, tal y como se muestra en el apartado "6.3.1 Gestión del ciclo de vida de las *Claves* del *Prestador de Servicios de Certificación*" de la *Declaración de Prácticas de Certificación.*

I.1.6.2.2 Almacenamiento, salvaguarda y recuperación de las *Claves* del *Prestador de Servicios de Certificación*

La FNMT-RCM utiliza los mecanismos necesarios para mantener su *Clave privada* confidencial y mantener su integridad en la forma que se muestra en el apartado "6.3.1 Gestión del

ciclo de vida de las *Claves* del *Prestador de Servicios de Certificación***"** de la *Declaración de Prácticas de Certificación.*

I.1.6.2.3 Distribución de los Datos de verificación de Firma del Prestador de Servicios de Certificación

La FNMT-RCM utiliza los mecanismos necesarios para mantener la integridad y autenticidad de su *Clave Pública*, así como su distribución en la forma que se muestra en el apartado "6.3.1 Gestión del ciclo de vida de las *Claves* del *Prestador de Servicios de Certificación***"** de la *Declaración de Prácticas de Certificación*.

I.1.6.2.4 Almacenamiento, salvaguarda y recuperación de las *Claves Privadas* de las *Entidades usuarias*

La FNMT-RCM bajo ningún concepto genera ni almacena las *Claves Privadas* de las *Entidades usuarias*, las cuales son generadas bajo su exclusivo control, y cuya custodia está bajo su responsabilidad.

I.1.6.2.5 Uso de los Datos de creación de Firma del Prestador de Servicios de Certificación

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:

- Firma de certificados.
- Firma de las *Listas de Revocación.*

I.1.6.2.6 Fin del ciclo de vida de las Claves del *Prestador de Servicios de Certificación*

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.

I.1.6.2.7 Ciclo de vida del hardware criptográfico utilizado para firmar *Certificados*

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 durante todo su ciclo de vida, estando situado dicho componente en un entorno físicamente seguro desde su recepción hasta su destrucción llegado el caso.

I.1.6.2.8 Servicios de Gestión de las *Claves* de las *Entidades usuarias*

La FNMT-RCM bajo ningún concepto genera ni almacena las *Claves Privadas* de las *Entidades usuarias*, que son generadas bajo su exclusivo control y cuya custodia esta bajo su responsabilidad.

I.1.6.2.9 Preparación de los Dispositivos seguros de creación de Firma

La FNMT-RCM proporciona a las *Entidades usuarias* que así lo requieran, *Tarjetas criptográficas* para la generación de sus *Claves Privadas* y el almacenamiento de los *Certificados*.

La *Tarjeta criptográfica* es entregada a la *Entidad usuaria* sin ningún tipo de contenido, con las utilidades software necesarias para conseguir una integración con los *navegadores* más utilizados. Así mismo, en el mismo momento se le proporcionan los códigos necesarios para el acceso a dicha tarjeta para que posteriormente desde su puesto, la *Entidad usuaria* genere sus *Claves* e inserte el *Certificado* en ella si así lo desea.

Todo esto se hace para ayudar a las *Entidades usuarias* a que cumpla con su obligación de mantener el "exclusivo control" sobre los *Datos de creación de Firma*.

I.1.6.3 Infraestructura de *Clave Pública*. Gestión del ciclo de vida de los *Certificados*

I.1.6.3.1 Registro de las *Entidades usuarias*

Con carácter previo al establecimiento de cualquier relación contractual con las *Entidades usuarias* la FNMT-RCM informa a las interesadas en adquirir este estatus, acerca de las condiciones del servicio, así como de la obligaciones, garantías y responsabilidades que asumen las partes implicadas en la expedición y uso de los *Certificados* emitidos por el *Prestador de Servicios de Certificación* de la FNMT-RCM.

La FNMT-RCM en su actividad como *Prestador de Servicios de Certificación* procede, por ella misma o por terceros con los que tenga firmados convenios de colaboración, a confirmar la identidad de los *Solicitantes* de *Certificados* mediante presencia física ante las *Oficinas de Registro* y comprobación de los documentos necesarios para tal propósito, siendo esta documentación diferente según se trate de una persona física, jurídica o cuando el *Solicitante* actúe en representación de tercero.

La FNMT-RCM recabará de los *Solicitantes* solo aquella información que sea necesaria para la expedición de los *Certificados* y para la comprobación de la identidad, almacenándolos datos un periodo de quince (15) años y tratándolos con la debida diligencia para el cumplimiento de la legislación nacional vigente en materia de protección de datos personales (a este respecto véase lo dispuesto en los apartados "9.22 Datos de Carácter Personal" y "9.20.1.5 Protección de los Datos de Carácter Personal").

La FNMT-RCM, dado que en su actividad como *Prestador de Servicios de Certificación* no genera el par de *Claves* de las *Entidades usuarias*, pone todos los mecanismos necesarios durante el proceso de *Solicitud de Certificados* para posibilitar que el *Solicitante* se encuentra en posesión de la *Clave Privada* asociada a la *Clave Pública* que se certificará.

Las *Prácticas de Certificación* puestas en funcionamiento para la gestión expuesta puede verse con detalle en el documento *Declaración de Prácticas de Certificación de la FNMT-RCM*.

I.1.6.3.2 Renovación de *Certificados*

Cuando se extingue la vigencia de un *Certificado* (bien por caducidad, bien por revocación) la FNMT-RCM obliga a las *Entidades usuarias* a la generación de un nuevo par de *Claves* para dar lugar a nuevos *Datos de creación de Firma* y *Datos de verificación de Firma*.

Únicamente en el caso de *Certificados* emitidos para personas físicas se permitirá la renovación de forma telemática autenticando a la *Entidad usuaria* en base al *Certificado* previamente expedido (cuya identificación se hizo de forma presencial) si bien esta operación sólo se podrá realizar cuando no se haya superado el plazo máximo de 5 años desde la personación e identificación física del Suscriptor que establece la Ley de firma electrónica 59/2003, de 19 de diciembre, en su artículo 13.4.

Para el resto de figuras jurídicas a las que se expiden *Certificados*, la FNMT-RCM obliga a la comparecencia física ante las *Oficinas de Registro*, para la comprobación de la identidad del *Solicitante* y, en su caso, de la vigencia y extensión de las facultades de representación sobre la *Persona jurídica* o persona física para la que realice dicha solicitud.

I.1.6.3.3 Generación de *Certificados*

La FNMT-RCM garantiza la confidencialidad e integridad de los datos recabados en el proceso de registro y el envío de forma segura a las instalaciones del *Prestador de Servicios de Certificación*.

La FNMT-RCM, dado que en su actividad como *Prestador de Servicios de Certificación* no genera el par de *Claves* de las *Entidades usuarias*, pone todos los mecanismos necesarios durante el proceso de solicitud de los *Certificados* para procurar que el *Solicitante* se encuentra en posesión de la *Clave Privada* asociada a la *Clave Pública* que se certificará.

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

Los *Certificados* emitidos por la FNMT-RCM en su actividad como *Prestador de Servicios de Certificación* bajo esta *Política de Certificación de Certificados Reconocidos*, cumplen, en cuanto a su formato, con el perfil definido en ETSI TS 101 862.

I.1.6.3.4 Difusión de Términos y Condiciones

La FNMT-RCM pone a disposición de la *Comunidad Electrónica* tanto el documento de *Política de Certificación de Certificados Reconocidos de la FNMT-RCM* como el documento de *Declaración de Prácticas de Certificación de la FNMT-RCM* en los que se detalla:

- Los términos y condiciones que regulan la utilización de los *Certificados* expedidos por la FNMT-RCM.
- La *Política de Certificación* aplicable a los *Certificados* expedidos por la FNMT-RCM.
- Los límites de uso para los *Certificados* expedidos bajo esta *Política de Certificación*.

- Las obligaciones, garantías y responsabilidades de las partes en el ámbito de la emisión y uso de los *Certificados*.
- Los períodos de retención de la información recabada en el proceso de registro y de los eventos producidos en los sistemas del *Prestador de Servicios de Certificación* relacionados con la gestión del ciclo de vida de los *Certificados* emitidos bajo esta *Política de Certificación.*
- El sistema legal aplicable, así como los procedimientos para la interposición de reclamaciones y la resolución de disputas.

I.1.6.3.5 Difusión de *Certificados*

La FNMT-RCM, en su actividad como *Prestador de Servicios de Certificación* pone a disposición de la *Comunidad Electrónica* un sistema de consulta del estado del propio *Certificado* de la Entidad usuaria, como un servicio *web* en el que el suscriptor se autenticará con su propio *Certificado*.

En ningún caso, la FNMT-RCM proporciona un servicio de consulta de *Certificados* de otros *Suscriptores*.

I.1.6.3.6 Suspensión y Revocación de *Certificados*

La FNMT-RCM dispone de diferentes procedimientos para la suspensión y revocación de *Certificados*. Estos procedimientos, así como las causas admitidas para la suspensión y revocación de los *Certificados* se exponen detalladamente en el apartado "9.12 Vigencia de los Certificados" de la *Declaración de Prácticas de Certificación*.

Únicamente las *Entidades usuarias* de Derecho Público tendrán acceso a las *Listas de Revocación*, ya sea ésta originaria o replicada, y en las condiciones establecidas en el correspondiente convenio de incorporación a la *Comunidad Electrónica*.

Las *Entidades usuarias* de Derecho Privado, previa incorporación a la *Comunidad Electrónica*, dispondrán de un *Cliente OCSP* para comprobar el estado de los *Certificados* mediante consultas vía OCSP, según se refiere en el apartado "9.15 Servicio de validación de Certificados mediante *OCSP*" de la *Declaración de Prácticas de Certificación*.

La FNMT-RCM utilizará mecanismos adecuados de firma electrónica para dotar de *Integridad* y autenticidad a la información sobre el estado de los *Certificados*, que proporcione.

La FNMT-RCM pondrá todos los medios a su alcance para que la disponibilidad de estos servicios de comprobación del estado de los *Certificados* sea la máxima posible.

I.1.6.4 Operación y Gestión de la *Infraestructura de Clave Pública*

Las operaciones y procedimientos realizados para la puesta en práctica de la presente *Política de Certificación* se realizan siguiendo los controles requeridos por los estándares reconocidos para tal efecto, describiéndose estas actuaciones en los apartados "6.2 Controles de seguridad física, de procedimientos y del personal**"** y "6.3 Controles de seguridad técnica**"** de la *Declaración de Prácticas de Certificación* de la FNMT-RCM.

De forma informativa cabe decir que la FNMT-RCM se encuentra inmersa en un proyecto de establecimiento de un *Sistema de Gestión de la Seguridad dela Información* (en adelante *SGSI*) para su Departamento CERES con el objetivo final de mantener y garantizar la seguridad de la información de los clientes, así como la suya propia, de forma que el servicio prestado por la FNMT-RCM-CERES tenga los niveles suficientes de fiabilidad que exige el Mercado. El SGSI de la FNMT-RCM-CERES es aplicable a los activos de información definidos en el Análisis de Riesgos realizado para todas las Áreas que componen el departamento, incluyendo como activos los servicios prestados a los Clientes.

En el documento *Declaración de Practicas de Certificación*, 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.

I.1.6.5 Aspectos organizativos

La FNMT-RCM es un Ente Público Empresarial dependiente del Ministerio de Economía, con capital 100% público y que goza del prestigio institucional de su larga tradición histórica y del respaldo del Estado.

La FNMT-RCM a pesar de contar con una larga trayectoria y el importante respaldo del Estado, ha apostado también fuerte por el reconocimiento del entorno privado en este nuevo sector que representa la certificación electrónica y las redes telemáticas abiertas, llegando a ser el primer y único prestador de servicios de certificación que ha alcanzado la acreditación de su sistema de gestión de la calidad de acuerdo a la normativa ISO 9001: 2000, otorgado por AENOR e IQNET para la prestación de servicios de certificación de firma electrónica, de sellado de tiempo y de desarrollo de sistemas operativos criptográficos para tarjetas inteligentes.

Así mismo, la FNMT-RCM tiene acreditada sus buenas prácticas y su código de conducta a través de la Agencia de la Calidad en Internet. El sello de calidad de IQUA es una garantía del nivel de calidad de las páginas web que lo obtienen basándose en los códigos de conducta sectoriales elaborados por los miembros adheridos de IQUA, y sus páginas son auditadas para garantizar su respeto a las normas de comportamiento aprobadas por el sector al que correspondan.

También citar, que los servicios de la FNMT-RCM son evaluados por el Centro de Evaluación de la Seguridad de las Tecnologías de la Información del INTA, dependiente del Ministerio de Defensa, garantizando así su idoneidad técnica.

I.1.7 EXCLUSIONES Y REQUISITOS ADICIONALES A ETSI TS 101456

a) De acuerdo con la norma en el apartado 8.2 b), se excluyen las cuestiones definidas en el apartado 7.5 j), k).

b) 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.

c) De acuerdo con la norma en el apartado 8.2 d), se excluyen las cuestiones definidas en el apartado 7.3.6 k). En este tema se estará a lo señalado en el apartado "Comprobación del estado del *Certificado"* de este anexo.

Respecto aquellos *Certificados Reconocidos* que usen *Dispositivos Seguros de creación de firma*, seguirán lo señalado en el apartado 7. "*Soporte del Certificado*" punto a) del documento *Declaración de Prácticas de Certificación de la FNMT-RCM*, así como a lo expuesto en los apartados sobre *"Ciclo de vida del certificado"* del citado documento.

I.2 POLÍTICA DE CERTIFICACIÓN PARA CERTIFICADO DE COMPONENTES DE LA FNMT-RCM

NO FORMAN PARTE DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA FNMT-RCM, ni se pueden considerar "Certificados" según se define en dicha DECLARACIÓN este concepto, los denominados "CERTIFICADOS DE COMPONENTES" por no adecuarse al concepto legal de "certificado electrónico" definido por la Ley de firma electrónica 59/2003, de 19 de diciembre. No obstante, se adjuntan provisionalmente como anexo exclusivamente informativo, por ser productos de gran utilidad que forman parte del Catálogo de Servicios y Productos de la FNMT-RCM.

I.2.1 TIPOLOGÍA DE LOS CERTIFICADOS DE COMPONENTES DE LA FNMT-RCM

Los "certificados de componentes" son aquellos certificados expedidos por la FNMT-RCM bajo esta política de certificación y que vinculan unos *Datos de verificación de Firma* a un componente o aplicación informática sobre la que existe una persona física determinada que actúa como responsable, siendo esta la que tiene el control sobre dicho componente o aplicación. La *Plave Privada* asociada a la *Clave Pública* estarán bajo la responsabilidad de dicho *Responsable del componente* que actuará como representante de la *Persona jurídica* titular del componente objeto del certificado.

Son "certificados" emitidos y firmados por la FNMT-RCM para ser instalados y utilizados por servidores con soporte SSL, aplicaciones de firma de componentes software o por aplicaciones que actúen como clientes de los servicios avanzados proporcionados por la FNMT-RCM, con el objeto de que se herede la confianza que representa la FNMT-RCM como *Prestador de Servicios de Certificación*. Solo podrán obtener certificados de componentes aquellas entidades que hayan suscrito un contrato con la FNMT-RCM en virtud del cual formen parte de la *Comunidad Electrónica* tal y como se contempla en la *Declaración de Prácticas de Certificación de la FNMT-RCM*.

Estos certificados, no suponen firma electrónica desde un punto de vista jurídico, aunque pueden obrar con los mismos medios técnicos, pero carecen de la imputabilidad del hecho de la firma a una persona física o incluso a una *Persona jurídica* por lo que no serán expedidos con la cualidad de *Certificados* definido por la Ley de firma electrónica núm. 59/2003.

La FNMT-RCM expide bajo la presente *Política de Certificación* los siguientes tipos de certificados de componentes:

- *Certificado de servidor [también denominado certificado de la FNMT-RCM Clase 2 CA para Servidores Web]:* Es aquel certificado que permite identificar a un servidor *web* o una URL.
- *Certificado de firma de código [también denominado certificado de la FNMT-RCM Clase 2 CA para firma de código]:* Es aquel certificado utilizado en aplicaciones que permite firmar código ejecutable como *applets de Java*.

- *Certificado de Clientes de Servicios Avanzados de la FNMT-RCM:* Certificado utilizado en aplicaciones que actúan como clientes de los servicios avanzados puestos a disposición de la *Comunidad Electrónica* por la FNMT-RCM.
- *Certificado de otros componentes informáticos:* Certificado distinto de los anteriores, utilizado para identificar unas aplicaciones frente a otras, y establecer sesiones seguras.

I.2.2 IDENTIFICACIÓN

La presente *Política de Certificación* de la FNMT-RCM para la expedición de *certificados de componentes* tiene la siguiente identificación:

Nombre	Política de Certificación de *certificados de componentes* de la FNMT-RCM
Referencia/OID	1.3.6.1.4.1.5734.3.6
Versión	1.0
Fecha de Emisión	1 de Enero de 2004
DPC relacionada	Declaración de Prácticas de Certificación de la FNMT-RCM OID: 1.3.6.1.4.1.5734.4 Localización: http://www.cert.fnmt.es/convenio/dpc.pdf
Localización	http://www.cert.fnmt.es/convenio/dpc.pdf

I.2.3 GESTIÓN DE LA POLÍTICA DEL CERTIFICADO

La FNMT-RCM dispone de una *Política de Certificación* efectiva; en particular la FNMT-RCM declara que:

- La FNMT-RCM tiene capacidad para especificar, revisar, y aprobar la *Política de Certificación* de los *certificados de componentes*, a través de su Dirección General.
- La FNMT-RCM dispone de una *Declaración de Prácticas de Certificación* en la que se detallan las prácticas de certificación empleadas para la expedición de *certificados de componentes* conformes a la política de certificación aquí expuesta.
- La FNMT-RCM dispone, dentro de las competencias de la Dirección, de capacidad y procedimientos de revisión y mantenimiento tanto para la *Declaración de Prácticas de Certificación* como para esta política de certificación.
- La FNMT-RCM realiza análisis de riesgos para evaluar las amenazas del sistema y proponer las medidas de seguridad adecuadas (salvaguardas) para todas las áreas implicadas.
- La *Declaración de Prácticas de Certificación*

  http://www.cert.fnmt.es/convenio/dpc.pdf
- La *Política de Certificación* de *certificados de componentes* se encuentra disponible en:

  http://www.cert.fnmt.es/convenio/dpc.pdf

- Esta política de certificación recoge las obligaciones y responsabilidades de las partes implicadas en la emisión y uso de los *certificados de componentes* emitidos por la FNMT-RCM bajo a esta política de certificación.
- Se dispone de un *OID* específico para identificar la política de certificación aquí desarrollada, siendo el *OID* asignado en el marco de la numeración de la FNMT-RCM: 1.3.6.1.4.1.5734.3.6.

I.2.4 COMUNIDAD Y ÁMBITO DE APLICACIÓN

La presente política de certificación es de aplicación en la expedición de certificados electrónicos que tienen las siguientes características:

a) No son expedidos como *Certificados Reconocidos.*

b) Los certificados emitidos bajo esta política de certificación son expedidos para *Entidades usuarias* que forma parte de la *Comunidad Electrónica* tal y como se define en el apartado "1. Definiciones" de la *Declaración de Prácticas de Certificación de la FNMT-RCM.*

I.2.5 RESPONSABILIDAD Y OBLIGACIONES DE LAS PARTES

Esta política de certificación recoge las obligaciones y responsabilidades de las partes implicadas en la emisión y uso de los *certificados de componentes*, emitidos bajo esta política de certificación.

I.2.5.1 Obligaciones de la FNMT-RCM como *Prestador de Servicios de Certificación*

Las obligaciones propias de la FNMT–RCM como *Prestador de Servicios de Certificación* quedan expuestas en el apartado "9.20 "Obligaciones y garantías de las partes" de la *Declaración de Prácticas de Certificación de la FNMT-RCM*.

I.2.5.1.1. Obligaciones del suscriptor y de las *Entidades usuarias*

Las obligaciones propias de los Suscriptores de Certificados emitidos por la FNMT–RCM bajo la presente Política de Certificación quedan expuestas en el apartado "9.20 Obligaciones y garantías de las partes" de la *Declaración de Prácticas de Certificación de la FNMT-RCM*.

I.2.5.1.2. Responsabilidades

Las responsabilidades de las partes implicadas en la expedición y uso de los *Certificados* emitidos bajo la presente *Política de Certificación* quedan expuestas en el apartado "9.21 Responsabilidad de las partes" de la *Declaración de Prácticas de Certificación* de la FNMT-RCM.

I.2.6 REQUERIMIENTOS DE LAS PRÁCTICAS DE LA FNMT-RCM COMO *PRESTADOR DE SERVICIOS DE CERTIFICACIÓN*

I.2.6.1 Declaración de Prácticas de Certificación

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 regulación de la prestación de los servicios de certificación por parte de la FNMT-RCM en su condición de *Prestador de Servicios de Certificación*, recogiendo en concreto la siguiente información:

- Las obligaciones que se compromete a cumplir en relación con la gestión de los *Datos de creación* y *verificación de Firma* y de los certificados.
- Las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados y, en su caso, la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata y confidencial sobre la vigencia de los poderes indicados en los *Certificados* y que deban figurar preceptivamente inscritos en dichos registros.
- Detalles del régimen de responsabilidad aplicable a los miembros de la *Comunidad Electrónica.*
- Los controles de seguridad aplicados a sus procedimientos e instalaciones en aquello que pueda ser publicado sin perjudicar la eficacia de los mismos, y las normas de secreto y confidencialidad, así como cuestiones relativas a la propiedad de sus bienes y activos, a la protección de datos de carácter personal, y demás cuestiones de tipo informativo que considere interesante poner a disposición del público.
- Definición de los procedimientos de revisión de dicha *Declaración de Prácticas de Certificación.*

I.2.6.2 Infraestructura de Clave Pública. Gestión del ciclo de vida de las *Claves*

I.2.6.2.1 Generación de las *Claves* del *Prestador de Servicios de Certificación*

Las *Claves* de la FNMT-RCM como *Prestador de Servicios de Certificación*, son generadas en circunstancias completamente controladas en un entorno físicamente seguro y, al menos, por dos personas autorizadas para ello, utilizando sistemas hardware y software que cumplen con la normativa actual en materia de protección criptográfica tal y como se muestra en el apartado "6.3.1 Gestión del ciclo de vida de las *Claves* del *Prestador de Servicios de Certificación*" de la *Declaración de Prácticas de Certificación.*

I.2.6.2.2 Almacenamiento, salvaguarda y recuperación de las *Claves* del *Prestador de Servicios de Certificación*

La FNMT-RCM utiliza los mecanismos necesarios para mantener su *Clave privada* confidencial y mantener su integridad en la forma que se muestra en el apartado "6.3.1 Gestión del ciclo de vida de las *Claves* del *Prestador de Servicios de Certificación*" de la *Declaración de Prácticas de Certificación.*

I.2.6.2.3 Distribución de los Datos de verificación de Firma del *Prestador de Servicios de Certificación*

La FNMT-RCM utiliza los mecanismos necesarios para mantener la integridad y autenticidad de su *Clave pública* así como la forma de distribución en la forma que se muestra en el apartado "6.3.1 Gestión del ciclo de vida de las *Claves* del *Prestador de Servicios de Certificación*" de la *Declaración de Prácticas de Certificación.*

I.2.6.2.4 Almacenamiento, salvaguarda y recuperación de las *Claves Privadas* de la *Entidad usuaria*

La FNMT-RCM bajo ningún concepto genera ni almacena las *Claves Privadas* de las *Entidades usuarias*, que son generadas bajo su exclusivo control y cuya custodia está bajo su responsabilidad.

I.2.6.2.5 Uso de los Datos de creación de Firma del *Prestador de Servicios de Certificación*

Las Claves de la FNMT-RCM en su actividad como *Prestador de Servicios de Certificación* serán utilizadas única y exclusivamente para los propósitos de:

- Firma de certificados.
- Firma de las *Listas de Revocación.*

I.2.6.2.6 Fin del ciclo de vida de los Datos de creación de Firma del Prestador de Servicios de Certificación

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.

I.2.6.2.7 Ciclo de vida del hardware criptográfico utilizado para firmar certificados

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

I.2.6.2.8 Servicios de Gestión de las *Claves* de las *Entidades usuarias*

La FNMT-RCM bajo ningún concepto genera ni almacena las *Claves Privadas* de las *Entidades usuarias* las cuales se generan bajo su exclusivo control y custodia.

I.2.6.2.9 Preparación de los *Dispositivos seguros de creación de Firma*

La FNMT-RCM proporciona a las *Entidades usuarias* que así lo requieran *Tarjetas criptográficas* para la generación de sus *Claves Privadas* y el almacenamiento de los *Certificados*.

La *Tarjeta criptográfica* es entregada a la *Entidad usuaria* sin ningún tipo de contenido, con las utilidades software necesarias para conseguir una integración con los *navegadores* más utilizados. Así mismo, en el mismo momento se le proporcionan los códigos necesarios para el acceso a dicha *Tarjeta* para que posteriormente desde su puesto, la *Entidad usuaria* genere sus *Claves* e inserte el *Certificado* en ella si así lo desea.

Todo esto se hace para ayudar a las *Entidades usuarias* a que cumpla con su obligación de mantener el "exclusivo control" sobre los *Datos de creación de Firma*.

I.2.6.3 Infraestructura de Clave Pública. Gestión del ciclo de vida de los *Certificados de componentes*

I.2.6.3.1 Registro de las *Entidades usuarias*

Con carácter previo al establecimiento de cualquier relación contractual con las Entidades usuarias la FNMT-RCM informa a las interesadas en adquirir dicho estatus, acerca de las condiciones del servicio así como de las obligaciones, garantías y responsabilidades de las partes implicadas en la expedición y uso de los certificados por ella emitidos en su labor como *Prestador de Servicios de Certificación*.

La FNMT-RCM en su actividad como *Prestador de Servicios de Certificación*, por ella misma y en exclusividad procede a la identificación de los peticionarios que soliciten c*ertificados de componentes* mediante aquellos procedimientos que así se dispongan para ello y confirma el poder de los peticionarios para actuar en nombre de la *Persona jurídica* titular del componente objeto del certificado.

La FNMT-RCM recabará de los solicitantes solo aquella información que sea necesaria para la expedición de los certificados y para la comprobación de la identidad de los peticionarios y sus Representados, almacenándola durante un periodo de quince (15) años, tratándola con la debida diligencia para el cumplimiento de la legislación nacional vigente en materia de protección de datos de carácter personal.

La FNMT-RCM, dado que en su actividad como *Prestador de Servicios de Certificación* no genera el par de *Claves* de las *Entidades usuarias*, pone todos los mecanismos necesarios durante el proceso de *Solicitud de Certificados* para posibilitar que el peticionario se encuentra en posesión de la *Clave Privada* asociada a la *Clave Pública* que se certificará.

Las *Prácticas de Certificación particulares de los certificados de componentes* puestas diseñadas para la gestión expuesta puede verse con detalle en el documento *Declaración de Prácticas de Certificación de la FNMT-RCM*.

I.2.6.3.2 Renovación de certificados de componentes

Cuando se extingue la vigencia de un *Certificado* (bien por caducidad, bien por revocación) la FNMT-RCM obliga a las *Entidades usuarias* a la generación de un nuevo par de *Claves* para dar lugar a nuevos *Datos de creación de Firma* y *Datos de verificación de Firma* comenzando de nuevo el proceso de registro de *Entidades usuarias*, teniendo los interesados que volver a presentar la documentación exigida en el apartado anterior.

I.2.6.3.3 Generación de certificados de componentes

La FNMT-RCM garantiza la confidencialidad e integridad de los datos recabados en el proceso de registro y el envío de forma segura a las instalaciones del *Prestador de Servicios de Certificación*.

La FNMT-RCM, dado que en su actividad como *Prestador de Servicios de Certificación* no genera el par de *Claves* de las *Entidades usuarias*, pone todos los mecanismos necesarios durante el proceso de solicitud de certificados para procurar que el peticionario se encuentra en posesión de la *Clave Privada* asociada a la *Clave Pública* que se certificará.

El nombre distintivo asignado al suscriptor del *Certificado* dentro del dominio del *Prestador de Servicios de Certificación* será único.

I.2.6.3.4 Difusión de Términos y Condiciones

La FNMT-RCM pone a disposición de la *Comunidad Electrónica* tanto el documento de *Política de Certificación de Certificados Reconocidos de la FNMT-RCM* como el documento de *Declaración de Prácticas de Certificación de la FNMT-RCM* en los que se detalla:

- Los términos y condiciones que regulan la utilización de los *Certificados* expedidos por la FNMT-RCM.
- La *Política de Certificación* aplicable a los *Certificados* expedidos por la FNMT-RCM.
- Los límites de uso para los *Certificados* expedidos bajo esta *Política de Certificación*.
- Las obligaciones, garantías y responsabilidades de las partes envueltas en la emisión y uso de los *Certificados.*
- Los períodos de retención de la información recabada en el proceso de registro y de los eventos producidos en los sistemas del *Prestador de Servicios de Certificación* relacionados con la gestión del ciclo de vida de los *Certificados* emitidos bajo esta *Política de Certificación.*
- El sistema legal aplicable así como los procedimientos para reclamaciones y disputas.

I.2.6.3.5 Difusión de certificados de componentes

La FNMT-RCM en su actividad como *Prestador de Servicios de Certificación* pone a disposición de la *Comunidad Electrónica* un sistema de consulta del estado del propio *Certificado* como un servicio web en el que el suscriptor se autenticará con su propio *Certificado*.

En ningún caso, la FNMT-RCM proporciona un servicio de recuperación de certificados de otros suscriptores.

I.2.6.3.6 Suspensión y Revocación de *certificados de componentes*

La FNMT-RCM dispone de diferentes procedimientos para la suspensión y revocación de los *certificados de componentes*. Estos procedimientos así como las causas admitidas para la suspensión y revocación de los *Certificados* se exponen detalladamente en el apartado "9.12 Vigencia de los Certificados" de la *Declaración de Prácticas de Certificación*.

Únicamente las *Entidades usuarias* de Derecho Público tendrán acceso a las *Listas de Revocación*, ya sea a la originaria o a la replicada, y en las condiciones establecidas en el correspondiente convenio de incorporación a la *Comunidad Electrónica*.

Las *Entidades usuarias* de Derecho Privado, previa incorporación a la *Comunidad Electrónica*, dispondrán de un *Cliente OCSP* para comprobar el estado de los *Certificados* mediante consultas vía OCSP, según se refiere en el apartado "Servicio de validación de Certificados mediante *OCSP*" de la *Declaración de Prácticas de Certificación.*

La integridad y autenticidad de la información sobre el estado de los *Certificados* proporcionada por la FNMT-RCM se obtendrá mediante los mecanismos de firma electrónica adecuados.

La FNMT-RCM pondrá todos los medios a su alcance para que la disponibilidad de estos servicios de comprobación del estado de los *Certificados* sea la máxima posible.

I.2.7 Operación y Gestión de la *Infraestructura de Clave Pública*

Las operaciones y procedimientos realizados para la puesta en práctica de la presente política de certificación se realizan siguiendo los controles requeridos por los estándares reconocidos para tal efecto, describiéndose estas actuaciones en los apartados "6.2 Controles de seguridad física, de procedimientos y del personal**"** y "6.3 Controles de seguridad técnica de la *Declaración de Prácticas de Certificación*" de la FNMT-RCM.

De forma informativa cabe decir que la FNMT-RCM se encuentra inmersa en un proyecto de establecimiento de un *Sistema de Gestión de la Seguridad dela Información* (en adelante *SGSI*) para su Departamento CERES con el objetivo final de mantener y garantizar la seguridad de la información de sus clientes así como la suya propia, de forma que el servicio prestado por la FNMT-RCM-CERES tenga los niveles suficientes de fiabilidad que exige el Mercado. El SGSI de la FNMT-RCM-CERES es aplicable a los activos de información definidos en el Análisis de Riesgos realizado para todas las Áreas que componen el departamento, incluyendo como activos los servicios prestados a los Clientes.

En el documento *Declaración de Practicas de Certificación*, 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.

I.2.8 Aspectos organizativos

La FNMT-RCM es un Ente Público Empresarial dependiente del Ministerio de Economía, con capital 100% público y que goza del prestigio institucional de su larga tradición histórica y del respaldo del Estado.

La FNMT-RCM a pesar de contar con una larga trayectoria y el importante respaldo del Estado, ha apostado también fuerte por el reconocimiento del entorno privado en este nuevo sector que representa la certificación electrónica y las redes telemáticas abiertas, llegando a ser el primer y único prestador de servicios de certificación que ha alcanzado la acreditación de su sistema de gestión de la calidad de acuerdo a la normativa ISO 9001: 2000, otorgado por AENOR e IQNET para la prestación de servicios de certificación de firma electrónica, de sellado de tiempo y de desarrollo de sistemas operativos criptográficos para tarjetas inteligentes.

Así mismo, la FNMT-RCM tiene acreditada sus buenas prácticas y su código de conducta a través de la Agencia de la Calidad en Internet. El sello de calidad de IQUA es una garantía del nivel de calidad de las páginas web que lo obtienen basándose en los códigos de conducta sectoriales elaborados por los miembros adheridos de IQUA, y sus páginas son auditadas para garantizar su respeto a las normas de comportamiento aprobadas por el sector al que correspondan.

También citar, que los servicios de la FNMT-RCM son evaluados por el Centro de Evaluación de la Seguridad de las Tecnologías de la Información del INTA, dependiente del Ministerio de Defensa, garantizando así su idoneidad técnica.

I.3 POLÍTICA DE CERTIFICACIÓN PARA CERTIFICADOS DE CLAVE PÚBLICA DE LA FNMT-RCM

I.3.1 TIPOLOGIA DE LOS CERTIFICADOS DE CLAVE PÚBLICA DE LA FNMT-RCM

Los *Certificados* expedidos por la FNMT-RCM bajo esta *Política de Certificación* vinculan a su *Suscriptor* unos *Datos de verificación de Firma* y confirman su identidad.

Estos *Certificados*, son expedidos con base en los criterios establecidos para tal en la normativa técnica EESSI, concretamente ETSI TS 102 042 - "Policy requirements for certification authorities issuing public key certificates" en su política de certificación indicada como NCP (Normalizad Certificate Policy), política que ofrece la misma calidad que la ofrecida por la Política de Certificados Reconocidos de la FNMT-RCM pero sin las restricciones legales de la Directiva Europea de Firma Electrónica (1999/93/EC), tanto en lo referente al *Prestador de Servicios de Certificación* como a la generación de los *Datos de creación de Firma* y al contenido de los propios *Certificados*.

La FNMT-RCM expide bajo esta *Política de Certificación* los siguientes tipos de *Certificados*:

- *Certificado de Persona jurídica para el ámbito tributario:* es la certificación electrónica expedida por la FNMT-RCM que vincula a su *Suscriptor* (siempre *Sujeto pasivo tributario*) unos *Datos de verificación de Firma* y confirma su identidad. Este certificado se corresponde con el certificado tradicional utilizado por el Ministerio de Hacienda o el Gobierno de Navarra para el ámbito tributario.
- *Certificado de Entidad sin personalidad jurídica para el ámbito tributario:* es la certificación electrónica expedida por la FNMT-RCM que vincula a su *Titular* o *Suscriptor* (siempre *Entidad sin personalidad jurídica a las que se refiere el articulo 35.4 de la Ley General Tributaria*) unos *Datos de verificación de Firma* y confirma su identidad a los solos efectos de su empleo en el ámbito tributario. Estos certificados se expiden según los términos expuestos en la ORDEN EHA/3256/2004, de 30 de septiembre, publicada en el B.O.E Nº 246 de 12 de octubre.

I.3.2 IDENTIFICACIÓN

La presente *Política de Certificación* de la FNMT-RCM para la expedición de *Certificados de Clave Publica* tiene la siguiente identificación:

Nombre	Política de Certificación de Certificados de Calve Pública de la FNMT-RCM
Referencia/OID	1.3.6.1.4.1.5734.3.7
Versión	1.0

Fecha de Emisión	1 de Octubre de 2004
DPC relacionada	Declaración de Prácticas de Certificación de la FNMT-RCM OID: 1.3.6.1.4.1.5734.4 Localización: http://www.cert.fnmt.es/convenio/dpc.pdf
Localización	http://www.cert.fnmt.es/convenio/dpc.pdf

I.3.3 GESTIÓN DE LA POLÍTICA DEL CERTIFICADO

La FNMT-RCM dispone de una *Política de Certificación* efectiva y, en particular, declara que:

- La FNMT-RCM tiene capacidad para especificar, revisar, y aprobar la *Política de Certificación* de *Certificados de Clave Publica,,* a través de su Dirección General.
- La FNMT-RCM dispone de una *Declaración de Prácticas de Certificación* en la que se detallan las prácticas de certificación empleadas para la expedición de Certificados de Clave Pública conformes a la Política de Certificación aquí expuesta.
- La FNMT-RCM dispone, dentro de las competencias de la Dirección, de capacidad, para especificar, revisar y aprobar los procedimientos de revisión y mantenimiento tanto para la *Declaración de Prácticas de Certificación* como para la *Política de Certificación*.
- La FNMT-RCM realiza análisis de riesgos para evaluar las amenazas del sistema y proponer las medidas de seguridad adecuadas (salvaguardas) para todas las áreas implicadas.
- La *Declaración de Prácticas de Certificación* se pone a disposición del público mediante el URL: http://www.cert.fnmt.es/convenio/dpc.pdf
- La *Política de Certificación* de *Certificados de Clave Pública* se pone a disposición del público mediante el URL: http://www.cert.fnmt.es/convenio/dpc.pdf
- Esta *Política de Certificación* recoge las obligaciones y responsabilidades de las partes implicadas en la emisión y uso de los *Certificados Calve Pública* emitidos por la FNMT-RCM bajo a esta *Política de Certificación.*
- Se dispone de un *OID* específico para identificar la *Política de Certificación* aquí desarrollada, siendo el *OID* asignado en el marco de la numeración de la FNMT-RCM: 1.3.6.1.4.1.5734.3.7.
- La presente *Política de Certificación* de la FNMT-RCM se define en ETSI TS 102042, como NCP (Normalized Certificate Policy) cumpliéndose los requisitos expuestos en los apartado 6 y 7 de la citada norma. En caso de discrepancia entre este documento y la referida norma, prevalecerá este documento.

I.3.4 COMUNIDAD Y ÁMBITO DE APLICACIÓN

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

e) Son expedidos por la FNMT-RCM como *Prestador de Servicios de Certificación* cumpliendo con los criterios establecidos en la Ley de Firma Electrónica (Ley

59/2003) y en la normativa técnica EESSI, concretamente ETSI TS 102 042 - "Policy requirements for certification authorities issuing public key certificates".

f) La *Tarjeta criptográfica* CERES utilizada como *Dispositivo seguro de creación de Firma*, cumple con los criterios establecidos en la Ley de Firma Electrónica (Ley 59/2003) para tales dispositivos.

g) Los *Certificados* emitidos bajo esta *Política de Certificación* son expedidos para *Entidades usuarias* que forma parte de la *Comunidad Electrónica* tal y como se define en el apartado ***Definiciones*** de la *Declaración de Prácticas de Certificación de la FNMT-RCM*.

I.3.5 RESPONSABILIDAD Y OBLIGACIONES DE LAS PARTES

Esta *Política de Certificación* recoge las obligaciones y responsabilidades de las partes implicadas en la emisión y uso de los *Certificados*, emitidos bajo esta *Política de Certificación.*

Por otro lado, los límites de uso quedan descritos en el apartado "Límites de uso del *Certificado*" de las distintas *Prácticas de Certificación* particulares (anexo II a IV) de los distintos tipos de *Certificados* que la FNMT-RCM expide bajo la presente *Política de Certificación.*

I.3.5.1 Obligaciones de la FNMT-RCM como Prestador de Servicios de Certificación

Las obligaciones propias de la FNMT–RCM como *Prestador de Servicios de Certificación* quedan expuestas en el apartado "9.20 "Obligaciones y garantías de las partes" de la *Declaración de Prácticas de Certificación de la FNMT-RCM.*

I.3.5.2 Obligaciones del Suscriptor y de las Entidades usuarias

Las obligaciones propias de los Suscriptores de Certificados emitidos por la FNMT–RCM bajo la presente Política de Certificación quedan expuestas en el apartado "9.20 Obligaciones y garantías de las partes" de la *Declaración de Prácticas de Certificación de la FNMT-RCM.*

I.3.5.3 Responsabilidades

Las responsabilidades de las partes implicadas en la expedición y uso de los *Certificados* emitidos bajo la presente *Política de Certificación* quedan expuestas en el apartado "9.21 Responsabilidad de las partes" de la *Declaración de Prácticas de Certificación* de la FNMT-RCM.

I.3.6 REQUERIMIENTOS DE LAS PRÁCTICAS DE LA FNMT-RCM COMO AUTORIDAD DE CERTIFICACIÓN

I.3.6.1 Declaración de Prácticas de Certificación

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 regulación de la prestación de los servicios de certificación por parte de la FNMT-RCM en su condición de *Prestador de Servicios de Certificación*, recogiendo en concreto la siguiente información:

- Las obligaciones que se compromete a cumplir en relación con la gestión de los *Datos de creación* y *verificación de Firma* y de los *Certificados.*
- Las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los *Certificados* y, en su caso, la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata y confidencial sobre la vigencia de los poderes indicados en los *Certificados* y que deban figurar preceptivamente inscritos en dichos registros.
- Detalles del régimen de responsabilidad aplicable a los miembros de la *Comunidad Electrónica.*
- Los controles de seguridad aplicados a sus procedimientos e instalaciones en aquello que pueda ser publicado, sin perjudicar la eficacia de los mismos, y las normas de secreto y confidencialidad, así como cuestiones relativas a la propiedad de sus bienes y activos, a la protección de datos de carácter personal, y demás cuestiones de tipo informativo que considere interesante poner a disposición del público.
- Definición de los procedimientos de revisión de dicha *Declaración de Prácticas de Certificación.*

I.3.6.2 Infraestructura de Clave Pública. Gestión del ciclo de vida de las *Claves*

I.3.6.2.1 Generación de las *Claves* de los *Prestadores de Servicios de Certificación*

Las *Claves* de la FNMT-RCM como *Prestador de Servicios de Certificación*, son generadas en circunstancias completamente controladas, en un entorno físicamente seguro y al menos por dos personas autorizadas para ello, utilizando sistemas hardware y software que cumplen con la normativa actual en materia de protección criptográfica, tal y como se muestra en el apartado "6.3.1 Gestión del ciclo de vida de las *Claves* del *Prestador de Servicios de Certificación*" de la *Declaración de Prácticas de Certificación.*

I.3.6.2.2 Almacenamiento, salvaguarda y recuperación de las *Claves* del *Prestador de Servicios de Certificación*

La FNMT-RCM utiliza los mecanismos necesarios para mantener su *Clave privada* confidencial y mantener su integridad en la forma que se muestra en el apartado "6.3.1 Gestión del

ciclo de vida de las *Claves* del *Prestador de Servicios de Certificación***"** de la *Declaración de Prácticas de Certificación.*

I.3.6.2.3 Distribución de los Datos de verificación de Firma del Prestador de Servicios de Certificación

La FNMT-RCM utiliza los mecanismos necesarios para mantener la integridad y autenticidad de su *Clave Pública*, así como su distribución en la forma que se muestra en el apartado "6.3.1 Gestión del ciclo de vida de las *Claves* del *Prestador de Servicios de Certificación***"** de la *Declaración de Prácticas de Certificación*.

I.3.6.2.4 Almacenamiento, salvaguarda y recuperación de las *Claves Privadas* de las *Entidades usuarias*

La FNMT-RCM bajo ningún concepto genera ni almacena las *Claves Privadas* de las *Entidades usuarias*, las cuales son generadas bajo su exclusivo control, y cuya custodia está bajo su responsabilidad.

I.3.6.2.5 Uso de los Datos de creación de Firma del Prestador de Servicios de Certificación

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:

- Firma de certificados.
- Firma de las *Listas de Revocación.*

I.3.6.2.6 Fin del ciclo de vida de las Claves del *Prestador de Servicios de Certificación*

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.

I.3.6.2.7 Ciclo de vida del hardware criptográfico utilizado para firmar *Certificados*

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 durante todo su ciclo de vida, estando situado dicho componente en un entorno físicamente seguro desde su recepción hasta su destrucción llegado el caso.

I.3.6.2.8 Servicios de Gestión de las *Claves* de las *Entidades usuarias*

La FNMT-RCM bajo ningún concepto genera ni almacena las *Claves Privadas* de las *Entidades usuarias*, que son generadas bajo su exclusivo control y cuya custodia esta bajo su responsabilidad.

I.3.6.2.9 Preparación de los Dispositivos seguros de creación de Firma

La FNMT-RCM proporciona a las *Entidades usuarias* que así lo requieran, *Tarjetas criptográficas* para la generación de sus *Claves Privadas* y el almacenamiento de los *Certificados*.

La *Tarjeta criptográfica* es entregada a la *Entidad usuaria* sin ningún tipo de contenido, con las utilidades software necesarias para conseguir una integración con los *navegadores* más utilizados. Así mismo, en el mismo momento se le proporcionan los códigos necesarios para el acceso a dicha tarjeta para que posteriormente desde su puesto, la *Entidad usuaria* genere sus *Claves* e inserte el *Certificado* en ella si así lo desea.

Todo esto se hace para ayudar a las *Entidades usuarias* a que cumpla con su obligación de mantener el "exclusivo control" sobre los *Datos de creación de Firma*.

I.3.6.3 Infraestructura de *Clave Pública*. Gestión del ciclo de vida de los *Certificados*

I.3.6.3.1 Registro de las *Entidades usuarias*

Con carácter previo al establecimiento de cualquier relación contractual con las *Entidades usuarias* la FNMT-RCM informa a las interesadas en adquirir este estatus, acerca de las condiciones del servicio, así como de la obligaciones, garantías y responsabilidades que asumen las partes implicadas en la expedición y uso de los *Certificados* emitidos por el *Prestador de Servicios de Certificación* de la FNMT-RCM.

La FNMT-RCM en su actividad como *Prestador de Servicios de Certificación* procede, por ella misma o por terceros con los que tenga firmados convenios de colaboración, a confirmar la identidad de los *Solicitantes* de *Certificados* mediante presencia física ante las *Oficinas de Registro* y comprobación de los documentos necesarios para tal propósito, siendo esta documentación diferente según se trate de una persona física, jurídica o cuando el *Solicitante* actúe en representación de tercero.

La FNMT-RCM recabará de los *Solicitantes* solo aquella información que sea necesaria para la expedición de los *Certificados* y para la comprobación de la identidad, almacenándolos datos un periodo de quince (15) años y tratándolos con la debida diligencia para el cumplimiento de la legislación nacional vigente en materia de protección de datos personales (a este respecto véase lo dispuesto en los apartados "9.22 Datos de Carácter Personal" y "9.20.1.5 Protección de los Datos de Carácter Personal").

La FNMT-RCM, dado que en su actividad como *Prestador de Servicios de Certificación* no genera el par de *Claves* de las *Entidades usuarias*, pone todos los mecanismos necesarios durante el proceso de *Solicitud de Certificados* para posibilitar que el *Solicitante* se encuentra en posesión de la *Clave Privada* asociada a la *Clave Pública* que se certificará.

Las *Prácticas de Certificación* puestas en funcionamiento para la gestión expuesta puede verse con detalle en el documento *Declaración de Prácticas de Certificación de la FNMT-RCM*.

I.3.6.3.2 Renovación de *Certificados*

Cuando se extingue la vigencia de un *Certificado* (bien por caducidad, bien por revocación) la FNMT-RCM obliga a las *Entidades usuarias* a la generación de un nuevo par de *Claves* para dar lugar a nuevos *Datos de creación de Firma* y *Datos de verificación de Firma*.

Para los *Certificados* emitidos bajo esta *Política de Certificación* se permitirá la renovación de forma telemática autenticando a la *Entidad usuaria* en base al *Certificado* previamente expedido (cuya identificación se hizo de forma presencial) si bien esta operación sólo se podrá realizar cuando no se haya superado el plazo máximo de 5 años desde la personación e identificación física del Suscriptor que establece la Ley de firma electrónica 59/2003, de 19 de diciembre, en su artículo 13.4.

I.3.6.3.3 Generación de *Certificados*

La FNMT-RCM garantiza la confidencialidad e integridad de los datos recabados en el proceso de registro y el envío de forma segura a las instalaciones del *Prestador de Servicios de Certificación*.

La FNMT-RCM, dado que en su actividad como *Prestador de Servicios de Certificación* no genera el par de *Claves* de las *Entidades usuarias*, pone todos los mecanismos necesarios durante el proceso de solicitud de los *Certificados* para procurar que el *Solicitante* se encuentra en posesión de la *Clave Privada* asociada a la *Clave Pública* que se certificará.

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

I.3.6.3.4 Difusión de Términos y Condiciones

La FNMT-RCM pone a disposición de la *Comunidad Electrónica* tanto el documento de *Política de Certificación de Certificados Reconocidos de la FNMT-RCM* como el documento de *Declaración de Prácticas de Certificación de la FNMT-RCM* en los que se detalla:

- Los términos y condiciones que regulan la utilización de los *Certificados* expedidos por la FNMT-RCM.
- La *Política de Certificación* aplicable a los *Certificados* expedidos por la FNMT-RCM.
- Los límites de uso para los *Certificados* expedidos bajo esta *Política de Certificación*.
- Las obligaciones, garantías y responsabilidades de las partes en el ámbito de la emisión y uso de los *Certificados*.
- Los períodos de retención de la información recabada en el proceso de registro y de los eventos producidos en los sistemas del *Prestador de Servicios de Certificación* relacionados con la gestión del ciclo de vida de los *Certificados* emitidos bajo esta *Política de Certificación*.
- El sistema legal aplicable, así como los procedimientos para la interposición de reclamaciones y la resolución de disputas.

I.3.6.3.5 Difusión de *Certificados*

La FNMT-RCM, en su actividad como *Prestador de Servicios de Certificación* pone a disposición de la *Comunidad Electrónica* un sistema de consulta del estado del propio *Certificado* de la Entidad usuaria, como un servicio *web* en el que el suscriptor se autenticará con su propio *Certificado*.

En ningún caso, la FNMT-RCM proporciona un servicio de consulta de *Certificados* de otros *Suscriptores*.

I.3.6.3.6 Suspensión y Revocación de *Certificados*

La FNMT-RCM dispone de diferentes procedimientos para la suspensión y revocación de *Certificados*. Estos procedimientos, así como las causas admitidas para la suspensión y revocación de los *Certificados* se exponen detalladamente en el apartado "9.12 Vigencia de los Certificados" de la *Declaración de Prácticas de Certificación*.

Únicamente las *Entidades usuarias* de Derecho Público tendrán acceso a las *Listas de Revocación*, ya sea ésta originaria o replicada, y en las condiciones establecidas en el correspondiente convenio de incorporación a la *Comunidad Electrónica*.

Las *Entidades usuarias* de Derecho Privado, previa incorporación a la *Comunidad Electrónica*, dispondrán de un *Cliente OCSP* para comprobar el estado de los *Certificados* mediante consultas vía OCSP, según se refiere en el apartado "9.15 Servicio de validación de Certificados mediante *OCSP*" de la *Declaración de Prácticas de Certificación*.

La FNMT-RCM utilizará mecanismos adecuados de firma electrónica para dotar de *Integridad* y autenticidad a la información sobre el estado de los *Certificados*, que proporcione.

La FNMT-RCM pondrá todos los medios a su alcance para que la disponibilidad de estos servicios de comprobación del estado de los *Certificados* sea la máxima posible.

I.3.6.4 Operación y Gestión de la *Infraestructura de Clave Pública*

Las operaciones y procedimientos realizados para la puesta en práctica de la presente *Política de Certificación* se realizan siguiendo los controles requeridos por los estándares reconocidos para tal efecto, describiéndose estas actuaciones en los apartados "6.2 Controles de seguridad física, de procedimientos y del personal**"** y "6.3 Controles de seguridad técnica**"** de la *Declaración de Prácticas de Certificación* de la FNMT-RCM.

De forma informativa cabe decir que la FNMT-RCM se encuentra inmersa en un proyecto de establecimiento de un *Sistema de Gestión de la Seguridad de la Información* (en adelante *SGSI*) para su Departamento CERES con el objetivo final de mantener y garantizar la seguridad de la información de los clientes, así como la suya propia, de forma que el servicio prestado por la FNMT-RCM-CERES tenga los niveles suficientes de fiabilidad que exige el Mercado. El SGSI de la FNMT-RCM-CERES es aplicable a los activos de información definidos en el Análisis de Riesgos realizado para todas las Áreas que componen el departamento, incluyendo como activos los servicios prestados a los Clientes.

En el documento *Declaración de Practicas de Certificación*, se da respuesta concreta para todos aquellos aspectos referentes a los siguientes apartados de la norma ETSI TS 102 042:

- 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.

I.3.6.5 Aspectos organizativos

La FNMT-RCM es un Ente Público Empresarial dependiente del Ministerio de Economía, con capital 100% público y que goza del prestigio institucional de su larga tradición histórica y del respaldo del Estado.

La FNMT-RCM a pesar de contar con una larga trayectoria y el importante respaldo del Estado, ha apostado también fuerte por el reconocimiento del entorno privado en este nuevo sector que representa la certificación electrónica y las redes telemáticas abiertas, llegando a ser el primer y único prestador de servicios de certificación que ha alcanzado la acreditación de su sistema de gestión de la calidad de acuerdo a la normativa ISO 9001: 2000, otorgado por AENOR e IQNET para la prestación de servicios de certificación de firma electrónica, de sellado de tiempo y de desarrollo de sistemas operativos criptográficos para tarjetas inteligentes.

Así mismo, la FNMT-RCM tiene acreditada sus buenas prácticas y su código de conducta a través de la Agencia de la Calidad en Internet. El sello de calidad de IQUA es una garantía del nivel de calidad de las páginas web que lo obtienen basándose en los códigos de conducta sectoriales elaborados por los miembros adheridos de IQUA, y sus páginas son auditadas para garantizar su respeto a las normas de comportamiento aprobadas por el sector al que correspondan.

También citar, que los servicios de la FNMT-RCM son evaluados por el Centro de Evaluación de la Seguridad de las Tecnologías de la Información del INTA, dependiente del Ministerio de Defensa, garantizando así su idoneidad técnica.

ANEXO II PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS CERTIFICADOS DE IDENTIDAD DE PERSONA FÍSICA

El Presente anexo trae causa y forma parte integrante de la *Declaración de Prácticas de Certificación* de la FNMT-RCM, adjuntándose a las mismas como addendum.

En especial deberá tenerse presente, a efectos interpretativos del presente anexo el apartado "1.DEFINICIONES" del cuerpo principal de la *Declaración de Practicas de Certificación.*

Estas *Prácticas de Certificación* particulares definen el conjunto de prácticas adoptadas por la FNMT-RCM como *Prestador de Servicios de Certificación* para la gestión del ciclo de vida de los *Certificados de Identidad de Persona Física*, expedidos bajo la *Política de Certificación de Certificados Reconocidos de la FNMT-RCM* identificada con el OID 1.3.6.1.4.1.5734.3.5.

II.1. TIPOLOGÍA DEL CERTIFICADO DE IDENTIDAD DE PERSONA FÍSICA

El *Certificado de identidad de persona física*, también conocido como *Certificado* de usuario de la FNMT-RCM (Clase 2 CA), es la certificación electrónica expedida por la FNMT-RCM que vincula a su *Suscriptor* unos *Datos de verificación de Firma* y confirma su identidad. Este *Certificado*, es emitido como *Certificado Reconocido* con base en los criterios establecidos para tal en la Ley de Firma Electrónica (Ley 59/2003) y en la normativa técnica EESSI, concretamente ETSI TS 101 456 - "Policy requirements for certification authorities issuing qualified certificates" y ETSI TS 101 862 – "Qualified Certificate Profile", tanto en lo referente al *Prestador de Servicios de Certificación* como a la generación de los *Datos de creación de Firma* y al contenido del propio *Certificado*.

II.2 GESTIÓN DEL CICLO DE VIDA DEL *CERTIFICADO* DE IDENTIDAD DE PERSONA FÍSICA

Se definen aquí aquellos aspectos que, si bien ya han sido apuntados en el cuerpo principal de la *Declaración de Prácticas de Certificación* de la que este anexo forma parte, necesitan ser explicados con un mayor nivel de detalle.

II.2.1 Procedimiento de solicitud del *Certificado de identidad de persona física*

A continuación se describe el procedimiento de solicitud por el que se toman los datos personales de un *Solicitante*, se confirma su identidad y se formaliza su contrato con la FNMT-RCM para la posterior emisión de un *Certificado de identidad de persona física* una vez realizadas las validaciones pertinentes.

Estas actividades serán realizadas por las *Oficinas de Registro* implantadas por las *Entidades usuarias* con las que la FNMT-RCM haya suscrito el convenio correspondiente.

II.2.1.1 Obtención de la *Tarjeta criptográfica* y del software de generación o importación de *los Datos de creación y de verificación de Firma* en la Tarjeta

La *Tarjeta criptográfica* es un *Dispositivo seguro de creación de Firma* que puede ser empleada para generar los *Datos de creación y de verificación de Firma* o para importar tales datos.

La FNMT-RCM recomienda para el uso del *Certificado* expedido, la utilización de una *Tarjeta criptográfica* para evitar la posibilidad de duplicación de los *Datos de creación y verificación de Firma* y poseer un mejor control de los mismos.

Si el interesado desea una *Tarjeta Criptográfica de la FNMT-RCM*, deberá proceder con carácter previo a la fase de presolicitud a obtener dicha Tarjeta. A este respecto consúltese la información que la FNMT-RCM pone a disposición del público a través de la dirección http://www.cert.fnmt.es.

El interesado puede desear la simple descarga del *Certificado* a este soporte, o la generación en el mismo de las *Claves*, que posteriormente serán utilizadas como *Datos de creación* y *verificación de Firma*. En ambos casos, además de la *Tarjeta criptográfica*, el interesado deberá obtener el software necesario para la importación y/o generación de las *Claves* por la propia Tarjeta.

En el procedimiento de obtención de *Certificados* por parte del interesado, la FNMT-RCM facilitará, en el caso de emplearse como soporte del *Certificado* la *Tarjeta Criptográfica*, los elementos necesarios para activar, en el puesto del *interesado*, el software pertinente para generar, a través de su *Navegador*, las *Claves* criptográficas que le permitan proteger la seguridad de sus comunicaciones a través de mecanismos de cifrado, así como autenticarse y firmar, constituyéndose en este último caso como *Datos de creación y de verificación de Firma*.

Asimismo, cuando el *Certificado* resida en soporte convencional y no en *Tarjeta criptográfica*, los *Datos de creación de Firma* también serán utilizados bajo el control del software de *navegación web* del que disponga el propio interesado, enviando la *Clave Pública* que será utilizada como *Datos de verificación de Firma* a la FNMT-RCM con el fin de integrarla en un *Certificado*.

En cualquier caso, y con independencia del soporte empleado para almacenar el *Certificado*, los *Datos de creación de Firma* permanecerán siempre bajo el exclusivo control del *Suscriptor* de los mismos, no guardándose copia de ellos por la FNMT-RCM.

Una vez obtenido este soporte y el software necesario para la operativa que desee realizar, o bien si el *Certificado* se almacenara en un soporte convencional de almacenamiento de software, el interesado procederá según se dispone a continuación.

II.2.1.2 Presolicitud

El interesado accede al *sitio web* del *Prestador de Servicios de Certificación* de la FNMT-RCM, a través de la dirección http://www.cert.fnmt.es/clase2/main.htm, donde se mostrarán las instrucciones del proceso completo. Deberá introducir su NIF o NIE en el punto de recogida de datos dispuesto para ello. Posteriormente se generarán las *Claves Pública* y *Privada* (en *Tarjeta criptográfica* o en el *navegador)* que serán vinculadas al *Certificado*, el cual deberá ser solicitado en una *Oficina de Registro,* y se asigna e indica al interesado un código de solicitud.

Con carácter previo el *Solicitante* podrá consultar la *Declaración de Prácticas de Certificación* en la dirección http://www.cert.fnmt.es/convenio/dpc.pdf con las condiciones de uso y obligaciones para las partes, sin perjuicio de que con posterioridad, *Solicitante*, *Oficina de Registro*, y FNMT-RCM, deban suscribir el contrato de solicitud y la *Declaración de Prácticas de Certificación.* En ningún caso la continuación del procedimiento de presolicitud implicará la conclusión de una contratación.

Al realizar esta presolicitud se envía a la FNMT-RCM la *Clave Pública* generada para la posterior emisión del *Certificado*, entregándose de forma automatizada la correspondiente prueba de posesión de la *Clave privada*.

La FNMT-RCM, tras recibir esta información, comprobará mediante la *Clave Pública* del peticionario la validez de la información de la presolicitud cifrada, comprobando únicamente que se corresponde con los datos facilitados por el peticionario. Asimismo esta operación servirá como indicador de la posesión y correspondencia de la pareja de *Claves* criptográficas por parte del peticionario.

Esta información no dará lugar a la generación de un *Certificado* por parte de la FNMT-RCM, en tanto que ésta no reciba firmada por la *Oficina de Registro* la solicitud del *Certificado* realizada por el interesado que, a partir de ese momento, tendrá la consideración de *Solicitante*.

II.2.1.3 Confirmación de la identidad personal

A) Personación ante las Oficinas de Registro

La personación podrá realizarse ante la FNMT-RCM o ante cualquier *Oficina de Registro* con la que ésta tenga suscrito un acuerdo. En ambos casos la comparecencia se llevará a cabo según el criterio vigente de la FNMT-RCM, al objeto de que ésta sea homogénea en todos los casos.

B) Comparecencia y documentación

En este acto el *Solicitante* aportará los datos que se le requieran y acreditará su identidad personal.

En todo caso, los *Solicitantes* de *Certificados* deberán comparecer físicamente para formalizar el procedimiento de confirmación de identidad personal, presentándose en la *Oficina de Registro* autorizada, en posesión de su DNI, válido y vigente, o de otros medios admitidos en derecho a efectos de identificación. Cuando el *Solicitante* sea extranjero y no posea el DNI, deberá estar en posesión del Documento Nacional de Identificación de Extranjeros. El encargado de acreditación de la *Oficina de Registro* verificará que los documentos aportados cumplen todos los requisitos para confirmar la identidad del *Solicitante*.

La personación del *Solicitante* no será indispensable si la firma en la solicitud de expedición de un *Certificado* ha sido legitimada en presencia notarial, o si se solicita una renovación de *Certificado*, de conformidad con lo dispuesto en el apartado "*9.16 Renovación de certificados*" de la presente *Declaración de Prácticas de Certificación*.

C) Envío de información a la FNMT-RCM

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

II.2.2 Emisión del *Certificado de identidad de persona física*

Una vez recibidos en la FNMT-RCM los datos personales del *Suscriptor*, así como el código de solicitud obtenido en la fase de presolicitud, se procederá a la emisión del *Certificado*.

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

La FNMT–RCM, por medio de su *Firma electrónica reconocida*, autentica los *Certificados* y confirma la identidad de sus *Suscriptores*. Por otro lado y con el fin de evitar la manipulación de la información contenida en los *Certificados*, la FNMT-RCM utilizará mecanismos criptográficos que doten de autenticidad e integridad al *Certificado*.

La FNMT-RCM en ningún caso incluirá en un *Certificado* información distinta de la aquí mostrada, ni circunstancias, atributos específicos de los firmantes o limites económicos diferentes a los expuestas en los siguientes apartados.

En cualquier caso la FNMT-RCM actuará diligentemente para:

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

II.2.2.1 Composición del nombre distintivo (*DN*) del *Suscriptor*

Con los datos personales del *Solicitante* recogidos durante el proceso de solicitud del *Certificado*, se procede a componer el nombre distintivo (*DN*) del *Solicitante* 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 un *Suscriptor* está compuesto de los siguientes elementos:

DN≡CN, OU, OU, OU, O, C

El conjunto de atributos OU, OU, OU, O, C representa la rama del directorio en la que se encuentra ubicada la entrada correspondiente al *Suscriptor* en cuestión.

El atributo *CN* contiene los datos de identificación del *Suscriptor* que para el caso de los *Certificados de Identidad de Persona Física* seguirá la siguiente sintaxis:

CN= NOMBRE a1 a2 n – NIF 12345678A

Donde:

NOMBRE y NIF son etiquetas [1]

n, a1 y a2 son los nombres, primer y segundo apellido del *Suscriptor* respectivamente[2]

12345678A es su correspondiente NIF [3].

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

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

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

Una vez compuesto el nombre distintivo (*DN*) que identificará al *Suscriptor*, 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*.

II.2.2.2 Composición de la identidad alternativa del *Suscriptor*

La identidad alternativa del *Suscriptor*, tal como se contempla en la presente tipología de *Certificados* contiene la misma información que el *CN*, distribuida en una serie de atributos, de forma que sea más sencilla la obtención de los datos personales del *Suscriptor* del *Certificado*. Se utiliza la extensión subjectAltName definida en *X.509* versión 3 para ofrecer esta información.

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

Tipo Certificado	Información	Atributo FNMT	OID (*)
Persona física [1]	Nombre	fnmtNombre	fnmtoid.1.1
	Primer apellido	fnmtApellido1	fnmtoid.1.2
	Segundo apellido	fnmtApellido2	fnmtoid.1.3
	NIF	fnmtNif	fnmtoid.1.4

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

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

II.2.2.3 Perfil del *Certificado de identidad de Persona Física*

El formato del *Certificado de Identidad de Persona Física* expedido por la FNMT-RCM bajo la *Política de Certificación de Certificados Reconocidos de la FNMT-RCM*, en consonancia con la norma UIT-T X.509 versión 3 y de acuerdo con la normativa legalmente aplicable en materia de *Certificados Reconocidos*, contiene los siguientes campos:

Campo	O.I.D	Valor
Campos Básicos		
Version		2 (X.509 v3)
SerialNumber		Número de serie del *Certificado.* **[1]**
Issuer		C=ES,O=FNMT,OU=FNMT Clase 2 CA
Validity		**[2]**
Subject		**Nombre distintivo del *Suscriptor*.** **[3]**
SubjectPublicKeyInfo		RsaEncryption, *Clave Pública.* **[4]**
SignatureAlgIdentifier	1.2.840.113549.1.1.5	Identificador de Algoritmo de Firma

		electrónica utilizado. **[5]**
Extensiones Estándar		
KeyUsage	2.5.29.15	**[6]**
PrivateKeyUsageperiod	2.5.29.16	El mismo que Validity
SubjectAltName	2.5.29.17	**[7]**
CertificatePolicies	2.5.29.32	*Política de Certificación* **[8]**
CRLDistributionPoints	2.5.29.31	Cn=CRLnnn,c=ES, o=FNMT,OU=FNMT Clase 2 CA **[9]**
AuthorityKeyIdentifier	2.5.29.35	Identificador de *Clave* del *Prestador de Servicios de Certificación*
SubjectKeyIdentifier	2.5.29.14	Identificador de *Clave* del *Suscriptor*
BasicConstraints	2.5.29.19	Restricciones básicas. Entidad Final
Extensiones Privadas		
NetscapeCertType	2.16.840.1.113730.1	**[10]**
QCStatement	1.3.6.1.5.5.7.1.3	**[11]**
fnmtTipoCertificado	1.3.6.1.4.1.5734.1.33	**[12]**

Donde:

[1] SerialNumber: Número de identificación para el *Certificado* único dentro de la infraestructura del *Prestador de Servicios de Certificación*.

[2] Validity: Período de validez del *Certificado* tal y como se muestra en el apartado "II.2.5 Periodo de validez del *Certificado*" del presente anexo.

[3] Subject: Identificación del *Suscriptor* del *Certificado*. Su composición ha sido detallada con anterioridad en este apartado.

[4] SubjectPublicKeyInfo: Es la *Clave Pública* que el *Suscriptor* generó en la fase de presolicitud de emisión del *Certificado*.

[5] SignatureAlgIdentifier: Identificación del algoritmo utilizado para realizar la *Firma electrónica* del *Certificado*. El algoritmo utilizado es SHA1WithRSAEncryption (*OID* 1.2.840.113549.1.1.5) siendo la longitud de la *Clave* utilizada de 1024 bits.

[6] KeyUsage: Valores admitidos para el uso de la *Clave*. **No está marcada como crítica.**

Toma los valores **{digitalSignature, keyEncipherment}.**

[7] SubjectAltName: Identidad Alternativa del *Suscriptor*. **No está marcada como crítica.**

Su concreta composición ha sido detallada con anterioridad en este apartado.

[8] *Políticas de Certificación* aplicables al *Certificado*: No está marcada como crítica.

Su contenido es el mostrado a continuación:

OID de Políticas: 1.3.6.1.4.1.5734.3.5

Texto de aviso= *Certificado Reconocido* expedido según legislación vigente. Uso limitado a la *Comunidad Electrónica* por valor máximo de 100 € salvo excepciones en DPC.

Contacto FNMT: C/Jorge Juan 106-28009-Madrid-España.

Localización de Política: http://www.cert.fnmt.es/convenio/dpc.pdf

[9] CRLDistributionPoint: El punto concreto de distribución de las *Listas de Revocación*, es generado por el *Prestador de Servicios de Certificación* en el mismo momento en que procede a la generación de *Certificado*. **No está marcada como crítica.**

[10] NetscapeCertType: Tipo de certificado según Netscape. **No está marcada como crítica.**

Toma los valores **{sSLCLIENT, sMIME}.**

[11] QCStatement: No está marcada como crítica. Contiene indicación expresa de que el *Certificado* ha sido emitido como *Certificado Reconocido* y el límite de uso monetario (100€) utilizando para ello los *OIDs* estipulados en la normativa vigente. Su contenido es el mostrado a continuación:

QcEuCompliance (OID 0.4.0.1862.1.1)

QcEuLimitValue (OID 0.4.0.1862.1.2) : 100 €

[12] fnmtTipoCertificado : No está marcada como crítica.

Se incluye un indicativo textual del tipo de *Certificado*, que para el *Certificado de Identidad de Persona Física* es:

"PERSONA FISICA"

II.2.3 Publicación del *Certificado de Identidad de persona física*

Una vez generado el *Certificado* por parte del *Prestador de Servicios de Certificación*, se publicará en el *Directorio*, concretamente en la entrada correspondiente al nombre distintivo del *Suscriptor*, tal como se ha definido en el apartado *"II.2.2 Emisión del Certificado"* de este anexo.

Si en el proceso de solicitud el *Solicitante* proporcionó una dirección de correo electrónico, se le enviará una comunicación de la disposición de su *Certificado* para su descarga.

II.2.4 Descarga e instalación del *Certificado de Identidad de persona física*

Una vez transcurrido el tiempo establecido desde que el *Solicitante* se persona en las *Oficinas de Registro* para acreditar su identidad, y una vez que el *Certificado* haya sido generado, se pone a disposición del *Solicitante* un mecanismo de descarga de *Certificado* en la dirección http://www.cert.fnmt.es/clase2/main.htm, accediendo a la opción "Descarga de su Certificado".

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

Si el *Certificado* ya ha sido puesto a disposición del *Solicitante*, éste será introducido en el soporte en el que se generaron las *Claves* durante el proceso de Presolicitud (*Tarjeta criptográfica* de la FNMT-RCM o soporte convencional de almacenamiento de software a través del *navegador*).

II.2.5 Período de validez del Certificado de Identidad de persona física

El periodo de validez de los *Certificados de Identidad de Persona Física* emitidos por la FNMT-RCM será de tres (3) años contados a partir del momento de la emisión del *Certificado*, siempre y cuando no se extinga su vigencia por las causas y procedimientos expuestos en el apartado "9.12.2 Extinción de la vigencia del Certificado" de la *Declaración de Prácticas de Certificación*.

II.2.6 Revocación del *Certificado de Identidad de persona física o*

La revocación de *Certificados* implica, además de su extinción, la finalización de la relación jurídica con la FNMT-RCM que se mantuviese al respecto.

La revocación de un *Certificado de Identidad de Persona Física* podrá ser solicitada por los entes descritos en el apartado "9.12.3 Revocación de *Certificados*" de la *Declaración de Prácticas de Certificación* en los términos y condiciones allí expresados.

A continuación se describe el procedimiento por el que se toman los datos personales de un *Solicitante*, se confirma su identidad y se formaliza la solicitud de revocación de un *Certificado* por parte de un legítimo interesado. Serán causas admitidas para la revocación de un *Certificado* las expuestas en el apartado "9.12.3.1 Causas de revocación de *Certificados*" de la *Declaración de Prácticas de Certificación*.

Estas actividades serán realizadas por las *Oficinas de Registro* implantadas por las *Entidades usuarias* con las que la FNMT-RCM haya suscrito el convenio correspondiente o bien de forma telemática, caso de estar en posesión del *Certificado* y de sus correspondientes *Datos de creación de Firma*.

II.2.6.1 Si el *Suscriptor* del *Certificado de Identidad de persona física* está en posesión del *Certificado*

En este caso, y dado que el *Suscriptor* puede ser autenticado con base en su *Certificado* deberán solicitar la revocación a través de Internet, o de cualquier otra vía equivalente que permita la conexión a la dirección http://www.cert.fnmt.es/clase2/revoca.htm, siguiendo los pasos que se indican en la opción "Revocación del *Certificado*".

II.2.6.2 Si el peticionario no está en posesión del *Certificado*, o no dispone del resto de herramientas necesarias para solicitar la revocación telemáticamente

En este caso podrá solicitar la revocación del *Certificado* personándose en una *Oficina de Registro* para identificarse. Una vez acreditada su identidad, el peticionario deberá firmar el modelo de solicitud de revocación del *Certificado* que se le presente. Este modelo se corresponderá con el mostrado en el apartado "II.5 Modelos de formulario" del presente anexo. Posteriormente las *Oficinas de Registro* transmitirán los registros tramitados a la FNMT-RCM para que ésta proceda a la revocación del *Certificado*.

Una vez que la FNMT-RCM ha procedido a la revocación del *Certificado*, se publicará en el *Directorio* seguro la correspondiente *Lista de Revocación* indicando el número de serie del *Certificado* revocado, la fecha y hora en que se ha realizado la revocación y la causa de revocación.

II.2.7 Suspensión del *Certificado de Identidad de persona física*

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

La suspensión de los *Certificados*, podrá ser solicitada por las entidades descritas en el apartado "9.12.4 Suspensión de Certificados" de la *Declaración de Prácticas de Certificación* en los términos y condiciones allí expresados.

A continuación se describe el procedimiento por el que se le toman los datos personales, se confirma su identidad, y en su caso se formaliza la solicitud de suspensión de un *Certificado* por parte de un legítimo interesado. Serán causas admitidas para la suspensión de un *Certificado* las expuestas en el apartado "9.12.4.1 Causas de suspensión de *Certificados*" de la *Declaración de Prácticas de Certificación.*

Estas actividades serán realizadas por las *Oficinas de Registro*, implantadas por las *Entidades usuarias* con las que la FNMT-RCM haya suscrito el convenio correspondiente, o bien de forma telemática, caso de estar en posesión del *Certificado* y de sus correspondientes *Datos de creación de Firma*.

Adicionalmente se podrá efectuar la solicitud de suspensión del *Certificado* con carácter general, solicitándolo en el teléfono 902 200 616 a la FNMT-RCM.

La FNMT-RCM procederá a suspender el *Certificado* de forma provisional durante un plazo de noventa (90) días, plazo tras el cual se extinguirá el *Certificado* mediante su revocación directa por parte del *Prestador de Servicios de Certificación* de la FNMT-RCM, salvo que se hubiera levantado la suspensión por parte del *Suscriptor*. No obstante lo anterior, el plazo previsto para la suspensión del *Certificado* podrá verse alterado en función de los procedimientos judiciales o administrativos que lo pudieran afectar.

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.

II.2.7.1 Si el *Suscriptor* del *Certificado de Identidad de persona física* está en posesión del *Certificado*

En este caso, y dado que el *Suscriptor* puede ser autenticado con base en su *Certificado*, podrá solicitar la suspensión a través de Internet, o de cualquier otra vía equivalente que permita la conexión a la dirección http://www.cert.fnmt.es/clase2/suspension.htm siguiendo los pasos que se indican en la opción "Suspensión del certificado".

II.2.7.2 Si el legítimo peticionario no está en posesión del *Certificado*, o no dispone del resto de herramientas necesarias para solicitar la suspensión telemáticamente

En este caso podrán solicitar la suspensión del *Certificado* personándose en una *Oficina de Registro* para identificarse. Una vez acreditada su identidad, el legítimo peticionario deberá firmar el modelo de solicitud de suspensión del *Certificado* que se le presente. Este modelo se corresponderá con el mostrado en el apartado "II.5 Modelos de formulario" del presente anexo.

Posteriormente las *Oficinas de Registro* transmitirán los registros tramitados a la FNMT-RCM para que ésta proceda a la suspensión del *Certificado*.

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

II.2.8 Cancelación de la suspensión del Certificado de Identidad de persona física

Podrán solicitar el Cancelación de la suspensión de los *Certificados* emitidos por la FNMT-RCM los *Suscriptores*, siempre que, con anterioridad a esta solicitud de Cancelación de la suspensión, conserven el *Certificado* y su *Clave Privada*, y dicha solicitud se efectúe durante los noventa (90) días siguientes a su suspensión.

La comparecencia se llevará ante la Oficina de Registro según el criterio vigente de la FNMT-RCM, al objeto de que ésta sea homogénea en todos los casos.

En este acto el *Solicitante* aportará los datos que se le requieran y acreditará su identidad personal, siguiendo el procedimiento descrito anteriormente para la solicitud de emisión del *Certificado de Identidad de persona física*.

La personación del *Solicitante* no será indispensable si la firma en la solicitud de levantamiento de suspensión del *Certificado* ha sido legitimada en presencia notarial.

Los datos personales del *Solicitant*e, una vez validados por la *Oficina de Registro*, se enviarán a la FNMT-RCM mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM.

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

II.2.9 Renovación del *Certificado de Identidad de persona física*

Podrán solicitar la renovación de los *Certificados* emitidos por la FNMT-RCM los *Suscriptores*, siempre que en el momento de la solicitud tengan un *Certificado* en vigor y sus *Datos de creación de Firma* asociados y, dicha solicitud, se efectúe durante los sesenta (60) días anteriores a su c*aducidad* (en este sentido véase el apartado "*9.12.1 Caducidad*" del cuerpo principal de la presente *Declaración de Prácticas de Certificación*).

Efectuada la renovación de los *Certificados*, su validez será la misma que la expresada en el apartado "*Período de validez del Certificado*"del presente anexo.

El antiguo *Certificado* que se haya procedido a renovar seguirá siendo válido hasta que caduque. En caso de solicitarse la revocación del *Certificado*, la FNMT-RCM procederá a revocar ambos *Certificados*. El procedimiento de renovación lleva asociado la generación de una nueva pareja de *Claves* criptográficas.

El peticionario deberá conectarse a la dirección http://www.cert.fnmt.es/clase2/main.htm y seguir los pasos que se indique en la opción "*Renovar Certificado*".

El procedimiento establecido no requiere la personación del peticionario, ya que se le identificará telemáticamente mediante la utilización de sus *Datos de creación de Firma*. Tanto el proceso de la solicitud como la obtención del *Certificado*, se realizará de forma telemática, requiriéndose en todo caso la generación por parte del peticionario, de una *Firma electrónica Reconocida* del documento de solicitud de renovación, si bien se indica que la renovación telemática del *Certificado* sólo se podrá realizar cuando no se haya superado el plazo máximo de 5 años desde la personación e identificación física del Suscriptor que establece la Ley de firma electrónica 59/2003, de 19 de diciembre, en su artículo 13.4.

La utilización de los *Certificados* renovados se sujeta a las mismas condiciones generales y particulares vigentes en cada momento y establecidas para el tipo de *Certificado* renovado. A este respecto se deberá tener presente por ser de aplicación, lo establecido en el apartado "*12 Modificación de la Declaración de Practicas de Certificación*".

II.2.10 Comprobación del estado del *Certificado de Identidad de persona física*

El *Suscriptor* del *Certificado* y las *Entidades usuarias* pertenecientes a la *Comunidad Electrónica* podrá realizar la comprobación del estado de un *Certificado* en la forma y condiciones que se expresan en los apartados "9.14 Procedimientos de consulta del estado de los *Certificados*" y "9.15 Servicio de validación de *Certificados* mediante *OCSP*" de la *Declaración de Prácticas de Certificación*.

II.2.11 Terminación de la FNMT-RCM en su actividad como *Prestador de Servicios de Certificación*

Esta circunstancia y sus consecuencias se describen en el apartado "9.18 Cese de la actividad del *Prestador de Servicios de Certificación*", de la *Declaración de Prácticas de Certificación*.

II.3 OBLIGACIONES, GARANTÍAS Y RESPONSABILIDAD DE LAS PARTES

Las obligaciones, garantías y responsabilidades de las partes implicadas en la emisión y uso de los *Certificados* expedidos por la FNMT-RCM en su labor como *Prestador de Servicios de Certificación* quedan reflejadas en los apartados "9.20 Obligaciones y Garantías de las Partes" y "9.21 Responsabilidad de las Partes" de la *Declaración de Prácticas de Certificación* de la que el presente anexo forma parte.

II.4 LÍMITES DE USO DE LOS *CERTIFICADOS* DE IDENTIDAD DE PERSONA FÍSICA

Para poder usar los *Certificados* o ser diligente a la hora de confiar en documentos firmados electrónicamente con base en los mismos, se deberá previamente formar parte de la *Comunidad Electrónica*, y adquirir la condición de *Entidad usuaria*. Fuera de la *Comunidad Electrónica* no se debe confiar en un *Certificado* o en una *Firma electrónica* que se base en un *Certificado* emitido bajo la *Política de Certificación de Certificados Reconocidos de la FNMT-RCM*. En cualquier caso, de producirse esta confianza por parte de un tercero, no se obtendrá cobertura de la presente *Declaración de Prácticas de Certificación*, y se carecerá de legitimidad alguna para reclamar o emprender acciones judiciales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado*.

Además, incluso dentro del ámbito de una *Comunidad Electrónica*, no se podrá emplear este tipo de *Certificado* para:

- Firmar otro certificado.
- Firmar software o componentes.
- Generar sellos de tiempo para procedimientos de *Fechado electrónico.*
- Prestar servicios a título gratuito u oneroso, como por ejemplo serían a título enunciativo:
    - Prestar servicios de *OCSP*.
    - Generar *Listas de Revocación.*
    - Prestar servicios de notificación.
- Realizar transacciones económicas superiores a 100€, salvo que:
    - Uno de los intervinientes sea una *Entidad usuaria* de Derecho Público; o
    - Medie autorización expresa y escrita de la FNMT-RCM para hacerlo y, en ese caso, en las condiciones que se establezcan en dicha autorización.

II.5 MODELOS DE FORMULARIO

Los modelos de formularios que se deben cumplimentar para realizar las operaciones descritas para la gestión del ciclo de vida de los *Certificados* de Identidad de Persona Física se ponen a disposición en http://www.ceres.fnmt.es

ANEXO III PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS CERTIFICADOS DE PERSONA JURÍDICA PARA EL ÁMBITO TRIBUTARIO

El presente anexo forma parte integrante de la *Declaración de Prácticas de Certificación de la FNMT-RCM*. Estos certificados se ajustan a la *Política de Certificación de Certificados de Clave Pública de la FNMT-RCM.*

Estas *Prácticas de Certificación particulares de los Certificados de Persona jurídica para el ámbito tributario* definen el conjunto de prácticas adoptadas por la FNMT-RCM *como Prestador de Servicios de Certificación* para la gestión del ciclo de vida de los *Certificados de Persona jurídica para el Ámbito Tributario,* expedidos bajo la *Política de Certificación de Certificados de Clave Pública de la FNMT-RCM* identificada con el OID 1.3.6.1.4.1.5734.3.7.

III.1 TIPOLOGÍA DEL CERTIFICADO DE PERSONA JURÍDICA PARA EL ÁMBITO TRIBUTARIO

Certificado de Persona jurídica para el ámbito tributario es la certificación electrónica expedida por la FNMT-RCM que vincula a su *Suscriptor* (siempre *Sujeto pasivo tributario*), unos *Datos de verificación de Firma* y confirma su identidad. El Suscriptor de este *Certificado* lo podrá ser una "persona jurídica". Podemos entender por "persona jurídica": como aquel conjunto de personas agrupadas que constituye una unidad con finalidad propia, la cual adquiere, como entidad, capacidad jurídica y de obrar distinta de la de los miembros que la componen.

Este *Certificado* se corresponde con el certificado tradicional utilizado por el Ministerio de Hacienda o el Gobierno de Navarra para el ámbito tributario.

La custodia de los *Datos de creación de Firma* asociados al *Certificado de Persona jurídica para el ámbito tributario s*erá siempre obligación de la persona física solicitante (*Solicitante*), cuya identificación se incluirá en el *Certificado*.

III.2 GESTIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS DE PERSONA JURÍDICA PARA EL ÁMBITO TRIBUTARIO

III.2.1 Procedimiento de solicitud del *Certificado*

A continuación se describe el procedimiento de solicitud por el que se toman los datos personales de un *Solicitante*, se confirma su identidad así como la extensión y vigencia de sus facultades de representación sobre la persona jurídica que será *Suscriptor* del *Certificado de Persona Jurídica para el ámbito tributario*, y se formaliza su contrato con la FNMT-RCM para la posterior emisión de un *Certificado*, una vez realizadas las validaciones pertinentes.

Estas actividades serán realizadas por las *Oficinas de Registro* implantadas por la Agencia Estatal de Administración Tributaria, o por la Comunidad Foral de Navarra.

III.2.1.1 Obtención de la *Tarjeta Criptográfica* y del software de generación o importación de los *Datos de creación y de verificación de Firma* en la *Tarjeta*

La *Tarjeta criptográfica* es un *Dispositivo Seguro de Creación de Firma* que puede ser empleada para generar los *Datos de creación y de verificación de Firma* o para importar tales datos.

La FNMT-RCM recomienda el uso del *Certificado* generado en Tarjeta criptográfica para evitar la posibilidad de duplicación de los *Datos de creación de Firma* y poseer un mejor control de los mismos, quedando así el *Suscriptor* del *Certificado* dotado de unos medios técnicos tales que le

permitan cumplir con su obligación de mantener el exclusivo control sobre los Datos de creación de Firma al que la Ley le obliga.

Si el interesado desea una *Tarjeta criptográfica de la FNMT-RCM*, deberá proceder con carácter previo a la fase de presolicitud a obtener dicha *Tarjeta*. A este respecto consúltese la información que la FNMT-RCM pone a disposición del público a través de la dirección http://www.cert.fnmt.es.

El interesado puede desear la simple descarga del *Certificado* a este soporte o la generación en el mismo de las *Claves*, que posteriormente conformarán los *Datos de creación* y *verificación de Firma*. En ambos casos, además de la *Tarjeta criptográfica*, deberá obtener el software necesario para la importación y/o generación de las *Claves* por la propia Tarjeta.

En el procedimiento de obtención de *Certificados* por parte del *interesado*, la FNMT-RCM facilitará, en el caso de emplearse como soporte del *Certificado* la *Tarjeta criptográfica*, los elementos necesarios para activar, en el puesto del *interesado*, el software pertinente para generar, a través de su *Navegador*, las *Claves* criptográficas que le permitirán proteger la seguridad de sus comunicaciones a través de mecanismos de cifrado, así como firmar y autenticarse, constituyéndose en estos caso como *Datos de creación y de verificación de Firma*.

Asimismo, cuando el *Certificado* resida en soporte convencional y no en *Tarjeta criptográfica*, los *Datos de creación de Firma* también serán utilizados bajo el control del software de *navegación web* del que disponga el propio *interesado*, enviando la *Clave Pública* que ha de constituir los *Datos de verificación de Firma* a la FNMT-RCM con el fin de integrarlos en un *Certificado*.

En cualquier caso y con independencia del soporte empleado, los *Datos de creación de Firma* deberán permanecer siempre bajo el control exclusivo del *Suscriptor*, no guardándose copia de ellos por la FNMT-RCM.

Una vez obtenido este soporte y el software necesario para la operativa que desee realizar, o bien si el *Certificado* se almacenara en un soporte convencional, el interesado procederá según se dispone a continuación.

III.2.1.2 Presolicitud

El interesado accede al *sitio web* del *Prestador de Servicios de Certificación* de la FNMT-RCM, a través de la dirección http://www.cert.fnmt.es/clase2/main.htm, donde se mostrarán las instrucciones del proceso completo. Deberá introducir el CIF de la Persona Jurídica, o de la "entidad sin personalidad jurídica", para la que se solicita como *Suscriptora* el *Certificado*. Se generan (en *Tarjeta criptográfica* o en *navegador)* las *Claves Pública* y *Privada*, correspondientes al *Certificado* que se solicitará en la *Oficina de Registro* y se asigna al interesado un "código de presolicitud".

Con carácter previo el interesado podrá consultar la *Declaración de Prácticas de Certificación* en la dirección http://www.cert.fnmt.es/convenio/dpc.pdf con las condiciones de uso y obligaciones para las partes, sin perjuicio de que con posterioridad, *Solicitante*, *Oficina de Registro*, y FNMT-RCM, deban suscribir el contrato de solicitud y la *Declaración de Prácticas de Certificación.* En ningún caso la continuación del procedimiento de presolicitud implicará la conclusión de una contratación.

Al realizar esta presolicitud se envía a la FNMT-RCM la *Clave Pública* generada para la posterior emisión del *Certificado*, entregándose de forma automatizada la correspondiente prueba de posesión de la *Clave privada*.

La FNMT-RCM tras recibir esta información, comprobará mediante la *Clave Pública* del peticionario, la validez de la información de la presolicitud cifrada recibida comprobando únicamente que se corresponde con los datos facilitados por el peticionario. Asimismo esta operación servirá como indicador de la posesión y correspondencia de la pareja de *Claves* criptográficas por parte del peticionario.

Esta información no dará lugar a la generación de un *Certificado* por parte de la FNMT-RCM, en tanto que ésta no reciba firmada por la *Oficina de Registro*, la solicitud del *Certificado* realizada por el interesado quien, a partir de ese momento, tendrá la consideración de *Solicitante*.

III.2.1.3 Confirmación de los datos relativos a la entidad y de la identidad de la persona física que solicita la emisión de un *Certificado de Persona jurídica para el ámbito tributario*

A) Personación ante las Oficinas de Registro

La personación podrá realizarse ante cualquier *Oficina de Registro* de la Agencia Estatal de Administración Tributaria o de la Comunidad Foral de Navarra con la que ésta tenga suscrito un acuerdo para la emisión de estos *Certificados*.

B) Comparecencia y documentación

En este acto el *Solicitante* y cualquier otro tercero cuya personación fuera necesaria, aportarán los datos que se les requieran y acreditará su identidad personal así como la extensión y vigencia de sus facultades de representación sobre la entidad representada. La FNMT-RCM comprobará directamente o a través de tercero, los datos relativos a la constitución y, en su caso, personalidad jurídica, así como a a la extensión y vigencia de las facultades de representación del *Solicitante*, mediante los documentos públicos que sirvan para acreditar los extremos citados de manera suficiente.

En todo caso se exigirá con carácter general a los *Solicitantes* de estos *Certificados*, su personación ante los encargados de verificar su identidad, y se acreditará mediante el Documento Nacional de Identidad o Documento de Identificación de Extranjeros. Podrá prescindirse de la personación si su firma en la solicitud de expedición ha sido legitimada en presencia notarial, sin perjuicio de la necesidad de acreditar suficientemente la extensión y vigencia de sus facultades de representación.

Asimismo, el *Prestador de Servicios de Certificación* de la FNMT-RCM, con carácter particular, comprobará directamente o a través de tercero:

- Los datos relativos a la constitución y, en su caso, personalidad jurídica de la entidad para la que se solicita la emisión del *Certificado de Persona jurídica para el ámbito tributario*, y a la extensión y vigencia de las facultades de representación del *Solicitante* para realizar la mencionada solicitud, todos los trámites que se requieran durante el procedimiento de solicitud y expedición del *Certificado*, incluida la suscripción de los acuerdos que fueren necesarios en nombre y representación de la *Persona jurídica*, bien mediante consulta en el Registro público en el que estén inscritos los documentos de constitución y apoderamiento, bien mediante el análisis de los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente, cuando aquellos no sean de inscripción obligatoria.

Para realizar estas comprobaciones, el *Solicitante* del *Certificado de Persona Jurídica para el ámbito tributario* deberá aportar la siguiente documentación según sea el caso de la sociedad para la que realice la solicitud:

- Las sociedades mercantiles y demás personas jurídicas cuya inscripción sea obligatoria en el Registro Mercantil, certificado del Registro Mercantil relativo a los datos de constitución y personalidad jurídica de las mismas.
- Las Asociaciones, Fundaciones y Cooperativas no inscribibles en el Registro Mercantil, certificado del registro público donde consten inscritas, relativo a su constitución.
- Las Sociedades Civiles y demás personas jurídicas, documento público que acredite su constitución de manera fehaciente.
- Si el Solicitante es administrador o representante legal del sujeto a inscripción registral, certificado del Registro correspondiente relativo a su nombramiento y vigencia de su cargo. Dicho certificado deberá haber sido expedido durante los diez días anteriores a la fecha de solicitud del *Certificado de Persona Jurídica para el ámbito tributario.*
- En el supuesto de representación voluntaria, poder notarial que contenga una cláusula especial para solicitar el *Certificado de Persona Jurídica para el ámbito tributario.*
- La persona física *Solicitante* del *Certificado de Persona Jurídica para el ámbito tributario*, a efectos de su identificación, deberá personarse en cualquier oficina de acreditación, y se acreditará mediante Documento Nacional de Identidad o Número de Identificación para Extranjeros. Podrá prescindirse de su personación si su firma en la solicitud del *Certificado de Persona Jurídica para el ámbito tributario* ha sido legitimada en presencia notarial.

C) Envío de información a la FNMT-RCM

Una vez confirmada la identidad del Solicitante, y cuando corresponda, de la persona física representante del *Suscriptor*, y suscrito el contrato de solicitud por el *Solicitante*, el *Suscriptor* y la *Oficina de Registro*, esta procederá a validar los datos y a enviarlos junto con el código de presolicitud recogido en la fase de presolicitud, a la FNMT-RCM mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM.

Asimismo, la *Oficina de Registro* enviará a la FNMT-RCM los documentos (o copia compulsada de los mismos) utilizados para realizar la comprobación de los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del *Solicitante* y, de cualquier otro tercero en representación de la *Persona jurídica*, cuya comparecencia hubiese sido necesaria, a los meros efectos de cumplir con las obligaciones legales de conservación que impone la Ley núm. 59/2003, de 19 de diciembre, de firma electrónica.

III.2.2 Emisión del *Certificado de persona jurídica para el ámbito tributario*

Una vez recibidos en la FNMT-RCM los datos de la solicitud[2] , firmados por la *Oficina de Registro*, así como el "código de solicitud" obtenido en la fase de presolicitud, se procederá a la emisión del *Certificado*.

La emisión de *Certificados* supone la generación de documentos electrónicos que acreditan la identidad y otros extremos a petición del *Solicitante*, así como su correspondencia con la *Clave Pública* asociada. La emisión de *Certificados* por parte de la FNMT-RCM sólo puede realizarla ella misma, en su calidad de *Prestador de Servicios de Certificación*, no existiendo ninguna otra entidad u organismo con capacidad de emisión de los mismos.

La FNMT–RCM por medio de su *Firma electrónica reconocida*, autentica los *Certificados de Persona jurídica para el ámbito tributario*, y confirma la identidad del *Solicitante* y del *Suscriptor*. así como la verificación de la identidad y cuando corresponda, otras circunstancias personales de sus titulares. Por otro lado, y con el fin de evitar la manipulación de la información contenida en los *Certificados*, la FNMT-RCM utilizará mecanismos criptográficos para dotar de autenticidad e integridad a los *Certificado*.

La FNMT-RCM actuará diligentemente para:

- Procurar que el *Solicitante* del *Certificado* disponga de la *Clave Privada* correspondiente a la *Clave Publica* vinculada a la identidad del *Suscriptor* del mismo. Para ello la FNMT-RCM comprobará la posesión de la *Clave privada* y la correspondencia entre la *Clave privada* y la *Clave pública*.
- Lograr que la información incluida en el *Certificado* se base en la información proporcionada por el *Solicitante*.
- No ignorar hechos conocidos que puedan afectar a la fiabilidad del *Certificado.*
- Lograr que el *DN* (nombre distintivo) asignado en el *Certificado* sea único en toda la *Infraestructura de Clave Pública* de la FNMT-RCM.

III.2.2.1 Composición del nombre distintivo del *Suscriptor*

Con los datos personales del *Solicitante* recogidos durante el proceso de solicitud del certificado, se procede a componer el *DN* (nombre distintivo) del *Solicitante*, 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 un *Suscriptor* está compuesto de los siguientes elementos:

DN≡CN, OU, OU, OU, O, C

El conjunto de atributos *OU*, *OU*, *OU*, O, C representa la rama del directorio en la que se encuentra ubicada la entrada correspondiente al *Suscriptor* en cuestión.

El atributo *CN* contiene los datos de identificación del *Suscriptor* que para el caso de los *Certificados de Persona jurídica para el Ámbito Tributario* seguirá los siguientes criterios:

---

[2] Datos del *Solicitante*, cuando corresponda, datos del tercero con poder bastante para vincular contractualmente a la *Persona jurídica*, y los propios datos de la *Persona jurídica* para la que se solicita la emisión del *Certificado de Persona jurídica para el ámbito tributario*.

El atributo *CN* contiene los datos de identificación de la persona jurídica *Suscriptora* que utilizará el *Certificado* y el nombre de la persona física que actúe como *Solicitante*. La sintaxis de dicho campo es la siguiente:

CN= ENTIDAD e - CIF 12345678B – NOMBRE a1 a2 n – NIF 12345678B

Donde;

ENTIDAD, CIF, NOMBRE y NIF son etiquetas, [1]

e es la denominación o razón social de la persona jurídica *Suscriptora* del certificado. [2]

12345678B es el CIF de la persona jurídica *Suscriptora* o el NIF de la persona física que actúe como *Solicitante*. [3]

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

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

[3] CIF del Suscriptor= 8 cifras + 1 letra mayúscula, sin ningún tipo de separación entre ellas. En el caso de un CIF del *Suscriptor* ocupe menos de 8 cifras, se incluirán ceros al comienzo del número hasta completar las 8 cifras.

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

III.2.2.2 Composición de la identidad alternativa

La identidad alternativa, tal como se contempla en la presente tipología de *Certificados* contiene información referente a la persona jurídica *Suscriptora* del *Certificado de Persona jurídica para el ámbito tributario*, y a la persona física que actúe como *Solicitante*. Se utiliza la extensión subjectAltName definida en *X.509* versión 3 para ofrecer esta información.

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

Tipo Certificado	***Información***	***Atributo FNMT***	***OID (*)***
Persona Jurídica Ámbito Tributario	Entidad	fnmtRepEntidad	fnmtoid.1.6
	CIF Entidad	fnmtRepCif	fnmtoid.1.7
	Nombre del *Solicitante*	fnmtNombre	fnmtoid.1.1
	Apellido 1 *Solicitante*	fnmtApellido1	fnmtoid.1.2
	Apellido 2 *Solicitante*	fnmtApellido2	fnmtoid.1.3
	NIF *Solicitante*	fnmtNIF	fnmtoif.1.4

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

III.2.2.3 Perfil del *Certificado de Persona jurídica para el ámbito tributario*

El formato del *Certificado* expedido por la FNMT-RCM bajo esta tipología, en consonancia con la norma UIT-T X.509 versión 3, contiene los siguientes campos:

Campo	O.I.D	Valor
Campos Básicos		
Version		2 (X.509 v3)
SerialNumber		Número de serie del *Certificado.* **[1]**
Issuer		C=ES,O=FNMT,OU=FNMT Clase 2 CA
Validity		**[2]**
Subject		**Nombre distintivo del *Suscriptor*.** **[3]**
SubjectPublicKeyInfo		RsaEncryption, *Clave Pública.* **[4]**
SignatureAlgIdentifier	1.2.840.113549.1.1.5	Identificador del Algoritmo de Firma electrónica utilizado. **[5]**
Extensiones Estándar		
KeyUsage	2.5.29.15	**[6]**
PrivateKeyUsageperiod	2.5.29.16	El mismo que Validity
SubjectAltName	2.5.29.17	**[7]**
CRLDistributionPoints	2.5.29.31	Cn=CRLnnn, c=ES, o=FNMT,OU=FNMT Clase 2 CA **[8]**
AuthorityKeyIdentifier	2.5.29.35	Identificador de *Clave* del *PSC*
SubjectKeyIdentifier	2.5.29.14	Identificador de *Clave* del *Suscriptor*
BasicConstraints	2.5.29.19	Restricciones básicas. Entidad Final
Extensiones Privadas		
NetscapeCertType	2.16.840.1.113730.1	**[9]**
fnmtTipoCertificado	1.3.6.1.4.1.5734.1.33	**[10]**

Donde:

[1] SerialNumber: Número de identificación para el *Certificado* único dentro de la infraestructura del *Prestador de Servicios de Certificación*.

[2] Validity: Periodo de validez del certificado tal y como se muestra en el apartado "III.2.5 Periodo de Validez del *Certificado de Persona jurídica para el ámbito tributario*" del presente anexo.

[3] Subject: Identificación del *Suscriptor* del *Certificado*. Su composición ha sido detallada con anterioridad en este anexo.

[4] SubjectPublicKeyInfo: Es la *Clave Pública* que el *Suscriptor* generó en la fase de presolicitud de emisión del *Certificado*. Se realiza una prueba de posesión de la *Clave Privada* correspondiente.

[5] SignatureAlgIdentifier: Identificación del algoritmo utilizado para realizar la *Firma electrónica* del certificado. El algoritmo utilizado es SHA1WithRSAEncryption (*OID* 1.2.840.113549.1.1.5) siendo la longitud de la *Clave* utilizada de 1024 bits.

[6] KeyUsage: Valores admitidos para el uso de la clave. **No está marcada como crítica.** Toma los valores **{digitalSignature, keyEncipherment}.**

[7] SubjectAltName: Identidad Alternativa del Sujeto. **No está marcada como crítica.**

Su concreta composición ha sido detallada con anterioridad en el presente anexo.

[8] CRLDistributionPoint: El punto concreto de distribución de las *Listas de Revocación*, es generado por el *Prestador de Servicios de Certificación* en el mismo momento en que procede a la generación de *Certificado*. **No está marcada como crítica.**

[9] NetscapeCertType: Tipo de certificado según Netscape. **No está marcada como crítica.**

Toma los valores **{sSLCLIENT, sMIME}.**

[10] fnmtTipoCertificado : No está marcada como crítica.

Se incluye un indicativo textual del tipo de *Certificado*, que para este caso es:

"CERTIFICADO EXCLUSIVO PARA EL AMBITO TRIBUTARIO"

III.2.3 Publicación del *Certificado de Persona jurídica para el ámbito tributario*

Una vez generado el Certificado, por parte del *Prestador de Servicios de Certificación*, se publicará en el *Directorio*, concretamente en la entrada correspondiente al nombre distintivo del *Suscriptor*, tal como se ha definido en el apartado *"III.2.2 Emisión del Certificado"* de este anexo.

Si en el proceso de solicitud el *Solicitante* proporcionó una dirección de correo electrónico válida, se le enviará una comunicación de la disposición de su *Certificado* para su descarga.

III.2.4 Descarga e instalación del *Certificado de Persona jurídica para el ámbito tributario*

Una vez transcurrido el tiempo establecido desde que el *Solicitante* se persona en las *Oficinas de Registro* para acreditar su identidad, y una vez que el *Certificado* haya sido generado, se pone a disposición de *Solicitante* un mecanismo de descarga de *Certificado* en la dirección http://www.cert.fnmt.es/clase2/main.htm, accediendo a la opción "Descarga del Certificado".

En este proceso guiado, se le pedirá al *Suscriptor* que introduzca el CIF con el que realizó el proceso de presolicitud, así como el código de solicitud devuelto por el sistema al finalizar dicho proceso. Si el *Certificado* no ha sido aún generado por cualquier motivo, se le indicará este hecho en el momento que intente su descarga.

Si el *Certificado* ya ha sido puesto a disposición del *Solicitante*, éste será introducido en el soporte en el que se generaron las *Claves* durante el proceso de Presolicitud (*Tarjeta criptográfica* de la FNMT-RCM o soporte convencional de almacenamiento de software a través del *navegador*).

III.2.5 Periodo de validez del *Certificado de Persona jurídica para el ámbito tributario*

El periodo de validez de los certificados emitidos por la FNMT-RCM para esta tipología de *Certificados* será de dos (2) años contados a partir del momento de la emisión del certificado, siempre y cuando no se extinga su vigencia por las causas y procedimientos expuestos en el apartado "9.12.2 Extinción de la vigencia de *Certificados*" de la *Declaración de Prácticas de Certificación*.

III.2.6 Revocación del *Certificado de persona jurídica para el ámbito tributario*

La revocación de estos certificados implica, además de su extinción, la finalización de la relación jurídica con la FNMT-RCM que se mantuviese al respecto.

La revocación de un *Certificado* de *Persona jurídica para el ámbito tributario* podrá ser solicitada por los entes descritos en el apartado "9.12.3 Revocación de certificados" de la *Declaración de Prácticas de Certificación* en los términos y condiciones allí expresados.

A continuación se describe el procedimiento por el que se toman los datos personales y se confirma la identidad y sus facultades de representación, y se formaliza la solicitud de revocación de un *Certificado* por parte de un legítimo interesado.

Estas actividades serán realizadas por las *Oficinas de Registro* implantadas por el Ministerio de Hacienda o por la Comunidad Foral de Navarra.

Si el *Suscriptor* del *Certificado de Persona jurídica para el ámbito tributario* o su representante están en posesión del *Certificado*

En este caso, y dado que el *Suscriptor* puede ser autenticado con base en su *Certificado* deberá solicitarse la revocación a través de Internet, o de cualquier otra vía equivalente que permita la conexión a la dirección http://www.cert.fnmt.es/clase2/revoca.htm, siguiendo los pasos que se indican en la opción "Revocación del certificado".

Si el peticionario no está en posesión del *Certificado de Persona jurídica para el ámbito tributario,* o no disponen del resto de herramientas necesarias para solicitar la revocación telemáticamente

En este caso podrá solicitar la revocación del *Certificado* personándose en una *Oficina de Registro* para identificarse. Una vez acreditada su identidad, el peticionario deberá firmar el modelo de solicitud de revocación de certificado que se le presente. Este modelo se corresponderá con el mostrado en el apartado "III.5 Modelos de formulario" del presente anexo. Posteriormente las *Oficinas de Registro* transmitirán los registros tramitados a la FNMT-RCM para que ésta proceda a la revocación del *Certificado*.

Una vez que la FNMT-RCM haya procedido a la revocación del *Certificado*, se publicará en el *Directorio* seguro la correspondiente *Lista de Revocación* indicando el número de serie del *certificado* revocado, la fecha y hora en que se ha realizado la revocación y la causa de revocación.

III.2.7 Suspensión del *Certificado de persona jurídica en el ámbito tributario*

La suspensión del *Certificado* deja sin efectos al mismo durante un periodo de tiempo y en unas condiciones determinadas.

La suspensión de estos *Certificados* podrá ser solicitada por los entes descritos en el apartado "9.12.4 Suspensión de certificados" de la *Declaración de Prácticas de Certificación* en los términos y condiciones allí expresados.

A continuación se describe el procedimiento por el que se toman los datos personales y se confirma la identidad y facultades de representación, y se formaliza la solicitud de suspensión de un *Certificado* por parte de un legítimo interesado. Serán causas admitidas para la suspensión de un *Certificado* las expuestas en el apartado 9.12.4.1 Causas de suspensión" de la *Declaración de Prácticas de Certificación.*

Estas actividades serán realizadas por las *Oficinas de Registro* implantadas por el Ministerio de Hacienda o por la Comunidad Foral de Navarra o bien de forma *on line*, en caso de estar en posesión del *Certificado* y de sus correspondientes *Datos de creación de Firma*.

Adicionalmente, se podrá efectuar la solicitud telefónica de suspensión del *Certificado* a la FNMT-RCM mediante el número de teléfono 902 200 616 a la FNMT-RCM.

La FNMT-RCM procederá a suspender el *Certificado* de forma provisional durante un plazo de noventa (90) días, plazo tras el cual se extinguirá mediante su revocación directa por parte del *Prestador de Servicios de Certificación* de la FNMT-RCM, salvo que se hubiera levantado la suspensión por parte del *Suscriptor*. No obstante lo anterior, el plazo previsto para la suspensión del *Certificado* podrá verse alterado en función de los procedimientos judiciales o administrativos que lo afecten.

Si durante el plazo de suspensión del *Certificado* éste caducara o se solicitará su revocación, se producirán las mismas consecuencias que para los *Certificados* no suspendidos a los que afectara la caducidad y la revocación.

Si el *Suscriptor* del *Certificado de Persona jurídica para el ámbito tributario* está en posesión del *Certificado*

En este caso, y dado que el *Suscriptor* puede ser autenticado con base en su *Certificado* podrá solicitar la suspensión a través de Internet, o de cualquier otra vía equivalente que permita la conexión a la dirección http://www.cert.fnmt.es/clase2/suspension.htm, siguiendo los pasos que se indican en la opción "Suspensión del certificado".

Si el legítimo peticionario no está en posesión del *Certificado*, o no dispone del resto de herramientas necesarias para solicitar la suspensión telemáticamente

En este caso podrán solicitar la suspensión del *Certificado* personándose en una de las *Oficinas de Registro* establecidas por el Ministerio de Hacienda o la Comunidad Foral de Navarra, para identificarse. Una vez confirmada su identidad y sus facultades de representación, el peticionario deberá firmar el modelo de solicitud de suspensión del *Certificado* que se le presente. Este modelo se corresponderá con el mostrado en el apartado "III.5 Modelos de formulario" del presente anexo.

Posteriormente las *Oficinas de Registro* transmitirán los registros tramitados a la FNMT-RCM para que ésta proceda a la suspensión del *Certificado*.

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

III.2.8 Cancelación de la suspensión del *Certificado de Persona jurídica para el ámbito tributario*

Podrán solicitar el Cancelación de la suspensión de los *Certificados* emitidos por la FNMT-RCM, los *Suscriptores* siempre que, con anterioridad a esta solicitud de Cancelación de la suspensión, conserven el *Certificado* y sus *Datos de creación de Firma*, y dicha solicitud se efectúe durante los noventa (90) días siguientes a su suspensión.

Para ello deberán personarse ante cualquier *Oficina de Registro* establecida por el Ministerio de Hacienda o por la Comunidad Foral de Navarra. En este acto el solicitante aportará los datos que se le requieran y acreditará su identidad personal, como en el proceso de emisión ya descrito.

La personación del solicitante no será indispensable si la firma de la solicitud de Cancelación de la suspensión de un *Certificado* ha sido legitimada en presencia notarial.

Los datos personales del solicitante, una vez validados por la *Oficina de Registro*, se enviarán a la FNMT-RCM mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM.

Una vez recibidos los datos validados por la *Oficina de Registro* de la petición de la suspensión la FNMT-RCM procederá a retirar este *Certificado* de la *Lista de Revocación*.

III.2.9 Renovación del *Certificado de Persona jurídica para el ámbito tributario*

Podrán solicitar la renovación de los *Certificados* emitidos por la FNMT-RCM los *Suscriptores*, siempre que en el momento de la solicitud tengan un *Certificado* en vigor y sus *Datos de creación de Firma* asociados y, dicha solicitud, se efectúe durante los sesenta (60) días anteriores a su c*aducidad* (en este sentido véase el apartado "*9.12.1 Caducidad*" del cuerpo principal de la presente *Declaración de Prácticas de Certificación*).

Efectuada la renovación de los *Certificados*, su validez será la misma que la expresada en el apartado "*Período de validez del Certificado*"del presente anexo.

El antiguo *Certificado* que se haya procedido a renovar seguirá siendo válido hasta que caduque. En caso de solicitarse la revocación del *Certificado*, la FNMT-RCM procederá a revocar ambos *Certificados*. El procedimiento de renovación lleva asociado la generación de una nueva pareja de *Claves* criptográficas.

El peticionario deberá conectarse a la dirección http://www.cert.fnmt.es/clase2/main.htm y seguir los pasos que se indique en la opción "*Renovar Certificado*".

El procedimiento establecido no requiere la personación del peticionario, ya que se le identificará telemáticamente mediante la utilización de sus *Datos de creación de Firma*. Tanto el proceso de la solicitud como la obtención del *Certificado*, se realizará de forma telemática,

requiriéndose en todo caso la generación por parte del peticionario, de una *Firma electrónica Reconocida* del documento de solicitud de renovación, si bien se indica que la renovación telemática del *Certificado* sólo se podrá realizar cuando no se haya superado el plazo máximo de 5 años desde la personación e identificación física del Suscriptor que establece la Ley de firma electrónica 59/2003, de 19 de diciembre, en su artículo 13.4.

La utilización de los *Certificados* renovados se sujeta a las mismas condiciones generales y particulares vigentes en cada momento y establecidas para el tipo de *Certificado* renovado. A este respecto se deberá tener presente por ser de aplicación, lo establecido en el apartado *"12 Modificación de la Declaración de Practicas de Certificación"*.

III.2.10 Comprobación del estado del *Certificado de Persona jurídica para el ámbito tributario*

El *Suscriptor* del *Certificado* y las *Entidades usuarias* pertenecientes a la *Comunidad Electrónica* podrán realizar la comprobación del estado de un *Certificado* en la forma y condiciones que se expresan en los apartados "9.14 Procedimientos de consulta del estado de los *Certificados*" y "9.15 Servicio de validación de certificados mediante *OCSP*" de la *Declaración de Prácticas de Certificación*.

III.2.11 Terminación de la FNMT-RCM en su actividad como *Prestador de Servicios de Certificación*

Esta circunstancia y sus consecuencias se describen en el apartado "9.18 Cese de la actividad del *Prestador de Servicios de Certificación*", de la *Declaración de Prácticas de Certificación*.

III.3 OBLIGACIONES, GARANTIAS Y RESPONSABILIDAD DE LAS PARTES

Las obligaciones, garantías y responsabilidades de las partes implicadas en la emisión y uso de los *Certificados*, expedidos por la FNMT-RCM en su labor como *Prestador de Servicios de Certificación* quedan reflejadas en los apartados "9.20 Obligaciones y Garantías de las partes" y "9.21 Responsabilidad de las Partes" de la *Declaración de Prácticas de Certificación* de la que el presente anexo forma parte.

III.4 LÍMITES DE USO DE LOS CERTIFICADOS DE PERSONA JURÍDICA PARA EL ÁMBITO TRIBUTARIO

Para poder usar los *Certificados* o ser diligente a la hora de confiar en documentos firmados electrónicamente con base en los mismos, se deberá previamente formar parte de la *Comunidad*

Electrónica, y adquirir la condición de *Entidad usuaria*. Fuera de la *Comunidad Electrónica* no se debe confiar en un *Certificado* o en una firma electrónica que se base en un *Certificado* emitido por la FNMT-RCM. En cualquier caso, de producirse esta confianza por parte de un tercero, no se obtendrá cobertura de la presente *Declaración de Prácticas de Certificación*, y se carecerá de legitimidad alguna para reclamar o emprender acciones judiciales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado*.

Además, incluso dentro del ámbito de una *Comunidad Electrónica*, no se podrá emplear este tipo de certificado para:

- Firmar otro certificado.
- Firmar software o componentes.
- Generar sellos de tiempo para procedimientos de *Fechado electrónico.*
- Prestar servicios a título gratuito u oneroso, como por ejemplo serían a título enunciativo:
    - Prestar servicios de OCSP.
    - Generar *Listas de Revocación.*
    - Prestar servicios de notificación.

En cualquier caso, estos certificados no podrán ser utilizados fuera del ámbito tributario.

III.5 MODELOS DE FORMULARIO

Los modelos de formularios que se deben cumplimentar para realizar las operaciones descritas para la gestión del ciclo de vida de los *Certificados de Persona jurídica para el Ámbito Tributario* se publicarán en http://www.ceres.fnmt.es.

ANEXO IV PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS CERTIFICADOS DE ENTIDADES SIN PERSONALIDAD JURÍDICA PARA EL ÁMBITO TRIBUTARIO

El presente anexo forma parte integrante de la *Declaración de Prácticas de Certificación de la FNMT-RCM*. Estos certificados se ajustan a la *Política de Certificación de Certificados de Clave Pública de la FNMT-RCM*.

En especial deberá tenerse presente, a efectos interpretativos del presente anexo el apartado "1. DEFINICIONES" del cuerpo principal de la *Declaración de Prácticas de Certificación*.

Estas *Prácticas de Certificación particulares de los Certificados de Entidad sin personalidad jurídica para el ámbito tributario* definen el conjunto de prácticas adoptadas por la FNMT-RCM *como Prestador de Servicios de Certificación* para la gestión del ciclo de vida de los *Certificados de Entidad sin de personalidad jurídica para el ámbito tributario*, expedidos bajo la *Política de Certificación de Certificados de Clave Pública de la FNMT-RCM* identificada con el OID 1.3.6.1.4.1.5734.3.7.

IV.1 TIPOLOGÍA DEL CERTIFICADO DE ENTIDAD SIN PERSONALIDAD JURÍDICA PARA EL ÁMBITO TRIBUTARIO

Certificado de Entidad sin de personalidad jurídica para el ámbito tributario es la certificación electrónica expedida por la FNMT-RCM que vincula a su *Suscriptor* unos *Datos de verificación de Firma* y confirma su identidad para ser utilizados únicamente en las comunicaciones y transmisiones de datos por medios electrónicos, informáticos y telemáticos en el ámbito tributario. El *Titular* (*Suscriptor)* de estos *Certificados* únicamente podrá ser una entidad sin personalidad jurídica a las que se refiere el artículo 35.4 de la Ley General Tributaria, debiendo tener asignado, necesariamente, un número de identificación fiscal definitivo. Según la citada orden, podrán expedirse certificados electrónicos a las siguientes entidades carentes de personalidad jurídica:

a) *Las comunidades de bienes a las que se refiere el Titulo III del Libro II del Código Civil, las comunidades de propietarios en régimen de propiedad horizontal, reguladas por la Ley 49/1960, de 21 de julio, y las comunidades titulares de montes vecinales en mano común, conforme a la Ley 55/1980, de 11 de noviembre, o la normativa de las Comunidades Autónomas que en cada caso les resulte aplicable.*

b) *Las sociedades civiles sin personalidad jurídica.*

c) *Las herencias yacentes, sin regulación específica pero inferida de diversos preceptos del Código Civil.*

d) *Los fondos de inversión de carácter financiero y los fondos de inversión inmobiliaria previstos en la Ley 35/2003, de 4 de noviembre, de Instituciones de Inversión Colectiva.*

e) *La uniones temporales de empresas, conforme a la Ley 18/1982, de 26 de mayo*

f) *Los fondos de capital-riesgo, regulados por la Ley 1/1999, de 5 de enero*

g) *Los fondos de pensiones, que se rigen por lo dispuesto en el Real Decreto Legislativo 1/2002, de 29 de noviembre.*

h) *Los fondos de regulación del mercado hipotecario previstos en la Ley 2/1981, de 25 de marzo.*

i) *Los fondos de titulación hipotecaria, regulados en la Ley 19/1992 de 7 de julio.*

j) *Los fondos de titulación de activos a los que se refiere la disposición adicional quinta de la Ley 3/1994, de 14 de abril.*

k) *Los fondos de garantía de inversiones previstos en el articulo 77 de la Ley 24/1988, de 28 de julio, según la redacción dada por la Ley 37/1998, de 1 de noviembre.*

l) *Otros entes sin personalidad jurídica no mencionados en las letras anteriores.*

La custodia de los *Datos de creación de Firma* asociados al *Certificado de Entidad sin personalidad jurídica para el ámbito tributario* será siempre obligación de la persona física solicitante (*Solicitante*), cuya identificación se incluirá en el *Certificado*.

IV.2 GESTIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS DE ENTIDAD SIN PERSONALIDAD JURÍDICA PARA EL ÁMBITO TRIBUTARIO

IV.2.1 Procedimiento de solicitud del *Certificado*

A continuación se describe el procedimiento de solicitud por el que se toman los datos personales de un *Solicitante*, se confirma su identidad así como la extensión y vigencia de sus facultades de representación sobre la entidad que será *Suscriptor* del *Certificado de Entidad sin personalidad jurídica para el ámbito tributario*, y se formaliza su contrato con la FNMT-RCM para la posterior emisión de un *Certificado*, una vez realizadas las validaciones pertinentes.

Para solicitar el *Certificado de Entidad sin personalidad jurídica para el ámbito tributario*, actuará en su representación el que la ostente, siempre que resulte acreditada fehacientemente, o un tercero con poder especial otorgado al efecto. En todos los casos, el solicitante será una persona física, y le corresponderá la custodia de los *Datos de Creación de Firma*. En los siguientes apartados se especifica la documentación a presentar por parte del *Solicitante* para acreditar estos extremos y los referentes a la entidad a la que representa.

Estas actividades serán realizadas por las Oficinas de Registro implantadas por la Agencia Estatal de Administración Tributaria.

IV.2.1.1 Obtención de la *Tarjeta Criptográfica* y del software de generación o importación de los *Datos de creación y de verificación de Firma* en la *Tarjeta*

La *Tarjeta criptográfica* es un *Dispositivo Seguro de Creación de Firma* que puede ser empleada para generar los *Datos de creación y de verificación de Firma* o para importar tales datos.

La FNMT-RCM recomienda el uso del *Certificado* generado en Tarjeta criptográfica para evitar la posibilidad de duplicación de los *Datos de creación de Firma* y poseer un mejor control de los mismos, quedando así el *Suscriptor* del *Certificado* dotado de unos medios técnicos tales que le permitan cumplir con su obligación de mantener el exclusivo control sobre los Datos de creación de Firma al que la Ley le obliga.

Si el interesado desea una *Tarjeta criptográfica de la FNMT-RCM*, deberá proceder con carácter previo a la fase de presolicitud a obtener dicha *Tarjeta*. A este respecto consúltese la información que la FNMT-RCM pone a disposición del público a través de la dirección http://www.cert.fnmt.es.

El interesado puede desear la simple descarga del *Certificado* a este soporte o la generación en el mismo de las *Claves*, que posteriormente conformarán los *Datos de creación* y *verificación de Firma*. En ambos casos, además de la *Tarjeta criptográfica*, deberá obtener el software necesario para la importación y/o generación de las *Claves* por la propia Tarjeta.

En el procedimiento de obtención de *Certificados* por parte del *interesado*, la FNMT-RCM facilitará, en el caso de emplearse como soporte del *Certificado* la *Tarjeta criptográfica*, los elementos necesarios para activar, en el puesto del *interesado*, el software pertinente para generar, a través de su *Navegador*, las *Claves* criptográficas que le permitirán proteger la seguridad de sus

comunicaciones a través de mecanismos de cifrado, así como firmar y autenticarse, constituyéndose en estos caso como *Datos de creación y de verificación de Firma*.

Asimismo, cuando el *Certificado* resida en soporte convencional y no en *Tarjeta criptográfica*, los *Datos de creación de Firma* también serán utilizados bajo el control del software de *navegación web* del que disponga el propio *interesado*, enviando la *Clave Pública* que ha de constituir los *Datos de verificación de Firma* a la FNMT-RCM con el fin de integrarlos en un *Certificado*.

En cualquier caso y con independencia del soporte empleado, los *Datos de creación de Firma* deberán permanecer siempre bajo el control exclusivo del *Suscriptor*, no guardándose copia de ellos por la FNMT-RCM.

Una vez obtenido este soporte y el software necesario para la operativa que desee realizar, o bien si el *Certificado* se almacenara en un soporte convencional, el interesado procederá según se dispone a continuación.

IV.2.1.2 Presolicitud

El interesado accede al *sitio web* del *Prestador de Servicios de Certificación* de la FNMT-RCM, a través de la dirección http://www.cert.fnmt.es/clase2/main.htm, donde se mostrarán las instrucciones del proceso completo. Deberá introducir el número de identificación fiscal definitivo de la entidad sin personalidad jurídica, para la que se solicita como *Suscriptora* el *Certificado*. Se generan (en *Tarjeta criptográfica* o en *navegador)* las *Claves Pública* y *Privada*, correspondientes al *Certificado* que se solicitará en la *Oficina de Registro* y se asigna al interesado un "código de presolicitud".

Con carácter previo el interesado podrá consultar la *Declaración de Prácticas de Certificación* en la dirección http://www.cert.fnmt.es/convenio/dpc.pdf con las condiciones de uso y obligaciones para las partes, sin perjuicio de que con posterioridad, *Solicitante*, *Oficina de Registro*, y FNMT-RCM, deban suscribir el contrato de solicitud y la *Declaración de Prácticas de Certificación.* En ningún caso la continuación del procedimiento de presolicitud implicará la conclusión de una contratación.

Al realizar esta presolicitud se envía a la FNMT-RCM la *Clave Pública* generada para la posterior emisión del *Certificado*, entregándose de forma automatizada la correspondiente prueba de posesión de la *Clave privada*.

La FNMT-RCM tras recibir esta información, comprobará mediante la *Clave Pública* del peticionario, la validez de la información de la presolicitud cifrada recibida comprobando únicamente que se corresponde con los datos facilitados por el peticionario. Asimismo esta operación servirá como indicador de la posesión y correspondencia de la pareja de *Claves* criptográficas por parte del peticionario.

Esta información no dará lugar a la generación de un *Certificad*o por parte de la FNMT-RCM, en tanto que ésta no reciba firmada por la *Oficina de Registro*, la solicitud del *Certificado* realizada por el interesado quien, a partir de ese momento, tendrá la consideración de *Solicitante*.

IV.2.1.3 Confirmación de los datos relativos a la entidad y de la identidad de la persona física que solicita la emisión de un *Certificado de Entidad sin personalidad jurídica para el ámbito tributario*

A) Personación ante las Oficinas de Registro

La personación podrá realizarse ante ante cualquier *Oficina de Registro* de la Agencia Estatal de Administración Tributaria con la que ésta tenga suscrito un acuerdo para la emisión de estos *Certificados*.

B) Comparecencia y documentación

En el momento de comparecencia ante la Oficina de Registro, el *Solicitante* deberá aportar la documentación necesaria para acreditar tanto la identidad de la entidad sin personalidad jurídica como la facultad de representación del Solicitante sobre la entidad. La documentación que es necesario aportar es la siguiente:

Documentación referente a la entidad

1.- Notas simples acreditativas de la inscripción de la entidad expedida en la fecha de solicitud o en los quince días anteriores, en particular:

a) De inscripción en el registro correspondiente del Ministerio de Economía y Hacienda o de la Comisión Nacional del Mercado de Valores, tratándose de fondos de inversión, fondos capital-riesgo, fondos de regulación del mercado de títulos hipotecarios, fondos de titulación hipotecaria, fondos de titulación de activos, fondos de garantía de inversiones y fondos de pensiones. Deberá constar en el certificado (nota simple) la identificación de la entidad gestora del fondo

b) De inscripción de los estatutos en el registro del Ministerio de Agricultura, Pesca y Alimentación o , en su caso, del registro correspondiente de la Comunidad Autónoma, tratándose de comunidades titulares de montes vecinales en mano común.

c) De inscripción en el registro especial de uniones temporales de empresas del Ministerio de Economía y Hacienda, adscrito a la Agencia Estatal de Administración Tributaria, tratándose de de uniones temporales de empresas que se hayan acogido al régimen fiscal especial regulado en el capitulo II del Titulo VII del texto refundido de la Ley del Impuesto de Sociedades, aprobado por Real Decreto Legislativo 4/2004, de 5 de marzo.

2.- La solicitud podrá acompañarse también con el certificado o nota simple de inscripción en el Registro Mercantil, expedido en la fecha de la solicitud o en los quince días anteriores.

3.- Siempre que las entidades solicitantes lo consideren conveniente y, en cualquier caso, cuando no deban estar inscritas en alguno de los registros a los que se refiere el apartado 1 anterior, presentarán en el momento de realizar la solicitud en la *Oficina de Registro* las escrituras públicas, contratos, estatutos, pactos o cualesquiera otros documentos que puedan acreditar su constitución, vigencia e identificación de los miembros que la integran.

4.- No será necesario aportar los documentos a los que se refiere el apartado 3 anterior cuando la Agencia Estatal de Administración Tributaria intervenga como *Oficina de Registro* en el proceso de solicitud del *Certificado de Entidad sin Personalidad Jurídica para el Ámbito Tributario*.

Documentación referente al representante de la Entidad

1.- Para solicitar el *Certificado de Entidad sin de personalidad jurídica para el ámbito tributario*, actuara en su representación el que la ostente, siempre que resulte acreditada fehacientemente, o un tercero con poder especial otorgado al efecto. En todos los casos, el solicitante será una persona física, y le corresponderá la custodia de los Datos de Creación de Firma. En los siguientes apartados se especifica la documentación a presentar por parte del Solicitante para acreditar estos extremos y los referentes a la entidad a la que representa.

2.- El *Solicitante* deberá acudir personalmente a las *Oficinas de Registro* con las que la Autoridad de Certificación para realizar la solicitud del *Certificado de Entidad sin Personalidad Jurídica para el Ámbito Tributaria,* identificándose con su DNI, pasaporte o cualquier otro medio admitido en derecho. El *Solicitante* debe tener asignado un número de identificación fiscal.

3.- La representación de entidades sin personalidad jurídica se justificará mediante los certificados o notas simples de los correspondientes registros públicos o especiales o mediante los documentos notariales que acrediten las facultades de representación del Solicitante del certificado. Los certificados o notas simples deberán haber sido expedidos en la fecha de la solicitud o en los quince días anteriores.

4.- Cuando no pueda acreditarse la representación en la forma indicada en le apartado anterior, se podrá justificar con los documentos privados de designación de representante que proceda en cada caso. En particular, podrá acreditarse la representación mediante los siguientes documentos:

- El documento de designación del representante de la herencia yacente, suscrito por todos lo herederos, con expresión del nombre, apellidos y DNI o número de pasaporte del representante, cuando no haya sido designado administrador judicial o albacea con plenas facultades de administración.
- Copia del Acta de la reunión en la que se nombró Presidente de la Comunidad, cuando se trate de comunidades en régimen de propiedad horizontal.
- Documento suscrito por un número de miembros que resulte suficiente para representar la mayoría de los intereses de la entidad, tratándose de comunidades de bienes y sociedades civiles sin personalidad jurídica, en el que se designa a la persona que la representa para solicitar el Certificado de Entidad sin Personalidad Jurídica para el Ámbito Tributario. No obstante, cuando se haya designado administrador judicial de la entidad, corresponderá a este la representación.

C) Envío de información a la FNMT-RCM

Una vez confirmada la identidad del *Solicitante*, y cuando corresponda, de la persona física representante del *Suscriptor*, y suscrito el contrato de solicitud por el *Solicitante*, el *Suscriptor* y la *Oficina de Registro*, esta procederá a validar los datos y a enviarlos junto con el código de presolicitud recogido en la fase de presolicitud, a la FNMT-RCM mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM.

Asimismo, la *Oficina de Registro* enviará a la FNMT-RCM los documentos (o copia compulsada de los mismos) utilizados para realizar la comprobación de los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del *Solicitante* y, de cualquier otro tercero en representación de la *Persona jurídica*, cuya comparecencia hubiese sido necesaria, a los meros efectos de cumplir con las obligaciones legales de conservación que impone la Ley núm. 59/2003, de 19 de diciembre, de firma electrónica.

IV.2.2 Emisión del *Certificado de Entidad sin personalidad jurídica para el ámbito tributario*

Una vez recibidos en la FNMT-RCM los datos de la solicitud[3] , firmados por la *Oficina de Registro*, así como el "código de solicitud" obtenido en la fase de presolicitud, se procederá a la emisión del *Certificado*.

La emisión de *Certificados* supone la generación de documentos electrónicos que acreditan la identidad y otros extremos a petición del *Solicitante*, así como su correspondencia con la *Clave Pública* asociada. La emisión de *Certificados* por parte de la FNMT-RCM sólo puede realizarla ella misma, en su calidad de *Prestador de Servicios de Certificación*, no existiendo ninguna otra entidad u organismo con capacidad de emisión de los mismos.

La FNMT–RCM por medio de su *Firma electrónica reconocida*, autentica los *Certificados de Entidad sin personalidad jurídica para el ámbito tributario*, y confirma la identidad del *Solicitante* y del *Suscriptor*. así como la verificación de la identidad y cuando corresponda, otras circunstancias personales de sus titulares. Por otro lado, y con el fin de evitar la manipulación de la información contenida en los *Certificados*, la FNMT-RCM utilizará mecanismos criptográficos para dotar de autenticidad e integridad a los *Certificado*.

La FNMT-RCM actuará diligentemente para:

- Procurar que el *Solicitante* del *Certificado* disponga de la *Clave Privada* correspondiente a la *Clave Publica* vinculada a la identidad del *Suscriptor* del mismo. Para ello la FNMT-RCM comprobará la posesión de la *Clave privada* y la correspondencia entre la *Clave privada* y la *Clave pública*.
- Lograr que la información incluida en el *Certificado* se base en la información proporcionada por el *Solicitante*.
- No ignorar hechos conocidos que puedan afectar a la fiabilidad del *Certificado.*
- Lograr que el *DN* (nombre distintivo) asignado en el *Certificado* sea único en toda la *Infraestructura de Clave Pública* de la FNMT-RCM.

IV.2.2.1 Composición del nombre distintivo del *Suscriptor*

Con los datos personales del *Solicitante* recogidos durante el proceso de solicitud del certificado, se procede a componer el *DN* (nombre distintivo) del *Solicitante*, 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 un *Suscriptor* está compuesto de los siguientes elementos:

DN≡CN, OU, OU, OU, O, C

El conjunto de atributos *OU*, *OU*, *OU*, O, C representa la rama del directorio en la que se encuentra ubicada la entrada correspondiente al *Suscriptor* en cuestión.

El atributo *CN* contiene los datos de identificación del *Suscriptor* que para el caso de los *Certificados de Entidad sin personalidad jurídica para el ámbito tributario* seguirá los siguientes criterios:

---

[3] Datos del *Solicitante*, cuando corresponda, datos del tercero con poder bastante para vincular contractualmente a la *Entidad sin personalidad jurídica*, y los propios datos de la *Persona jurídica* para la que se solicita la emisión del *Certificado de entidad sin personalidad jurídica para el ámbito tributario*.

El atributo *CN* contiene los datos de identificación de la entidad sin personalidad jurídica *Suscriptora* que utilizará el *Certificado* y el número de identificación fiscal de la persona física que actúe como *Solicitante*. La sintaxis de dicho campo es la siguiente:

CN= ENTIDAD e - CIF 12345678B – NOMBRE a1 a2 n – NIF 12345678B

Donde;

ENTIDAD, CIF, NOMBRE y NIF son etiquetas, [1]

e es la denominación o razón social de la entidad sin personalidad jurídica *Suscriptora* del certificado. [2]

a1, a2, n son el primer apellido, segundo apellido y nombre respectivamente de la persona física que actúa como *Solicitante.*

12345678B es el CIF de la entidad sin personalidad jurídica *Suscriptora* o el NIF de la persona física que actúe como *Solicitante*. [3]

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

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

[3] CIF del Suscriptor= 8 cifras + 1 letra mayúscula, sin ningún tipo de separación entre ellas. En el caso de un CIF del *Suscriptor* ocupe menos de 8 cifras, se incluirán ceros al comienzo del número hasta completar las 8 cifras.

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

IV.2.2.2 Composición de la identidad alternativa

La identidad alternativa, tal como se contempla en la presente tipología de *Certificados* contiene información referente a la entidad *Suscriptora* del *Certificado de Entidad sin personalidad jurídica para el ámbito tributario,* y a la persona física que actúe como *Solicitante*. Se utiliza la extensión subjectAltName definida en *X.509* versión 3 para ofrecer esta información.

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

Tipo Certificado	***Información***	***Atributo FNMT***	***OID (*)***
Entidad Sin personalidad Jurídica Ámbito Tributario	Entidad	fnmtRepEntidad	fnmtoid.1.6
	CIF Entidad	fnmtRepCif	fnmtoid.1.7
	Nombre del *Solicitante*	fnmtNombre	fnmtoid.1.1
	Apellido 1 *Solicitante*	fnmtApellido1	fnmtoid.1.2
	Apellido 2 *Solicitante*	fnmtApellido2	fnmtoid.1.3
	NIF *Solicitante*	fnmtNIF	fnmtoif.1.4

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

IV.2.2.3 Perfil del *Certificado de Entidad sin personalidad jurídica para el ámbito tributario*

El formato del *Certificado* expedido por la FNMT-RCM bajo esta tipología, en consonancia con la norma UIT-T X.509 versión 3, contiene los siguientes campos:

Campo	O.I.D	Valor
Campos Básicos		
Version		2 (X.509 v3)
SerialNumber		Número de serie del *Certificado*. **[1]**
Issuer		C=ES,O=FNMT,OU=FNMT Clase 2 CA
Validity		**[2]**
Subject		**Nombre distintivo del *Suscriptor*.** **[3]**
SubjectPublicKeyInfo		RsaEncryption, *Clave Pública*. **[4]**
SignatureAlgIdentifier	1.2.840.113549.1.1.5	Identificador del Algoritmo de Firma electrónica utilizado. **[5]**
Extensiones Estándar		
KeyUsage	2.5.29.15	**[6]**
PrivateKeyUsageperiod	2.5.29.16	El mismo que Validity
SubjectAltName	2.5.29.17	**[7]**
CRLDistributionPoints	2.5.29.31	Cn=CRLnnn, c=ES, o=FNMT,OU=FNMT Clase 2 CA **[8]**
AuthorityKeyIdentifier	2.5.29.35	Identificador de *Clave* del *PSC*
SubjectKeyIdentifier	2.5.29.14	Identificador de *Clave* del *Suscriptor*
BasicConstraints	2.5.29.19	Restricciones básicas. Entidad Final
Extensiones Privadas		
NetscapeCertType	2.16.840.1.113730.1	**[9]**
fnmtTipoCertificado	1.3.6.1.4.1.5734.1.33	**[10]**
fnmtTipoEntidadSinPJ	1.3.6.1.4.1.5734.1.36	**[11]**

Donde:

[1] SerialNumber: Número de identificación para el *Certificado* único dentro de la infraestructura del *Prestador de Servicios de Certificación*.

[2] Validity: Periodo de validez del certificado tal y como se muestra en el apartado "IV.2.5 Periodo de Validez del *Certificado de Entidad sin personalidad jurídica para el ámbito tributario*" del presente anexo.

[3] Subject: Identificación del *Suscriptor* del *Certificado*. Su composición ha sido detallada con anterioridad en este anexo.

[4] SubjectPublicKeyInfo: Es la *Clave Pública* que el *Suscriptor* generó en la fase de presolicitud de emisión del *Certificado*. Se realiza una prueba de posesión de la *Clave Privada* correspondiente.

[5] SignatureAlgIdentifier: Identificación del algoritmo utilizado para realizar la *Firma electrónica* del certificado. El algoritmo utilizado es SHA1WithRSAEncryption (*OID* 1.2.840.113549.1.1.5) siendo la longitud de la *Clave* utilizada de 1024 bits.

[6] KeyUsage: Valores admitidos para el uso de la clave. **No está marcada como crítica.** Toma los valores **{digitalSignature, keyEncipherment}.**

[7] SubjectAltName: Identidad Alternativa del Sujeto. **No está marcada como crítica.**

Su concreta composición ha sido detallada con anterioridad en el presente anexo.

[8] CRLDistributionPoint: El punto concreto de distribución de las *Listas de Revocación*, es generado por el *Prestador de Servicios de Certificación* en el mismo momento en que procede a la generación de *Certificado*. **No está marcada como crítica.**

[9] NetscapeCertType: Tipo de certificado según Netscape. **No está marcada como crítica.**

Toma los valores **{sSLCLIENT, sMIME}.**

[10] fnmtTipoCertificado : No está marcada como crítica.

Se incluye un indicativo textual del tipo de *Certificado*, que para este caso es:

"CERTIFICADO DE ENTIDAD SIN PERSONALIDAD JURÍDICA EXCLUSIVO PARA EL AMBITO TRIBUTARIO"

[11] fnmtTipoEntidadSinPJ : No está marcada como crítica.

En esta extensión se incluirá un indicativo textual del tipo de Entidad sin Personalidad Jurídica para el que se expedirá el Certificado junto con un código de identificación. Concretamente, su contenido será uno de los reflejados en la siguiente tabla:

RA - Comunidad de bienes
RB - Comunidad propietarios propiedad horizontal
RC - Comunidad titular montes vecinales
RD - Sociedad civil
RE - Herencia yacente
RF - Fondo de inversión
RG - Unión temporal de empresas

RH - Fondo de capital-riesgo
RI - Fondo de pensiones
RJ - Fondo de regulación mercado hipotecario
RK - Fondo de titulación hipotecaria
RL - Fondo de titulación activos
RM - Fondo de garantía de inversiones
RN - Otros entes sin personalidad jurídica

IV.2.3 Publicación del *Certificado de Entidad SIN personalidad jurídica para el ámbito tributario*

Una vez generado el Certificado, por parte del *Prestador de Servicios de Certificación*, se publicará en el *Directorio*, concretamente en la entrada correspondiente al nombre distintivo del *Suscriptor*, tal como se ha definido en el apartado *"IV.2.2 Emisión del Certificado"* de este anexo.

Si en el proceso de solicitud el *Solicitante* proporcionó una dirección de correo electrónico válida, se le enviará una comunicación de la disposición de su *Certificado* para su descarga.

IV.2.4 Descarga e instalación del *Certificado de Entidad sin personalidad jurídica para el ámbito tributario*

Una vez transcurrido el tiempo establecido desde que el *Solicitante* se persona en las *Oficinas de Registro* para acreditar su identidad, y una vez que el *Certificado* haya sido generado, se pone a disposición de *Solicitante* un mecanismo de descarga de *Certificado* en la dirección http://www.cert.fnmt.es/clase2/main.htm, accediendo a la opción "Descarga del Certificado".

En este proceso guiado, se le pedirá al *Suscriptor* que introduzca el CIF con el que realizó el proceso de presolicitud, así como el código de solicitud devuelto por el sistema al finalizar dicho proceso. Si el *Certificado* no ha sido aún generado por cualquier motivo, se le indicará este hecho en el momento que intente su descarga.

Si el *Certificado* ya ha sido puesto a disposición del *Solicitante*, éste será introducido en el soporte en el que se generaron las *Claves* durante el proceso de Presolicitud (*Tarjeta criptográfica* de la FNMT-RCM o soporte convencional de almacenamiento de software a través del *navegador*).

IV.2.5 Periodo de validez del *Certificado de Entidad sin personalidad jurídica para el ámbito tributario*

El periodo de validez de los certificados emitidos por la FNMT-RCM para esta tipología de *Certificados* será de dos (2) años contados a partir del momento de la emisión del certificado, siempre y cuando no se extinga su vigencia por las causas y procedimientos expuestos en el

apartado "9.12.2 Extinción de la vigencia de *Certificados*" de la *Declaración de Prácticas de Certificación*.

IV.2.6 Revocación del *Certificado de Entidad sin personalidad jurídica para el ámbito tributario*

La revocación de estos certificados implica, además de su extinción, la finalización de la relación jurídica con la FNMT-RCM que se mantuviese al respecto.

La revocación de un *Certificado* de *Entidad sin personalidad jurídica para el ámbito tributario* podrá ser solicitada por los entes descritos en el apartado "9.12.3 Revocación de certificados" de la *Declaración de Prácticas de Certificación* en los términos y condiciones allí expresados.

A continuación se describe el procedimiento por el que se toman los datos personales y se confirma la identidad y sus facultades de representación, y se formaliza la solicitud de revocación de un *Certificado* por parte de un legítimo interesado.

Estas actividades serán realizadas por las Oficinas de Registro implantadas por el Ministerio de Hacienda, o por la Comunidad Foral de Navarra.

Si el *Suscriptor* del *Certificado de Entidad sin personalidad jurídica para el ámbito tributario* o su representante están en posesión del *Certificado*

En este caso, y dado que el *Suscriptor* puede ser autenticado con base en su *Certificado* deberá solicitarse la revocación a través de Internet, o de cualquier otra vía equivalente que permita la conexión a la dirección http://www.cert.fnmt.es/clase2/revoca.htm, siguiendo los pasos que se indican en la opción "Revocación del certificado".

Si el peticionario no está en posesión del *Certificado de Entidad sin personalidad jurídica para el ámbito tributario*, o no disponen del resto de herramientas necesarias para solicitar la revocación telemáticamente

En este caso podrá solicitar la revocación del *Certificado* personándose en una *Oficina de Registro* para identificarse. Una vez acreditada su identidad, el peticionario deberá firmar el modelo de solicitud de revocación de certificado que se le presente. Este modelo se corresponderá con el mostrado en el apartado "IV.5 Modelos de formulario" del presente anexo. Posteriormente las *Oficinas de Registro* transmitirán los registros tramitados a la FNMT-RCM para que ésta proceda a la revocación del *Certificado*.

Una vez que la FNMT-RCM haya procedido a la revocación del *Certificado*, se publicará en el *Directorio* seguro la correspondiente *Lista de Revocación* indicando el número de serie del *certificado* revocado, la fecha y hora en que se ha realizado la revocación y la causa de revocación.

IV.2.7 Suspensión del *Certificado de entidad sin personalidad jurídica para el ámbito tributario*

La suspensión del *Certificado* deja sin efectos al mismo durante un periodo de tiempo y en unas condiciones determinadas.

La suspensión de estos *Certificados* podrá ser solicitada por los entes descritos en el apartado "9.12.4 Suspensión de certificados" de la *Declaración de Prácticas de Certificación* en los términos y condiciones allí expresados.

A continuación se describe el procedimiento por el que se toman los datos personales y se confirma la identidad y facultades de representación, y se formaliza la solicitud de suspensión de un *Certificado* por parte de un legítimo interesado. Serán causas admitidas para la suspensión de un *Certificado* las expuestas en el apartado 9.12.4.1 Causas de suspensión" de la *Declaración de Prácticas de Certificación.*

Estas actividades serán realizadas por las *Oficinas de Registro* implantadas por el Ministerio de Hacienda o por la Comunidad Foral de Navarra o bien de forma *on line*, en caso de estar en posesión del *Certificado* y de sus correspondientes *Datos de creación de Firma*.

Adicionalmente, se podrá efectuar la solicitud telefónica de suspensión del *Certificado* a la FNMT-RCM mediante el número de teléfono 902 200 616 a la FNMT-RCM.

La FNMT-RCM procederá a suspender el *Certificado* de forma provisional durante un plazo de noventa (90) días, plazo tras el cual se extinguirá mediante su revocación directa por parte del *Prestador de Servicios de Certificación* de la FNMT-RCM, salvo que se hubiera levantado la suspensión por parte del *Suscriptor*. No obstante lo anterior, el plazo previsto para la suspensión del *Certificado* podrá verse alterado en función de los procedimientos judiciales o administrativos que lo afecten.

Si durante el plazo de suspensión del *Certificado* éste caducara o se solicitará su revocación, se producirán las mismas consecuencias que para los *Certificados* no suspendidos a los que afectara la caducidad y la revocación.

Si el *Suscriptor* del *Certificado de Entidad sin personalidad jurídica para el ámbito tributario* está en posesión del *Certificado*

En este caso, y dado que el *Suscriptor* puede ser autenticado con base en su *Certificado* podrá solicitar la suspensión a través de Internet, o de cualquier otra vía equivalente que permita la conexión a la dirección http://www.cert.fnmt.es/clase2/suspension.htm, siguiendo los pasos que se indican en la opción "Suspensión del certificado".

Si el legítimo peticionario no está en posesión del *Certificado*, o no dispone del resto de herramientas necesarias para solicitar la suspensión telemáticamente

En este caso podrán solicitar la suspensión del *Certificado* personándose en una de las *Oficinas de Registro* establecidas por el Ministerio de Hacienda o la Comunidad Foral de Navarra, para identificarse. Una vez confirmada su identidad y sus facultades de representación, el peticionario deberá firmar el modelo de solicitud de suspensión del *Certificado* que se le presente. Este modelo se corresponderá con el mostrado en el apartado "IV.5 Modelos de formulario" del presente anexo. Posteriormente las *Oficinas de Registro* transmitirán los registros tramitados a la FNMT-RCM para que ésta proceda a la suspensión del *Certificado*.

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

IV.2.8 Cancelación de la suspensión del *Certificado de Entidad sin personalidad jurídica para el ámbito tributario*

Podrán solicitar el Cancelación de la suspensión de los *Certificados* emitidos por la FNMT-RCM, los *Suscriptores* siempre que, con anterioridad a esta solicitud de Cancelación de la

suspensión, conserven el *Certificado* y sus *Datos de creación de Firma*, y dicha solicitud se efectúe durante los noventa (90) días siguientes a su suspensión.

Para ello deberán personarse ante cualquier *Oficina de Registro* establecida por el Ministerio de Hacienda o por la Comunidad Foral de Navarra. En este acto el solicitante aportará los datos que se le requieran y acreditará su identidad personal, como en el proceso de emisión ya descrito.

La personación del solicitante no será indispensable si la firma de la solicitud de Cancelación de la suspensión de un *Certificado* ha sido legitimada en presencia notarial.

Los datos personales del solicitante, una vez validados por la *Oficina de Registro*, se enviarán a la FNMT-RCM mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM.

Una vez recibidos los datos validados por la *Oficina de Registro* de la petición de la suspensión la FNMT-RCM procederá a retirar este *Certificado* de la *Lista de Revocación*.

IV.2.9 Renovación del *Certificado de Entidad sin personalidad jurídica para el ámbito tributario*

Podrán solicitar la renovación de los *Certificados* emitidos por la FNMT-RCM los *Suscriptores*, siempre que en el momento de la solicitud tengan un *Certificado* en vigor y sus *Datos de creación de Firma* asociados y, dicha solicitud, se efectúe durante los sesenta (60) días anteriores a su c*aducidad* (en este sentido véase el apartado "*9.12.1 Caducidad*" del cuerpo principal de la presente *Declaración de Prácticas de Certificación*).

Efectuada la renovación de los *Certificados*, su validez será la misma que la expresada en el apartado "*Período de validez del Certificado*"del presente anexo.

El antiguo *Certificado* que se haya procedido a renovar seguirá siendo válido hasta que caduque. En caso de solicitarse la revocación del *Certificado*, la FNMT-RCM procederá a revocar ambos *Certificados*. El procedimiento de renovación lleva asociado la generación de una nueva pareja de *Claves* criptográficas.

El peticionario deberá conectarse a la dirección http://www.cert.fnmt.es/clase2/main.htm y seguir los pasos que se indique en la opción "*Renovar Certificado*".

El procedimiento establecido no requiere la personación del peticionario, ya que se le identificará telemáticamente mediante la utilización de sus *Datos de creación de Firma*. Tanto el proceso de la solicitud como la obtención del *Certificado*, se realizará de forma telemática, requiriéndose en todo caso la generación por parte del peticionario, de una *Firma electrónica Reconocida* del documento de solicitud de renovación.

La utilización de los *Certificados* renovados se sujeta a las mismas condiciones generales y particulares vigentes en cada momento y establecidas para el tipo de *Certificado* renovado. A este respecto se deberá tener presente por ser de aplicación, lo establecido en el apartado *"12 Modificación de la Declaración de Practicas de Certificación"*.

IV.2.10 Comprobación del estado del *Certificado de Entidad sin personalidad jurídica para el ámbito tributario*

El *Suscriptor* del *Certificado* y las *Entidades usuarias* pertenecientes a la *Comunidad Electrónica* podrán realizar la comprobación del estado de un *Certificado* en la forma y condiciones

que se expresan en los apartados "9.14 Procedimientos de consulta del estado de los *Certificados*" y "9.15 Servicio de validación de certificados mediante *OCSP*" de la *Declaración de Prácticas de Certificación*.

IV.2.11 Terminación de la FNMT-RCM en su actividad como *Prestador de Servicios de Certificación*

Esta circunstancia y sus consecuencias se describen en el apartado "9.18 Cese de la actividad del *Prestador de Servicios de Certificación*", de la *Declaración de Prácticas de Certificación*.

IV.3 OBLIGACIONES, GARANTÍAS Y RESPONSABILIDAD DE LAS PARTES

Las obligaciones, garantías y responsabilidades de las partes implicadas en la emisión y uso de los *Certificados*, expedidos por la FNMT-RCM en su labor como *Prestador de Servicios de Certificación* quedan reflejadas en los apartados "9.20 Obligaciones y Garantías de las partes" y "9.21 Responsabilidad de las Partes" de la *Declaración de Prácticas de Certificación* de la que el presente anexo forma parte.

IV.4 LÍMITES DE USO DE LOS CERTIFICADOS DE ENTIDAD SIN PERSONALIDAD JURÍDICA PARA EL ÁMBITO TRIBUTARIO

Para poder usar los *Certificados* o ser diligente a la hora de confiar en documentos firmados electrónicamente con base en los mismos, se deberá previamente formar parte de la *Comunidad Electrónica*, y adquirir la condición de *Entidad usuaria*. Fuera de la *Comunidad Electrónica* no se debe confiar en un *Certificado* o en una firma electrónica que se base en un *Certificado* emitido por la FNMT-RCM. En cualquier caso, de producirse esta confianza por parte de un tercero, no se obtendrá cobertura de la presente *Declaración de Prácticas de Certificación*, y se carecerá de legitimidad alguna para reclamar o emprender acciones judiciales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado*.

Según lo dispuesto en la ORDEN EHA/3256/2004 de 30 de septiembre, por la que se establecen los términos en los que podrán expedirse certificados electrónicos a las entidades sin personalidad jurídica a las que se refiere el artículo 35.4 de la Ley General Tributaria, en su articulo primero, apartado 3:

"Estos certificados electrónicos únicamente podrán utilizarse en las comunicaciones y transmisiones de datos por medios electrónicos, informáticos y telemáticos en el ámbito tributario".

La FNMT-RCM no será responsable de la posible utilización de estos certificados fuera del ámbito de actuación dispuesto en la citada orden.

Además, no se podrá emplear este tipo de certificado para:

- Firmar otro certificado.
- Firmar software o componentes.
- Generar sellos de tiempo para procedimientos de *Fechado electrónico.*
- Prestar servicios a título gratuito u oneroso, como por ejemplo serían a título enunciativo:
    - Prestar servicios de OCSP.
    - Generar *Listas de Revocación.*
    - Prestar servicios de notificación.

IV.5 MODELOS DE FORMULARIO

Los modelos de formularios que se deben cumplimentar para realizar las operaciones descritas para la gestión del ciclo de vida de los *Certificados de Entidad sin personalidad jurídica para el ámbito tributario* se publicarán en http://www.ceres.fnmt.es.

ANEXO V. PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS CERTIFICADOS DE COMPONENTES

El Presente anexo tiene únicamente carácter informativo, y no es parte de la *Declaración de Prácticas de Certificación* de la FNMT-RCM,.

Estas *Prácticas de certificación particulares de los certificados de componentes* definen el conjunto de prácticas adoptadas por la FNMT-RCM como Prestador de Servicios de Certificación para la gestión del ciclo de vida de los diferentes tipos de ”certificados”, expedidos bajo la *Política de Certificación de certificados de componente de la FNMT-RCM* identificada con el OID 1.3.6.1.4.1.5734.3.6.

Este tipo de “certificados” no se pueden considerar “Certificados” en el sentido definido en el apartado “1. DEFINICIONES” de la Declaración de Prácticas de Certificación de la FNMT-RCM, por no adecuarse al concepto legal de “certificado electrónico” definido por la Ley de firma electrónica 59/2003, de 19 de diciembre. No obstante, se adjuntan provisionalmente como anexo exclusivamente informativo, por ser productos de gran utilidad que forman parte del Catálogo de Servicios de la FNMT-RCM.

V.1 TIPOLOGÍA DE LOS DISTINTOS CERTIFICADOS DE COMPONENTES

Los "certificados de componente" son aquellos certificados expedidos por la FNMT-RCM bajo la *Política de Certificación de certificados de componentes de la FNMT*-RCM identificada por el OID: 1.3.6.1.4.1.5734.3.6 para ser instalados y utilizados por componentes o aplicaciones informáticas sobre la que existe una persona física determinada que actúa como responsable, siendo esta la que tiene el control sobre dicho componente o aplicación. Los *Datos de creación de firma* asociados a los *Datos de verificación de firma* estarán bajo la responsabilidad de dicho *Responsable del componente* que actuará como representante de la persona jurídica para que se expidió el Certificado.

Son "certificados" emitidos y firmados por la FNMT-RCM para ser instalados y utilizados por servidores con soporte SSL, aplicaciones de firma de componentes software o por aplicaciones que actúen como clientes de los servicios avanzados proporcionados por la FNMT-RCM, con el objeto de que se herede la confianza que representa la FNMT-RCM como *Prestador de Servicios de Certificación*. Solo podrán obtener certificados de componentes aquellas entidades que hayan suscrito un contrato con la FNMT- RCM en virtud del cual formen parte de la *Comunidad Electrónica* tal y como se contempla en la *Declaración de Prácticas de Certificación de la FNMT-RCM*.

Estos certificados, no suponen firma jurídica, aunque pueden obrar con los mismos medios técnicos, pero carecen de la imputabilidad del hecho de la firma a una persona física o incluso a una persona jurídica por lo que no serán expedidos con la cualidad de *Certificados Reconocidos*.

La FNMT-RCM expide los siguientes tipos de Certificados de Componentes:

- *Certificado de servidor [también denominado certificado de la FNMT-RCM Clase 2 CA para Servidores Web]:* Es aquel certificado que permite identificar a un servidor *web* o una URL.
- *Certificado de firma de código [también denominado certificado de la FNMT-RCM Clase 2 CA para firma de código]:* Es aquel certificado utilizado en aplicaciones que permite firmar código ejecutable como *applets de Java*.
- *Certificado de Clientes de Servicios Avanzados de la FNMT-RCM:* Certificado utilizado en aplicaciones que actúan como clientes de los servicios avanzados puestos a disposición de la *Comunidad Electrónica* por la FNMT-RCM.
- *Certificado de otros componentes informáticos:* Certificado distinto de los anteriores, utilizado para identificar unas aplicaciones frente a otras, y establecer sesiones seguras.

V.2. GESTIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS DE COMPONENTES

V.2.1 Solicitud del *certificado de componente*

A continuación se describe el procedimiento de solicitud por el que se toman los datos personales de un *Solicitante* de certificado de componente, se confirma su identidad, la propiedad del dominio en su caso y la capacidad para realizar la solicitud en nombre de la entidad para la que se emite el *certificado de componente* y se formaliza su contrato con la FNMT-RCM para la posterior emisión de un *certificado de componente* una vez realizadas las validaciones pertinentes.

Estas actividades serán realizadas directamente por el Área de Registro de la FNMT-RCM.

Para solicitar estos productos se debe formar parte, previamente, de la *Comunidad Electrónica*.

Contacto Previo

El organismo interesado en solicitar un *certificado de componente*, deberá mantener previamente un contacto con la FNMT-RCM a fin de que se le facilite la información necesaria para la emisión del *certificado de componente* solicitado, así como los formularios que deben cumplimentar:

Una vez recibida esta documentación, la FNMT-RCM comprueba la corrección de la misma, que en todo caso deberá incluir:

- Formulario de solicitud de componente perfectamente cumplimentado y firmado por el *Responsable del componente*. Este formulario puede verse en el apartado "Modelos de Formulario".
- Formulario de autorización de petición de componente informático como responsable del mismo. Este formulario puede verse en el apartado "Modelos de Formulario".
- Fotocopia del Documento Nacional de Identidad, o Documento Nacional de Identidad de Extranjeros, estando el original válido y vigente, del *Responsable del componente*.
- Documento acreditativo de la propiedad del Nombre de Dominio o dirección IP o documento interno acreditando la Intranet.
- Escritura de Constitución o Boletín Oficial de la *Persona jurídica*, ya sea privada o pública.
- Fichero PKCS#10 de la petición del certificado de componente
- En el caso de un componente para Firma de Código, para Cliente de Servicios Avanzados y de un Componente Informático Genérico, el PKCS#10 podrá ser generado e insertado en la infraestructura de la FNMT-RCM siguiendo el mismo proceso que en la Presolicitud para Certificados de Personas Físicas. Debe adjuntarse a la documentación el Código de Solicitud generado durante dicho proceso de Presolicitud.

Tramitación de la solicitud y de la documentación por la FNMT-RCM

La FNMT-RCM una vez recibida la solicitud y la documentación pertinente, dará curso a la petición mediante sus aplicaciones informáticas internas, generará, en papel específico para contratos, los contratos a presentar al *Solicitante* para su firma, y firmará la petición específica de componente, para su procesamiento por la FNMT-RCM.

En función del tipo de componente que se haya especificado en la petición, el procedimiento generará:

- Para el caso de un Servidor Web: un código de descarga tras haberse validado el registro, que será impreso para la posterior descarga del PKCS#7 o certificado.
- Para el caso de una Firma de Código o de un Componente Informático, una vez validado el registro aparecerá un mensaje de confirmación de la petición. Para descargar ese *Certificado* de *componentes*, se utilizará el código de solicitud proporcionado por el *Solicitante*.

V.2.2 Emisión del certificado de componente

La FNMT –RCM, por medio de su firma electrónica, garantizará los certificados. Por otro lado, y con el fin de evitar la manipulación de la información contenida en los certificados, la FNMT-RCM utilizará mecanismos criptográficos para dotar de autenticidad e integridad a los certificados.

La FNMT-RCM actuará diligentemente para:

· Comprobar que el *Solicitante* del *Certificado* disponga de la *Clave Privada* correspondiente a la *Clave Publica.* Para ello la FNMT-RCM comprobará la posesión de la *Clave privada* y la correspondencia entre la *Clave privada* y la *Clave pública*.

· Lograr que la información incluida en el *Certificado* se base en la información proporcionada por el *Solicitante*.

· No ignorar hechos conocidos que puedan afectar a la fiabilidad del *Certificado.*

· Lograr que el nombre distintivo asignado en el *Certificado* sea único en toda la *Infraestructura de Clave Pública* de la FNMT-RCM.

Composición del nombre distintivo del componente

Para la composición del nombre distintivo de los componentes, debemos realizar una división en función de si el componente será un Servidor Web, componente de Firma de Código o un componente genérico. La FNMT-RCM no considerará nombres distintivos para los certificados de componentes informáticos distintos a los aquí mostrados, y de forma particular no considerará la utilización de “wildcards” en los nombres distintivos de los certificados de componente ni en ninguna de las extensiones del certificado.

Para certificados de Servidores con soporte SSL

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

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

DN≡CN, OU, OU, OU, O, C

El conjunto de atributos OU, OU, OU, O, C representa la rama del directorio en la que se encuentra ubicada la entrada correspondiente al Componente en cuestión.

El atributo CN contiene el nombre del servidor web. El nombre podrá ser **dns** o **ip** y deberá corresponderse con la forma de invocación del servicio.

Ej.:

CN=www.cert.fnmt.es

CN=213.170.35.210

Una vez compuesto el nombre distintivo que identificará al componente, se crea la correspondiente entrada en el directorio asegurando que el nombre distintivo es único en toda la infraestructura de la autoridad de certificación.

Para certificados de componentes de Firma de Código, Cliente de Servicios Avanzados y Componentes Informáticos.

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

El DN para un usuario está compuesto de los siguientes elementos:

DN≡CN, OU, OU, OU, O, C

El conjunto de atributos OU, OU,OU, O, C representa la rama del directorio en la que se encuentra ubicada la entrada correspondiente al usuario en cuestión.

El atributo CN contiene los datos de identificación del componente que será el encargado de firmar código y de la entidad propietaria de dicho componente. La sintaxis de dicho campo depende del tipo de usuario que para el caso de Componentes de Firma de Código es:

CN= DESCRIPCION d – ENTIDAD e – CIF 12345678B

Dónde:

DESCRIPCION, ENTIDAD, CIF son etiquetas, [1]

d es la descripción del equipo o programa. Es conveniente que esta descripción tenga sentido. [2]

e es la entidad propietaria del equipo o programa [2]

12345678B es el CIF de la entidad propietaria [3],

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

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

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

Una vez compuesto el nombre distintivo que identificará al componente, se crea la correspondiente entrada en el directorio asegurando que el nombre distintivo es único en toda la infraestructura de la autoridad de certificación.

Composición de la identidad alternativa

La identidad alternativa del componente objeto del certificado, tal como se contempla en la presente política de certificación contiene información referente a la entidad propietaria del componente y a la persona física que actúa como responsable. Se utiliza la extensión subjectAltName definida en *X.509* versión 3 para ofrecer esta información.

Dentro de dicha extensión, se utilizará el subcampo directoryName para incluir un conjunto de atributos definidos por la FNMT-RCM, que incorporan información sobre la entidad que será *Suscriptora* del *Certificado*, siguiendo el siguiente criterio:

Tipo Certificado	*Información*	*Atributo FNMT*	*OID (*)*
Componentes Informáticos [1],[2]	Descripción	fnmtDescripcion	fnmtoid.1.8
	Entidad Propietaria	fnmtPropEntidad	fnmtoid.1.14
	CIF Entidad	fnmtPropCif	fnmtoid.1.15

[1] Por otra parte, además del subcampo *directoryName* de la extensión *subjectAltName*, en el caso de que la entidad proporcione una dirección de correo electrónico de contacto en el momento del registro, estará incluido el subcampo *rfc822Name*, el cual contendrá dicha dirección de correo. [2] La extensión *subjectAltName* del certificado puede contener, además del subcampo *directoryName*, los subcampos *dNSName* y/o *iPAddress* para incluir, respectivamente, el nombre de dominio y/o la dirección IP del componente informático.

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

Perfil del certificado de componente

En este caso debemos realizar una distinción entre el formato del certificado para Servidores Web con soporte SSL para componentes de Firma de Código y para Componente Informático. Esta distinción se debe a que hay dos campos del certificado que contendrán valores diferentes en función de si el componente es uno u otro. Esto se indicará en el campo concreto.

El formato del certificado emitido, en consonancia con la norma UIT-T X.509 versión 3, contiene los siguientes campos:

Campo	O.I.D	Valor
Campos Básicos		
Version		2 (X.509 v3)
SerialNumber		Número de serie del *Certificado.* **[1]**
Issuer		C=ES,O=FNMT,OU=FNMT Clase 2 CA
Validity		**[2]**
Subject		**Nombre distintivo del *Suscriptor*.** **[3]**
SubjectPublicKeyInfo		RsaEncryption, *Clave Pública.* **[4]**
SignatureAlgIdentifier	1.2.840.113549.1.1.5	Identificador del Algoritmo de Firma utilizado. **[5]**
Extensiones Estándar		
KeyUsage	2.5.29.15	**[6]**
PrivateKeyUsageperiod	2.5.29.16	El mismo que Validity

SubjectAltName	2.5.29.17	**[7]**
CRLDistributionPoints	2.5.29.31	Cn=CRLnnn, c=ES, o=FNMT,OU=FNMT Clase 2 CA **[8]**
AuthorityKeyIdentifier	2.5.29.35	Identificador de *Clave* del *PSC*
SubjectKeyIdentifier	2.5.29.14	Identificador de *Clave* del *Suscriptor*
BasicConstraints	2.5.29.19	Restricciones básicas. Entidad Final
Extensiones Privadas		
NetscapeCertType	2.16.840.1.113730.1	**[9]**

Donde:

[1] SerialNumber: Número de identificación para el *Certificado* único dentro de la infraestructura del *Prestador de Servicios de Certificación*.

[2] Validity: Periodo de validez del certificado tal y como se muestra en el apartado "Periodo de Validez del Certificado" del presente anexo.

[3] Subject: Identificación del Suscriptor del Certificado. Su composición ha sido detallada con anterioridad en este anexo.

[4] SubjectPublicKeyInfo: Es la *Clave Pública* que el *Suscriptor* generó en la fase de presolicitud de emisión del *Certificado*. Se realiza una prueba de posesión de la *Clave Privada* correspondiente.

[5] SignatureAlgIdentifier: Identificación del algoritmo utilizado para realizar la *Firma electrónica* del certificado. El algoritmo utilizado es SHA1WithRSAEncryption (*OID* 1.2.840.113549.1.1.5) siendo la longitud de la *Clave* utilizada de 1024 bits.

[6] KeyUsage: Valores admitidos para el uso de la clave. **No está marcada como crítica.** Toma los siguientes valores:

Para Servidor Web con soporte SSL: {digitalSignature, keyEncipherment}.

Para Componente de Firma de Código:{digitalSignature}.

Para Cliente de Servicios Avanzados y Componente Informáticos Genéricos: {digitalSignature, keyEncipherment}.

[7] SubjectAltName: Identidad Alternativa del Sujeto. **No está marcada como crítica.**

Su concreta composición ha sido detallada con anterioridad en el presente anexo.

[8] CRLDistributionPoint: El punto concreto de distribución de las *Listas de Revocación*, es generado por el *Prestador de Servicios de Certificación* en el mismo momento en que procede a la generación de *Certificado*. **No está marcada como crítica.**

[9] NetscapeCertType: Tipo de certificado según Netscape. **No está marcada como crítica.**

Toma los siguientes valores:

Para Servidor Web con soporte SSL: {sSLSERVER}.

Para Componente de Firma de Código:{objectSigning}

Para Cliente de Servicios Avanzados y Componente Informáticos Genéricos: {sSLCLIENT, sMIME}

V.2.3. Publicación del *certificado de componente*

Una vez generado el Certificado por parte de la Autoridad de Certificación, dicho certificado es publicado en el directorio seguro en la entrada correspondiente al nombre distintivo asignado al componente tal como se ha definido en el apartado "Emisión del Certificado".

V.2.4 Envío del *certificado de componente* por la FNMT-RCM

La FNMT-RCM enviará el *Certificado* de *componente* generado al *Responsable del componente*, a través de la dirección de correo electrónico que se le haya indicado, en el formato correspondiente.

Asimismo, la FNMT-RCM enviará al *Responsable del componente* los contratos definitivos generados por la aplicación interna, por correo postal, a la dirección indicada en la solicitud.

V.2.5 Suscripción por parte del *Responsable del componente*

El *Responsable del componente* firmará las dos copias enviadas, guardará una para sí y remitirá la otra copia al Área de Registro de la FNMT-RCM, para su archivo.

La FNMT-RCM archivará la copia firmada por el *Responsable del componente* y la archivará junto con toda la documentación referida a ese componente informático, poniendo fin al proceso de emisión del *certificado de componente*.

V.2.6 Periodo de Validez del *certificado de componente*

El periodo de validez de los certificados emitidos por la FNMT-RCM para la Política de Certificación que nos ocupa será de 48 meses contados a partir del momento de la emisión del Certificado siempre y cuando no se extinga su vigencia por las causas y procedimientos expuestos en el apartado 9.12.2 Extinción de la Vigencia de Certificados de la Declaración de Prácticas de Certificación.

V.2.7 Revocación del *certificado de componente*

La revocación de certificados consiste en la cancelación de la garantía de identidad u otras propiedades del usuario y su correspondencia con la clave pública asociada.

La revocación de un certificado de componente podrá ser solicitada por los entes descritos en el apartado 9.12.3 Revocación de Certificados de la Declaración de Prácticas de Certificación, en los términos y condiciones allí expresados.

A continuación se describe el procedimiento por el que se obtienen los datos personales del *Responsable del componente*, se confirma su identidad y la responsabilidad sobre el certificado de

componente y se formaliza la solicitud de revocación de un certificado de componente por parte de un legítimo interesado. Serán causas admitidas para la revocación de un certificado las expuestas en el apartado 9.12.3.1 de la Declaración de Prácticas de Certificación para la FNMT-RCM.

Estas actividades serán realizadas únicamente por El Área de Registro de la FNMT-RCM, no siendo posible en ningún caso realizarlas ante *Oficinas de Registro*.

Solicitud del Suscriptor propietario del componente

El propietario del componente enviará el formulario de solicitud de revocación, cumplimentado y firmado a la FNMT-RCM, por correo ordinario. El formulario citado puede consultarse en el apartado "Modelos de Formulario".

Tramitación de la solicitud por la FNMT-RCM

El registrador de la FNMT-RCM tramitará la revocación del *Certificado de componente*, consignando en el mismo: la opción de prioridad que considere oportuna para la misma; el nombre del componente, el Dominio o IP si lo hubiera, el CN, la identidad del propietario del componente y su CIF, la identidad del *Responsable del componente* y su NIF, el correspondiente código de solicitud, y el OU.

Tan pronto se resuelva la revocación, el registrador de la FNMT-RCM procederá a notificar al *Suscriptor* del Certificado de componente la revocación del mismo, en los términos del apartado 9.14 de la Declaración de Prácticas de Certificación.

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.

V.2.8 Suspensión del Certificado de Componente

La suspensión (revocación temporal) de certificados consiste en la cancelación de la garantía de identidad u otras propiedades del usuario y su correspondencia con la clave pública asociada durante un periodo de tiempo y en determinadas condiciones.

La suspensión de un certificado de componente podrá ser solicitada por los entes descritos en el apartado 9.12.4 Suspensión de Certificados de la Declaración de Prácticas de Certificación, en los términos y condiciones allí expresados.

A continuación se describe el procedimiento por el que se obtienen los datos personales del *Responsable del componente*, se confirma su identidad, la responsabilidad sobre el certificado de componente y se formaliza la solicitud de suspensión de un certificado por parte de un legítimo interesado.

Estas actividades serán realizadas únicamente por El Área de Registro de la FNMT-RCM, no siendo posible en ningún caso realizarlas ante *Oficinas de Registro*.

Serán causas admitidas para la suspensión de un certificado las expuestas en el apartado 9.12.4.1 del documento principal de Declaración de Prácticas de Certificación para la FNMT-RCM.

Adicionalmente, se podrá efectuar la solicitud de suspensión del *Certificado* con carácter general, solicitándolo en el teléfono 902 200 616 a la FNMT-RCM.

La FNMT-RCM procederá a suspender el *Certificado* de forma provisional durante un plazo de noventa (90) días, plazo tras el cual se procederá a la extinción del *Certificado* mediante el procedimiento de revocación (sin mediar petición expresa por parte del interesado) salvo que se hubiera levantado la suspensión por parte del Suscriptor. No obstante lo anterior, el plazo previsto

para la suspensión del *Certificado* podrá verse alterado en función de los procedimientos judiciales o administrativos que lo afecten.

Si durante el plazo de suspensión del *Certificado* éste caducara, se producirán las mismas consecuencias que para los *Certificados* no suspendidos a los que afectara la caducidad.

Solicitud del Suscriptor propietario del componente

El propietario del componente enviará el formulario de solicitud de suspensión, cumplimentado y firmado a la FNMT-RCM, por correo ordinario. El formulario citado puede consultarse en el apartado "Modelos de Formulario" del presente anexo.

Tramitación de la solicitud por la FNMT-RCM

El registrador de la FNMT-RCM tramitará la petición de suspensión del *Certificado de componente*, consignando en el mismo: la opción de prioridad que considere oportuna para la misma; el nombre del componente, el Dominio o IP si lo hubiera, el CN, la identidad del propietario del componente y su CIF, la identidad del *Responsable del componente* y su NIF, el correspondiente código de solicitud, y el OU.

Tan pronto se resuelva la suspensión, el registrador de la FNMT-RCM procederá a notificar al *Suscriptor* del Certificado de componente la suspensión del mismo, en los términos del apartado 9.14 de la Declaración de Prácticas de Certificación.

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 suspendido, la fecha y hora de suspensión y como causa de revocación: suspensión temporal.

V.2.9 Cancelación de la suspensión del Certificado

Podrán solicitar el Cancelación de la suspensión de los *Certificados* emitidos por la FNMT-RCM, los *Suscriptores* siempre que, con anterioridad a esta solicitud de Cancelación de la suspensión, conserven el *Certificado* y su *Clave Privada*, y dicha solicitud se efectúe durante los noventa (90) días siguientes a su suspensión.

Para ello deberán personarse ante cualquier *Oficina de Registro* con la que ésta tenga suscrito un acuerdo. En ambos casos la comparecencia se llevará a cabo según el criterio vigente de la FNMT-RCM, al objeto de que ésta sea homogénea en todos los casos.

En este acto el *Solicitante* aportará los datos que se le requieran y acreditará su identidad personal, como en el proceso de emisión ya descrito.

La personación del *Solicitante* no será indispensable si la firma en la solicitud de expedición de un *Certificado* ha sido legitimada en presencia notarial, o si se solicita una renovación de *Certificado*, de conformidad con lo dispuesto en el apartado "*9.16 Renovación de certificados*" de la presente *Declaración de Prácticas de Certificación*.

Los datos personales del *Solicitante*, una vez validados por la Oficina de Registro, se enviarán a la FNMT-RCM mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM.

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

V.2.10 Renovación del Certificado de Componente

Para los Certificados en este anexo contemplados no existe un procedimiento de renovación *on line*, debiéndose proceder de igual forma que el procedimiento de solicitud, esto es, confirmar la identidad del *Solicitante*, la propiedad del dominio en su caso y la capacidad para realizar la solicitud en nombre de la entidad para la que se emite el *certificado de componente* y se formaliza su contrato con la FNMT-RCM. En cualquier caso no se podrá solicitar una renovación de cualquiera de los certificados aquí contemplados cuando el periodo restante para su caducidad sea menor de 60 días.

Efectuada la renovación de los *Certificados*, su validez será de cuatro (4) años a partir de la fecha de la misma.

El antiguo *Certificado* que se haya procedido a renovar, seguirá siendo válido hasta que caduque. En caso de solicitarse la revocación del *Certificado*, la FNMT-RCM procederá a revocar ambos *Certificados*. El procedimiento de renovación lleva asociada la generación de una nueva pareja de *Claves criptográficas*.

La utilización de los *Certificados* renovados se sujeta a las mismas condiciones generales y particulares vigentes en cada momento y establecidas para el tipo del *Certificado* renovado. A este respecto, se deberá tener presente, por ser de aplicación, lo establecido en el apartado "*12 Modificación de la Declaración de Practicas de Certificación*".

V.2.11 Comprobación del estado del Certificado

El Suscriptor del Certificado u otras Entidades usuarias pertenecientes a la Comunidad Electrónica podrá realizar la comprobación del estado de un Certificado en la forma y condiciones que se expresan en los apartados 9.14 Procedimientos de consulta del estado de los Certificados y 9.15 Servicio de validación de certificados mediante OCSP de la Declaración de Prácticas de Certificación, exceptuando para este tipo de certificados la comprobación del mismo mediante el servicio web de comprobación de certificados.

V.2.12 Terminación de la FNMT-RCM en su actividad como Prestador de Servicios de Certificación

Esta circunstancia y sus consecuencias se describen en el apartado 9.18 Cese de la actividad del Prestador de Servicios de Certificación, de la Declaración de Prácticas de Certificación.

V.3 OBLIGACIONES, GARANTIAS Y RESPONSABILIDAD DE LAS PARTES

Las obligaciones, garantías y responsabilidades de las partes implicadas en la emisión y uso de los *Certificados*, expedidos por la FNMT-RCM en su labor como *Prestador de Servicios de Certificación* quedan reflejadas en los apartados "9.20 Obligaciones y Garantías de las partes" y "9.21 Responsabilidad de las Partes" de la *Declaración de Prácticas de Certificación.*

V.4 LÍMITES DE USO DE LOS CERTIFICADOS

Para poder usar los *Certificados* o ser diligente a la hora de confiar en documentos firmados electrónicamente con base en los mismos, se deberá previamente formar parte de la *Comunidad Electrónica*, y adquirir la condición de *Entidad usuaria*. Fuera de la *Comunidad Electrónica* no se debe confiar en un *Certificado* o en una firma electrónica que se base en un *Certificado* emitido por la FNMT-RCM. En cualquier caso, de producirse esta confianza por parte de un tercero, no se obtendrá cobertura de la presente *Declaración de Prácticas de Certificación*, y se carecerá de legitimidad alguna para reclamar o emprender acciones judiciales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado*.

Además, incluso dentro del ámbito de una *Comunidad Electrónica*, no se podrá emplear este tipo de certificado para:

- Firmar otro certificado.
- Generar sellos de tiempo para procedimientos de *Fechado electrónico.*
- Prestar servicios a título gratuito u oneroso, como por ejemplo serían a título enunciativo:
  - Prestar servicios de OCSP.
  - Prestar servicios de facturación electrónica.
  - Generar *Listas de Revocación.*
  - Prestar servicios de notificación.

V.5 MODELOS DE FORMULARIO

Los modelos de formularios que se deben cumplimentar para realizar las operaciones descritas para la gestión del ciclo de vida de los Certificados de Componentes se publicarán en http://www.ceres.fnmt.es.