Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

POLÍTICA Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS

CERTIFICADOS DE COMPONENTE FNMT CLASE 2 CA

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM / v1.4	06/02/2013
Revisado por:	FNMT-RCM / v1.4	06/02/2013
Aprobado por:	FNMT-RCM / v1.4	06/02/2013

Referencia: DPC/PC-DPC-C2COMP-0104/SGPSC/2013

Documento clasificado como: *Público*

HISTÓRICO DEL DOCUMENTO – CONTROL DE CAMBIOS			
Versión	**Fecha**	**Descripción**	**Autor**
1.0	01/08/2010	Creación del documento según lo dispuesto en el anexo VI de la Declaración de Prácticas de Certificación versión 2.7. Se elimina el procedimiento de renovación de certificados Se añade la extensión extKeyUsage en los certificados de firma de código. Se añade la extensión extKeyUsage en los certificados de servidor web	FNMT-RCM
1.1	19/7/2011	Nuevo tipo de certificado de componente para unidades de sellado de tiempo. Nuevo tipo de certificado de componente para servidores web con varios nombres de dominio (SAN).	FNMT-RCM
1.2	17/4/2012	Se eliminan los apartados relacionados con la información sobre la gestión de las políticas de este documento por estar ya incluida en la DGPC. Se cambia el periodo de validez de los certificados (excepto el de TSU que se mantiene en dos años). Su vigencia se reduce de 4 a 2 años.	FNMT-RCM
1.3	29/8/2012	Se modifica el perfil de los *Certificados* de firma de código poniendo la extensión *keyUsage* como "crítica"	FNMT-RCM
1.4	06/02/2013	Se añade como opcional el uso extendido de clave "emailProtection" para certificados de servidor SSL.	FNMT-RCM

ÍNDICES

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN Y TIPOLOGÍA DEL CERTIFICADO

1. Los *Certificados de Componentes* son aquellos *Certificados* expedidos por la FNMT-RCM bajo la presente *Política de Certificación* y que vinculan unos *Datos de Verificación de Firma* a un *Componente* o aplicación informática sobre la que existe una persona física o jurídica determinada que actúa como responsable, siendo esta la que tiene el control sobre dicho *Componente* o aplicación. La *Clave Privada* asociada a la *Clave Pública* estará bajo la responsabilidad del *Responsable del Componente* que actuará como representante de la persona física o jurídica titular del *Componente* objeto del *Certificado*.

2. A los efectos del artículo 6 de la Ley 59/2003, los *Certificados de Componentes* se considerarán *Certificados* electrónicos cuando exista vinculación indubitada entre el *Certificado de Componente* y la persona física o jurídica *Titular* del *Certificado*. FNMT-RCM emitirá estos *Certificados* siempre que sea solicitado por los miembros de la *Comunidad Electrónica* para las diversas relaciones que puedan producirse y no se encuentre prohibido o limitado su utilización por la legislación aplicable.

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

4. Estos *Certificados de Componentes* son emitidos y firmados por la FNMT-RCM para ser instalados y utilizados por servidores con soporte SSL, aplicaciones de firma de componentes software, *Unidades de Sellado de Tiempo* 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 o convenio 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.

5. Estos *Certificados de Componentes*, no conllevan el efecto jurídico de equivalencia de firma electrónica reconocida con las actuaciones realizadas a través de firma manuscrita tradicional. No obstante, tendrán la validez y eficacia jurídica atendiendo a su respectiva naturaleza según la legislación aplicable. FNMT-RCM solamente expedirá estos *Certificados* para su uso en el ámbito de la *Comunidad Electrónica* para actuaciones que no resulten incompatibles con el ámbito y uso del *Certificado* correspondiente, al que se encuentre indubitadamente vinculado el componente.

6. La FNMT-RCM, como *Prestador de Servicios de Certificación* se reserva el derecho de no expedir o revocar este tipo de *Certificados* si el usuario del *Certificado* y/o el *Responsable del Componente* o aplicación que se sirve de tal *Certificado*, no hace un uso adecuado del mismo conculcando derechos de propiedad industrial o intelectual de terceros sobre las aplicaciones, sitios web o equipos que se desean proteger con tales *Certificados*, o su uso se presta a engaño o confusión sobre la titularidad de tales sitios web, aplicaciones, *Unidades de Sellado de Tiempo* o equipos. En especial, tal reserva de derechos se podrá ejecutar por la

FNMT-RCM cuando en la utilización de tales *Certificados* se atente contra los siguientes principios:

- La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.
- La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.
- El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y
- La protección de la juventud y de la infancia.

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

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

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

8. La FNMT-RCM expide bajo la presente *Política de Certificación* los siguientes tipos de *Certificados de Componentes*:

   - *Certificado* de servidor: Es aquel *Certificado* que permite identificar a un servidor web o una URL.

     Dentro de esta categoría de *Certificado* de servidor con funcionalidad de identificación de un servidor web o una URL, la FNMT-RCM dos tipos especiales de ***Certificados* de servidor, los denominados Wildcard**, que permiten a sus *Titulares*, miembros de la *Comunidad Electrónica*, asegurar todos los subdominios asociados a un dominio determinado, sin necesidad de adquirir y gestionar múltiples *Certificados* electrónicos; y los denominados SAN, que permiten a sus Titulares asegurar varios dominios con un único Certificado electrónico incorporando los dominios que desee asegurar, en el Subject Alternative Name.

     Asimismo se expiden ***Certificados* electrónicos para servidores *RADIUS*** ("Remote Authentication Dial-In User Service" o "Servicio de usuario de acceso telefónico de autenticación remota") consistentes en un protocolo estándar incluido en Windows 2000, y que se utiliza para facilitar la conectividad en redes de área local inalámbrica.

   - *Certificado* de firma de código: Es aquel *Certificado* utilizado en aplicaciones que permite firmar código ejecutable como *applets de Java*.
   - *Certificado* para *Unidades de Sellado de Tiempo*: Es aquel *Certificado* utilizado por una *Unidad de Sellado de Tiempo* (perteneciente a una *Autoridad de Sellado de Tiempo*) para la emisión de *Sellos de Tiempo*
   - *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.

2. ORGANIZACIÓN DEL DOCUMENTO

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

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

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

11. Deberá tenerse presente, a efectos interpretativos del presente anexo, el apartado "Definiciones" de la DGPC y de este documento.

12. El objetivo del presente documento la información pública del conjunto de prácticas, condiciones y características de los servicios de certificación que presta la FNMT-RCM como *Prestador de Servicios de Certificación* en relación al ciclo de vida *Certificados* electrónicos de *Componente*.

13. Así pues, el presente anexo trae causa y forma parte integrante de la *Declaración de Prácticas de Certificación* de la FNMT-RCM en lo relativo a los *Certificados de Componente*. Contiene la *Política de Certificación* para este tipo de *Certificados*, así como las *Prácticas de Certificación* empleadas en el ciclo de vida de estos.

14. En resumen, estas *Políticas de Certificación* y *Prácticas de Certificación Particulares* concretan lo articulado en el cuerpo principal de la DGPC y, por tanto, son parte integrante de ella, conformando, ambos documentos, la *Declaración de Prácticas de Certificación* de la FNMT-RCM para los *Certificados de Componente*. Así pues, lo descrito en este documento, sólo es de aplicación para el conjunto de *Certificados* caracterizado e identificado en esta *Política y Prácticas Particulares de Certificación* y pueden revestir, además, especialidades plasmadas a través de la *Ley de Emisión* del *Certificado* o grupo de *Certificados* correspondiente, en caso de que existan características o funcionalidades específicas.

3. DEFINICIONES

15. A las definiciones dispuestas en la DGPC, para el presente documento se añaden las siguientes:

- *Componente (informático)*: Conjunto de elementos interrelacionados entre sí para el desempeño de una función informática
- *Certificado de Componente*: *Certificado* empleado por un *Componente* informático para ampliar la funcionalidad o garantías para las que fue diseñado
- *Responsable del Componente*: Persona física o jurídica que tiene a su cargo la dirección y control del *Componente* informático para el cual se solicita un *Certificado de Componente*. El *Responsable del Componente* será a su vez el *Titular* y *Suscriptor* de este tipo de *Certificados* (Véase DGPC).
- *Representante del Responsable de Componente*: Persona física que tiene capacidad suficiente para realizar la solicitud del *Certificado* en nombre del *Responsable del Componente* para el cual se emite
- *Responsable del Certificado de Componente*: Persona física o jurídica que tiene a su cargo la dirección y control del *Certificado de Componente*
- *Solicitante*: Ver DGPC. En el marco del presente documento, consideraremos al *Solicitante* como la persona que solicita una operación relativa al *Certificado* y que tiene la responsabilidad de la correcta custodia de los *Datos de Creación de Firma Electrónica*. Esta persona será el *Responsable del Certificado de Componente* y vendrá autorizado por el *Responsable del Componente* o su *Representante*.

4. ORDEN DE PRELACIÓN

16. El orden de prelación es el siguiente:

- Las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares* de *Certificados de Componente* forman parte de la *Declaración de Prácticas de Certificación* y tendrán prelación, en lo que corresponda y con carácter particular sobre este tipo de *Certificado*, sobre lo dispuesto en la *Declaración General de Prácticas de Certificación*.

  Por tanto, en caso de que existiera contradicción entre el presente documento y lo dispuesto en la DGPC, tendrá preferencia lo aquí articulado.

- La *Ley de Emisión* de cada *Certificado* o grupo de *Certificados* constituirá, en su caso y por su singularidad, norma especial sobre lo dispuesto en las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares*. La *Ley de Emisión*, en caso de que se constituya, quedará recogida en el documento de relación a formalizar entre la FNMT-RCM y la *Entidad Usuaria*, y/o en las condiciones de utilización o contrato de emisión, y/o en el propio *Certificado*.

5. POLÍTICA DE CERTIFICACIÓN DE LOS CERTIFICADOS DE COMPONENTE FNMT CLASE 2 CA

5.1. IDENTIFICACIÓN

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

Tabla 1 - Identificación Política Certificación

Nombre	*Política de Certificación* de *Certificados de componente* de la FNMT-RCM (FNMT Clase 2 CA)
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 General de Prácticas de Certificación de la FNMT-RCM
Localización	http://www.ceres.fnmt.es/dpcs

5.2. COMUNIDAD Y ÁMBITO DE APLICACIÓN

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

- Son aquellos *Certificados* expedidos por la FNMT-RCM que vinculan unos *Datos de Verificación de Firma* a un *Componente* o aplicación informática sobre la que existe una persona física o jurídica determinada que actúa como responsable último, siendo esta la que tiene el control sobre dicho *Componente* o aplicación
- No son expedidos como *Certificados Reconocidos.*
- Los *Certificados* emitidos bajo esta *Política de Certificación* son expedidos para *Entidades usuarias* que forman parte de la *Comunidad Electrónica* tal y como se define en el apartado "Definiciones" de la DGPC de la FNMT-RCM.

5.3. RESPONSABILIDADES Y OBLIGACIONES DE LAS PARTES

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

20. FNMT-RCM no será responsable de la utilización de los *Certificados de Componente* cuando el responsable y/o *Titular* del *Certificado Electrónico* vinculado realice actuaciones

sin facultades o extralimitándose de las mismas, si no existe notificación fehaciente que permita trasladar los efectos pretendidos a la gestión de los *Certificados*.

5.3.1. Responsabilidades de las partes

21. 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*.

22. En cualquier caso, de producirse esta confianza por parte de un tercero, no se obtendrá cobertura de la *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*.

5.3.1.1. Responsabilidad del Prestador de Servicios de Certificación

23. 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 *Titular* mediante documento público.

24. 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 la DGPC.

25. 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 *Responsables del Certificado de Componente, Titulares, 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*.

26. FNMT-RCM no responderá en los supuestos de caso fortuito, fuerza mayor, atentado terrorista, huelga salvaje, así como en los supuestos que se trate de acciones constitutivas de delito o falta que afecten a sus infraestructuras prestadoras, salvo que hubiera mediado culpa grave de la entidad. En todo caso, en los correspondientes contratos y/o convenios FNMT podrá establecer cláusulas de limitación de responsabilidad adicionales a las recogidas en este documento.

27. 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.

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

29. 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.

30. Para el caso específico de los *Certificados* de *Componente* para su uso en las *Unidades de Sellado de Tiempo* pertenecientes a *Autoridades de Sellado de Tiempo* de terceros, se hace constar que la FNMT-RCM no tendrá responsabilidad alguna ni garantizará ningún aspecto del servicio de *Sellado de Tiempo* que puedan ofrecer las entidades *Titulares* de tales *Unidades* y *Autoridades de Sellado de Tiempo*. En especial la exención de responsabilidad alcanzará a la gestión de cualquiera de los aspectos relacionados con los sistemas de información empleados por dichas *Unidades* o *Autoridades* así como la validez de las fuentes de tiempo, o su sincronismo, empleadas en el servicio.

31. En todo caso y con la condición de cláusula penal, las cuantías que la FNMT-RCM debiera satisfacer, en concepto de daños y perjuicios, por imperativo judicial a terceros perjudicados o miembro de la *Comunidad Electrónica,* en defecto de regulación específica en los contratos o convenios, se limitan a un máximo de SEIS MIL EUROS (6.000€)

5.3.1.2. Responsabilidad del Solicitante

32. El *Solicitante* responderá de la veracidad y exactitud de la información presentada durante la solicitud del *Certificado*.

33. 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*.

5.3.1.3. Responsabilidad del Responsable del Componente (Titular y Suscriptor)

34. Será en todo caso obligación del *Responsable del Componente* 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.

35. 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.

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

5.3.1.4. Responsabilidad de la Entidad Usuaria

37. Será responsabilidad de la *Entidad usuaria*, salvo contratación de esta obligación con la FNMT-RCM, la verificación de las *Firmas Electrónicas* de los documentos, así como la comprobación del estado de los *Certificados*, no cabiendo en ningún caso presumir la autenticidad de los documentos o *Certificados* sin dichas comprobaciones.

38. 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 la *Declaración de Prácticas de Certificación* y comprobado que dicha *Firma Electrónica* puede ser verificada por referencia a una *Cadena de Certificación* válida.

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

40. Asimismo, será responsabilidad de la *Entidad Usuaria* observar lo dispuesto en la *Declaración de Prácticas de Certificación* y sus posibles modificaciones futuras, con especial atención a los límites de uso establecidos para los *Certificados* en esta *Política de Certificación*.

5.3.2. Obligaciones y garantías de las partes

5.3.2.1. Obligaciones y Garantías del Prestador de Servicios de Certificación

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

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

43. Con carácter previo a la emisión del *Certificado*:

- Identificar y comprobar la identidad y circunstancias personales del *Solicitante* del *Certificado* con arreglo a lo dispuesto en la *Declaración de Prácticas de Certificación*. En ningún caso se emitirán *Certificados* a menores de edad salvo que ostenten la cualidad de emancipados.

  En todo caso, se estará a lo establecido en la legislación específica respecto de las funcionalidades previstas respecto del DNIe a los efectos antes señalados

- En el proceso de solicitud, comprobar los datos relativos a la constitución y personalidad jurídica de la entidad y a la extensión y vigencia de las facultades de representación del *Solicitante* y exigir la acreditación de las circunstancias en las que se fundamenten los supuestos de representación. Todas estas comprobaciones se realizarán según lo dispuesto en las *Prácticas de Certificación Particulares* expresadas en este documento.

  En los procesos de comprobación de los extremos antes señalados anteriormente la FNMT-RCM podrá realizar estas comprobaciones mediante la intervención de

terceros que ostenten facultades fedatarias, siendo los costes, en caso de estas intervenciones, por cuenta de los interesados.

- Verificar que toda la información contenida en la solicitud del *Certificado* se corresponde con la aportada por el *Solicitante*.
- Comprobar que el *Responsable del Certificado de Componente* 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.
- 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.
- Realizar la comunicación de información al interesado o *Solicitante* de tal forma que se procure su *Confidencialidad*.
- Poner a disposición del *Solicitante* y responsables interesados (http://www.ceres.fnmt.es) la *Declaración de Prácticas de Certificación* y cuanta información sea relevante para el desarrollo de los procedimientos relacionados con el ciclo de vida de los *Certificados* objeto de esta *Política* de conformidad con la normativa aplicable.

44. Conservación de la información por la FNMT-RCM

- 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.
- 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. 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, en su caso, de la UE.
- Mantener un servicio de información y consulta sobre el estado de los *Certificados*.
- 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.
- Conservar la *Declaración de Prácticas de Certificación* durante 15 años desde su derogación por publicación de una nueva versión de la misma, en las debidas condiciones de seguridad.

45. 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 Española de Protección de Datos, conservación y acceso a la información, así como con las medidas de seguridad establecidas en la reglamentación correspondiente. 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 la DGPC.

46. Revocación de *Certificados*:

- Acerca de la revocación de *Certificados* y de las obligaciones que la FNMT-RCM se compromete a asumir al respecto, se puede consultar el procedimiento de revocación de *Certificados* reflejado en el presente documento.

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

- A este respecto se puede consultar el apartado correspondiente de la DGPC.

5.3.2.2. Obligaciones de la Oficina de Registro

48. Para la gestión del ciclo de vida de los *Certificados de Componente*, la FNMT-RCM será la única *Oficina de Registro* autorizada, teniendo como obligaciones:

- Con carácter general, seguir los procedimientos establecidos por la FNMT-RCM en la *Política y Prácticas de Certificación* de aplicación en el desempeño de sus funciones de gestión, emisión, renovación y revocación de *Certificados* y no salirse de dicho marco de actuación.
- 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 DGPC y con carácter particular en la presente *Política y Prácticas de Certificación Particulares*
- Conservar toda la información y documentación relativa a los *Certificados*, cuya solicitud, renovación, suspensión o revocación gestiona durante quince (15) años.
- Tramitar la formalización de los contratos de emisión de *Certificados* con el *Suscriptor* de los mismos
- Comprobar diligentemente las causas de revocación y suspensión que pudieran afectar a la vigencia de los *Certificados*.
- Las personas adscritas a la *Oficina de Registro* con independencia de la naturaleza de su relación laboral o funcionarial, deberán ejercer funciones públicas de acuerdo con la legislación específica aplicable a la FNMT-RCM. FNMT-RCM podrá utilizar la función de registro realizada por cualesquiera de los puestos correspondientes, incluyendo *Oficinas de Registro* telemáticas para la emisión de otros *Certificados*, siempre que existiera consentimiento de los titulares de los *Certificados*.

5.3.2.3. Obligaciones del Responsable del Componente (Titular y Suscriptor)

- No usar el *Certificado* fuera de la *Comunidad electrónica*, ni de los límites especificados en la presente *Política y Prácticas de certificación* particulares.
- No usar el *Certificado* en caso de que el *Prestador de Servicios de Certificación* haya cesado su actividad como Entidad emisora de *Certificados* que emitió el certificado en cuestión, especialmente en los casos en los que los *Datos de Creación de Firma* del prestador puedan estar comprometidos, y así se haya comunicado.
- Aportar información verdadera en la solicitud de los *Certificados,* y mantenerla actualizada.
- 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.
- 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*
- Conocer y cumplir las modificaciones que se produzcan en la *Declaración de Prácticas de Certificación*.
- Solicitar la revocación del correspondiente *Certificado*, según el procedimiento descrito en el presente documento, notificando diligentemente a la FNMT-RCM, las circunstancias o sospecha de pérdida de la *Confidencialidad*, la divulgación, modificación o uso no autorizado de los *Datos de creación de Firma*,
- Revisar la información contenida en el *Certificado*, y notificar a la FNMT-RCM cualquier error o inexactitud.
- Verificar con carácter previo a confiar en los *Certificados,* la *Firma electrónica reconocida* del *Prestador de Servicios de Certificación* emisor del *Certificado.*
- Notificar diligentemente a la FNMT-RCM cualquier modificación de los datos aportados en la solicitud del *Certificado*, solicitando cuando consecuentemente fuere pertinente la revocación del mismo.
- Devolver o destruir el *Certificado* cuando así lo exija la FNMT-RCM, y no usarlo con propósito de firmar o identificarse electrónicamente cuando el *Certificado* caduque, o sea revocado.

5.3.2.4. Obligaciones de la Entidad Usuaria

- Verificar con carácter previo a confiar en los *Certificados*, la *Firma Electrónica* reconocida del *Prestador de Servicios de Certificación* emisor del *Certificado*.
- Verificar que el *Certificado* del *Titular* recibido continúa vigente.

- 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 de Información y Consulta sobre el Estado de los Certificados* de la FNMT-RCM .
- Comprobar las limitaciones de uso del *Certificado* que se verifica.
- Conocer las condiciones de utilización del *Certificado* conforme a las *Políticas y Declaraciones de Prácticas de Certificación* de aplicación .
- Notificar a la FNMT-RCM cualquier anomalía o información relativa al *Certificado* y que pueda ser considerada como causa de revocación del mismo, aportando todos los elementos probatorios de los que disponga.

5.4. LÍMITES DE USO DE LOS CERTIFICADOS Y ACEPTACIÓN DEL MISMO

49. Para poder usar los *Certificados* de forma diligente y, por tanto, poder 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* con la finalidad que puedan ser prestados por la FNMT-RCM los servicios de comprobación de vigencia de los diferentes *Certificados*. 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.

50. FNMT-RCM no será responsable de emisiones de *Certificados* con apariencia fraudulenta de haber sido emitidos por la FNMT-RCM. FNMT-RCM, emprenderá las acciones legales contra estas actuaciones fraudulentas si tuviera conocimiento de las mismas, bien directamente, bien en caso de denuncia de los interesados.

51. 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*.

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

- Firmar otro *Certificado*.
- Generar *Sellos de Tiempo* para procedimientos de *Sellado de Tiempo* –a excepción de los *Certificados* emitidos por la FNMT-RCM para *Unidades de Sellado de Tiempo*-.
- 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.

6. PRÁCTICAS DE CERTIFICACIÓN PARTICULARES PARA LOS CERTIFICADOS DE COMPONENTE "FNMT CLASE 2 CA"

53. Estas *Prácticas de Certificación Particulares* para los *Certificados de Componente* 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* 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.

54. Los *Certificados de Componente* son aquellos *Certificados* expedidos por la FNMT-RCM bajo la *Política de Certificación de Certificados de Componente* 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 o jurídica determinada que actúa como responsable, siendo ésta la que tiene el control sobre dicho *Componente* o aplicación.

55. Los *Datos de Creación de Firma* asociados a los *Datos de Verificación de Firma* estarán bajo la custodia del *Solicitante* (persona física) del *Componente* para el que se expidió el *Certificado*.

56. 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, *Unidades de Sellado de Tiempo* 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*.

57. Solo podrán obtener *Certificados de Componente* 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*.

58. **Estos *Certificados*, salvo que se encuentren vinculados de forma indubitada a persona y/o *Certificado Reconocido* no producen los efectos de los actos realizados con firma manuscrita,** aunque pueden obrar con los mismos medios técnicos y contar con los efectos jurídicos que los miembros de la *Comunidad Electrónica* acuerden en sus respectivos convenios/contratos, de conformidad con lo establecido en el artículo 3.10 de la Ley de firma electrónica y resto de legislación aplicable.

59. Se hace constar expresamente que este tipo de *Certificados* no serán expedidos con la cualidad de *Certificados Reconocidos* salvo la previsión de vinculación antes dicha.

60. Se entenderá que existe vinculación indubitada a persona y/o *Certificado Reconocido* cuando en determinado tipo de *Certificado* emitidos por la FNMT-RCM se incluya en el campo del *Certificado* el atributo correspondiente a la vinculación al *Certificado de Componente*. También podrá considerarse vinculación indubitada cuando ésta se instrumente a través de instrumento público declarativo de la vinculación dicha. FNMT-RCM se reserva la facultad de incluir este tipo de atributos atendiendo a las condiciones técnicas y disponibilidad de la infraestructura prestadora.

6.1. GESTIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS DE COMPONENTE

61. Se definen aquí aquellos aspectos que, si bien ya han sido apuntados en la DGPC de la que este documento forma parte, revisten determinadas especialidades que necesitan un mayor nivel de detalle.

6.1.1. Procedimiento de solicitud del Certificado de Componente

62. 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.

63. Estas actividades serán realizadas directamente por el Área de Registro de la FNMT-RCM.

64. Para solicitar estos productos se debe formar parte, previamente, de la *Comunidad Electrónica*.

65. Se tendrá en cuenta la funcionalidad informática prevista para el DNIe de conformidad con la legislación específica.

6.1.1.1. Contacto previo

66. El organismo y/o entidad interesada 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.

67. El *Solicitante* elaborará o recopila la documentación a presentar y se la remite a la FNMT-RCM. Una vez recibida esta documentación, la FNMT-RCM comprueba la corrección de la misma, que en todo caso deberá incluir:

- Formulario de solicitud del *Certificado de Componente* perfectamente cumplimentado y firmado por el *Solicitante*.
- Formulario de autorización del *Responsable del Componente* o su *Representante* para la solicitud del *Certificado de Componente* informático por parte del *Solicitante*.
- Fotocopia del Documento Nacional de Identidad, del Documento Nacional de Identidad de Extranjeros o del Pasaporte del solicitante del *Certificado de Componente*, estando el original válido y vigente. No será necesaria la aportación de la fotocopia del DNI del *Solicitante* siempre que en el formulario de solicitud conste la autorización a la FNMT-RCM para que consulte sus datos personales en el Sistema de Verificación de Datos de Identidad.
- Documento acreditativo de la propiedad del Nombre de Dominio o dirección IP o documento interno acreditando la Intranet.

- Si fuera de aplicación, escritura de constitución y/o copia del acuerdo de creación y, en su caso, documento acreditativo de la inscripción en el registro correspondiente de la entidad interesada, ya sea privada o pública.
- En el caso de *Certificados* para *Unidades de Sellado de Tiempo*, la *Declaración de Prácticas de Sellado de Tiempo*, conforme a la norma "ETSI 101 023 – Requisitos para las políticas de las autoridades de sellado de tiempo", de la entidad que prestará el servicio como *Autoridad de Sellado de Tiempo* y *Titular* del *Certificado*.

  La entidad *Titular* del *Certificado* deberá figurar inscrita en el registro de *Prestadores de Servicios de Certificación* del Ministerio de Industria Turismo y Comercio como entidad prestadora de servicios de *Sellado de Tiempo*.
- 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.

6.1.1.2. Tramitación de la solicitud y de la documentación por la FNMT-RCM

68. La FNMT-RCM una vez recibida la solicitud y la documentación pertinente, dará curso a la petición mediante sus aplicaciones informáticas internas, generará el contrato a presentar al *Solicitante* para su firma y firmará la petición específica de componente para su procesamiento.

69. En función del tipo de *Componente* que se haya especificado en la petición, el procedimiento generará:

- Para el caso de un Servidor Web tipo "Wildcard" o "SAN", o para *Unidades de Sellado de Tiempo*: un código PKCS#7 que será remitido al solicitante por correo electrónico.
- Para el caso de un *Certificado* de Servidor Web, 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 Componente*, se utilizará el código de solicitud proporcionado por el *Solicitante*.

6.1.2. Suscripción por parte del Responsable del Componente

70. El *Responsable del Componente* o su *Representante* firmará las dos copias del contrato generado, guardará una para sí y remitirá la otra copia al Área de Registro de la FNMT-RCM para su archivo.

71. La no remisión de la copia del contrato firmado por parte del *Responsable del Componente*, será causa de revocación del *Certificado* o de interrupción del proceso de emisión del mismo

72. La FNMT-RCM archivará la copia firmada por el *Responsable del Componente* o su *Representante* y la archivará junto con toda la documentación referida a ese *Componente* informático, poniendo fin al proceso de solicitud del *Certificado de Componente.*

6.1.3. Emisión del Certificado de Componente

73. La FNMT–RCM, por medio de su *Firma Electrónica*, autenticará 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.

74. La FNMT-RCM actuará para:

- Comprobar que el *Solicitante* del *Certificado* utiliza la *Clave Privada* correspondiente a la *Clave Publica.* Para ello la FNMT-RCM comprobará la correspondencia entre la *Clave privada* y la *Clave pública*.
- Lograr que la información incluida en el *Certificado* se base en la información proporcionada por el *Solicitante*.
- 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.

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

1. Composición del nombre distintivo del *Certificado de Componente*

   Para la composición del nombre distintivo del *Certificado* se tendrá en cuenta su tipología según clasificación que más adelante se muestra. La FNMT-RCM no considerará nombres distintivos para los *Certificados de Componentes* informáticos distintos a los aquí mostrados.

   a) Para *Certificados* de servidor 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 *Certificado de 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.ceres.fnmt.es**

   CN=213.170.35.210

En el caso de los *Certificados* de servidor "wildcard" el CN del *Certificado* será de la forma:

CN=*.nombredominiosegundonivel.TLD

siendo,

[nombredominiosegundonivel] el nombre de dominio cuyo titular es la Entidad solicitante

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

En el caso de los Certificado de servidor "SAN" el CN del Certificado contiene el nombre del servidor web considerado como principal.

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.

b) Para *Certificados* de componente de Firma de Código, Cliente de Servicios Avanzados, *Unidades de Sellado de Tiempo* 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. En los casos relativos a

Unidades de Sellado de Tiempo, suele tomar un valor del tipo "TSU n", siendo n un número identificativo del sistema.

[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.

2. 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 *Responsable del Componente* y, opcionalmente, a la persona física que actúa como custodio. 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:

Tabla 2 – Extensión SubjectAltName

Tipo Certificado	***Información***	***Atributo FNMT***	***OID (*)***
Componentes Informáticos [1],[2]	Descripción	fnmtDescripcion	fnmtoid.1.8
	Entidad Propietaria	fnmtPropEntidad	fnmtoid.1.14
	NIF Entidad	fnmtPropCif	fnmtoid.1.15
Opcionales	Nombre Responsable	fnmtRespNombre	fnmtoid.1.16
	Apellido 1 Responsable	fnmtRespApellido1	fnmtoid.1.17
	Apellido 2 Responsable	fnmtRespApellido2	fnmtoid.1.18
	NIF Responsable	fnmtRespNIF	fnmtoif.1.19

[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/los nombre(s) de dominio(s) y/o la(s) dirección(es) 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.

3. Generación del *Certificado* conforme al 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:

Tabla 3 - Perfil del Certificado de Componente

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]**
extKeyUsage	2.5.29.37	**[7]**
PolicyIdentifier	2.5.29.32	1.3.6.1.4.1.5734.3.6
PrivateKeyUsageperiod	2.5.29.16	El mismo que Validity
SubjectAltName	2.5.29.17	**[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 *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	**[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 "Caducidad" del presente documento.

[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 salvo en el caso de los *Certificados* para Firma de Código que sí lo está.** Toma los siguientes valores:

Para Servidor Web con soporte SSL: {digitalSignature, keyEncipherment}.

Para Componente de Firma de Código y *Unidad de Sellado de Tiempo*:{digitalSignature}.

Para Cliente de Servicios Avanzados y Componente Informáticos Genéricos: {digitalSignature, keyEncipherment}.

[7] extKeyUsage: Extensión que añade más información sobre el uso de la clave

Para Servidor web: {serverAuth (1.3.6.1.5.5.7.3.1)} -- TLS Web server authentication.

Para Servidor web con protección de correos: {serverAuth (1.3.6.1.5.5.7.3.1), emailProtection (1.3.6.1.5.5.7.3.4)}.Para Componente de Firma de Código:{Code Signing (1.3.6.1.5.5.7.3.3)}.

Para *Unidades de Sellado de Tiempo*: {timeStamping (1.3.6.1.5.5.7.3.8)}.

[8] SubjectAltName: Identidad Alternativa del Sujeto. **No está marcada como crítica.**

Su concreta composición ha sido detallada con anterioridad en el presente anexo.

[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 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}

Para *Unidades de Sellado de Tiempo*: No se incluye

6.1.4. Publicación y distribución del Certificado de Componente

76. Una vez emitido 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*".

77. La FNMT-RCM enviará el *Certificado de Componente* emitido al *Responsable del Componente*, a través de la dirección de correo electrónico que se le haya indicado, en el formato correspondiente. También podrá ponerlo a su disposición mediante aplicativo seguro en la página web creada a tal efecto.

6.1.5. Vigencia de los Certificados

6.1.5.1. Caducidad

78. El periodo de validez de los Certificados emitidos por la FNMT-RCM para la *Política de Certificación* que nos ocupa será de 24 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 "Extinción de la vigencia del Certificado"

6.1.5.2. Extinción de la vigencia del Certificado

79. Los *Certificados de Componente* emitidos por la FNMT-RCM quedarán sin efecto en los siguientes casos:

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

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

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

c) Revocación del *Certificado* por cualquiera de las causas recogidas en el presente documento.

d) En los supuestos de *Certificados* vinculados indubitadamente a *Certificado* y/o persona, la revocación y/o suspensión del *Certificado* al que se vinculará el de componentes, conllevará la revocación/suspensión de este último

80. A los efectos enumerados anteriormente, se hace constar que la solicitud de emisión de un *Certificado de Componente* cuando exista otro vigente a favor del mismo *Titular* y perteneciente a la misma *Ley de Emisión* conllevará la revocación del primero obtenido.

81. 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*.

6.1.6. Revocación

82. La solicitud de revocación de los *Certificados* de componente podrá efectuarse durante el período de validez que consta en el *Certificado*. Consiste en la cancelación de la garantía de identidad u otras propiedades del usuario y su correspondencia con la *Clave Pública* asociada.

83. La revocación de un *Certificado de Componente* podrá ser solicitada por

- El *Titular* propietario del *Componente* o tercero que lo represente con poder suficiente
- El *Responsable del Certificado de Componente*

6.1.6.1. Causas de revocación

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

- Que la revocación se debiera haber efectuado por haberse extinguido el contrato suscrito con el *Suscriptor.*
- Que la revocación le haya sido solicitada por el *Titular o Responsable* siguiendo el procedimiento establecido a tal efecto
- Que la solicitud de revocación o la causa que la motiva, le haya sido notificada mediante resolución judicial o administrativa.

- Que en las causas c) a e) del presente apartado le sean acreditados dichos extremos fehacientemente, previa identificación del *Solicitante* de la revocación.

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

a) La solicitud de revocación por parte del *Titular, Responsable del Componente* o un tercero debidamente autorizado. En todo caso deberá dar lugar a esta solicitud:

- Pérdida del soporte del *Certificado.*
- La utilización por un tercero de los *Datos de Creación de Firma* del *Titular*, correspondientes a los *Datos de Verificación de Firma* contenidos en el *Certificado* y vinculados a la identidad del *Titular*.
- La violación o puesta en peligro del secreto de los *Datos de creación de Firma* del *Titular o* de los responsables de la custodia de los *Datos de creación de Firma*.
- La no aceptación de las nuevas condiciones que puedan suponer la emisión de nuevas *Declaraciones de Prácticas de Certificación*, durante el periodo de un mes tras su publicación.

b) Resolución judicial o administrativa que así lo ordene.

c) Fallecimiento, extinción o disolución de la personalidad jurídica del *Titular*.

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

e) 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.

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

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

h) 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.

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

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

88. **La falta de adecuación de los datos a la realidad, cuando estos datos se encuentren en Registros públicos no serán imputables a la FNMT-RCM hasta tanto no existan**

instrumentos de comunicación telemática directa de la FNMT-RCM con los diferentes Registros públicos, salvo que se proceda a su comunicación a la FNMT a través de medios fehacientes.

6.1.6.2. Efectos de la revocación

89. 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* y en sus servicios de comprobación del estado de los *Certificados*

6.1.6.3. Procedimiento para la revocación de Certificados

90. A continuación se describe el procedimiento por el que se obtienen los datos personales del *Solicitante*, 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.

91. 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*.

1. Solicitud del *Titular* propietario del *Componente*

   El propietario del *Componente* o su *Representante*, enviará el formulario de solicitud de revocación, cumplimentado y firmado a la FNMT-RCM, por correo ordinario.

   Se tendrá en cuenta la funcionalidad informática prevista para el DNI-e de conformidad con la legislación específica.

2. 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 NIF, 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 *Responsable del Componente* la revocación del mismo, en los términos del apartado Disponibilidad de la Información y Comunicaciones de la **DGPC**.

   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.

6.1.7. Suspensión del Certificado de Componente

92. 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.

93. La suspensión de un *Certificado de Componente* podrá ser solicitada por las mismas personas autorizadas para la revocación.

94. La suspensión del *Certificado de Componente* constituye la revocación temporal del mismo. El procedimiento de suspensión se desarrollará de forma análoga al procedimiento de revocación.

95. 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 *Titular*. 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.

96. 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.

6.1.8. Cancelación de la suspensión del Certificado de Componente

97. Podrán solicitar el Cancelación de la suspensión de los *Certificados* emitidos por la FNMT-RCM, los *Titulares y Responsables* 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.

98. Para ello deberán solicitarlo al Área de Registro de la FNMT-RCM. 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.

6.1.9. Comprobación del estado del Certificado

99. El *Titular* 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 el apartado "Sobre el servicio de información y consulta sobre el estado de validez de los certificados" de la DGPC, exceptuando para este tipo de *Certificados* la comprobación del mismo mediante el servicio web de comprobación de *Certificados*.

100. Para la difusión y confianza en los sistemas que cuenten estos *Certificados*, la FNMT-RCM, podrá proporcionar la posibilidad de verificar, por el miembro de la *Comunidad Electrónica* o un tercero, que el *Certificado de Componente* es un *Certificado* válido emitido por la FNMT-RCM, así como otras características del mismo.

6.2. MODELOS DE FORMULARIO

101. 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