Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

POLÍTICA Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS

CERTIFICADOS DE COMPONENTE

"AC COMPONENTES INFORMÁTICOS"

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM / v1.0	21/11/2013
Revisado por:	FNMT-RCM / v1.0	21/11/2013
Aprobado por:	FNMT-RCM / v1.0	21/11/2013

HISTÓRICO DEL DOCUMENTO – CONTROL DE CAMBIOS			
Versión	**Fecha**	**Descripción**	**Autor**
(1.0)	21/11/2013	Primera versión	FNMT-RCM

Referencia: DPC/PC-DPC-ACCOMP-0100/SGPSC/2013

Documento clasificado como: *Público*

ÍNDICES

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

1. Las presentes *Políticas* y *Prácticas de Certificación Particulares* describen la emisión o expedición de los *Certificados de Componentes* por parte de la FNMT-RCM para su uso por *Componentes informáticos*. Dichos *Certificados* vinculan unos *Datos de Verificación de Firma* a un *Suscriptor* que tiene el control del funcionamiento del *Componente* que utiliza el *Certificado*.

2. 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 un *Suscriptor*, que actúa como responsable y que tiene el control sobre dicho *Componente* o aplicación. La *Clave Privada* asociada a la *Clave Pública* estará, hasta la instalación del *Certificado de Componente*, bajo la responsabilidad del *Solicitante* y, una vez instalado, bajo la responsabilidad del *Suscriptor*.

3. A los efectos del artículo 6 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, los *Certificados de Componentes* se considerarán *Certificados* electrónicos cuando exista vinculación indubitada entre el *Certificado de Componente* y la persona física o jurídica o administración *Suscriptora* del *Certificado*. FNMT-RCM emitirá estos *Certificados* siempre que sea solicitado por un *Solicitante* autorizado y no se encuentre prohibido o limitado su utilización por la legislación aplicable.

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

5. Los *Certificados de Componentes* son expedidos y firmados por la FNMT-RCM para ser instalados y utilizados por *Componentes* informáticos, 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* aquellos *Suscriptores* 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.

6. FNMT-RCM solamente expedirá estos *Certificados* para actuaciones que no resulten incompatibles con el ámbito y uso del *Certificado* correspondiente, al que se encuentre indubitadamente vinculado el *Componente*.

7. La FNMT-RCM, como *Prestador de Servicios de Certificación* se reserva el derecho de no expedir o revocar este tipo de *Certificados* si el *Suscriptor* que se sirve de tal *Certificado*, no hace un uso adecuado del mismo, conculcando derechos de propiedad industrial o intelectual de terceros respecto de 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 *Componentes*. 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.

8. La FNMT–RCM quedará exonerada y se mantendrá indemne de cualquier reclamación o reivindicación por el uso inadecuado de los *Certificados de Componentes* que incumpla lo previsto en la *Declaración de Prácticas de Certificación*.

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*" (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, lo que se refleja en el presente documento para el caso de los *Certificados de Componente*.

10. Por tanto, se considera como *Declaración de Prácticas de Certificación* de un determinado tipo de *Certificado* expedido 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 el de este documento.

12. El objetivo del presente documento es la información pública del conjunto de prácticas, condiciones y características de los servicios de certificación que presta la FNMT-RCM como *Prestador de Servicios de Certificación*, en relación al ciclo de vida *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 la interpretación del presente documento se añaden las siguientes:

- *Componente*: Conjunto de elementos informáticos interrelacionados entre sí para transmitir o tratar información y con capacidad de firmarla o cifrarla de manera autónoma.
- *Certificado de Componente*: *Certificado* empleado por un *Componente* informático en una infraestructura de clave pública.
- *Representante*: Administrador, cargo público o apoderado general del *Suscriptor* cuando este es una persona jurídica, órgano u organismo público y que actúa en nombre del *Suscriptor*. Es también la persona física a la que se reconoce la capacidad de autorizar al *Solicitante*.
- *Solicitante*: Persona física, mayor de edad, que realiza la solicitud de expedición del *Certificado* y entrega la clave pública a la FNMT-RCM y recibe de esta el *Certificado*.
- *Sujeto del Certificado*: Campo "Subject" del *Certificado* que identifica al *Suscriptor* y al *Componente*.
- *Suscriptor*: Persona física, jurídica, órgano u organismo público destinatario de las actividades de la FNMT-RCM como *Prestador de Servicios de Certificación*, que suscribe los términos y condiciones del servicio y se referencia en el *Sujeto* en el *Certificado*. Es el titular y responsable del uso del *Certificado* que posee el control exclusivo y la capacidad de decisión sobre el *Componente.*

(Los términos señalados en cursiva se definen en el presente documento o en la Declaración General de Prácticas de Certificación)

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 expedición y/o en el propio *Certificado*.

5. POLÍTICA DE CERTIFICACIÓN DE LOS CERTIFICADOS DE COMPONENTE

5.1. IDENTIFICACIÓN

17. La presente *Política de Certificación* de la FNMT-RCM para la expedición de *Certificados de Componentes* se descompone en las identificadas a continuación:

Tabla 1 - Identificación de Política de Certificación

Denominación general	*Política de Certificación* de *Certificados de componente* de la FNMT-RCM (AC Componentes Informáticos)
Referencia/OID y nombre específico	1.3.6.1.4.1.5734.3.9.1 – *Certificados de componente* de sello de entidad (perfil de *Suscriptor* persona física) 1.3.6.1.4.1.5734.3.9.2 – *Certificados de componente* de sello de entidad (perfil de *Suscriptor* persona jurídica) 1.3.6.1.4.1.5734.3.9.3 – *Certificados de componente* de firma de código (perfil de *Suscriptor* persona física) 1.3.6.1.4.1.5734.3.9.4 – *Certificados de componente* de firma de código (perfil de *Suscriptor* persona jurídica) 1.3.6.1.4.1.5734.3.9.5 – *Certificados de componente* SSL estándar (perfil de *Suscriptor* persona física) 1.3.6.1.4.1.5734.3.9.6 – *Certificados de componente* SSL estándar (perfil de *Suscriptor* persona jurídica) 1.3.6.1.4.1.5734.3.9.7 – *Certificados de componente* SSL wildcard (perfil de *Suscriptor* persona física) 1.3.6.1.4.1.5734.3.9.8 – *Certificados de componente* SSL wildcard (perfil de *Suscriptor* persona jurídica) 1.3.6.1.4.1.5734.3.9.9 – *Certificados de componente* SSL plus (perfil de *Suscriptor* persona física) 1.3.6.1.4.1.5734.3.9.10 – *Certificados de componente* SSL plus (perfil de *Suscriptor* persona jurídica)

	1.3.6.1.4.1.5734.3.9.11 – *Certificados de componente* SSL multidominio (SAN/UCC) (perfil de *Suscriptor* persona física) 1.3.6.1.4.1.5734.3.9.12 – *Certificados de componente* SSL multidominio (SAN/UCC) (perfil de *Suscriptor* persona jurídica)
Versión	1.0
Fecha de Creación	21 de noviembre de 2013
DPC relacionada	Declaración General de Prácticas de Certificación de la FNMT-RCM
Localización	http://www.ceres.fnmt.es/dpcs

La tabla anterior identifica un OID de política para cada perfil de *Certificado*, aunque todas ellas se describen conjuntamente en este mismo documento. La razón de ello es doble, por un lado, se permite diferenciar de manera automatizada la estructura de campos a interpretar en cada tipo de *Certificado*, y por el otro, se unifican las reglas de aplicación de los *Certificados* a una misma comunidad y con los mismos requisitos de seguridad.

Cada una de las políticas se ha relacionado con el tipo de *Certificado* y con la naturaleza del *Suscriptor*, pudiendo ser este o bien una persona física o bien una persona jurídica.

Los tipos de *Certificado* contemplados en esta DPC son:

- Certificado SSL estándar: Permite establecer comunicaciones seguras utilizando el protocolo SSL/TSL. Este tipo de *Certificado* garantiza la identidad del dominio donde se encuentre una web.
- Certificado SSL plus: Tiene la misma finalidad que el *Certificado* SSL estándar, pero añade la posibilidad de elegir el uso extendido de claves del *Certificado* (autenticación de cliente y/o protección de correo electrónico).
- Certificado SSL wildcard: Garantiza la seguridad de un conjunto de subdominios ilimitado, a partir del tercer nivel, con un único *Certificado* SSL.
- Certificado SSL multidominio (SAN/UCC): Garantiza la seguridad de un conjunto de dominios independientes entre sí. Además, se permite elegir el uso extendido de claves del *Certificado* (autenticación de cliente y/o protección de correo electrónico).
- Certificado de firma de código: Permite firmar software y garantizar la identidad del propietario y la integridad del código.
- Certificado de sello de entidad: Se utiliza para la automatización de procesos de firma y autenticación entre componentes informáticos. Además, se permite al usuario elegir el uso extendido de claves del *Certificado* (autenticación de cliente, protección de correo electrónico, cualquier uso extendido de la clave).

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* y a un *Suscriptor* que lo mantiene bajo su control.
- 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 expedición y uso de los *Certificados de Componente*, expedidos bajo la presente *Política.*

20. FNMT-RCM no será responsable de la utilización de los *Certificados de Componente* cuando el *Suscriptor* del *Certificado* y, en su caso, su *Representante*, realice actuaciones sin facultades o extralimitándose en 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* de *Componente* expedidos por la FNMT-RCM se deberá previamente formar parte de la *Comunidad Electrónica* y adquirir la condición de *Entidad Usuaria*. Para confiar en un *Certificado* de *Componente*, será imprescindible comprobar el estado de validez del *Certificado* mediante el *Servicio de Información y Consulta sobre el Estado de los Certificados* de la FNMT-RCM.

22. De producirse esta confianza por parte de un miembro de la *Comunidad Electrónica*, *Entidad Usuaria* o por parte de un tercero, sin realizar la comprobación del estado del *Certificado*, 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* de *Componente*.

5.3.1.1. Responsabilidad del Prestador de Servicios de Certificación

23. La FNMT-RCM únicamente responde de la correcta identificación personal del *Solicitante, Suscriptor* y, en su caso, del *Representante*. 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*.

24. La FNMT-RCM responde de realizar la comprobación, en las bases de datos correspondientes, de que el *Suscriptor* es el titular de los nombres de dominio consignados en la solicitud del *Certificado*.

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. En ningún caso será responsable de las acciones o de las pérdidas en las que incurran, *Solicitantes*, *Suscriptores*, *Representantes*, *Entidades usuarias*, o, en su caso, terceros involucrados, que no se deban a errores graves 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 con el 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, la cuantía máxima 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 limita 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*, de que cuenta con autorización o apoderamiento del *Suscriptor* para realizar la solicitud y de que instalará adecuadamente el *Certificado* en el *Componente* designado por el *Suscriptor*.

33. El *Solicitante* mantendrá a salvo y defenderá a su costa a la FNMT-RCM contra cualquier acción que pudiese emprenderse contra esta Entidad y contra cualquier daño y perjuicio que sufra la FNMT-RCM como consecuencia de la inadecuada instalación del *Certificado*, de la falsedad o errores graves sobre la información suministrada en el procedimiento de expedición del *Certificado*, o como consecuencia de un acto u omisión culposa o negligente del *Solicitante*.

5.3.1.3. Responsabilidad del Suscriptor

34. Será en todo caso responsabilidad del *Suscriptor* utilizar de manera adecuada y custodiar diligentemente el *Certificado*, según el propósito y función para el que ha sido expedido, así como 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, en todo caso, ante la FNMT-RCM, las *Entidades usuarias* y, en su caso, ante terceros, de la actuación del *Solicitante*, del uso indebido del *Certificado*, o de la falsedad o errores de las manifestaciones en él recogidas en el proceso de solicitud, o actos u omisiones que provoquen daños y perjuicios a la FNMT-RCM o a terceros.

36. Será responsabilidad y, por tanto, obligación del *Suscriptor* no usar el *Certificado* en caso de que el *Prestador de Servicios de Certificación* haya cesado en la actividad como Entidad emisora de *Certificados* que realizó la expedición del *Certificado* en cuestión y no se hubiera producido la subrogación prevista en la ley. En todo caso, el *Suscriptor* 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.

5.3.1.4. Responsabilidad de la Entidad Usuaria

37. Será responsabilidad de la *Entidad usuaria* la verificación y comprobación del estado de los *Certificados*, no cabiendo en ningún caso presumir la validez de los *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* expedido 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 expedición del *Certificado*:

- Comprobar la identidad y circunstancias personales del *Solicitante* del *Certificado* y del *Suscriptor* y/o su *Representante* y recoger la manifestación de que el *Solicitante* está autorizado por el *Suscriptor* para realizar la solicitud. En ningún caso se expedirán *Certificados* a menores de edad, salvo que ostenten la cualidad de emancipados.

  La identificación se realizará a través de certificados de firma electrónica admitidos y de las funcionalidades previstas respecto del DNIe a los efectos antes señalados.

- En el proceso de registro, comprobar los datos relativos a la personalidad jurídica del *Suscriptor* y a la capacidad del *Representante*. Todas estas comprobaciones se realizarán según lo dispuesto en las *Prácticas de Certificación Particulares* expresadas en este documento y según los procedimientos de registro de la FNMT-RCM.

  En los procesos de comprobación de los extremos señalados anteriormente la FNMT-RCM podrá realizar verificaciones mediante la intervención de terceros que ostenten facultades fedatarias o de registros públicos o privados.

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

- Comprobar que el *Solicitante* está en posesión de la *Clave Privada* que constituirá, una vez expedido 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 *Suscriptor*, *Representante* y *Solicitante* de tal forma que se procure su *Confidencialidad*.

- Poner a disposición del *Solicitante*, *Suscriptor*, *Representante* y demás 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 Certificación* y *Prácticas de Certificación Particulares* 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.
- 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 cumplir la legislación vigente en materia de Protección de Datos de Carácter Personal, fundamentalmente, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y el resto de normas de aplicación.
- 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, a través de su Área de Registro, 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, expedición y revocación de *Certificados* y no alterar dicho marco de actuación.

- En particular, comprobar la identidad y cualesquiera circunstancias personales de los *Solicitantes*, *Suscriptores* y *Representantes* 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.*
- Comprobar que la titularidad del nombre de dominio se corresponde con la identidad del *Suscriptor* o, en su caso, obtener la autorización de éste, que se asociará al *Certificado de Componente*, por los medios a su alcance que, razonablemente, permitan acreditar tal titularidad, de conformidad con el estado de la técnica.
- Recoger expresamente la manifestación del *Suscriptor* en relación con la titularidad del *Componente*, manifestando que tiene el poder único de decisión sobre el mismo.
- Conservar toda la información y documentación relativa a los *Certificados*, cuya solicitud, renovación, suspensión o revocación gestiona durante quince (15) años.
- Realizar la recepción y gestión de las solicitudes y los contratos de expedición (formulario pdf) de *Certificados* con el *Suscriptor* de los mismos.
- Comprobar diligentemente las causas de revocación que pudieran afectar a la vigencia de los *Certificados*.

5.3.2.3. Obligaciones del Solicitante y Suscriptor

- No usar el *Certificado* fuera 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 expidió 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 veraz en la solicitud de los *Certificados* y mantenerla actualizada, suscribiendo los contratos por persona con capacidad suficiente.
- No solicitar para el *Sujeto* del certificado signos distintivos, denominaciones u otros derechos de propiedad industrial o intelectual de las que no sea titular, licenciatario o cuente con autorización demostrable para su uso.
- 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* previstas en las condiciones de uso y 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 para la revocación 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 y de terceros confiantes

- 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 *Suscriptor* continúa vigente y activo.
- Verificar el estado de los *Certificados* en la *Cadena de Certificación*, 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. FNMT-RCM no será responsable de *Certificados* con apariencia fraudulenta de haber sido expedidos por la FNMT-RCM y emprenderá las acciones legales contra estas actuaciones fraudulentas si tuviera conocimiento de las mismas, directamente o por denuncia de los interesados.

50. Si un miembro de la *Comunidad Electrónica*, una *Entidad Usuaria* o un tercero confiaran en un *Certificado* de *Componente* sin realizar la comprobación del estado del *Certificado*, 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* de *Componente*.

51. 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* expedidos 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 "AC COMPONENTES INFORMÁTICOS"

52. 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.

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

53. 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

54. En el procedimiento de solicitud se toman los datos personales del *Solicitante* de *Certificado de Componente*, del *Suscriptor* y, en su caso, su *Representante*. Además, se verifica la información específica que ha de contener el *Certificado* y se formaliza su contrato con la FNMT-RCM para su posterior expedición. Como desarrollo de este esquema, existirá un procedimiento de registro detallado, poniéndose a disposición de los *Solicitantes* los aspectos necesarios para la solicitud del *Certificado*. Estas actividades serán realizadas únicamente por la *Oficina de Registro* autorizada.

55. El *Suscriptor* (a través del *Solicitante*) realizará la solicitud del *Certificado* mediante un formulario web de la FNMT-RCM, que deberá incluir:

- Los datos identificativos del *Componente*

- Los datos relativos a la titularidad de los Nombres de Dominio, o manifestación de titularidad del *Componente*, que se vincularán a cada tipo de *Certificado*
- Los datos correspondientes al *Suscriptor* como persona o entidad interesada en la expedición de un *Certificado de Componente*, ya sea pública o privada.
- Los datos correspondientes al *Representante* del *Suscriptor* del *Certificado* cuando el *Suscriptor* sea una entidad.
- Los datos del *Solicitante* del *Certificado*
- El PKCS#10 o SPKAC de la petición del *Certificado de Componente*

56. En cualquier caso, se completarán todos los campos del formulario que sean consignados como obligatorios y el formulario en su totalidad será firmado electrónicamente por el *Solicitante*, firma que será verificada por la FNMT-RCM.

57. 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[1] que prestará el servicio como *Autoridad de Sellado de Tiempo* y *Suscriptora* del *Certificado*.

6.1.2. Suscripción y envío del contrato por el *Suscriptor*

58. Tras la solicitud, el *Suscriptor* firmará electrónicamente el contrato (formulario pdf, donde consta la aceptación de las condiciones de uso del *Certificado* solicitado y que estará disponible en la página web correspondiente) y lo remitirá, a través de la dirección electrónica proporcionada, a la *Oficina de Registro* de la FNMT-RCM para su tratamiento.

59. La firma del contrato pdf se realizará, preferentemente, con el *Certificado de Persona Jurídica* del *Suscriptor* expedido por la FNMT-RCM, pudiéndose utilizar otros *Certificados* admitidos.

60. No remitir el contrato firmado por el *Suscriptor*, no realizar el pago, la ausencia de datos o de la documentación exigida, serán causas de interrupción del proceso de expedición del *Certificado*.

61. La FNMT-RCM conservará la copia firmada por el *Suscriptor* y la archivará junto con toda la documentación referida a ese *Componente* informático.

6.1.3. Expedición

62. La FNMT-RCM comprobará la veracidad de los datos incluidos en la solicitud y, en su caso, la capacidad del *Representante* a través de las verificaciones correspondientes y conservando las evidencias electrónicas oportunas.

[1] La entidad *Suscriptora* 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*

63. La firma electrónica generada para la suscripción del contrato será verificada por la FNMT-RCM.

64. La FNMT-RCM, una vez recibida en su Oficina de Registro la solicitud web y el contrato, dará curso a la petición mediante sus aplicaciones informáticas internas.

65. Si el *Certificado* estuviera asociado a uno o varios dominios de Internet, la *Oficina de Registro* comprobará, en las bases de datos de los registradores autorizados de dominios, la coincidencia entre el titular del dominio y el *Suscriptor* del *Certificado*, conservando evidencias de la consulta.

66. La *Oficina de Registro* verificará la personalidad del *Suscriptor* y, en su caso, la personalidad y capacidad del *Representante* mediante la verificación de las *Firmas Electrónicas* y *Certificados* utilizados en el proceso y/o consulta de las bases de datos del Registro Mercantil o de terceras partes de confianza.

67. En caso de que existan errores o contradicciones, la FNMT-RCM contactará con el *Solicitante* y *Suscriptor* para su aclaración y, en su caso, subsanación.

68. La FNMT-RCM, por medio de su *Firma Electrónica*, suscribirá la información contenida en los *Certificados* que expida dotándola así de autenticidad e integridad.

69. La FNMT-RCM actuará para:

- Comprobar que el *Solicitante* del *Certificado* posee la *Clave Privada* correspondiente a la *Clave Pública* a certificar.
- Determinar que la información incluida en el *Certificado* se base en la información proporcionada por el *Solicitante* y el *Suscriptor* y que, utilizando una normal diligencia en la realización de las comprobaciones, tal información es veraz.

6.1.4. Publicación y distribución

70. La entrega del *Certificado* se realiza, previa notificación, poniéndolo a disposición del *Solicitante* en la aplicación de descarga de *Certificados*, una vez sean cumplidos el resto de requisitos para su expedición.

6.1.5. Vigencia

6.1.5.1. Caducidad

71. La duración máxima de los *Certificados de Componente* será de tres años contados a partir del momento de su expedición, siempre y cuando no se extinga su vigencia por las causas y procedimientos expuestos en el apartado "Extinción de la vigencia del Certificado". En el caso de los *Certificados* para *Unidades de Sellado de Tiempo*, la duración máxima será de cinco años.

6.1.5.2. Extinción de la vigencia del Certificado

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

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

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

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

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

73. A los efectos enumerados anteriormente, se hace constar que la solicitud de expedición de un *Certificado de Componente*, cuando exista otro vigente con los mismos datos de identificación y perteneciente a la misma *Ley de Emisión*, no producirá la revocación del primero obtenido. Por tanto, podrán existir varios *Certificados* en vigor con el mismo *Sujeto*, pero diferente número de serie.

74. Los efectos de la extinción de vigencia del *Certificado* por revocación , 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 Información y Consulta sobre el Estado de los Certificados*.

6.1.6. Revocación

75. 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.

76. La revocación de un *Certificado de Componente*, sin perjuicio de las causas de revocación que se señalan a continuación, sólo podrá ser solicitada por el *Suscriptor*.

6.1.6.1. Causas de revocación

77. 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 le haya sido solicitada por el *Suscriptor* 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 siguiente apartado, le sean acreditados dichos extremos fehacientemente, previa identificación del solicitante de la revocación (el *Suscriptor*).

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

a) La solicitud de revocación por parte del *Suscriptor*, o un tercero debidamente autorizado, realizada de manera fehaciente. En todo caso deberá dar lugar a esta solicitud, siendo de obligado cumplimiento para el Suscriptor:

- Pérdida del soporte del *Certificado.*
- La utilización por un tercero de los *Datos de Creación de Firma*, asociados a los *Datos de Verificación de Firma* contenidos en el *Certificado* y vinculados a la identidad del *Suscriptor*.
- La puesta en peligro de los *Datos de Creación de Firma*.
- La no aceptación de las nuevas condiciones tras la redacción y publicación de nuevas versiones de *Declaraciones de Prácticas de Certificación* o de *Políticas y Prácticas Particulares*, 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 *Suscriptor*.

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

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.*

f) Solicitar para el *Sujeto del Certificado* signos distintivos, denominaciones u otros derechos de propiedad industrial o intelectual de las que el *Suscriptor* no sea titular, licenciatario o usuario autorizado.

g) El impago de los servicios prestados.

h) Contravención de una obligación sustancial de esta *Política de Certificación* por parte del *Suscriptor del Certificado* que haya sido conocida por la FNMT-RCM o por parte de la *Oficina de Registro* si hubiese podido afectar al procedimiento de expedición del *Certificado*.

i) Puesta en peligro del secreto de los *Datos de creación de Firma* de la FNMT-RCM, con los que firma los *Certificados* que emite.

j) Utilizar el Certificado con el propósito de generar dudas a los usuarios sobre la procedencia de los productos o servicios ofertados, haciendo ver que su origen es distinto del realmente ofertado. Para ello, se seguirán los criterios sobre actividad infractora de las normas sobre consumidores y usuarios, comercio, competencia y publicidad.

79. En ningún caso se debe entender que la FNMT-RCM asume obligación alguna de comprobar los extremos mencionados en las letras c) a f) del presente apartado. El resto de supuestos, serán efectivos desde que son conocidos por la FNMT-RCM.

80. 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.

81. 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

82. 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 su *Servicio de Información y Consulta sobre el Estado de los Certificados*.

6.1.6.3. Procedimiento para la revocación de Certificados

83. La revocación será realizada únicamente por la *Oficina de Registro* de la FNMT-RCM.

1. Solicitud del *Suscriptor*

   El *Suscriptor* enviará el formulario de solicitud de revocación, cumplimentado y firmado electrónicamente a la FNMT-RCM, con los mismos *Certificados* que son admitidos para la solicitud y por los canales electrónicos habilitados por esta Entidad.

2. Tramitación de la solicitud por la FNMT-RCM

   El registrador de la FNMT-RCM recibirá el contrato de revocación y realizará las mismas comprobaciones sobre identidad y capacidad del *Suscriptor* y *Representante* que para el caso de la solicitud de expedición y, si procediera, tramitará la revocación del *Certificado de Componente*.

   Tan pronto se resuelva la revocación, el *Suscriptor* recibirá a través de la dirección de correo electrónico consignada en la solicitud, la notificación de 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*, conteniendo el número de serie del *Certificado* revocado, la fecha y hora de revocación y la causa de revocación.

6.1.7. Suspensión

84. Serán causas de suspensión de un *Certificado de Componente*:

a) La solicitud por parte del *Suscriptor* o un tercero debidamente autorizado, realizada de manera fehaciente por el mismo procedimiento que para la revocación.

b) Resolución judicial o administrativa.

c) Existencia de dudas fundadas acerca de la concurrencia de las siguientes causas de extinción:

- La puesta en peligro de los *Datos de Creación de Firma* del *Certificado*.

- Puesta en peligro del secreto de los *Datos de Creación de Firma* de la FNMT-RCM, con los que firma los *Certificados* que emite.
- Alteración de los datos aportados para la obtención del *Certificado*, que hagan invalidante su uso.

6.1.8. Comprobación del estado del Certificado

85. La comprobación del estado de los *Certificados* se proporciona mediante el protocolo *OCSP*, accediendo a través de la dirección indicada para ello dentro del propio *Certificado* al *Servicio de Información y Consulta sobre el Estado de los Certificados*.

7. PERFILES DE CERTIFICADOS

7.1. AUTORIDAD DE CERTIFICACIÓN

Campo		Contenido	Obligatoriedad	Criticidad
1. Version		2	Sí	
2. Serial Number		Número identificativo único del certificado.	Sí	
3. Signature Algorithm		Sha256withRsaEncryption	Sí	
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Raíz)	Sí	
	4.1. Country	C=ES	Sí	
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM	Sí	
	4.3. Organization Unit	OU=AC RAIZ FNMT-RCM	Sí	
5. Validity		15 años	Sí	
6. Subject		Entidad emisora del certificado (CA Subordinada)	Sí	
	6.1. Country	C=ES	Sí	
	6.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí	
	6.3. Organization Unit	OU=AC Componentes Informáticos	Sí	
7. Authority Key Identifier		Identificador de la clave pública de la entidad raíz. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de esta CA Subordinada	Sí	
8. Subject Public Key Info		Clave pública de la CA de Componentes, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	
9. Subject Key Identifier		Identificador de la clave pública de la CA de Componentes.	Sí	
10. Key Usage		Uso permitido de las claves del certificado.	Sí	Sí
	10.1. Digital Signature	0	Sí	

	10.2. Content Commitment		0	Sí	
	10.3. Key Encipherment		0	Sí	
	10.4. Data Encipherment		0	Sí	
	10.5. Key Agreement		0	Sí	
	10.6. Key Certificate Signature		1	Sí	
	10.7. CRL Signature		1	Sí	
11. Certificate Policies			Política de certificación	Sí	No
	11.1. Policy Identifier		2.5.29.32.0 (anyPolicy)	Sí	
	11.2. Policy Qualifier Id				
		11.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	
		11.2.2 User Notice	Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)	Sí	
12. CRL Distribution Point				Sí	No
	12.1. Distribution Point 1		Punto de distribución 1 de la CRL (ARL) ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí	
	12.2. Distribution Point 2		Punto de distribución 2 de la CRL (ARL) http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl	Sí	
13. Basic Constraints					Sí
	13.1. Subject Type		CA		
	13.2. Path Length		0		
14. Authority Info Access				Sí	
	14.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)		
	14.2. Acces Location 1		http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder		
	Access Method 2		Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)		
	Access Location 2		http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt		

7.2. CERTIFICADOS EMITIDOS

7.2.1. Sello de Entidad PF

Campo		Contenido	Obligatoriedad	Criticidad
1. Version		2	Sí	
2. Serial Number		Número identificativo único del certificado.	Sí	
3. Signature Algorithm		Sha256withRsaEncryption	Sí	
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí	
	4.1. Country	C=ES	Sí	
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí	
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí	
5. Validity		Variable	Sí	
6. Subject		Identificación/descripción del suscriptor del certificado y del componente.	Sí	
	6.1. Country	C=ES	Sí	
	6.2. GivenName	Nombre del suscriptor para el que se emite el certificado.	Sí	
	6.3. Surname	Apellidos del suscriptor para el que se emite el certificado.	Sí	
	6.4. Serial Number	NIF del suscriptor para el que se emite el certificado.	Sí	
	6.5. Common Name	Denominación del componente	Sí	
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	

Campo			Contenido	Obligatoriedad	Criticidad
10. Key Usage			Uso permitido de las claves certificadas.		Sí
	10.1. Digital Signature		1	Sí	
	10.2. Content Commitment		0	No	
	10.3. Key Encipherment		1	Sí	
	10.4. Data Encipherment		1	Sí	
	10.5. Key Agreement		0	Sí	
	10.6. Key Certificate Signature		0	Sí	
	10.7. CRL Signature		0	Sí	
11. Extended Key Usage			Uso mejorado o extendido de las claves	No	No
	11.1. Email Protection		1.3.6.1.5.5.7.3.4	No	
	11.2. Client Authentication		1.3.6.1.5.5.7.3.2	No	
	11.3. AnyExtendedKeyUsage		2.5.29.37.0	No	
12. Certificate Policies			Política de certificación	Sí	No
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.1	Sí	
	12.2. Policy Qualifier Id			Sí	
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	
13. Subject Alternative Names					
	14.1. Nombre del suscriptor		Id Campo / Valor: 1.3.6.1.4.1.5734.1.1 = <Nombre>	Sí	
	14.2. Primer apellido del suscriptor		Id Campo / Valor: 1.3.6.1.4.1.5734.1.2 = <Primer apellido>	Sí	
	14.3. Segundo apellido del suscriptor		Id Campo / Valor: 1.3.6.1.4.1.5734.1.3 = <Segundo apellido>	No	
	14.4. NIF del suscriptor		Número único de identificación del suscriptor (NIF) Id Campo / Valor: 1.3.6.1.4.1.5734.1.4 = <NIF>	Sí	
	14.5. Denominación del componente		Id Campo / Valor: 1.3.6.1.4.1.5734.1.8 = < Denominación del componente>	Sí	

Campo		Contenido	Obligatoriedad	Criticidad
14. CRL Distribution Point		Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No
	14.1. Distribution Point 1	Punto de publicación de la CRL1. ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	
	14.2. Distribution Point 2	Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Sí	
15. Authority Info Access			Sí	No
	15.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	
	15.2. Acces Location 1	http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder	Sí	
	15.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí	
16. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	No
	16.1. Subject Type	Valor FALSE (entidad final)		

7.2.2. Sello de Entidad PJ

Campo		Contenido	Obligatoriedad	Criticidad
1. Version		2	Sí	
2. Serial Number		Número identificativo único del certificado.	Sí	
3. Signature Algorithm		Sha256withRsaEncryption	Sí	
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí	
	4.1. Country	C=ES	Sí	
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí	
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí	
5. Validity		Variable	Sí	
6. Subject		Identificación/descripción del suscriptor del certificado y del componente.	Sí	
	6.1. Country	C=ES	Sí	
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí	
	6.3. Organization	Denominación del suscriptor	Sí	
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No	
	6.5. Serial Number	NIF del suscriptor	Sí	
	6.6. Common Name	Denominación del componente	Sí	
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	
10. Key Usage		Uso permitido de las claves certificadas.		Sí

Campo			Contenido	Obligatoriedad	Criticidad
	10.1. Digital Signature		1	Sí	
	10.2. Content Commitment		0	No	
	10.3. Key Encipherment		1	Sí	
	10.4. Data Encipherment		1	Sí	
	10.5. Key Agreement		0	Sí	
	10.6. Key Certificate Signature		0	Sí	
	10.7. CRL Signature		0	Sí	
11. Extended Key Usage			Uso mejorado o extendido de las claves	No	No
	11.1. Email Protection		1.3.6.1.5.5.7.3.4	No	
	11.2. Client Authentication		1.3.6.1.5.5.7.3.2	No	
	11.3. AnyExtendedKeyUsage		2.5.29.37.0	No	
12. Certificate Policies			Política de certificación	Sí	No
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.2	Sí	
	12.2. Policy Qualifier Id			Sí	
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	
13. Subject Alternative Names					
	13.1. Denominación del componente		Id Campo / Valor: 1.3.6.1.4.1.5734.1.8 = < Denominación del componente>	Sí	
14. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No
	14.1. Distribution Point 1		Punto de publicación de la CRL1. ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	
	14.2. Distribution Point 2		Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Sí	
15. Authority Info Access				Sí	No

Campo		Contenido	Obligatoriedad	Criticidad
	15.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	
	15.2. Acces Location 1	http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder	Sí	
	15.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí	
16. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	No
	16.1. Subject Type	Valor FALSE (entidad final)		

7.2.3. Componente de firma de código PF

Campo		Contenido	Obligatoriedad	Criticidad
1. Version		2	Sí	
2. Serial Number		Número identificativo único del certificado.	Sí	
3. Signature Algorithm		Sha256withRsaEncryption	Sí	
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí	
	4.1. Country	C=ES	Sí	
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí	
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí	
5. Validity		Variable	Sí	
6. Subject		Identificación/descripción del suscriptor del certificado y del componente.	Sí	
	6.1. Country	C=ES	Sí	
	6.2. GivenName	Nombre del suscriptor para el que se emite el certificado.	Sí	
	6.3. Surname	Apellidos del suscriptor para el que se emite el certificado.	Sí	
	6.4. Serial Number	NIF del suscriptor para el que se emite el certificado.	Sí	
	6.5. Common Name	Denominación del componente	Sí	
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	
10. Key Usage		Uso permitido de las claves certificadas.	Sí	Sí

Campo			Contenido	Obligatoriedad	Criticidad
	10.1. Digital Signature		1		
	10.2. Content Commitment		0		
	10.3. Key Encipherment		0		
	10.4. Data Encipherment		0		
	10.5. Key Agreement		0		
	10.6. Key Certificate Signature		0		
	10.7. CRL Signature		0		
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí	No
	11.1. Code Signing		1.3.6.1.5.5.7.3.3	Sí	
12. Certificate Policies			Política de certificación	Sí	No
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.3	Sí	
	12.2. Policy Qualifier Id			Sí	
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	
13. Subject Alternative Names					No
	13.1. Nombre del suscriptor		Id Campo / Valor: 1.3.6.1.4.1.5734.1.1 = <Nombre>	Sí	
	13.2. Primer apellido del suscriptor		Id Campo / Valor: 1.3.6.1.4.1.5734.1.2 = <Primer apellido>	Sí	
	13.3. Segundo apellido del suscriptor		Id Campo / Valor: 1.3.6.1.4.1.5734.1.3 = <Segundo apellido>	No	
	13.4. NIF del suscriptor		Número único de identificación del suscriptor (NIF) Id Campo / Valor: 1.3.6.1.4.1.5734.1.4 = <NIF>	Sí	
	13.5. Denominación del componente		Id Campo / Valor: 1.3.6.1.4.1.5734.1.8 = < Denominación del componente>	Sí	
14. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No
	14.1. Distribution Point 1		Punto de publicación de la CRL1. ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-	Sí	

Campo		Contenido	Obligatoriedad	Criticidad
		RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)		
	14.2. Distribution Point 2	Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Sí	
15. Authority Info Access			Sí	No
	15.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	
	15.2. Acces Location 1	http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder	Sí	
	15.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí	
16. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	No
	16.1. Subject Type	Valor FALSE (entidad final)		

7.2.4. Componente de firma de código PJ

Campo		Contenido	Obligatoriedad	Criticidad
1. Version		2	Sí	
2. Serial Number		Número identificativo único del certificado.	Sí	
3. Signature Algorithm		Sha256withRsaEncryption	Sí	
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí	
	4.1. Country	C=ES	Sí	
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí	
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí	
5. Validity		Variable	Sí	
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí	
	6.1. Country	C=ES	Sí	
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí	
	6.3. Organization	Denominación del suscriptor	Sí	
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No	
	6.5. Serial Number	NIF del suscriptor	Sí	
	6.6. Common Name	Denominación del componente	Sí	
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	
10. Key Usage		Uso permitido de las claves certificadas.	Sí	Sí

Campo			Contenido	Obligatoriedad	Criticidad
	10.1. Digital Signature		1		
	10.2. Content Commitment		0		
	10.3. Key Encipherment		0		
	10.4. Data Encipherment		0		
	10.5. Key Agreement		0		
	10.6. Key Certificate Signature		0		
	10.7. CRL Signature		0		
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí	No
	11.1. Code Signing		1.3.6.1.5.5.7.3.3	Sí	
12. Certificate Policies			Política de certificación	Sí	No
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.4	Sí	
	12.2. Policy Qualifier Id			Sí	
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	
13. Subject Alternative Names					No
	13.1. Denominación del componente		Id Campo / Valor: 1.3.6.1.4.1.5734.1.8 = < Denominación del componente>	Sí	
14. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No
	14.1. Distribution Point 1		Punto de publicación de la CRL1. ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	
	14.2. Distribution Point 2		Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Sí	
15. Authority Info Access				Sí	No
	15.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	

Campo		Contenido	Obligatoriedad	Criticidad
	15.2. Acces Location 1	http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder	Sí	
	15.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí	
16. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	No
	16.1. Subject Type	Valor FALSE (entidad final)		

7.2.5. SSL estándar PF

Campo		Contenido	Obligatoriedad	Criticidad
1. Version		2	Sí	
2. Serial Number		Número identificativo único del certificado.	Sí	
3. Signature Algorithm		Sha256withRsaEncryption	Sí	
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí	
	4.1. Country	C=ES	Sí	
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí	
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí	
5. Validity		Variable	Sí	
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí	
	6.1. Country	C=ES	Sí	
	6.2. GivenName	Nombre del suscriptor para el que se emite el certificado.	Sí	
	6.3. Surname	Apellidos del suscriptor para el que se emite el certificado.	Sí	
	6.4. Serial Number	NIF del suscriptor para el que se emite el certificado.	Sí	
	6.5. Common Name	Dominio para el que se expide el certificado	Sí	
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	
10. Key Usage		Uso permitido de las claves certificadas.	Sí	Sí

Campo			Contenido	Obligatoriedad	Criticidad
	10.1. Digital Signature		1		
	10.2. Content Commitment		0		
	10.3. Key Encipherment		1		
	10.4. Data Encipherment		0		
	10.5. Key Agreement		0		
	10.6. Key Certificate Signature		0		
	10.7. CRL Signature		0		
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí	No
	11.1. Server Authentication		1.3.6.1.5.5.7.3.1	Sí	
12. Certificate Policies			Política de certificación	Sí	No
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.5	Sí	
	12.2. Policy Qualifier Id			Sí	
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	
13. Subject Alternative Names					No
	13.1. Nombre del suscriptor		Id Campo / Valor: 1.3.6.1.4.1.5734.1.1 = <Nombre>	Sí	
	13.2. Primer apellido del suscriptor		Id Campo / Valor: 1.3.6.1.4.1.5734.1.2 = <Primer apellido>	Sí	
	13.3. Segundo apellido del suscriptor		Id Campo / Valor: 1.3.6.1.4.1.5734.1.3 = <Segundo apellido>	No	
	13.4. NIF del suscriptor		Número único de identificación del suscriptor (NIF) Id Campo / Valor: 1.3.6.1.4.1.5734.1.4 = <NIF>	Sí	
	13.5. DNSName		Id Campo / Valor: NombreDNS = <Dominio>	Sí	
14. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No
	14.1. Distribution Point 1		Punto de publicación de la CRL1. ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;bina	Sí	

Campo		Contenido	Obligatoriedad	Criticidad
		ry?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)		
	14.2. Distribution Point 2	Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Sí	
15. Authority Info Access			Sí	No
	15.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	
	15.2. Acces Location 1	http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder	Sí	
	15.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí	
16. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	No
	16.1. Subject Type	Valor FALSE (entidad final)		

7.2.6. SSL estándar PJ

Campo		Contenido	Obligatoriedad	Criticidad
1. Version		2	Sí	
2. Serial Number		Número identificativo único del certificado.	Sí	
3. Signature Algorithm		Sha256withRsaEncryption	Sí	
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí	
	4.1. Country	C=ES	Sí	
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí	
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí	
5. Validity		Variable	Sí	
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí	
	6.1. Country	C=ES	Sí	
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí	
	6.3. Organization	Denominación del suscriptor	Sí	
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No	
	6.5. Serial Number	NIF del suscriptor	Sí	
	6.6. Common Name	Dominio para el que se expide el certificado	Sí	
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	
10. Key Usage		Uso permitido de las claves certificadas.	Sí	Sí

Campo			Contenido	Obligatoriedad	Criticidad
	10.1. Digital Signature		1		
	10.2. Content Commitment		0		
	10.3. Key Encipherment		1		
	10.4. Data Encipherment		0		
	10.5. Key Agreement		0		
	10.6. Key Certificate Signature		0		
	10.7. CRL Signature		0		
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí	No
	11.1. Server Authentication		1.3.6.1.5.5.7.3.1	Sí	
12. Certificate Policies			Política de certificación	Sí	No
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.6	Sí	
	12.2. Policy Qualifier Id			Sí	
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	
13. Subject Alternative Names					No
	13.1. DNSName		Id Campo / Valor: NombreDNS = Dominio	Sí	
14. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No
	14.1. Distribution Point 1		Punto de publicación de la CRL1. ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	
	14.2. Distribution Point 2		Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Sí	
15. Authority Info Access				Sí	No
	15.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	

Campo		Contenido	Obligatoriedad	Criticidad
	15.2. Acces Location 1	http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder	Sí	
	15.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí	
16. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	No
	16.1. Subject Type	Valor FALSE (entidad final)		

7.2.7. SSL wildcard PF

Campo		Contenido	Obligatoriedad	Criticidad
1. Version		2	Sí	
2. Serial Number		Número identificativo único del certificado.	Sí	
3. Signature Algorithm		Sha256withRsaEncryption	Sí	
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí	
	4.1. Country	C=ES	Sí	
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí	
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí	
5. Validity		Variable	Sí	
6. Subject		Identificación/descripción del suscriptor del certificado y del componente.	Sí	
	6.1. Country	C=ES	Sí	
	6.2. GivenName	Nombre del suscriptor para el que se emite el certificado.	Sí	
	6.3. Surname	Apellidos del suscriptor para el que se emite el certificado.	Sí	

Campo			Contenido	Obligatoriedad	Criticidad
	6.4. Serial Number		NIF del suscriptor para el que se emite el certificado.	Sí	
	6.5. Common Name		Dominio wildcard para el que se expide el certificado.	Sí	
7. Authority Key Identifier			Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	
8. Subject Public Key Info			Clave pública del componente, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	
9. Subject Key Identifier			Identificador de la clave pública del componente.	Sí	
10. Key Usage			Uso permitido de las claves certificadas.	Sí	Sí
	10.1. Digital Signature		1		
	10.2. Content Commitment		0		
	10.3. Key Encipherment		1		
	10.4. Data Encipherment		0		
	10.5. Key Agreement		0		
	10.6. Key Certificate Signature		0		
	10.7. CRL Signature		0		
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí	No
	11.1. Server Authentication		1.3.6.1.5.5.7.3.1	Sí	
12. Certificate Policies			Política de certificación	Sí	No
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.7	Sí	
	12.2. Policy Qualifier Id			Sí	
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	
13. Subject Alternative Names					No
	13.1. Nombre del suscriptor		Id Campo / Valor: 1.3.6.1.4.1.5734.1.1 = <Nombre>	Sí	
	13.2. Primer apellido del suscriptor		Id Campo / Valor: 1.3.6.1.4.1.5734.1.2 = <Primer apellido>	Sí	

Campo		Contenido	Obligatoriedad	Criticidad
	13.3. Segundo apellido del suscriptor	Id Campo / Valor: 1.3.6.1.4.1.5734.1.3 = <Segundo apellido>	No	
	13.4. NIF del suscriptor	Número único de identificación del suscriptor (NIF) Id Campo / Valor: 1.3.6.1.4.1.5734.1.4 = <NIF>	Sí	
	13.5. DNSName	Id Campo / Valor: NombreDNS = Dominio wildcard	Sí	
14. CRL Distribution Point		Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No
	14.1. Distribution Point 1	Punto de publicación de la CRL1. ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	
	14.2. Distribution Point 2	Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Sí	
15. Authority Info Access			Sí	No
	15.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	
	15.2. Acces Location 1	http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder	Sí	
	15.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí	
16. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	No
	16.1. Subject Type	Valor FALSE (entidad final)		

7.2.8. SSL wildcard PJ

Campo		Contenido	Obligatoriedad	Criticidad
1. Version		2	Sí	
2. Serial Number		Número identificativo único del certificado.	Sí	
3. Signature Algorithm		Sha256withRsaEncryption	Sí	
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí	
	4.1. Country	C=ES	Sí	
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí	
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí	
5. Validity		Variable	Sí	
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí	
	6.1. Country	C=ES	Sí	
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí	
	6.3. Organization	Denominación del suscriptor	Sí	
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No	
	6.5. Serial Number	NIF del suscriptor	Sí	
	6.6. Common Name	Dominio wildcard para el que se expide el certificado.	Sí	
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	
10. Key Usage		Uso permitido de las claves certificadas.	Sí	Sí

Campo			Contenido	Obligatoriedad	Criticidad
	10.1. Digital Signature		1		
	10.2. Content Commitment		0		
	10.3. Key Encipherment		1		
	10.4. Data Encipherment		0		
	10.5. Key Agreement		0		
	10.6. Key Certificate Signature		0		
	10.7. CRL Signature		0		
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí	No
	11.1. Server Authentication		1.3.6.1.5.5.7.3.1	Sí	
12. Certificate Policies			Política de certificación	Sí	No
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.8	Sí	
	12.2. Policy Qualifier Id			Sí	
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	
13. Subject Alternative Names					No
	13.1. DNSName		Id Campo / Valor: NombreDNS = Dominio wildcard	Sí	
14. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No
	14.1. Distribution Point 1		Punto de publicación de la CRL1. ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	
	14.2. Distribution Point 2		Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Sí	
15. Authority Info Access				Sí	No
	15.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	

Campo		Contenido	Obligatoriedad	Criticidad
	15.2. Acces Location 1	http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder	Sí	
	15.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí	
16. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	No
	16.1. Subject Type	Valor FALSE (entidad final)		

7.2.9. SSL plus PF

Campo		Contenido	Obligatoriedad	Criticidad
1. Version		2	Sí	
2. Serial Number		Número identificativo único del certificado.	Sí	
3. Signature Algorithm		Sha256withRsaEncryption	Sí	
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí	
	4.1. Country	C=ES	Sí	
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí	
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí	
5. Validity		Variable	Sí	
6. Subject		Identificación/descripción del suscriptor del certificado y del componente.	Sí	
	6.1. Country	C=ES	Sí	
	6.2. GivenName	Nombre del suscriptor para el que se emite el certificado.	Sí	
	6.3. Surname	Apellidos del suscriptor para el que se emite el certificado.	Sí	
	6.4. Serial Number	NIF del suscriptor para el que se emite el certificado.	Sí	
	6.5. Common Name	Dominio para el que se expide el certificado	Sí	
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	
10. Key Usage		Uso permitido de las claves certificadas.		Sí

Campo			Contenido	Obligatoriedad	Criticidad
	10.1. Digital Signature		1	Sí	
	10.2. Content Commitment		0	No	
	10.3. Key Encipherment		1	Sí	
	10.4. Data Encipherment		0	Sí	
	10.5. Key Agreement		0	Sí	
	10.6. Key Certificate Signature		0	Sí	
	10.7. CRL Signature		0	Sí	
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí	No
	11.1. Server Authentication		1.3.6.1.5.5.7.3.1	Sí	
	11.2. Email Protection		1.3.6.1.5.5.7.3.4	No	
	11.3. Client Authentication		1.3.6.1.5.5.7.3.2	No	
12. Certificate Policies			Política de certificación	Sí	No
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.9	Sí	
	12.2. Policy Qualifier Id			Sí	
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	
13. Subject Alternative Names					No
	13.1. Nombre del suscriptor		Id Campo / Valor: 1.3.6.1.4.1.5734.1.1 = <Nombre>	Sí	
	13.2. Primer apellido del suscriptor		Id Campo / Valor: 1.3.6.1.4.1.5734.1.2 = <Primer apellido>	Sí	
	13.3. Segundo apellido del suscriptor		Id Campo / Valor: 1.3.6.1.4.1.5734.1.3 = <Segundo apellido>	No	
	13.4. NIF del suscriptor		Número único de identificación del suscriptor (NIF) Id Campo / Valor: 1.3.6.1.4.1.5734.1.4 = <NIF>	Sí	
	13.5. DNSName		Id Campo / Valor: NombreDNS = Dominio	Sí	
14. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No

Campo		Contenido	Obligatoriedad	Criticidad
	14.1. Distribution Point 1	Punto de publicación de la CRL1. ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	
	14.2. Distribution Point 2	Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Sí	
15. Authority Info Access			Sí	No
	15.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	
	15.2. Acces Location 1	http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder	Sí	
	15.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí	
16. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	No
	16.1. Subject Type	Valor FALSE (entidad final)		

7.2.10. SSL plus PJ

Campo		Contenido	Obligatoriedad	Criticidad
1. Version		2	Sí	
2. Serial Number		Número identificativo único del certificado.	Sí	
3. Signature Algorithm		Sha256withRsaEncryption	Sí	
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí	
	4.1. Country	C=ES	Sí	
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí	
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí	
5. Validity		Variable	Sí	
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí	
	6.1. Country	C=ES	Sí	
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí	
	6.3. Organization	Denominación del suscriptor	Sí	
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No	
	6.5. Serial Number	NIF del suscriptor	Sí	
	6.6. Common Name	Dominio para el que se expide el certificado	Sí	
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	
10. Key Usage		Uso permitido de las claves certificadas.		Sí

Campo			Contenido	Obligatoriedad	Criticidad
	10.1. Digital Signature		1	Sí	
	10.2. Content Commitment		0	No	
	10.3. Key Encipherment		1	Sí	
	10.4. Data Encipherment		0	Sí	
	10.5. Key Agreement		0	Sí	
	10.6. Key Certificate Signature		0	Sí	
	10.7. CRL Signature		0	Sí	
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí	No
	11.1. Server Authentication		1.3.6.1.5.5.7.3.1	Sí	
	11.2. Email Protection		1.3.6.1.5.5.7.3.4	No	
	11.3. Client Authentication		1.3.6.1.5.5.7.3.2	No	
12. Certificate Policies			Política de certificación	Sí	No
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.10	Sí	
	12.2. Policy Qualifier Id			Sí	
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	
13. Subject Alternative Names					No
	13.1. DNSName		Id Campo / Valor: NombreDNS = Dominio	Sí	
14. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No
	14.1. Distribution Point 1		Punto de publicación de la CRL1. ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	
	14.2. Distribution Point 2		Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Sí	
15. Authority Info Access				Sí	No

Campo		Contenido	Obligatoriedad	Criticidad
	15.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	
	15.2. Acces Location 1	http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder	Sí	
	15.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí	
16. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	No
	16.1. Subject Type	Valor FALSE (entidad final)		

7.2.11. SSL multidominio (SAN / UCC) PF

Campo		Contenido	Obligatoriedad	Criticidad
1. Version		2	Sí	
2. Serial Number		Número identificativo único del certificado.	Sí	
3. Signature Algorithm		Sha256withRsaEncryption	Sí	
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí	
	4.1. Country	C=ES	Sí	
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí	
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí	
5. Validity		Variable	Sí	
6. Subject		Identificación/descripción del suscriptor del certificado y del componente.	Sí	
	6.1. Country	C=ES	Sí	
	6.2. GivenName	Nombre del suscriptor para el que se emite el certificado.	Sí	
	6.3. Surname	Apellidos del suscriptor para el que se emite el certificado.	Sí	
	6.4. Serial Number	NIF del suscriptor para el que se emite el certificado.	Sí	
	6.5. Common Name	Dominio principal para el que se expide el certificado	Sí	
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	
10. Key Usage		Uso permitido de las claves certificadas.	No	Sí

Campo			Contenido	Obligatoriedad	Criticidad
	10.1. Digital Signature		1	Sí	
	10.2. Content Commitment		0	No	
	10.3. Key Encipherment		1	Sí	
	10.4. Data Encipherment		0	Sí	
	10.5. Key Agreement		0	Sí	
	10.6. Key Certificate Signature		0	Sí	
	10.7. CRL Signature		0	Sí	
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí	No
	11.1. Server Authentication		1.3.6.1.5.5.7.3.1	Sí	
	11.2. Email Protection		1.3.6.1.5.5.7.3.4	No	
	11.3. Client Authentication		1.3.6.1.5.5.7.3.2	No	
12. Certificate Policies			Política de certificación	Sí	No
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.11	Sí	
	12.2. Policy Qualifier Id			Sí	
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	
13. Subject Alternative Names					No
	13.1. Nombre del suscriptor		Id Campo / Valor: 1.3.6.1.4.1.5734.1.1 = <Nombre>	Sí	
	13.2. Primer apellido del suscriptor		Id Campo / Valor: 1.3.6.1.4.1.5734.1.2 = <Primer apellido>	Sí	
	13.3. Segundo apellido del suscriptor		Id Campo / Valor: 1.3.6.1.4.1.5734.1.3 = <Segundo apellido>	No	
	13.4. NIF del suscriptor		Número único de identificación del suscriptor (NIF) Id Campo / Valor: 1.3.6.1.4.1.5734.1.4 = <NIF>	Sí	
	13.5. DNSName		Id Campo / Valor: NombreDNS = Dominio	Sí	
	13.6. DNSName		Id Campo / Valor: NombreDNS = Dominio_*2*	Sí	

Campo		Contenido	Obligatoriedad	Criticidad
	13.7. DNSName	Id Campo / Valor: NombreDNS = Dominio_*n*	No	
14. CRL Distribution Point		Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No
	14.1. Distribution Point 1	Punto de publicación de la CRL1. ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	
	14.2. Distribution Point 2	Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Sí	
15. Authority Info Access			Sí	No
	15.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	
	15.2. Acces Location 1	http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder	Sí	
	15.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí	
16. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	No
	16.1. Subject Type	Valor FALSE (entidad final)		

7.2.12. SSL multidominio (SAN / UCC) PJ

Campo		Contenido	Obligatoriedad	Criticidad
1. Version		2	Sí	
2. Serial Number		Número identificativo único del certificado.	Sí	
3. Signature Algorithm		Sha256withRsaEncryption	Sí	
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí	
	4.1. Country	C=ES	Sí	
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí	
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí	
5. Validity		Variable	Sí	
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí	
	6.1. Country	C=ES	Sí	
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí	
	6.3. Organization	Denominación del suscriptor	Sí	
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No	
	6.5. Serial Number	NIF del suscriptor	Sí	
	6.6. Common Name	Dominio principal para el que se expide el certificado	Sí	
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	
10. Key Usage		Uso permitido de las claves certificadas.	No	Sí

Campo			Contenido	Obligatoriedad	Criticidad
	10.1. Digital Signature		1	Sí	
	10.2. Content Commitment		0	No	
	10.3. Key Encipherment		1	Sí	
	10.4. Data Encipherment		0	Sí	
	10.5. Key Agreement		0	Sí	
	10.6. Key Certificate Signature		0	Sí	
	10.7. CRL Signature		0	Sí	
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí	No
	11.1. Server Authentication		1.3.6.1.5.5.7.3.1	Sí	
	11.2. Email Protection		1.3.6.1.5.5.7.3.4	No	
	11.3. Client Authentication		1.3.6.1.5.5.7.3.2	No	
12. Certificate Policies			Política de certificación	Sí	No
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.12	Sí	
	12.2. Policy Qualifier Id			Sí	
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	
13. Subject Alternative Names					No
	13.1. DNSName		Id Campo / Valor: NombreDNS = Dominio	Sí	
	13.2. DNSName		Id Campo / Valor: NombreDNS = Dominio_*2*	Sí	
	13.3. DNSName		Id Campo / Valor: NombreDNS = Dominio_*n*	No	
14. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No
	14.1. Distribution Point 1		Punto de publicación de la CRL1. ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí	

Campo		Contenido	Obligatoriedad	Criticidad
	14.2. Distribution Point 2	Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Sí	
15. Authority Info Access			Sí	No
	15.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	
	15.2. Acces Location 1	http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder	Sí	
	15.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí	
16. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	No
	16.1. Subject Type	Valor FALSE (entidad final)		