Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

# POLÍTICAS Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES EN EL ÁMBITO DE LAS ADMINISTRACIONES PÚBLICAS, ORGANISMOS Y ENTIDADES DE DERECHO PÚBLICO

| | NOMBRE | FECHA |
|---|---|---|
| Elaborado por: | FNMT-RCM / v3.1 | 17/05/2017 |
| Revisado por: | FNMT-RCM / v3.1 | 02/10/2017 |
| Aprobado por: | FNMT-RCM / v3.1 | 09/10/2017 |

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

| HISTÓRICO DEL DOCUMENTO | | |
|---|---|---|
| **Versión** | **Fecha** | **Descripción** |
| 1.3 | 03/07/2011 | Se eliminan los apartados relacionados con la información sobre la gestión de las políticas de este documento por estar ya incluida en la DGPC.<br>Se modifican los perfiles de certificados para modificar el valor del campo AIA en los certificados para entidades finales. |
| 1.4 | 19/12/2011 | Se añaden definiciones sobre las personas relacionadas con las gestiones de los certificados.<br>Se añaden definiciones sobre las Oficinas de Registro delegadas y Oficinas de Registro peticionarias para la implementación de las actividades de registro de usuarios de forma delegada.<br>Modificación de la tabla de perfiles de certificados: Los números de serie de los certificados AP se asignan de forma aleatoria. |

| HISTÓRICO DEL DOCUMENTO | | |
|---|---|---|
| **Versión** | **Fecha** | **Descripción** |
| 1.5 | 31/10/2012 | Eliminación referencias a la AC conocida como "AC APE". La información relacionada con este tipo de certificados puede consultarse en versiones anteriores de este documento. Eliminadas tablas de perfiles de certificados 2,4,7 y 9.<br><br>Corrección de erratas en perfiles de certificados: El punto de distribución de CRL's en los certificados de entidad final es http://www.cert.fnmt.es/crlsacap/CRLxxx.crl<br><br>Los certificados de entidad final pasan a tener un periodo de validez de 3 años.<br><br>Modificación de las políticas de auto-revocación de certificados. No se revocan los certificados de sede y sello ante la petición de emisión de nuevos Certificados de igual Titular<br><br>Aclaraciones sobre la consideración de la Tarjeta Criptográfica como Dispositivo Seguro de Creación de Firma<br><br>Subsanación erratas sobre la referencia a apartados ETSI 101 456 en las exclusiones realizadas a esta norma.<br><br>Se eliminan los apartados de "Modelos de formulario" por estar éstos disponibles a través de las correspondientes aplicaciones de solicitud. |
| 1.6 | 29/5/2013 | Sustitución del término titular por firmante o suscriptor.<br><br>Eliminación del último párrafo de la descripción de tipología de certificado de empleado público, en el que se interpretaba la aplicación de la Ley de Firma Electrónica al certificado para el personal al servicio de la Administración Pública.<br><br>Matización del uso particular del certificado de empleado público. |

| HISTÓRICO DEL DOCUMENTO | | |
|---|---|---|
| **Versión** | **Fecha** | **Descripción** |
| 1.7 | 3/7/2013 | Aclaración en el párrafo 51 del uso particular permitido al certificado de empleado público. |
| 2.0 | 16/06/2014 | Alineación con la LFE del régimen de responsabilidad general del PSC en cuanto a las Oficinas de Registro y en cuanto a la recogida del consentimiento del "firmante" en caso de cese de actividad del PSC.<br>Se actualizan algunos enlaces a la aplicación de Registro.<br>Revisión conforme WebTrust. |
| 2.1 | 17/11/2014 | Expedición de los tipos de certificados incluidos en las presentes Políticas con algoritmo SHA-256.<br>Reducción del periodo máximo de suspensión de certificados a 30 días.<br>Eliminación del campo QcLimitValue de los perfiles de los certificados.<br>Revocación de certificados de personal al servicio de la Administración vía telefónica 24x7 |
| 2.2 | 10/07/2015 | Revisión conforme ETSI 101 456 |
| 2.3 | 27/01/2016 | Inclusión de la posibilidad de revocar certificados de sede y sello en horario 24x7. |
| 2.4 | 24/06/2016 | Modificación de perfiles para alinearlos con requisitos de CAB/Forum (certificado de sede electrónica). |
| 2.5 | 03/01/2017 | Alineación con el Reglamento eIDAS de los certificados de firma electrónica de personal al servicio de la Administración Pública. |
| 3.0 | 03/01/2017 | Alineación con el Reglamento eIDAS de los certificados de sede y de sello electrónicos. |

| HISTÓRICO DEL DOCUMENTO | | |
|---|---|---|
| **Versión** | **Fecha** | **Descripción** |
| 3.1 | 09/10/2017 | Incorporación del certificado electrónico con seudónimo para empleados públicos AAPP y requisitos del CAB/Forum. |

**Referencia:** DPC/PCPAA0301/SGPSC/2017

**Documento clasificado como:** *Público*

# Índices

# 1. PRELIMINAR

1. El Artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y de Orden Social habilita la prestación de servicios de seguridad por parte de la Fábrica Nacional de Moneda y Timbre, en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos, en su apartado Uno, establece que:

   *"sin perjuicio de las competencias atribuidas en la Ley a los órganos administrativos en materia de registro de solicitudes, escritos y comunicaciones, se faculta a la Fábrica Nacional de Moneda y Timbre (FNMT) para la prestación de los servicios técnicos y administrativos necesarios para garantizar la seguridad, validez y eficacia de la emisión y recepción de comunicaciones y documentos a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT) en las relaciones que se produzcan entre*:

   *a) Los órganos de la Administración General del Estado entre sí o con los organismos públicos vinculados o dependientes de aquélla, así como las de estos organismos entre sí.*
   *b) Las personas físicas y jurídicas con la Administración General del Estado (AGE) y los organismos públicos vinculados o dependientes de ella"*

2. De otro lado, su apartado Dos, establece:

   *"Asimismo, se habilita a la FNMT a prestar, en su caso, a las Comunidades Autónomas, las entidades locales y las entidades de Derecho público vinculadas o dependientes de ellas, los servicios a que se refiere el apartado anterior, en las relaciones que se produzcan a través de técnicas y medios EIT entre sí, con la Administración General del Estado o con personas físicas y jurídicas; siempre que, previamente, se hayan formalizado los convenios o acuerdos procedentes."*

3. La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, consagró el derecho de los ciudadanos a relacionarse electrónicamente con las diferentes Administraciones Públicas. El marco jurídico resultante de la aprobación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, viene a sistematizar toda la regulación relativa al procedimiento administrativo, clarificando e integrando el contenido de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y de la citada Ley 11/2007, de 22 de junio. Así mismo, la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, regula los sistemas de identificación y firma electrónicas utilizados en el ámbito de la Administración de Justicia.

4. En un entorno en el que la utilización de los medios electrónicos ha de ser lo habitual, la firma, las sedes electrónicas, el intercambio electrónico de datos en entornos cerrados de comunicación y la actuación administrativa automatizada, con la obligación de que las Administraciones Públicas se relacionen entre sí por medios electrónicos, requieren de los correspondientes sistemas de identificación, firma y sello electrónicos.

   Entre los mencionados sistemas de identificación, firma y sello electrónicos admitidos en el actual marco jurídico se encuentran los *Certificados electrónicos* a los que se refiere la presente Declaración y que se relacionan a continuación:

1) ***Certificado de firma electrónica del personal al servicio de la Administración Pública***.

2) *Certificado* de autenticación de sitio web para identificar y garantizar una comunicación segura con una *Sede electrónica* (***Certificado* de *Sede electrónica***).

3) ***Certificado* de *Sello electrónico*** de Administración Pública, órgano, organismo público o entidad de derecho público, como sistema de identificación y para la actuación administrativa automatizada y para la actuación judicial automatizada**,** que permite autenticar documentos expedidos por dicha Administración o cualquier activo digital.

5. Adicionalmente, el Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, establece un marco jurídico general para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web.

## 2. INTRODUCCIÓN

6. El presente documento forma parte integrante de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica (DGPC)* de la FNMT-RCM y tiene por objeto la información pública de las condiciones y características de los servicios de confianza y, especialmente, los servicios de emisión de *Certificados* electrónicos por parte de la FNMT-RCM como *Prestador de Servicios de Confianza*, recogiendo, en particular las obligaciones y procedimientos que se compromete a cumplir en relación con la emisión de *Certificados* de *Firma electrónica* del *Personal al servicio de la Administración Pública*, así como de *Certificados de sede electrónica* y *Certificados de Sello electrónico* expedidos a las Administraciones Públicas, organismos públicos y entidades de derecho público.

7. En especial deberá tenerse presente, a efectos interpretativos de estas *Políticas y Prácticas de Certificación Particulares*, el apartado "Definiciones" de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*, y, en su caso, la *Ley de Emisión* correspondiente a cada órgano y/u organismo o entidad usuaria de los servicios de certificación de la FNMT-RCM.

8. Los *Certificados* emitidos por la FNMT-RCM bajo las presentes *Políticas de Certificación y Prácticas de Certificación Particulares* se consideran técnicamente *Certificados Cualificados* o reconocidos, conforme a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, conforme a los artículos 17, 18, 19, 21 y 22 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, conforme a la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, y conforme al Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

## 3. ORGANIZACIÓN DEL DOCUMENTO

9. La *Declaración de Prácticas de Certificación* de la FNMT-RCM como *Prestador de Servicios de Confianza* está estructurada, de un lado, por la parte común de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* (DGPC) de la FNMT-RCM, pues existen niveles de actuación análogos para todos los servicios de confianza de la Entidad y, de otro lado, por los apartados específicos del presente documento de *Políticas de Certificación y Prácticas de Certificación Particulares*. No obstante lo anterior, la *Ley de Emisión* de cada tipo de *Certificado* o grupo de *Certificados* podrá establecer características especiales aplicables a los órganos, organismos, entidades y personal usuarios de los servicios de confianza de la FNMT-RCM.

10. De acuerdo con lo anterior, la estructura de la *Declaración de Prácticas de Certificación de la FNMT-RCM* es la siguiente:

    1) Por una parte, la ***Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica***, que debe considerarse cuerpo principal de la *Declaración de Prácticas de Certificación* en el que se describe el régimen de responsabilidad aplicable a los miembros de la *Comunidad Electrónica*, los controles de seguridad aplicados a los procedimientos e instalaciones de la FNMT-RCM, en aquello que pueda ser publicado sin perjudicar la eficacia de los mismos, las normas de secreto y confidencialidad, así como cuestiones relativas a la propiedad de sus bienes y activos, a la protección de datos de carácter personal y demás cuestiones de tipo informativo general que deben ponerse a disposición del público, independientemente de su papel en la Comunidad Electrónica.

    2) Y, por otra parte, para cada conjunto o grupo de *Certificados*, identificado y diferenciado del resto por su tipología y régimen particular o diferenciador, existe una ***Política de Certificación*** específica en la que se describen las obligaciones de las partes, los límites de uso de los *Certificados* y responsabilidades y unas ***Prácticas de Certificación Particulares*** que desarrollan los términos definidos en la política correspondiente y otorgan prestaciones adicionales o específicas sobre las generales establecidas en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*.

       Estas *Políticas de Certificación* y *Prácticas de Certificación Particulares* concretan lo articulado en el cuerpo principal de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* y, por tanto, son parte integrante de ella, conformando, ambos, la *Declaración de Prácticas de Certificación* de la FNMT-RCM. No obstante, sólo son de aplicación para el conjunto de *Certificados* caracterizado e identificado en las correspondientes *Políticas y Prácticas Particulares de Certificación* y pueden revestir, además, 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.

11. El presente documento representa, por tanto, las *Políticas de Certificación y Prácticas de Certificación Particulares* para los siguientes *Certificados*:

    1) *Certificado* de *Firma electrónica* de *Personal al servicio de la Administración Pública*,

    2) *Certificado de Sede electrónica*, y

3) *Certificado* de *Sello electrónico*.

12. En lo relativo a la expedición de *Certificados de Sede electrónica,* la FNMT-RCM gestiona sus servicios de certificación y emite certificados de conformidad con los "Requisitos base para la emisión y gestión de certificados de confianza", requisitos establecidos por la entidad CA/Browser forum y que pueden consultarse en la siguiente dirección https://cabforum.org/baseline-requirements-documents/

13. La FNMT-RCM revisará sus políticas y prácticas de certificación y actualizará anualmente la correspondiente Declaración de la Política de Certificados para mantenerla acorde a la última versión de los referidos requisitos, incrementando el número de versión y agregando una entrada de registro de cambios con fecha, incluso si no se realizaron otros cambios en el documento.

## 4. ORDEN DE PRELACIÓN

14. El orden de prelación es el siguiente:

- Las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares* de *Certificados* forman parte de la *Declaración de Prácticas de Certificación* y tendrán prelación, en lo que corresponda y con carácter particular sobre cada tipo de *Certificado*, sobre lo dispuesto en el cuerpo principal de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*.

  Por tanto, en caso de que existiera contradicción entre el presente documento y lo dispuesto en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*, tendrá preferencia lo aquí articulado.

- La *Ley de Emisión* de cada *Certificado* o grupo de *Certificados* constituirá, en su caso y por su singularidad, norma especial sobre lo dispuesto en las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares* para los diferentes órganos y organismos o entidades públicas usuarias de los servicios de la FNMT-RCM, cuando así lo requiera la naturaleza de sus competencias o funciones. La *Ley de Emisión*, en caso de que se constituya, quedará recogida en el documento de relación a formalizar entre la FNMT-RCM y las Administraciones, organismos y entidades públicas, y/o en las condiciones de utilización o contrato de emisión, y/o en el propio *Certificado*.

## 5. DEFINICIONES

15. A los efectos de lo dispuesto en el presente documento, particularizando las definiciones de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* y únicamente cuando los términos comiencen con letra mayúscula y estén en cursiva, se entenderá por:

- *Actuación administrativa / judicial automatizada*: Actuación administrativa / judicial producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular. Incluye la producción de actos de trámite o resolutorios de procedimientos, así como de meros actos de comunicación.

- *Certificado de autenticación de sitio web*: Declaración que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el *Certificado*.
- *Certificado de Sede electrónica*: *Certificado de autenticación de sitio web* que permite identificar las *Sedes electrónicas* y garantizar la comunicación segura con las mismas.
- *Certificado de Sello electrónico*: Declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona.
- *Personal al servicio de la Administración Pública*: Funcionarios, personal laboral, estatutario a su servicio y personal autorizado, al servicio de la Administración Pública, órgano, organismo público o entidad de derecho público.
- *Registro AAC (CAA records):* Registro de recursos DNS (Sistema de Nombres de Dominio) de Autorización de Autoridad de Certificación (AAC). Permite a un titular de nombre de dominio DNS especificar las Autoridades de Certificación (AC) autorizadas para emitir certificados para ese dominio. La publicación de los registros de recursos de AAC permite a un titular de nombres de dominio implementar controles adicionales para reducir el riesgo de que se produzca una emisión no autorizada de un *Certificado de autenticación de sitio web* para su nombre de dominio.
- *Responsable de Operaciones de Registro*: Persona física nombrada por el representante de la Administración pública, organismo público o entidad de derecho público, bajo cuya responsabilidad se realizan las tareas asignadas a la *Oficina de Registro*, con las obligaciones y responsabilidades asignadas en las presentes *Políticas y Prácticas de Certificación Particulares*.
- *Sede electrónica*: Dirección electrónica, disponible para los ciudadanos a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública, o bien a uno o varios organismos públicos o entidades de Derecho Público en el ejercicio de sus competencias.
- *Suscriptor*: La administración pública, órgano, organismo público o entidad de derecho público.

## 6. GESTIÓN DEL CICLO DE VIDA DE LAS CLAVES DEL PRESTADOR DE SERVICIOS DE CONFIANZA

16. La FNMT-RCM en su actividad *como Prestador de Servicios de Confianza*, en relación con las claves criptográficas empleadas para la emisión de los *Certificados* de *Firma electrónica* del *Personal al servicio de la Administración Pública*, *Certificados de Sede electrónica* y *Certificados de Sello electrónico*, declara que realizará la siguiente gestión.

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

### 6.1.1. Generación de las Claves del Prestador de Servicios de Confianza

17. Las *Claves* de la FNMT-RCM, como *Prestador de Servicios de Confianza*, son generadas en circunstancias completamente controladas, en un entorno físicamente seguro y, al menos, por dos personas autorizadas para ello, utilizando sistemas hardware y software que cumplen con la normativa actual en materia de protección criptográfica, tal y como se muestra en la *DGPC*.

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

18. La FNMT-RCM utiliza los mecanismos necesarios para mantener su *Clave privada* confidencial y mantener su integridad en la forma que se muestra en la *DGPC*.

### 6.1.3. Distribución de los Datos de verificación de Firma del Prestador de Servicios de Confianza

19. La FNMT-RCM utiliza los mecanismos necesarios para mantener la integridad y autenticidad de su *Clave Pública*, así como su distribución en la forma que se muestra en la *DGPC*.

20. El perfil del *Certificado* de la *Autoridad de Certificación "AC Administración Pública"*, que con sus *Datos de Creación de Firma* o *de Sello* expide los *Certificados* emitidos bajo las *Políticas de Certificación* identificadas en este documento, se puede consultar en la página http://www.cert.fnmt.es/dpcs/.

### 6.1.4. Uso de los Datos de Creación de Firma / Sello del Prestador de Servicios de Confianza

21. Los *Datos de Creación de Firma* / *Sello* de la FNMT-RCM, en su actividad como *Prestador de Servicios de Confianza*, serán utilizados única y exclusivamente para los propósitos de:

1) Firma / Sello de *Certificados*.
2) Firma / Sello de las *Listas de Revocación*.
3) Otros usos previstos en esta *Declaración* y/o en la legislación aplicable.

### 6.1.5. Fin del ciclo de vida de las Claves del Prestador de Servicios de Confianza

22. La FNMT-RCM dispondrá de los medios necesarios para lograr que una vez finalizado el período de validez de las *Claves* del *Prestador de Servicios de Confianza*, estas *Claves* no vuelven a ser utilizadas, bien destruyéndolas o almacenándolas de forma apropiada para dicha finalidad.

### 6.1.6. Ciclo de vida del hardware criptográfico utilizado para firmar / sellar Certificados

23. La FNMT-RCM dispondrá de los medios necesarios para posibilitar que el hardware criptográfico utilizado para la protección de sus *Claves* como *Prestador de Servicios de Confianza*, no sufra manipulaciones de acuerdo con el estado de la técnica a la fecha durante

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

## 7. OPERACIÓN Y GESTIÓN DE LA INFRAESTRUCTURA DE *CLAVE PÚBLICA*

### 7.1. OPERACIÓN Y GESTIÓN DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA

24. Las operaciones y procedimientos realizados para la puesta en práctica de las *Políticas de Certificación* reflejadas en este documento se realizan siguiendo los controles requeridos por los estándares reconocidos para tal efecto, describiéndose estas actuaciones en los apartados "Controles de seguridad física, de procedimientos y del personal" y "Controles de seguridad técnica" de la *DGPC* de la FNMT-RCM.

25. Adicionalmente cabe destacar que la FNMT-RCM posee un *Sistema de Gestión de la Seguridad de la Información* (en adelante SGSI) para su Departamento CERES con el objetivo final de mantener y garantizar la seguridad de la información de los miembros de la *Comunidad Electrónica*, así como la suya propia, de forma que el servicio prestado por la FNMT-RCM-CERES tenga los niveles suficientes de fiabilidad que exige el Mercado. El SGSI de la FNMT-RCM-CERES es aplicable a los activos de información definidos en el Análisis de Riesgos realizado para todas las Áreas que componen el departamento, incluyendo como activos los servicios prestados a los miembros de la *Comunidad Electrónica*.

26. En el documento *DGPC*, se da respuesta concreta para todos aquellos aspectos referentes a los siguientes apartados del estándar ETSI EN 319 411:

1) Controles de seguridad física
2) Controles de procedimiento
3) Controles de seguridad de personal
4) Procedimientos de registro de auditoría
5) Datos relevantes que serán registrados
6) Cambio de Claves
7) Restablecimiento de los servicios en caso de fallo o desastre
8) Gestión de la continuidad de negocio y gestión de incidentes
9) Terminación de la actividad de la FNMT-RCM como PSC

## 8. DIFUSIÓN DE TÉRMINOS Y CONDICIONES

27. La FNMT-RCM pone a disposición de la *Comunidad Electrónica* y demás interesados, tanto el presente documento como el documento de *DGPC* de la FNMT-RCM en los que se detalla:

1) Los términos y condiciones que regulan la utilización de los *Certificados* expedidos por la FNMT-RCM, con expresión, en su caso, de la correspondiente *Ley de Emisión*.
2) La *Política de Certificación* aplicable a los *Certificados* expedidos por la FNMT-RCM.
3) Los límites de uso para los *Certificados* expedidos bajo esta *Política de Certificación*.

4) Las obligaciones, garantías y responsabilidades de las partes involucradas en la emisión y uso de los *Certificados*.

5) Los períodos de conservación de la información recabada en el proceso de registro y de los eventos producidos en los sistemas del *Prestador de Servicios de Confianza* relacionados con la gestión del ciclo de vida de los *Certificados* emitidos bajo esta *Política de Certificación*.

## 9. SEUDÓNIMOS

28. Los *Certificados* de *Firma electrónica de Personal al servicio de la Administración Pública* que la FNMT – RCM expida bajo las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares* haciendo uso de seudónimos, indicarán claramente esta característica, de conformidad con el Reglamento eIDAS y la normativa nacional aplicable.

29. En el procedimiento de acreditación de la identidad, como paso previo a la expedición de un *Certificado* de *Firma electrónica* de *Personal al servicio de la Administración Pública* con seudónimo, la FNMT-RCM, a través de la *Oficina de Registro,* constatará la verdadera identidad del *Firmante* y conservará la documentación que la acredite.

## 10. PERFIL DE LOS CERTIFICADOS

30. Todos los *Certificados* emitidos bajo las presentes *Políticas de Certificación* son de conformidad con el estándar X.509 versión 3. En la página http://www.cert.fnmt.es/dpcs/ se puede consultar el perfil completo de cada *Certificado*.

### 10.1. RESTRICCIONES DE LOS NOMBRES

31. La codificación de los *Certificados* sigue el estándar RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Todos los campos definidos en el perfil de los *Certificados,* excepto en los campos que específicamente se exprese lo contrario, emplean la codificación UTF8String.

### 10.2. USO DE LA EXTENSIÓN POLICY CONSTRAINS

32. La extensión Policy Constrains del certificado raíz de la AC no es utilizado.

### 10.3. SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS

33. La extensión Certificate Policies incluye dos campos de Policy Qualifiers:

- CPS Pointer: contiene la URL donde se publica la *DGPC* y las *Políticas de Certificación* y *Prácticas de Certificación Particulares* aplicables a los *Certificados.*
- User notice: contiene un texto que puede ser desplegado en la pantalla del usuario del *Certificado* durante la verificación del mismo.

### 10.4. TRATAMIENTO SEMÁNTICO DE LA EXTENSIÓN "CERTIFICATE POLICY"

34. La extensión Certificate Policy incluye el campo OID de política, que identifica la política asociada al *Certificado* por parte de la FNMT – RCM, así como los dos campos relacionados en el apartado anterior.

## 11. RECONOCIMIENTO Y AUTENTICACIÓN DE MARCAS REGISTRADAS

35. La FNMT–RCM no asume compromiso alguno sobre el uso de signos distintivos, registrados o no, en la emisión de los *Certificados* expedidos bajo la presente *Política de Certificación.* Solo se permite la solicitud de *Certificados* que incluyan signos distintivos cuyo derecho de uso sea propiedad del *Titular* o se encuentre debidamente autorizado. La FNMT–RCM no está obligada a verificar previamente la titularidad o registro de los signos distintivos antes de la emisión de los *Certificados,* aunque figuren en registros públicos.

## 12. CERTIFICADO DE FIRMA ELECTRÓNICA DEL PERSONAL AL SERVICIO DE LA ADMINISTRACIÓN PÚBLICA

### 12.1. POLÍTICA DE CERTIFICACIÓN DE LOS CERTIFICADOS DE FIRMA ELECTRÓNICA DEL PERSONAL AL SERVICIO DE LA ADMINISTRACIÓN PÚBLICA

#### 12.1.1. Identificación

36. La presente *Política de Certificación* de la FNMT-RCM para la expedición de *Certificados* de *Firma electrónica* del *Personal al servicio de la Administración Pública* tiene la siguiente identificación:

**Nombre**: Política de Certificación de *Certificados* de *Firma electrónica* del personal al servicio de la Administración Pública

**Referencia / OID**[1]:

- 1.3.6.1.4.1.5734.3.3.4.4.1: *Certificado* en *Tarjeta criptográfica*

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

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

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

- 1.3.6.1.4.1.5734.3.3.4.4.2: *Certificado* en software.
- 1.3.6.1.4.1.5734.3.3.5.2: *Certificado* con seudónimo para el ámbito de la Administración de Justicia.
- 1.3.6.1.4.1.5734.3.3.11.1: *Certificado* con seudónimo para el ámbito de las Administraciones Públicas.

**Versión**: 3.1

**Fecha de aprobación**: 9 de octubre de 2017

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

**DPC relacionada**: Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica de la FNMT-RCM

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

### 12.1.2. Tipología del Certificado de Firma electrónica del Personal al servicio de la Administración Pública.

37. El *Certificado* para el *Personal al servicio de la Administración Pública*, es la certificación electrónica emitida por la FNMT-RCM que vincula al *Firmante* con unos *Datos de verificación de Firma* y confirma, de forma conjunta:

- la identidad del *Firmante* (*Personal al servicio de la Administración Pública*), incluyendo en su caso, su número de identificación personal, cargo, puesto de trabajo y/o condición de autorizado, y
- la identidad del *Suscriptor* del *Certificado*, donde el *Firmante* ejerce sus competencias, presta sus servicios, o desarrolla su actividad.

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

39. El *Certificado de firma electrónica del Personal al servicio de la Administración Pública* es expedido por la FNMT-RCM basándose en actuaciones de identificación y registro realizadas por la red de *Oficinas de Registro* designadas por el órgano, organismo o entidad *Suscriptora* del *Certificado*. Las "*Leyes de Emisión*" podrán establecer, en el ámbito de actuación de las Administraciones Públicas, *Oficinas de Registro* comunes para este ámbito de actuación con efectos uniformes para cualesquiera Administraciones, organismos y/o entidades públicas.

40. La *Ley de Emisión* suplirá, atendiendo a las diferentes funcionalidades del ámbito de actuación de los *Certificados*, elementos o campos ordinariamente expresados en el propio *Certificado*, atendiendo a la especialidad de actuación de las diferentes Administraciones Públicas.

41. Este *Certificado* es expedido como "cualificado" de conformidad con los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons".

### 12.1.3. Comunidad y ámbito de aplicación

42. Los *Certificados* emitidos bajo esta *Política de Certificación* son expedidos a funcionarios, personal laboral, estatutario a su servicio y personal autorizado, al servicio de las Administraciones Públicas, órganos, organismos públicos o entidades de derecho público. Estos Certificados son válidos como sistemas de firma electrónica de conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y de conformidad con la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia. El ámbito de aplicación de los *Certificados* expedidos bajo las Políticas identificadas con el OID 1.3.6.1.4.1.5734.3.3.5.2, *Certificados* de *Firma electrónica* con seudónimo es, exclusivamente, para la Administración de Justicia.

43. La *Ley de Emisión* de estos *Certificados* podrá determinar, en defecto de normativa específica, las condiciones de uso y régimen de estos *Certificados* que permitirán la atribución a las Administraciones, organismos y entidades de los diferentes actos y resoluciones realizados por el personal a su servicio; todo ello, sin modificación legal o variación respecto de la actuación que vienen realizando estas Administraciones Públicas en los soportes tradicionales.

### 12.1.4. Responsabilidad y obligaciones de las partes

44. Las obligaciones y responsabilidades expresadas en este apartado se entienden sin perjuicio de las correspondientes derivadas de la legislación y normativa de aplicación, específicamente de las aplicables a la FNMT-RCM como *Prestador de Servicios de Confianza* y que para tal condición se establecen en el articulado del Reglamento eIDAS y en la Ley de Firma Electrónica y su reglamentación de desarrollo.

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

- La Administración, organismos y entidades públicas representadas a través de los diferentes órganos competentes que, dependiendo de la *Ley de Emisión* (si la hubiere), serán los *Suscriptores*.
- *Oficinas de Registro*, que, a través del personal designado por la Administración competente, serán responsables de los requisitos y condiciones que ostenten los *Firmantes* del *Certificado*.
- El *Firmante* del *Certificado*, que será el *Personal al servicio de la Administración Pública*.
- FNMT-RCM, en cuanto *Prestador de Servicios de Confianza*.
- En su caso, resto de *Comunidad Electrónica* y terceros.

46. El régimen de derechos y obligaciones de las Administraciones, organismos, entidades públicas y la FNMT-RCM se regirá mediante el correspondiente acuerdo o convenio regulador de la prestación de los servicios de confianza. En estos acuerdos o convenios podrá establecerse la *Ley de Emisión* de estos *Certificados* con el contenido y finalidad prevista en esta Declaración.

47. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en este documento y en la *DGPC*, la Entidad *Suscriptora* del *Certificado* y/o el *Responsable de Operaciones de Registro* tienen la obligación de:

- No realizar registros o tramitar solicitudes de personal que preste sus servicios en una entidad diferente a la que representa como *Oficina de Registro*, sin perjuicio de la creación de *Oficinas de Registro* centralizadas o de convenios entre administraciones para efectuar registros.
- Comprobar fehacientemente los datos del *Personal al servicio de la Administración Pública* como usuario del *Certificado*, que actuará como *Firmante* del mismo, referido a su identidad y a la condición del cargo, puesto de trabajo, empleo o cualquier otro dato que refleje o caracterice la relación de éste con la Administración, organismo o entidad a la que presta sus servicios. El *Prestador de Servicios de Confianza*, a través del *Responsable de Operaciones de Registro* velará por el cumplimiento de los procedimientos aprobados por FNMT-RCM en materia de identificación de los *Solicitantes* de los *Certificados*, y de forma específica para el caso de la expedición de *Certificados* de *Firma electrónica del Personal al servicio de la Administración Pública* con seudónimo, lo relativo a la constatación de la verdadera identidad del *Firmante* y la conservación de la documentación que la acredite.
- No utilizar el *Certificado* en caso de que los *Datos de Creación de Firma* puedan estar amenazados y/o comprometidos.
- Solicitar la revocación o suspensión del *Certificado* del personal al servicio del órgano al que representa la *Oficina de Registro* cuando alguno de los datos referidos a la condición del cargo, puesto de trabajo, empleo o cualquier otro que refleje o caracterice la relación del usuario *Firmante* del *Certificado* con el órgano, organismo o entidad pública, *Suscriptora* del *Certificado,* en la que presta sus servicios, sea inexacto, incorrecto, haya variado o sea de necesaria revocación por razones de seguridad.
- Solicitar a la FNMT-RCM, a través de la *Oficina de Registro*, la revocación del *Certificado* cuando, directamente o a través de comunicación del *Personal al servicio de la Administración Pública*, exista pérdida, extravío de la tarjeta o soporte del *Certificado*, o presunción de ello.
- En el caso de que el *Certificado* esté en un soporte tipo tarjeta, descargar el *Certificado* y sus claves directamente en la tarjeta criptográfica que se proporcione a su personal. En cualquier caso, no conservar las claves privadas asociadas a los *Certificados* en los equipos de la *Oficina de Registro*, de conformidad con las directrices de la FNMT-RCM plasmadas en los manuales de procedimiento que se entregan a las *Oficinas de Registro*, en las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares* y en la *DGPC*.
- No utilizar el *Certificado* en caso de que el *Prestador de Servicios de Confianza* haya cesado en la actividad como Entidad emisora de *Certificados* que originó la expedición del *Certificado* en cuestión y no se hubiera producido la subrogación prevista en la Ley. En todo caso, no utilizar el *Certificado* en los casos en los que los *Datos de Creación de Firma / Sello* del *Prestador* puedan estar amenazados y/o comprometidos, y así se

haya comunicado por el *Prestador* o, en su caso, la Administración *Suscriptora* hubiera tenido noticia de estas circunstancias.

48. Las relaciones de la FNMT-RCM con el *Suscriptor* y el *Personal al servicio de la Administración Pública* (usuario del *Certificado* proporcionado por el citado *Suscriptor)* quedarán determinadas principalmente, a los efectos del régimen de uso de los *Certificados*, a través del documento relativo a las condiciones de utilización o, en su caso, contrato de emisión del Certificado, y, subsidiariamente, por las presentes *Políticas de Certificación y Prácticas de Certificación Particulares* y por la *DGPC*, atendiendo a los acuerdos, convenios o documento de relación entre la FNMT-RCM y la Administración Pública correspondiente.

49. Las relaciones de la Administración Pública *Suscriptora* del *Certificado* y de su personal con la FNMT-RCM, se realizarán siempre a través de la *Oficina de Registro* y su responsable.

50. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la *DGPC*, el *Personal al servicio de la Administración Pública*, como *Firmante* del *Certificado* y sus *Claves*, tiene la obligación de:

- No utilizar el *Certificado* cuando alguno de los datos referidos al cargo, puesto de trabajo, empleo o cualquier otro sea inexacto o incorrecto o no refleje o caracterice su relación, con el órgano, organismo o entidad en la que presta sus servicios; o, existan razones de seguridad que así lo aconsejen.
- Realizar un uso adecuado del *Certificado* en base a las competencias y facultades atribuidas por el cargo, puesto de trabajo o empleo como *Personal al servicio de la Administración Pública*.
- Comunicar al *Responsable de Operaciones de Registro,* la pérdida, extravío, o sospecha de ello, de la tarjeta o soporte del *Certificado* del que es usuario y custodio, con el fin de iniciar, en su caso, los trámites de su revocación.

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

### 12.1.5. Límites de uso de los Certificados

52. Constituyen límites de uso de este tipo de *Certificados* las diferentes competencias y funciones propias de la Administración Pública *Suscriptora* (actuando a través del personal a su servicio en calidad de *Firmante* de los *Certificados*), de acuerdo con su cargo, empleo y, en su caso, condiciones de autorización. La FNMT-RCM y la Administración, organismos y entidades públicas podrán fijar en los acuerdos o convenios, a través del documento de relación correspondiente o, si fuera procedente, en la *Ley de Emisión* de estos *Certificados*, otros límites adicionales.

53. FNMT-RCM no tendrá control sobre las actuaciones y usos de los *Certificados* que se realicen por el *Personal al servicio de la Administración Pública* en nombre de estas, por lo que la FNMT-RCM quedará exonerada de responsabilidad a efectos de tales usos, así como de las consecuencias y efectos que pudieran producirse en el marco de reclamaciones o, en su caso, de posibles responsabilidades patrimoniales llevadas a cabo por terceros.

54. En cuanto a las actividades del personal de las *Oficinas de Registro*, la FNMT – RCM quedará sujeta a las obligaciones y responsabilidades contenidas en la Ley 59/2003, de 19 de diciembre, de firma electrónica, sin perjuicio de las especialidades contenidas en el artículo 11 del RD 1317/2001, de 30 de noviembre, por el que se desarrolla el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas fiscales, administrativas y del orden social en materia de prestación de servicios de seguridad por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, en las comunicaciones a través de medios electrónicos, informáticos y telemáticos con las Administraciones Públicas. Para poder usar los *Certificados* de *Firma electrónica* de *Personal al servicio de la Administración Pública* de forma diligente, se deberá previamente formar parte de la *Comunidad Electrónica* y, la Administración actuante, adquirir la condición de *Suscriptor*.

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

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

- Firmar o sellar otro *Certificado*, salvo supuestos expresamente autorizados previamente.
- Usos particulares o privados, salvo para relacionarse con las Administraciones cuando éstas lo admitan.
- Firmar o sellar software o componentes.
- Generar sellos de tiempo para procedimientos de *Fechado electrónico.*
- Prestar servicios a título gratuito u oneroso, salvo supuestos expresamente autorizados previamente, como por ejemplo serían a título enunciativo:
    - Prestar servicios de *OCSP*.
    - Generar *Listas de Revocación.*
    - Prestar servicios de notificación

## 12.2. PRÁCTICAS DE CERTIFICACIÓN PARTICULARES PARA LOS CERTIFICADOS DE FIRMA ELECTRÓNICA DE PERSONAL AL SERVICIO DE LA ADMINISTRACIÓN PÚBLICA

57. La FNMT-RCM en su labor como *Prestador de Servicios de Confianza* y para demostrar la necesaria fiabilidad para la prestación de dichos servicios, cuenta con una *Declaración de Prácticas de Certificación* cuyo objeto es la información pública sobre las condiciones generales de prestación de los mismos.

58. En especial deberá tenerse presente, a efectos interpretativos del presente documento el apartado “Definiciones” de la *DGPC*.

59. El Presente documento trae causa y forma parte integrante de la *Declaración de Prácticas de Certificación* de la FNMT-RCM y define el conjunto de prácticas particulares adoptadas por la FNMT-RCM como *Prestador de Servicios de Confianza* para la gestión del ciclo de vida de los *Certificados* de *Firma electrónica* de *Personal al servicio de la Administración Pública*, expedidos bajo las *Políticas de Certificación* identificadas con los OIDs 1.3.6.1.4.1.5734.3.3.4.4.1, 1.3.6.1.4.1.5734.3.3.4.4.2, 1.3.6.1.4.1.5734.3.3.5.2 y 1.3.6.1.4.1.5734. 3.3.11.1.

### 12.2.1. Servicios de Gestión de las Claves

60. La FNMT-RCM no genera ni almacena las *Claves Privadas* asociadas a los *Certificados* expedidos bajo las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares*, que son generadas bajo el exclusivo control del *Firmante* y, en su caso, con la intervención de la *Oficina de Registro* correspondiente, y cuya custodia está bajo responsabilidad del *Personal al servicio de la Administración Pública*. La FNMT-RCM no presta, por tanto, servicios de depósito de *Datos de creación de Firma*. Las aplicaciones solo permiten la generación de claves RSA con tamaño 2.048 bits asociadas a los *Certificados* de *Firma electrónica* de *Personal al servicio de la Administración Pública*.

### 12.2.2. Gestión del ciclo de vida de los Certificados

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

#### *12.2.2.1. Procedimiento de solicitud del Certificado*

62. A continuación se describe el procedimiento de solicitud por el que la *Oficina de Registro* toma los datos del *Personal al servicio de la Administración Pública*, confirma su identidad, vigencia del cargo o empleo y se formaliza, entre el citado personal y el órgano, organismo o entidad donde el personal presta sus servicios, el documento de condiciones de utilización o el contrato de emisión, según proceda por el cargo del personal, según lo previsto en el documento de relación, o convenio o acuerdo de la FNMT-RCM con el citado órgano, organismo y/o entidad para la posterior emisión de un *Certificado* de *Firma electrónica* de *Personal* al servicio de la Administración Pública.

63. Se hace constar que FNMT-RCM, en función de la relación de personal usuario dependiente remitida por la Administración, organismos o entidad pública, considerará, bajo responsabilidad de los correspondientes órganos, organismos y/o entidades, que actuarán a través de las *Oficinas de Registro*, que este personal se encuentra con su cargo vigente, que su número de Identificación Personal, empleo o autorización es auténtico y está en vigor y, por tanto, habilitados para obtener y usar el *Certificado*. FNMT-RCM, no tendrá, en este tipo de *Certificado*, la responsabilidad de comprobar el cargo o empleo del citado personal, así como que estos requisitos se mantienen durante toda la vida del *Certificado*, al no ostentar, la FNMT-RCM, relación jurídica funcionarial, administrativa o laboral con tal personal, más allá del documento de condiciones de utilización o, en su caso, contrato de emisión, cuyo efecto es estrictamente instrumental para el desempeño de las funciones propias del cargo.

64. Las actividades de comprobación anteriores serán realizadas por los responsables de las *Oficinas de Registro* implantadas por el órgano, organismo o entidad de la Administración Pública en cuestión, y que se corresponde, en cada caso, con el organismo o entidad donde el personal presta sus servicios. Por tanto y a estos efectos las *Oficinas de Registro* no serán autoridades delegadas o dependientes de la FNMT-RCM.

65. Una vez realizado satisfactoriamente por la *Oficina de Registro* lo señalado anteriormente, las actuaciones serán las siguientes:

1) Obtención, en su caso, de la *Tarjeta criptográfica* que sirve de soporte al *Certificado* y del software de generación o importación de los *Datos de creación y de verificación de Firma* en dicho soporte.

   Los *Datos de Creación de Firma* permanecerán siempre bajo el exclusivo control del *Firmante*, no guardándose copia de ellos por la FNMT-RCM, ni por la *Oficina de Registro*.

   Una vez obtenido este soporte y el software necesario para la operativa que desee realizar, el interesado procederá según se dispone a continuación.

2) Solicitud

   El interesado accede al *sitio web* del *Prestador de Servicios de Confianza,* a través de la dirección de la sede electrónica de la FNMT – RCM:

   https://www.sede.fnmt.gob.es/

   donde se mostrarán las instrucciones del proceso completo de obtención del *Certificado*, comenzando con la generación de las *Claves Pública* y *Privada* (en *Tarjeta criptográfica* si el *Certificado* se emite con el OID 1.3.6.1.4.1.5734.3.3.4.4.1*)* que serán vinculadas al *Certificado*, convirtiéndose en *Datos de verificación y creación de firma* respectivamente. Al realizar esta solicitud se envía a la FNMT-RCM, utilizando un canal seguro y mediante un formato estándar (PKCS#10 o SPKAC), la *Clave Pública* generada, junto con las correspondientes pruebas de posesión de la *Clave Privada*, para la posterior emisión del *Certificado*. La FNMT-RCM asocia a esta solicitud un código de solicitud único, que es mostrado o comunicado al *Solicitante*.

   Con carácter previo, el *Personal al servicio de la Administración Pública* y el órgano, organismo o entidad pública deberán consultar la *DGPC,* y las presentes *Políticas de Certificación y Prácticas de Certificación Particulares* en la dirección

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

   con las condiciones de uso y obligaciones propias como *Firmante* y *Suscriptor*, respectivamente, del *Certificado*, que se plasmarán en el documento de condiciones de utilización o, si procede, el contrato de emisión.

   La FNMT-RCM, una vez realizadas las comprobaciones pertinentes por la *Oficina de Registro*, comprobará mediante la *Clave Pública* del *Solicitante* la validez de la información de la solicitud firmada, comprobando la posesión y correspondencia de la pareja de *Claves* criptográficas por parte del *Solicitante* y el tamaño de las claves generadas.

Esta información no dará lugar a la generación de un *Certificado* por parte de la FNMT-RCM, en tanto que ésta no reciba firmada, por la *Oficina de Registro*, la solicitud del *Certificado* realizada por la Administración *Suscriptora*.

Si la generación de las claves se realiza en el interior de la *Tarjeta Criptográfica*, la operación de solicitud puede desarrollarse en la *Oficina de Registro* correspondiente siguiendo el procedimiento que garantiza la confidencialidad y el control exclusivo, por parte del *Firmante*, de la *Clave Privada*.

3) Confirmación de la identidad personal, cargo o empleo.

*12.2.2.2. Personación en las Oficinas de Registro*

66. La personación se realizará en la *Oficina de Registro* designada a tal efecto por el órgano, organismo o entidad pública *Suscriptora* de la que depende el personal a su servicio. Dicha *Oficina de Registro* es creada por la Administración *Suscriptora*, que notifica a la FNMT-RCM la relación de personas habilitadas para realizar estas actividades de Registro, de acuerdo con los procedimientos establecidos a tal efecto, así como cualquier variación en la estructura de dicha Oficina.

67. A estos efectos FNMT-RCM podrá tener en cuenta las funcionalidades previstas en la legislación aplicable en relación con el DNIe, así como los sistemas de identificación y comprobación del cargo, función o empleo aplicables en las Administraciones Públicas, por lo que el requisito de personación podrá ser sustituido por otros procedimientos que permitan la identificación, siempre que estén amparados por la intervención de la *Oficina de Registro*. En estos supuestos de procedimientos especiales de identificación propios del ámbito público, no será necesaria la personación cuando por el órgano competente de la Administración se proceda a certificar los requisitos de identidad, vigencia del cargo y demás condiciones a comunicar a la *Oficina de Registro*, de acuerdo con lo previsto en el artículo 13.1 in fine de la Ley 59/2003 de Firma electrónica, el artículo 43 de la Ley 40/2015, y el artículo 21 de la Ley 18/2011.

*12.2.2.3. Comparecencia y documentación*

68. En el supuesto que se actúe mediante comparecencia en la *Oficina de Registro*, el *Solicitante* aportará los datos que se le requieran, acreditará su identidad personal y su condición de *Personal al servicio de la Administración Pública*, sin perjuicio de la aplicación de lo previsto en el párrafo anterior. En el caso de la expedición de *Certificados* de *Firma electrónica del Personal al servicio de la Administración Pública* con seudónimo, la FNMT-RCM, a través de la *Oficina de Registro,* constatará la verdadera identidad del *Firmante* y conservará la documentación que la acredite. FNMT-RCM admitirá, en todo caso, la función e informe que realice la *Oficina de Registro* designada por la Administración.

1. Envío de información a la FNMT-RCM

Una vez confirmadas por la *Oficina de Registro* la identidad del *Solicitante* y la vigencia del cargo o empleo, y suscritas las condiciones de utilización o, en su caso, el contrato de solicitud por el citado *Solicitante* y la *Oficina de Registro*, ésta procederá a validar los datos y a enviarlos, junto con el código de solicitud generado en la fase de solicitud. La FNMT-RCM recabará de los *Solicitantes* solo aquella información, recibida de la

*Oficina de Registro*, que sea necesaria para la expedición de los *Certificados* y para la comprobación de la identidad, almacenando la información exigida por la legislación de firma electrónica durante el periodo de quince (15) años, tratándola con la debida diligencia para el cumplimiento de la legislación nacional vigente en materia de protección de datos de carácter personal.

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

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

2. Extensión de la función de registro

La FNMT-RCM, podrá acordar con las Administraciones, organismos y entidades públicas que así lo soliciten, la creación de *Oficinas de Registro* delegadas con el fin de centralizar la realización de los procedimientos de registro con destino a otras Administraciones, vinculadas o dependientes, que no dispongan de medios suficientes para hacerlo en aplicación de las leyes sobre racionalización del gasto.

*12.2.2.4. Emisión del Certificado*

69. Una vez recibidos en la FNMT-RCM los datos personales del *Solicitante*, la información que describe su relación con la Administración Pública, así como el código de solicitud obtenido en la fase de solicitud, se procederá a la emisión del *Certificado*.

70. La emisión de *Certificados* supone la generación de documentos electrónicos que confirman la identidad del personal, su relación, cargo o empleo con la Administración Pública, así como su correspondencia con la *Clave Pública* asociada. La emisión de *Certificados* de la FNMT-RCM sólo puede realizarla ella misma, en calidad de *Prestador de Servicios de Confianza*, no existiendo ninguna otra entidad u organismo con capacidad de emisión de los mismos. La *Autoridad de Certificación* de la FNMT-RCM solo acepta solicitudes de generación de *Certificados* provenientes de fuentes autorizadas. Todos los datos contenidos en cada solicitud están protegidos contra alteraciones a través de mecanismos de firma o sello electrónicos realizados mediante el uso de *Certificados* emitidos a dichas fuentes autorizadas.

71. La FNMT-RCM, por medio de su *Firma o Sello electrónicos*, autentica los *Certificados* y confirma la identidad del *Firmante,* así como la vigencia del cargo o empleo de su personal, de conformidad con la información recibida por la *Oficina de Registro*. Por otro lado, y con el fin de evitar la manipulación de la información contenida en los *Certificados*, la FNMT-RCM utilizará mecanismos criptográficos que doten de autenticidad e integridad al *Certificado*.

72. La FNMT-RCM en ningún caso incluirá en un *Certificado* información distinta de la aquí mostrada, ni circunstancias, atributos específicos de los *Firmantes* o límites distintos a los previstos en los acuerdos, convenios y, en su caso, a los previstos en la *Ley de Emisión* correspondiente.

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

- Comprobar que la *Oficina de Registro* o, en su caso, el personal *Firmante* del *Certificado* utilizan la *Clave Privada* correspondiente a la *Clave Pública* vinculada a la

identidad del *Firmante* del mismo. Para ello, la FNMT-RCM comprobará la correspondencia entre la *Clave Privada* y la *Clave Pública*.

- Lograr que la información incluida en el *Certificado* se base en la información proporcionada por la *Oficina de Registro* correspondiente.
- No ignorar hechos notorios que puedan afectar a la fiabilidad del *Certificado.*
- Lograr que el *DN* (nombre distintivo) asignado en el *Certificado* sea único en toda la *Infraestructura de Clave Pública* de la FNMT-RCM.

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

1. Composición de la estructura de datos que conforman el *Certificado* de *Firma electrónica* de *Personal al servicio de la Administración Pública*.

   Con los datos personales del citado personal recogidos durante el proceso de solicitud del *Certificado*, se procede a componer el nombre distintivo (*DN*) conforme al estándar *X.500*, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.

   El atributo *CN* contiene los datos de identificación del *Personal al servicio de la Administración Pública*. En el caso de la expedición de *Certificados* electrónicos de *Personal al servicio de la Administración Pública con seudónimos,* el atributo *CN* incluye dicho seudónimo.

2. Generación del *Certificado* conforme al perfil del *Certificado* de *Personal al servicio de la Administración Pública*.

   El formato del *Certificado* de *Personal al servicio de la Administración Pública*, expedido por la FNMT-RCM bajo la presente *Política de Certificación*, en consonancia con la norma UIT-T X.509 versión 3 y de acuerdo con la normativa legalmente aplicable en materia de *Certificados Cualificados*, puede consultarse en la página http://www.cert.fnmt.es/dpcs/

*12.2.2.5. Información de la emisión del Certificado al personal al servicio de la Administración Pública*

75. Una vez emitido el *Certificado*, FNMT-RCM envía una comunicación a la dirección de correo electrónico del *Personal al servicio de la Administración Pública* anunciando que está disponible dicho *Certificado* para su descarga.

*12.2.2.6. Descarga e instalación del Certificado de Personal al servicio de la Administración Pública*

76. En un plazo máximo de 24 horas desde que el *Personal al servicio de la Administración Pública* acredita su identidad y vigencia del cargo o empleo, el *Certificado* es generado y puesto a su disposición o a la de la *Oficina de Registro* mediante un mecanismo de descarga de *Certificado* desde la sede electrónica de la FNMT-RCM:

https://www.sede.fnmt.gob.es/

77. En este proceso guiado se le pedirá al *Personal al servicio de la Administración Pública* o al responsable o encargado de la *Oficina de Registro* que introduzca el NIF o NIE con el que se realizó el proceso de solicitud, así como el código de solicitud devuelto por el sistema al

finalizar dicho proceso. Si el *Certificado* no ha sido aún generado por cualquier motivo, se le indicará este hecho en el momento que intente su descarga.

78. Si el *Certificado* ya ha sido puesto a disposición del *Personal al servicio de la Administración Pública* o de la *Oficina de Registro*, aquél será introducido en el soporte en el que se generaron las *Claves* durante el proceso de solicitud.

*12.2.2.7. Vigencia del Certificado de personal al servicio de la Administración Pública*

**12.2.2.7.1. Caducidad**

79. Los *Certificados* de *Personal al servicio de la Administración Pública* emitidos por la FNMT-RCM tendrán validez durante un período de tres (3) años contados a partir del momento de la emisión del *Certificado*, siempre y cuando no se extinga su vigencia. Transcurrido este período y si el *Certificado* sigue activo, caducará, siendo necesaria la emisión de uno nuevo en caso de que el *Suscriptor* desee seguir utilizando los servicios del *Prestador de Servicios de Certificación.*

**12.2.2.7.2. Extinción de la vigencia**

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

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

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

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

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

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

*12.2.2.8. Revocación del Certificado de Personal al servicio de la Administración Pública*

**12.2.2.8.1. Causas de revocación**

82. Adicionalmente a lo previsto en el apartado "Extinción de la vigencia del *Certificado*" en relación con la solicitud de un *Certificado* existiendo otro en vigor a favor del mismo *Firmante* y mismo *Suscriptor* y perteneciente a la misma *Ley de Emisión*, serán causas de revocación de un *Certificado* de *Personal al servicio de la Administración Pública*:

a) La solicitud de revocación por parte de las personas autorizadas. En todo caso deberá dar lugar a esta solicitud:

- La pérdida del soporte del Certificado.

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

b) Resolución judicial o administrativa que así lo ordene.

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

d) Terminación de la cualidad de pertenencia, por parte del *Firmante*, al órgano administrativo *Suscriptor* del *Certificado.*

e) Incapacidad sobrevenida, total o parcial, del *Firmante*.

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

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

h) Resolución del contrato suscrito entre el *Suscriptor* y la FNMT-RCM.

i) Violación o puesta en peligro del secreto de los *Datos de Creación de Firma*.

83. 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.

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

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

85. Las actuaciones constitutivas de delito o falta de las que no tenga conocimiento la FNMT-RCM que se realicen sobre los datos o el *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.

#### 12.2.2.8.2. Efectos de la revocación

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

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

#### 12.2.2.8.3. Procedimiento para la revocación

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

89. La revocación de un *Certificado* para el *Personal al servicio de la Administración Pública* podrá ser solicitada por el *Suscriptor* a través de la *Oficina de Registro* habilitada para tal efecto o por el *Firmante*, bien a través de dicha *Oficina de Registro*, bien a través del teléfono habilitado para tal fin (previa identificación del *Solicitante*) cuyo número se hace público en la web de la FNMT – RCM y que estará operativo en horario 24x7. En este último caso se pide al *Solicitante* de la revocación, entre otros datos, el código único de solicitud que recibió en el proceso de solicitud del certificado, al objeto de verificar su identidad.

90. No obstante, la FNMT-RCM podrá revocar los *Certificados* para el *Personal al servicio de la Administración Pública* en los supuestos recogidos en la *Declaración de Prácticas de Certificación*.

91. A continuación, se describe el procedimiento a observar por la *Oficina de Registro* por el que se formaliza la solicitud de revocación de un *Certificado*.

92. En todo caso, FNMT-RCM recibirá de la Administración, organismos y/o entidad, aquella información relevante a efectos de la revocación de un *Certificado*, a través del modelo de solicitud de revocación del *Certificado* que se le presente, en formato papel o electrónico, por la *Oficina de Registro*.

93. La *Oficina de Registro* transmitirá los registros tramitados a la FNMT-RCM para que ésta proceda a la revocación del *Certificado*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

94. FNMT-RCM igualmente considerará que el peticionario de la revocación de un *Certificado* de este tipo cuenta con la autorización correspondiente si la petición es realizada a través de su *Oficina de Registro*. FNMT-RCM no realizará valoración alguna sobre la conveniencia o no de la revocación solicitada, cuando sea realizada a través de la citada *Oficina de Registro*. Tan pronto se resuelva la revocación, el *Firmante* recibirá, a través de la dirección de correo electrónico consignada en la solicitud, la notificación de la revocación del *Certificado*.

95. Una vez que la FNMT-RCM ha procedido a la revocación del *Certificado*, se publicará en el *Directorio* seguro la correspondiente *Lista de Certificados Revocados,* conteniendo el número de serie del *Certificado* revocado, así como la fecha, hora y causa de revocación. Una vez que

un *Certificado* ha sido revocado, su vigencia queda definitivamente extinguida, sin posibilidad de revertir su estado.

96. Este servicio estará operativo en horario 24x7. El periodo máximo entre la recepción en la FNMT-RCM de la solicitud de revocación y la publicación del cambio de estado de revocación del *Certificado* a efectos del *Servicio de información y consulta del estado de los certificados*, es de 24 horas.

*12.2.2.9. Suspensión del Certificado de personal al servicio de la Administración Pública*

97. La suspensión de los *Certificados* será considerada una revocación temporal de la vigencia del *Certificado* por lo que los procedimientos y entidades habilitadas para la solicitud y tramitación de la revocación del *Certificado* son de aplicación en el caso de la suspensión.

**12.2.2.9.1. Causas de la suspensión del Certificado**

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

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

**12.2.2.9.2. Efectos de la suspensión**

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

**12.2.2.9.3. Procedimiento para la suspensión de Certificados**

101. La suspensión de los *Certificados* solamente podrá ser realizada a través de la *Oficina de Registro* correspondiente, a petición del *Firmante* o del *Suscriptor* del *Certificado*.

102. La FNMT-RCM procederá a suspender el *Certificado* de forma provisional durante un plazo de treinta (30) días, plazo tras el cual se extinguirá el *Certificado* mediante su revocación directa por parte del *Prestador de Servicios de Confianza* de la FNMT-RCM, salvo que se hubiera cancelado la suspensión. No obstante lo anterior, el plazo previsto para la suspensión del *Certificado* podrá verse alterado en función de los procedimientos judiciales o administrativos que lo pudieran afectar.

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

104. La *Oficina de Registro* del ámbito correspondiente al órgano, organismo o entidad pública *Suscriptora* recogerá la solicitud de suspensión del *Certificado* y facilitará al *Solicitante* de la misma el contrato de suspensión del *Certificado*.

Las *Oficinas de Registro* transmitirán los registros tramitados a la FNMT-RCM para que ésta proceda a la suspensión del *Certificado*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

Una vez que la FNMT-RCM ha procedido a la suspensión del *Certificado*, se publicará en el *Directorio* la correspondiente *Lista de Revocación*, conteniendo el número de serie del *Certificado* suspendido, la fecha y hora en que se ha realizado la suspensión y como causa de revocación: "suspensión".

En todos los supuestos anteriores de estas *Prácticas de Certificación* particulares donde sea necesaria la identificación y sea posible la identificación telemática, se tendrá en cuenta por el *Prestador de Servicios de Confianza* las funcionalidades previstas para el DNI-e, de acuerdo con la legislación específica y el uso de otro *Certificado* emitido por la FNMT-RCM o reconocido por ésta.

*12.2.2.10. Cancelación de la suspensión del Certificado de Personal al servicio de la Administración Pública*

105. La cancelación de la suspensión de los *Certificados* solamente podrá ser realizada a través de la *Oficina de Registro* correspondiente, a petición del *Firmante* o del *Suscriptor* del *Certificado*, siempre que dicha solicitud se efectúe durante los treinta (30) días siguientes a su suspensión. En este acto la *Oficina de Registro* aportará los datos que se le requieran y acreditará la identidad del personal a su servicio cuya identidad conste en el *Certificado*, siguiendo el procedimiento descrito anteriormente para la solicitud de emisión del *Certificado* del *Personal al servicio de la Administración Pública*. FNMT-RCM aceptará el informe de acreditación que pudiera emitir la *Oficina de Registro* considerando lo establecido en el artículo 13.1, in fine, de la Ley de Firma Electrónica.

Los datos personales del *Personal al servicio de la Administración Pública* y de la Administración Pública *Suscriptora*, una vez validados por la *Oficina de Registro*, se enviarán a la FNMT-RCM mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

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

106. Como en supuestos anteriores a efectos de identificación, se tendrá en cuenta las funcionalidades previstas para el DNI-e, de acuerdo con la legislación específica y otras previstas en el ámbito de las Administraciones Públicas.

*12.2.2.11. Información del cambio de estado del Certificado*

107. Una vez se ha hecho efectiva la revocación, la suspensión o la cancelación de la suspensión del *Certificado,* FNMT-RCM envía una comunicación a la dirección de correo electrónico

del *Firmante* informando del cambio de estado del *Certificado* de *Personal al servicio de la Administración Pública.*

*12.2.2.12. Renovación del Certificado de personal al servicio de la Administración Pública*

108. La renovación del *Certificado* de *Personal al servicio de la Administración Pública* se realiza siempre emitiendo nuevas claves, por lo que el proceso es realmente el mismo que el seguido para la obtención de un *Certificado* nuevo.

*12.2.2.13. Comprobación del estado del Certificado del Personal al servicio de la Administración*

109. El *Suscriptor* del *Certificado,* las Administraciones, organismos y entidades usuarias pertenecientes a la *Comunidad Electrónica* y terceros que confían podrán realizar la comprobación del estado de un *Certificado* en la forma y condiciones que se expresan en este apartado.

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

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

112. El funcionamiento del *Servicio de información y consulta del estado de los certificados* es de la siguiente manera: el servidor OCSP de la FNMT-RCM recibe la petición OCSP efectuada por un Cliente OCSP y comprueba el estado de los *Certificados* incluidos en la misma. En caso de que la petición sea válida, se emitirá una respuesta de OCSP informando acerca del estado en el que se encuentran en ese momento los Certificados incluidos en la petición. Dicha respuesta es firmada con los *Datos de Creación de Firma* / *Sello* de la FNMT-RCM garantizando así la integridad y la autenticidad de la información suministrada sobre el estado de revocación de los *Certificados* consultados.

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

### 12.2.3. Plazo máximo de resolución de fallos del sistema

114. El plazo máximo para la resolución de fallos del sistema relacionados con la provisión de los servicios que FNMT-RCM ofrece durante las veinticuatro (24) horas del día, todos los días del año, es de veinticuatro (24) horas, a excepción de las operaciones de mantenimiento. La FNMT-RCM notificará dichas operaciones de mantenimiento en http://www.ceres.fnmt.es, si es posible al menos con cuarenta y ocho (48) horas de antelación.

# 13. CERTIFICADO DE SEDE ELECTRÓNICA

## 13.1. POLÍTICA DE CERTIFICACIÓN DEL CERTIFICADO DE SEDE ELECTRÓNICA

### 13.1.1. Identificación

115. El establecimiento de una *Sede electrónica* conlleva la responsabilidad de la Administración u organismo actuante en relación con la integridad, veracidad y actualización de la información y servicios a los que pueda accederse a través de la misma. Las condiciones de publicidad oficial relativas a las *Sedes electrónicas*, así como los principios aplicables a la *Sede electrónica* serán competencia de cada Administración titular de la misma. La FNMT-RCM se limita a la expedición del *Certificado de Sede electrónica*.

116. La presente *Política de Certificación Particular* de la FNMT-RCM para la expedición de *Certificados de Sede electrónica* de la Administración Pública, organismo público o entidad de derecho público tiene la siguiente identificación:

**Nombre**: *Política de Certificación* de *Certificados de Sede electrónica* de la Administración Pública, organismo público o entidad de derecho público

**Referencia / OID**[2]:

- 1.3.6.1.4.1.5734.3.3.8.1

**Versión**: 3.1

**Fecha de aprobación**: 9 de octubre de 2017

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

**DPC relacionada**: Declaración General de Prácticas de *Servicios de Confianza y de Certificación electrónica* de la FNMT-RCM

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

### 13.1.2. Tipología del *Certificado de Sede electrónica*

117. Los "*Certificados* de *Sede electrónica*", de conformidad con la definición de *Sede electrónica* de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, son aquellos *Certificados de autenticación de sitio web* expedidos por la FNMT-RCM bajo esta política de

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

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

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

certificación a la Administración Pública, o bien a uno o varios organismos públicos o entidades de Derecho Público como titulares de la *Sede electrónica*.

118. Corresponderá al *Responsable de Operaciones de Registro* la condición de custodio y, por tanto, el control de las claves del *Certificado de Sede electrónica*. Por tanto, la *Clave Privada* asociada a la *Clave Pública* estará bajo la responsabilidad de dicho custodio y actuará como representante de la Entidad Pública que tiene la titularidad, gestión y administración de la dirección electrónica correspondiente.

119. FNMT-RCM emitirá estos *Certificados* siempre que sea solicitado por los miembros de la *Comunidad Electrónica* en el ámbito de la Ley 40/2015 y de la Ley 18/2011, para las diversas relaciones que puedan producirse en el ámbito de la *Sede electrónica* y no se encuentre prohibida o limitada su utilización por la legislación aplicable.

120. FNMT-RCM emitirá y/o revocará estos *Certificados* siempre que sea solicitado por el *Responsable de Operaciones de Registro* correspondiente, el cual se presumirá que ostenta capacidad y competencia suficientes a los efectos de este tipo de *Certificados*.

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

122. FNMT-RCM no será responsable de las actuaciones realizadas con este tipo de *Certificados* cuando se produzcan abuso de facultades o insuficiencia de las mismas y/o cuando se produzcan decisiones de la persona que actúa como representante de la Entidad Pública titular de la *Sede electrónica* que afecten a la vigencia de las facultades del *Certificado*, produciendo en su caso supuestos de responsabilidad patrimonial, por lo que cualquier modificación, revocación o restricción en el *Certificado* y su uso no será oponible a la FNMT-RCM salvo que sea fehacientemente notificada por persona con competencia al efecto o, en su caso, por el *Responsable de Operaciones de Registro* correspondiente.

123. Del mismo modo, FNMT-RCM no será responsable de las actuaciones realizadas con este tipo de *Certificados* cuando los datos identificativos de la *Sede electrónica*, consignados en el *Certificado* y para la cual se ha emitido, sean diferentes de los asociados a la *Sede electrónica* en la que se esté empleando, por lo que cualquier modificación, revocación o restricción en el *Certificado* y su uso no será oponible a la FNMT-RCM salvo que sea fehacientemente notificada. FNMT-RCM no es competente para acreditar o valorar la titularidad de las *Sedes electrónicas* y/o dominios de las Administraciones, organismos o entidades públicas a las que pertenezca dicha *Sede electrónica*.

124. La FNMT-RCM, como *Prestador de Servicios de Confianza,* se reserva el derecho de no expedir o revocar este tipo de *Certificados* si el representante de la Administración Pública titular de la *Sede electrónica* en la que se emplea tal *Certificado*, no hace un uso adecuado del mismo, conculcando derechos de propiedad industrial o intelectual de terceros sobre las aplicaciones, sitios web o *Sedes electrónicas* que se desean proteger con tales *Certificados*, o su uso se presta a engaño o confusión sobre la titularidad de tales aplicaciones, sitios Web o *Sedes electrónicas* y, por tanto, de sus contenidos. En especial, tal reserva de derechos se podrá ejecutar por la FNMT-RCM cuando en la utilización de tales *Certificados* se atente contra los siguientes principios:

a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.

b) La protección de la salud pública o de las personas físicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.

c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y

d) La protección de la juventud y de la infancia.

125. La FNMT–RCM, se mantendrá indemne por parte de los titulares o responsables de los equipos, aplicaciones o *Sedes electrónicas* que incumplan lo previsto en este apartado y que tengan relación con el *Certificado*, quedando exonerada de cualquier reclamación o reivindicación por el uso inadecuado de tales *Certificados*.

126. Este *Certificado* se emite por la FNMT-RCM por cuenta de la Administración Pública, organismo público o entidad de Derecho Público correspondiente a la que la FNMT-RCM presta los servicios técnicos, administrativos y de seguridad necesarios como *Prestador de Servicios de Confianza*.

127. El *Certificado de Sede electrónica* de la Administración Pública, organismo público o entidad de derecho público es expedido por la FNMT-RCM mediante una infraestructura PKI, basada en actuaciones de identificación y registro realizadas por las *Oficinas de Registro* designadas por el órgano, organismo o entidad de la Administración Pública que tiene la titularidad, gestión y administración de la dirección electrónica de la *Sede electrónica*.

128. Las *Leyes de Emisión* podrán establecer, en el ámbito de actuación de las Administraciones Públicas, *Oficinas de Registro* comunes para este ámbito de actuación con efectos uniformes para cualesquiera Administraciones, organismos y/o entidades públicas.

### 13.1.3. Comunidad y ámbito de aplicación

129. Los *Certificados* emitidos bajo esta *Política de Certificación* son expedidos para los órganos y entidades encuadrables en el concepto legal de Administración Pública, organismo público o entidad de derecho público que forman parte de la *Comunidad Electrónica,* tal y como se define en el apartado *Definiciones* de la *DGPC* de la FNMT-RCM, y con objeto exclusivo de identificar una *Sede electrónica* de titularidad de cualesquiera de estos sujetos públicos.

130. En el marco de esta *Política de Certificación*, el *Solicitante* del *Certificado* se corresponde con personal con competencia suficiente y que presta sus servicios en la Administración Pública, organismo público o entidad de derecho público que tiene la titularidad, gestión y administración de la dirección electrónica a través de la que se accede a la *Sede electrónica*.

131. Los *Certificados* emitidos bajo esta *Política de Certificación* se consideran idóneos como parte integrante de sistemas de identificación electrónica que requieran niveles de seguridad específicos y, en especial, para el establecimiento de comunicaciones seguras entre una dirección electrónica y el usuario que se conecte a ella, además de ser una herramienta para autenticar e identificar a la dirección electrónica para la cual han sido emitidos. Por tanto, dichos *Certificados* se consideran adecuados para el desarrollo de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de

Justicia, a los efectos de identificación de las *Sedes electrónicas* en el ámbito público y para el establecimiento de comunicaciones seguras con ellas.

132. La *Ley de Emisión* de estos *Certificados* podrá determinar, en defecto de normativa específica, las condiciones de uso y régimen específico o individualizado de estos *Certificados* que permitirán la identificación de las *Sedes electrónicas* y atribución a las Administraciones, organismos y entidades titulares de tales *Sedes electrónicas* y responsables de sus contenidos de los diferentes actos y resoluciones realizados; todo ello, sin modificación legal o variación respecto de la actuación que vienen realizando las Administraciones, organismos y entidades en los soportes tradicionales en papel y otros.

### 13.1.4. Responsabilidad y obligaciones de las partes

133. Las obligaciones y responsabilidades expresadas en este apartado se entienden sin perjuicio de las correspondientes derivadas de la legislación y normativa de aplicación, específicamente de las aplicables a la FNMT-RCM como Prestador de Servicios de *Confianza* y que para tal condición se establecen en el articulado del Reglamento eIDAS, en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y su reglamentación de desarrollo.

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

- La Administración, organismos, entidades públicas representadas a través de los diferentes órganos competentes. Salvo indicación en contrario, corresponderá la representación a la *Oficina de Registro* correspondiente a través de su responsable.
- Los *Suscriptores*: Órganos, organismos y entidades públicas que tengan la titularidad, gestión y administración de la dirección electrónica a través de la cual se accede a la *Sede electrónica* o, en su caso, órgano en quién se deleguen las atribuciones o facultades. FNMT-RCM considerará como entidades u órgano delegados, salvo indicación en contrario, a las *Oficinas de Registro.*
- Los custodios: *Personal al servicio de la Administración Pública* que realiza la solicitud del *Certificado* y que, por tanto, toma el papel de custodio de la *Clave Privada* asociada a dicho *Certificado*. FNMT-RCM considerará, salvo indicación en contrario, que el *Responsable de Operaciones de Registro* es el custodio del *Certificado* y de la *Clave Privada* asociada al *Certificado*.
- FNMT-RCM, en cuanto *Prestador de Servicios de Confianza*.
- En su caso, resto de *Comunidad Electrónica* y terceros.

135. El régimen de derechos y obligaciones de las Administraciones, organismos, entidades públicas y la FNMT-RCM se regirá mediante el correspondiente acuerdo o convenio regulador de la prestación de los servicios de certificación. En estos acuerdos o convenios podrá establecerse la *Ley de Emisión* de estos *Certificados*; sin perjuicio de lo dispuesto en la presente Declaración en relación con las características o requisitos comunes aplicables a la *Ley de Emisión* de cada tipo de *Certificado* que se establece, con carácter general y efecto subsidiario, a lo no previsto en los acuerdos o convenios correspondientes.

136. Con carácter general y de forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la *DGPC*, las entidades públicas *Suscriptoras*, representadas a través de los

diferentes órganos competentes, actuando a través del *Responsable de Operaciones de Registro* para la emisión de este tipo de *Certificados*, tienen la obligación de:

- No realizar registros o tramitar solicitudes de *Certificados de Sede electrónica* por personal que preste sus servicios en una entidad diferente a la que representa como *Oficina de Registro*, salvo habilitación expresa de otra entidad.
- No realizar registros o tramitar solicitudes de *Certificados* emitidos bajo esta política y cuyo *Suscriptor* se corresponda con una entidad pública sobre la que no tenga potestades o no tenga competencias para actuar como *Oficina de Registro*.
- No realizar registros o tramitar solicitudes de *Certificados* emitidos bajo esta política y cuyo *Suscriptor* no se corresponda con la titularidad de la dirección electrónica a través de la que se accede a la *Sede electrónica* que identificará el *Certificado* objeto de la solicitud.
- No realizar registros o tramitar solicitudes de *Certificados* emitidos bajo esta política y cuyo *Solicitante* se corresponda con una *persona física* que no preste sus servicios en la entidad *Suscriptora* del *Certificado* y/o no haya sido autorizado por la persona que actúa como representante de la Entidad Pública para la gestión y administración de la dirección electrónica a través de la que se accede a la *Sede electrónica* que identificará el *Certificado* objeto de la solicitud.
- Comprobar fehacientemente los datos identificativos y competenciales del *Suscriptor* del *Certificado* (la Entidad titular de la *Sede electrónica* y de la dirección electrónica, dominio o URL, a través del cual se accede a tal *Sede*) y del *Solicitante* (la persona física con atribución suficiente para solicitar un *Certificado* de *Sede electrónica*) del *Certificado* y verificar su correspondencia con el titular y contactos establecidos en las bases de datos correspondientes, para la gestión y administración de la dirección electrónica a través de la que se accede a la *Sede electrónica* que identificará el *Certificado* objeto de la solicitud.
- Solicitar la revocación del *Certificado de Sede electrónica* emitido bajo esta política cuando alguno de los datos referidos al *Suscriptor* o a la dirección electrónica incluida en el *Certificado* sean incorrectos, inexactos o hayan variado respecto a lo consignado en el *Certificado,* o no se correspondan con el titular y contactos establecidos en las bases de datos correspondientes para la gestión y administración de la dirección electrónica consignada en el *Certificado* objeto de la revocación.

137. Las relaciones de la FNMT-RCM y el *Suscriptor* quedarán determinadas principalmente, a los efectos del régimen de uso de los *Certificados,* a través del documento relativo a las condiciones de utilización o en su caso, contrato de emisión del *Certificado* y atendiendo a los acuerdos, convenios o documento de relación entre la FNMT-RCM y la Entidad Pública correspondiente.

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

139. FNMT-RCM no será responsable de la utilización de los *Certificados* emitidos bajo esta *Política* cuando el *Suscriptor* del *Certificado* electrónico, a través de su representante, realice actuaciones sin facultades, extralimitándose en las mismas, no se corresponda con los titulares y contactos autorizados para la gestión de la dirección electrónica para la cual ha sido emitido el *Certificado* o en fraude de ley o de terceros, si no existe notificación fehaciente que permita trasladar los efectos pretendidos a la gestión de los *Certificados.*

### 13.1.5. Límites de uso de los Certificados de Sede electrónica

140. Constituyen límites de uso de este tipo de *Certificados* las competencias administrativas correspondientes a cada *Suscriptor* identificado al amparo de las *Sedes electrónicas* de las Administraciones Públicas, organismos públicos o entidades de derecho público, de conformidad con la Ley 40/2015 y con la Ley 18/2011, para la identificación de *Sedes electrónicas* y el establecimiento de comunicaciones seguras con éstas. La FNMT-RCM y la Administración, organismos y entidades podrán fijar en los acuerdos o convenios, o a través del documento de relación correspondiente o, si fuera procedente en la *Ley de Emisión* de estos *Certificados*, otros límites adicionales.

141. El *Certificado de Sede electrónica* no se podrá emplear para:

- Firmar o sellar otro *Certificado*.
- Usos particulares o privados.
- Firmar o sellar software o componentes.
- Generar *Listas de* Revocación.
- Cualquier uso que exceda de la finalidad de este tipo de *Certificados* sin la autorización previa de la FNMT-RCM.

## 13.2. PRÁCTICAS DE CERTIFICACIÓN PARTICULARES PARA LOS CERTIFICADOS DE SEDE ELECTRÓNICA

142. La FNMT-RCM en su labor como *Prestador de Servicios de Confianza* y para demostrar la necesaria fiabilidad para la prestación de dichos servicios, cuenta con una *Declaración de Prácticas de Certificación* cuyo objeto es la información pública sobre las condiciones generales de prestación de los mismos.

143. En especial deberá tenerse presente, a efectos interpretativos del presente documento, el apartado "Definiciones" del cuerpo principal de la *DGPC*.

144. El presente documento trae causa y forma parte integrante de la *DGPC* de la FNMT-RCM y define el conjunto de prácticas particulares adoptadas por la FNMT-RCM como *Prestador de Servicios de Confianza* para la gestión del ciclo de vida de los *Certificados de Sede electrónica*, expedidos bajo la *Política de Certificación* identificada con el OID 1.3.6.1.4.1.5734.3.3.8.1.

### 13.2.1. Servicios de Gestión de las *Claves*

145. La FNMT-RCM no genera ni almacena las *Claves Privadas* asociadas a los *Certificados* expedidos bajo la presente *Política de Certificación*, que son generadas bajo el exclusivo control del *Responsable de Operaciones de Registro* o la persona autorizada por éste.

### 13.2.2. Gestión del ciclo de vida de los Certificados

*13.2.2.1. Registro de los Suscriptores*

146. Con carácter previo al establecimiento de cualquier relación institucional con los *Suscriptores*, la FNMT-RCM informa a través de los medios y direcciones web citadas en estas *Prácticas de Certificación Particulares* y, subsidiariamente, en la *DGPC*, acerca de las condiciones del servicio, así como de las obligaciones, garantías y responsabilidades de las partes implicadas en la expedición y uso de los *Certificados* por ella emitidos en su labor como *Prestador de Servicios de Confianza*.

147. La FNMT-RCM, en su actividad como *Prestador de Servicios de Confianza*, a través de las *Oficinas de Registro,* procede a la identificación de los *Solicitantes* de los C*ertificados de Sede electrónica* mediante aquellos procedimientos que así se dispongan para ello. FNMT-RCM considerará con competencia al efecto cualquier solicitud que venga realizada por el *Responsable de Operaciones de Registro* correspondiente, en su condición de representante del *Suscriptor*.

148. La FNMT-RCM recabará de los *Solicitantes* solo aquella información, recibida de la *Oficina de Registro*, que sea necesaria para la expedición de los *Certificados* y para la comprobación de la identidad, legitimidad y competencia de los representantes, almacenando la información legalmente exigida durante el periodo de quince (15) años, tratándola con la debida diligencia para el cumplimiento de la legislación nacional vigente en materia de protección de datos de carácter personal.

149. La FNMT-RCM no genera el par de *Claves* asociado a los *Certificados* expedidos bajo la presente *Política de Certificación*, poniendo todos los mecanismos necesarios durante el proceso de *Solicitud de Certificados* para posibilitar que el *Responsable de Operaciones de Registro* y/o el representante del *Suscriptor* se encuentran en posesión de la *Clave Privada* asociada a la *Clave Pública* que se certificará.

*13.2.2.2. Procedimiento de solicitud del Certificado*

150. A continuación se describe el procedimiento de solicitud del *Certificado* por el que se toma la denominación oficial de la Administración, organismo o entidad pública, que será el *Suscriptor* de los *Certificados*, los datos personales del representante del *Suscriptor*, se confirma su identidad, vigencia del cargo o empleo y se formaliza, entre el *Suscriptor* y la FNMT-RCM, el documento de condiciones de utilización o el contrato tipo de emisión para la posterior expedición de un *Certificado de Sede electrónica*.

151. Se hace constar que FNMT-RCM, en función de la relación de *Solicitantes* habilitados remitida por la Administración, organismo o entidad pública, considerará, bajo responsabilidad de los correspondientes órganos, organismos y/o entidades que actuarán a

través de las *Oficinas de Registro*, que dichos *Solicitantes* cumplen los requisitos establecidos en la presente Declaración y, por tanto, tienen la legitimidad y competencia necesarias para solicitar y obtener el *Certificado de Sede electrónica*. La FNMT-RCM presumirá con facultades y competencia suficientes a los representantes de los *Suscriptores* que tengan encomendada la responsabilidad de la *Oficina de Registro*.

152. Con carácter previo el *Solicitante* y el representante del *Suscriptor* titular de la *Sede electrónica* deberán consultar la *DGPC* y las presentes *Políticas de Certificación y Prácticas de Certificación Particulares* en la dirección

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

con las condiciones de uso y obligaciones para las partes, pudiendo realizar las consultas que estimen oportunas sobre el alcance de esta Declaración; todo ello, sin perjuicio de que, con posterioridad, el representante del *Suscriptor* deba suscribir el documento de condiciones de utilización o si procede el contrato de emisión. En ningún caso la continuación del procedimiento de solicitud implicará la conclusión del proceso.

153. La FNMT-RCM comprueba si hay un *Registro AAC* para cada nombre de dominio que incluye en un *Certificado de sede electrónica* emitido, de acuerdo con el procedimiento establecido en RFC 6844 y siguiendo las instrucciones de procesamiento establecidas en RFC 6844 para cualquier registro encontrado. Si existe dicho *Registro AAC*, no emitirá dicho *Certificado* a menos que determine que la solicitud del *Certificado* es consistente con el conjunto de registro de recursos AAC aplicable.

154. El *Solicitante*, como representante del *Suscriptor,* (o la persona autorizada por éste para este fin), que habitualmente será el *Responsable de Operaciones de Registro,* genera las *Claves Pública* y *Privada* que serán vinculadas al *Certificado* y compone una solicitud electrónica del *Certificado,* que incluye la *Clave Pública*, generalmente en formato PKCS#10.

155. Dicho *Solicitante* se identifica, mediante un *Certificado de firma electrónica* de los admitidos para tal fin, en el *sitio web* de la FNMT-RCM, a través de la dirección

https://apuc20.cert.fnmt.es/PreregistroComponentes/indexCRDinamicos.jsp

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

157. La FNMT-RCM, tras comprobar que el *Solicitante* ha sido habilitado por el representante del *Suscriptor* para llevar a cabo dicha solicitud, le muestra un formulario en el que deberá introducir los datos del órgano *Suscriptor* titular de la *Sede electrónica* para la cual se emitirá el *Certificado,* los datos de la *persona física* en su condición de responsable de la custodia diligente de la *Clave privada* asociada al *Certificado de Sede electrónica* y la solicitud electrónica generada anteriormente. Toda esta información es firmada por el *Solicitante* con los *Datos de creación de firma* asociados a su *Certificado de firma electrónica* y remitida a la FNMT-RCM.

158. FNMT-RCM asignará e indicará al *Solicitante* un código de solicitud para su utilización posterior. Adicionalmente, el *Solicitante* suscribe las condiciones de utilización o, en su caso, contrato de solicitud del *Certificado*, cuya custodia recae en la *Oficina de Registro*.

159. Esta información no dará lugar a la generación de un *Certificado* por parte de la FNMT-RCM, en tanto que ésta no reciba la declaración responsable, en cuanto al cumplimiento de los

procedimientos aquí descritos y la veracidad de los datos incluidos en la solicitud, firmada por el *Responsable de Operaciones de Registro*.

160. La FNMT-RCM, tras recibir esta información, comprobará la validez de la información de la solicitud firmada, así como la posesión y correspondencia de la pareja de *Claves criptográficas* asociadas al *Certificado* de *Sede electrónica* y el tamaño de las mismas.

*13.2.2.3. Validación del dominio.*

161. Para validar el dominio del *Certificado*, la FNMT-RCM utiliza uno de los métodos descritos en el documento CA/Browser Forum's Baseline Requirements (versión 1.4.1), concretamente el definido en la sección "3.2.2.4.5 Domain Authorization Document".

162. La FNMT-RCM confirma que el *Solicitante* posee el control sobre los nombres completos de los dominios o FQDN (siglas en inglés de Fully Qualified Domain Name) que son incorporados a los *Certificados*. Para ello, la FNMT-RCM consulta, a través de la aplicación que registra las solicitudes de estos *Certificados*, la identidad del *Solicitante* y el nombre del citado FQDN. A continuación, verifica que la solicitud proviene del contacto que tiene el control sobre dicho dominio (según los registros de dominios WHOIS, RED.ES, etc.) o tiene autorización por parte de este. Adicionalmente se comprueba que la solicitud del *Certificado* ha sido realizada con posterioridad al alta en dichos registros.

*13.2.2.4. Extensión de la función de registro.*

163. La FNMT-RCM, podrá acordar con las Administraciones, organismos y entidades públicas que así lo soliciten, la creación de *Oficinas de Registro* delegadas con el fin de centralizar la realización de los procedimientos de registro con destino a otras Administraciones, vinculadas o dependientes, que no dispongan de medios suficientes para hacerlo en aplicación de las leyes sobre racionalización del gasto.

*13.2.2.5. Emisión del Certificado de Sede electrónica*

164. La FNMT-RCM recibe la declaración responsable, en cuanto al cumplimiento de los procedimientos aquí descritos y la veracidad de los datos incluidos en la solicitud, firmada por el *Responsable de Operaciones de Registro*, y que incluye el código de solicitud. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

165. A continuación, la FNMT-RCM comprueba los datos que confirman la relación del representante con la Administración Pública, así como la información que confirma la titularidad y gestión de la dirección electrónica de la *Sede electrónica* por parte del *Suscriptor*. Una vez realizadas dichas comprobaciones, se procede a la emisión del *Certificado*.

166. La FNMT-RCM, en ningún caso, incluirá en un *Certificado* información distinta de la aquí mostrada, ni límites distintos a los previstos en los acuerdos, convenios y, en su caso, a los previstos en la *Ley de Emisión* correspondiente.

167. En cualquier caso, la FNMT-RCM actuará diligentemente para:

- Comprobar que el *Solicitante* del *Certificado* o el *Responsable de Operaciones de Registro* utilicen la *Clave Privada* correspondiente a la *Clave Publica* vinculada al *Certificado.*
- Lograr que la información incluida en el *Certificado* se base en la información proporcionada por el *Solicitante* y/o por el *Responsable de Operaciones de Registro* correspondiente.
- No ignorar hechos notorios que puedan afectar a la fiabilidad del *Certificado.*
- Lograr que el *DN* (nombre distintivo) asignado en el *Certificado* sea único en toda la *Infraestructura de Clave Pública* de la FNMT-RCM.

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

1. Composición de la estructura de datos que conforman el *Certificado de Sede electrónica.*

   Con los datos de la dirección electrónica de la *Sede electrónica* recogidos durante el proceso de solicitud del *Certificado*, se procede a componer el nombre distintivo (*DN*) conforme al estándar *X.500*, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades. No se contempla el uso de seudónimos como forma de identificación del *Suscriptor*.

   El atributo *CN* contiene la dirección electrónica a través de la cual se accede a la *Sede electrónica* objeto del *Certificado*. La identidad alternativa del *Certificado* está compuesta exclusivamente por dicha dirección electrónica.

2. Generación del *Certificado* conforme al Perfil del *Certificado de Sede electrónica*

   El formato del *Certificado de Sede electrónica* expedido por la FNMT-RCM bajo la presente *Política de Certificación*, en consonancia con la norma UIT-T X.509 versión 3 y de acuerdo con la normativa legalmente aplicable en materia de *Certificados*, puede consultarse en la página http://www.cert.fnmt.es/dpcs/.

*13.2.2.6. Información de la emisión del Certificado*

169. Una vez emitido el *Certificado*, FNMT-RCM envía una comunicación a la dirección de correo electrónico de la persona designada para la gestión de la dirección electrónica a través de la que se accede a la *Sede electrónica,* anunciando que está disponible dicho *Certificado* para su descarga.

*13.2.2.7. Descarga e instalación del Certificado*

170. En un plazo máximo de 72 horas desde la recepción en la FNMT – RCM de la documentación necesaria para realizar las comprobaciones ya comentadas de forma previa a la expedición del *Certificado de Sede electrónica*, la FNMT-RCM pondrá a disposición del *Solicitante* un mecanismo de descarga del *Certificado*, en la dirección de titularidad de la Administración u organismo, a través del siguiente enlace:

https://apuc20.cert.fnmt.es/PreregistroComponentes/indexCRDinamicos.jsp

171. En este proceso guiado se le pedirá al *Responsable de Operaciones de Registro* del ámbito del *Suscriptor* que introduzca el NIF del órgano, organismo o entidad pública con el que realizó el proceso de solicitud, así como el código de solicitud asignado al finalizar dicho proceso. Si el *Certificado* no ha sido aún generado por cualquier motivo, se le indicará este hecho en el momento que intente su descarga.

172. El *Certificado* puesto a disposición del *Personal al servicio de la Administración Pública* o de la *Oficina de Registro*, será introducido directamente en el soporte en el que se generaron las *Claves* durante el proceso de solicitud.

*13.2.2.8. Vigencia del Certificado de Sede electrónica*

**13.2.2.8.1. Caducidad**

173. Los *Certificados de Sede electrónica* emitidos por la FNMT-RCM tendrán validez durante un período de dos (2) años contados a partir del momento de la emisión del *Certificado*, siempre y cuando no se extinga su vigencia. Transcurrido este período y si el *Certificado* sigue activo, caducará, siendo necesaria la emisión de uno nuevo en caso de que el *Suscriptor* desee seguir utilizando los servicios del *Prestador de Servicios de Confianza.*

**13.2.2.8.2. Extinción de la vigencia**

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

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

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

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

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

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

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

*13.2.2.9. Revocación del Certificado de Sede electrónica*

177. La FNMT-RCM pone a disposición de los *Suscriptores*, terceros que confían, proveedores de software y terceras partes una vía de comunicación a través de la sede electrónica de la FNMT-RCM

https://www.sede.fnmt.gob.es/

con instrucciones claras, para permitirles reportar cualquier asunto relacionado con este tipo de *Certificados*, en cuanto a un supuesto compromiso de *Clave Privada*, uso indebido de los *Certificados* u otros tipos de fraude, compromiso, mal uso o conducta inapropiada.

#### 13.2.2.9.1. Causas de revocación

178. Adicionalmente a lo previsto en el apartado "Extinción de la vigencia del *Certificado*" en relación con la solicitud de un *Certificado* existiendo otro en vigor a favor del mismo *Firmante* y mismo *Suscriptor* y perteneciente a la misma *Ley de Emisión*, serán causas de revocación de un *Certificado de Sede electrónica*:

a) La solicitud de revocación por parte de las personas autorizadas. En todo caso deberá dar lugar a esta solicitud:

- La pérdida del soporte del *Certificado*.
- La utilización por un tercero de la *Clave Privada* asociada al *Certificado*.
- La violación o puesta en peligro del secreto de la *Clave Privada* asociada al *Certificado*.
- La no aceptación de las nuevas condiciones que puedan suponer la emisión de nuevas *Declaraciones de Prácticas de Certificación*, durante el periodo de un mes tras su publicación.

b) Resolución judicial o administrativa que así lo ordene.

c) Extinción, disolución o cierre de la sede electrónica.

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

e) Terminación de la forma de representación del representante del *Suscriptor* del *Certificado.*

f) Incapacidad sobrevenida, total o parcial, del representante del *Suscriptor*.

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

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

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

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

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

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

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

181. Las actuaciones constitutivas de delito o falta de las que no tenga conocimiento la FNMT-RCM que se realicen sobre los datos o el *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.

#### 13.2.2.9.2. Efectos de la revocación

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

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

#### 13.2.2.9.3. Procedimiento para la revocación

184. La solicitud de revocación de los *Certificados de Sede electrónica* podrá efectuarse durante el período de validez que consta en el *Certificado*.

185. La revocación de *Certificados* consiste en la cancelación de la garantía de identidad, autenticidad u otras propiedades del *Suscriptor* y sus representantes y su correspondencia con la *Clave pública* asociada. Implica, además de su extinción, la finalización de la relación y régimen de uso del *Certificado* con la FNMT-RCM.

186. Estarán legitimados para solicitar la revocación de un *Certificado de Sede electrónica*, con base en la inexactitud de datos, variación de los mismos o cualquier otra causa a valorar por el *Suscriptor*:

- El órgano directivo, organismo o entidad pública *Suscriptora* del *Certificado* o persona en quien delegue.
- La *Oficina de Registro*, —a través de su responsable— que esté designada a tal efecto, por la Administración, organismo o entidad de derecho público, *Suscriptora* del *Certificado* a revocar, cuando detecte que alguno de los datos consignados en el *Certificado*

- es incorrecto, inexacto o haya variado respecto a lo consignado en el *Certificado,* o
- la persona física, custodio del *Certificado,* no se corresponda con el responsable máximo o designado para la gestión y administración de la dirección electrónica consignada en el *Certificado* objeto de la revocación

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

187. A continuación, se describe el procedimiento a observar por la *Oficina de Registro* por el que se formaliza la solicitud de revocación de un *Certificado*. En todo caso FNMT-RCM, presumirá la competencia y capacidad del *Solicitante* cuando se trate del *Responsable de Operaciones de Registro* correspondiente.

1. Personación del *Solicitante* ante las *Oficinas de Registro*

   Para revocar el *Certificado*, el *Solicitante* con capacidad y competencia suficientes, se personará ante una *Oficina de Registro* designada a tal efecto por el órgano, organismo o entidad *Suscriptora* del *Certificado* a revocar o se realizará directamente por el *Responsable de Operaciones de Registro*.

2. Comparecencia y documentación

   El *Solicitante* aportará los datos que se le requieran y que acrediten:

   - su identidad personal,
   - su condición de *Personal al servicio de la Administración Pública, Suscriptora* del *Certificado* y titular de la dirección electrónica a través de la que se accede a la *Sede electrónica* objeto del *Certificado* o su condición de *Responsable de Operaciones de Registro*.
   - su condición de persona designada para la gestión de la dirección electrónica a través de la que se accede a la *Sede electrónica* objeto del *Certificado* a revocar o de personal adscrito a la *Oficina de Registro* designada a tal efecto por el organismo o entidad *Suscriptora* del *Certificado* a revocar.

   FNMT-RCM admitirá, en todo caso, la función e informe que realice la *Oficina de Registro* designada por la Administración. En el caso de que no se acrediten los puntos anteriores, la *Oficina de Registro* no procederá con la solicitud de revocación del *Certificado.*

3. Envío de la solicitud de revocación a la FNMT-RCM y tramitación

   Sin que existan causas notorias de falta de competencia del *Responsable de Operaciones de Registro* y/o una vez confirmada la identidad del *Solicitante*, vigencia de las condiciones exigidas a éste y suscrito el documento de solicitud de revocación, la *Oficina de Registro* procederá a validar los datos y a enviarlos a la FNMT-RCM para la revocación efectiva del *Certificado*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

   Dicho envío sólo se producirá si la *Oficina de Registro* tiene potestad para actuar como tal en nombre del órgano, organismo o entidad de la Administración Pública

*Suscriptora* del *Certificado* y si éste es titular de la dirección electrónica a través de la que se accede a la sede electrónica objeto del *Certificado.*

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

188. Adicionalmente, existe un servicio de atención telefónica, en horario 24 x 7, en el teléfono 902 200 616, al que se pueden dirigir las solicitudes de revocación. La comunicación quedará grabada y registrada, sirviendo de soporte y garantía de la aceptación de la solicitud de revocación solicitada.

189. Para solicitar una revocación telefónica de un *Certificado*, el *Solicitante* de la misma debe ser el representante del *Suscriptor*.

190. Una vez que la FNMT-RCM ha procedido a la revocación del *Certificado*, se publicará en el *Directorio* seguro la correspondiente *Lista de Certificados Revocados,* conteniendo el número de serie del *Certificado* revocado, así como la fecha, hora y la causa de revocación. El representante del *Suscriptor* recibirá, a través de la dirección de correo electrónico consignada en la solicitud, la notificación del cambio de estado de vigencia del *Certificado*.

*13.2.2.10. Suspensión del Certificado de Sede electrónica*

191. No se contempla.

*13.2.2.11. Información del cambio de estado del Certificado*

192. Una vez se ha hecho efectiva la revocación del *Certificado,* FNMT-RCM envía una comunicación a la dirección de correo electrónico de la persona designada para la gestión de la dirección electrónica a través de la que se accede a la *Sede electrónica,* informando del cambio de estado del *Certificado.*

*13.2.2.12. Renovación del Certificado de Sede electrónica*

193. La renovación del *Certificado de Sede electrónica* se realiza siempre emitiendo nuevas claves, por lo que el proceso es realmente el mismo que el seguido para la obtención de un *Certificado* nuevo.

*13.2.2.13. Comprobación del estado del Certificado*

194. El *Suscriptor* del *Certificado,* las Administraciones, organismos y entidades usuarias pertenecientes a la *Comunidad Electrónica* y terceros que confían podrán realizar la comprobación del estado de un *Certificado* en la forma y condiciones que se expresan en este apartado.

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

196. Estos servicios estarán disponibles las veinticuatro (24) horas del día, todos los días del año, salvo por circunstancias ajenas a la FNMT-RCM u operaciones de mantenimiento. La FNMT-

RCM notificará esta última circunstancia en la dirección http://www.ceres.fnmt.es si es posible con al menos cuarenta y ocho (48) horas de antelación y tratará de solventarla en un periodo no superior a veinticuatro (24) horas.

197. El funcionamiento del *Servicio de información y consulta del estado de los certificados* es el siguiente: el servidor OCSP recibe la petición OCSP efectuada por un *Cliente OCSP* y comprueba el estado de vigencia de los *Certificados* incluidos en la misma. En caso de que la petición sea válida, se emitirá una respuesta de OCSP informando acerca del estado en el que se encuentran en ese momento los *Certificados* incluidos en la petición. Dicha respuesta es firmada / sellada con los *Datos de Creación de Firma* / *Sello* de la FNMT-RCM garantizando así la integridad y la autenticidad de la información suministrada sobre el estado de revocación de los *Certificados* consultados.

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

199. La FNMT-RCM opera y mantiene sus capacidades de mantenimiento de sus CRL y servicio OCSP con recursos suficientes para proporcionar un tiempo de respuesta máximo de diez segundos bajo condiciones normales de operación.

## 14. CERTIFICADO DE SELLO ELECTRÓNICO

### 14.1. POLÍTICA DE CERTIFICACIÓN DE LOS CERTIFICADOS DE SELLO ELECTRÓNICO

#### 14.1.1. Identificación

200. FNMT-RCM expide el *Certificado de Sello electrónico* en el ámbito de las presentes *Prácticas y Políticas de Certificación Particulares*, sobre la base de su consideración del concepto legal previsto en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, correspondiente a los artículos 40 y 42, así como en la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, correspondiente al artículo 19.

201. La presente *Política de Certificación Particular* de la FNMT-RCM para la expedición de *Certificados de Sello electrónico* tiene la siguiente identificación

**Nombre**: *Política de Certificación* de *Certificados de Sello electrónico* de la Administración Pública, organismo público o entidad de derecho público.

**Referencia / OID**[3]:

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

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

- 1.3.6.1.4.1.5734.3.3.9.1

**Versión**: 3.1

**Fecha de aprobación**: 9 de octubre de 2017

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

**DPC relacionada**: Declaración General de Prácticas de *Servicios de Confianza y de Certificación electrónica* de la FNMT-RCM

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

### 14.1.2. Tipología del Certificado de Sello electrónico

202. Los "*Certificados de Sello electrónico*" expedidos por la FNMT-RCM bajo esta política de certificación cuentan con las garantías necesarias para ser utilizados como sistema de identificación y de firma / sello para la actuación administrativa / judicial automatizada de aquellas Administraciones, organismos o entidades de derecho público (y, en su caso, sus respectivas unidades organizativas) a las que se expiden dichos *Certificados*.

203. Corresponderá al *Responsable de Operaciones de Registro* la condición de custodio y, por tanto, el control de las claves del *Certificado de Sello electrónico.* Por tanto, la *Clave Privada* asociada a la *Clave Pública* estará bajo la responsabilidad de dicho custodio, que tiene el control sobre dicho *Certificado* y los *Datos de creación y verificación de firma / sello*, sin perjuicio de las delegaciones que puedan producirse, de acuerdo con el régimen legal correspondiente.

204. FNMT-RCM emitirá estos *Certificados de Sello electrónico* siempre que sea solicitado por los miembros de la *Comunidad Electrónica* del ámbito de la Ley 40/2015 y de la Ley 18/2011, para las diversas relaciones que puedan producirse en cuanto a la identificación y a la actuación administrativa / judicial automatizada, y no se encuentre prohibido o limitado su uso por la legislación aplicable.

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

206. Del mismo modo, FNMT-RCM no será responsable de las actuaciones realizadas con este tipo de *Certificados* cuando los datos identificativos y de autenticación de la unidad organizativa de la entidad de la administración consignada en el *Certificado* no se corresponda con una unidad dependiente de dicha entidad de la administración.

---

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

207. La FNMT-RCM, como *Prestador de Servicios de Confianza,* se reserva el derecho de no expedir o revocar este tipo de *Certificados,* con exoneración de responsabilidad a estos efectos, si el usuario del *Certificado* y/o la unidad organizativa en la que se emplea tal *Certificado*, carecen de competencia, no hacen un uso adecuado del mismo, conculcando derechos de explotación, de propiedad industrial o intelectual de terceros sobre las aplicaciones y actuaciones realizadas o cualquier legislación vigente.

208. La FNMT–RCM, se mantendrá indemne por parte del *Suscriptor* y las personas responsables o representantes del mismo, respecto de cuestiones de titularidad de derechos y/o los vicios o defectos de los equipos, aplicaciones o sistemas que incumplan lo previsto en este apartado y que tenga relación con el *Certificado*, quedando exonerada de cualquier reclamación o reivindicación por el uso inadecuado de tales *Certificados*.

209. Este *Certificado* se emite por la FNMT-RCM por cuenta de la Administración Pública, organismo público o entidad de derecho público correspondiente a la que la FNMT-RCM presta los servicios técnicos, administrativos y de seguridad necesarios como *Prestador de Servicios de Confianza*.

210. El *Certificado de Sello electrónico* es desarrollado por la FNMT-RCM mediante una infraestructura PKI específica, basada en actuaciones de identificación, autenticación y registro realizadas por la red de *Oficinas de Registro* designadas por el órgano, organismo o entidad de la Administración Pública de la que depende la unidad organizativa consignada en el *Certificado*.

211. Las *Leyes de Emisión* podrán establecer, en el ámbito de actuación de las Administraciones Públicas, *Oficinas de Registro* comunes para este ámbito de actuación con efectos uniformes para cualesquiera Administraciones, organismos y/o entidades públicas.

212. Este *Certificado* es expedido como "cualificado" de conformidad con los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 412-3 "Certificate profile for certificates issued to legal persons".

### 14.1.3. Comunidad y ámbito de aplicación

213. Los *Certificados* emitidos bajo esta *Política de Certificación* son expedidos para la Administración Pública, organismos públicos o entidades de derecho público y que forman parte de la *Comunidad Electrónica,* tal y como se define en el apartado *Definiciones* de la *DGPC* de la FNMT-RCM, y con objeto exclusivo de realizar la identificación, autenticación y de firma / sello para la actuación administrativa / judicial automatizada en ejercicio de sus competencias, mediante *Sello electrónico*.

214. En el marco de esta *Política de Certificación*, el *Solicitante* del *Certificado* se corresponde con el *Responsable de Operaciones de Registro* y/o el representante del *Suscriptor* o persona en quien delegue la unidad organizativa que requiere identificarse o realizar la actuación administrativa / judicial automatizada con este tipo de *Certificados* y que presta sus servicios en una Administración Pública, organismo público o entidad de derecho público bajo la que se enmarca dicha unidad organizativa.

215. Los *Certificados* emitidos bajo esta *Política de Certificación* son válidos como sistemas de identificación y creación de *Sello electrónico* de Administración Pública, órgano, organismo o entidad de derecho público, de conformidad con la Ley 40/2015, de 1 de octubre, de

Régimen Jurídico del Sector Público y con la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, a los efectos de identificación y autenticación de la competencia en la actuación administrativa automatizada y la actuación judicial automatizada.

216. La *Ley de Emisión* de estos *Certificados* podrá determinar, en defecto de normativa específica, las condiciones de uso y régimen de estos *Certificados* que permitirán la atribución a las Administraciones, organismos y entidades de los diferentes actos y resoluciones realizados por los *Creadores del Sello electrónico*. Todo ello, sin modificación legal o variación respecto de la actuación que vienen realizando estos *Creadores* en los soportes tradicionales en papel u otros.

### 14.1.4. Responsabilidad y obligaciones de las partes

217. Las obligaciones y responsabilidades expresadas en este apartado se entienden sin perjuicio de las correspondientes derivadas de la legislación y normativa de aplicación, específicamente de las aplicables a la FNMT-RCM como *Prestador de Servicios de Confianza* y que para tal condición se establecen en el articulado del Reglamento eIDAS, en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y su reglamentación de desarrollo.

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

- Los *Suscriptores*: la Administración, organismos, entidades públicas representadas a través de los diferentes órganos competentes.
- Los custodios de los *Certificados* y de los *Datos de Creación de Sello*: *Personal al servicio de la Administración Pública* que realiza la solicitud del *Certificado* y/o el *Responsable de Operaciones de Registro* correspondiente.
- FNMT-RCM, en cuanto *Prestador de Servicios de Confianza.*
- En su caso, resto de *Comunidad Electrónica* y terceros

219. El régimen de derechos y obligaciones de las Administraciones, organismos, entidades públicas y la FNMT-RCM se regirá mediante el correspondiente acuerdo o convenio regulador de la prestación de los servicios de certificación. En estos acuerdos o convenios podrá establecerse la *Ley de Emisión* de estos *Certificados*.

220. Con carácter general y de forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la *DGPC*, las entidades públicas *Suscriptoras*, representadas a través de los diferentes órganos competentes y la *Oficina de Registro* que actúan para la solicitud de emisión de este tipo de *Certificados* a la FNMT-RCM tienen la obligación de:

- No realizar registros o tramitar solicitudes de *Certificados de Sello electrónico* emitidos bajo esta política, por parte de personal que preste sus servicios en una entidad diferente a la que representa como *Oficina de Registro.*
- No realizar registros o tramitar solicitudes de *Certificados* emitidos bajo esta política y cuya titularidad, referida al órgano de la administración, se corresponda con una entidad de la administración pública sobre la que no tenga potestades o no tenga competencias para actuar como *Oficina de Registro*.

- No realizar registros o tramitar solicitudes de *Certificados*, emitidos bajo esta política, para una unidad organizativa que no sea dependiente del órgano de la administración *Suscriptora* del *Certificado.*
- No realizar registros o tramitar solicitudes de *Certificados* emitidos bajo esta política y cuyo *Solicitante* se corresponda con una *persona física* que no sea el máximo responsable de la unidad organizativa a consignar en el *Certificado*, salvo que se trate del *Responsable de Operaciones de Registro*.
- Comprobar fehacientemente los datos identificativos del *Solicitante,* representante del *Suscriptor* del *Certificado*, y verificar su pertenencia a la unidad organizativa como máximo responsable de ésta.
- Revocar el *Certificado* emitido bajo esta política cuando alguno de los datos referidos a los *Suscriptores* del *Certificado*
  - sea incorrecto o inexacto, o
  - la *persona física* (custodio) representante del *Suscriptor* del *Certificado*, no sea un responsable con capacidad suficiente de la unidad organizativa consignada en él, o
  - la denominación de la unidad organizativa consignada en el *Certificado* sea inexacta o no se corresponda con una unidad operativa.
- No utilizar el *Certificado* cuando sean inexactos o incorrectos:
  - alguno de los datos referidos a su condición de responsable con capacidad suficiente de la unidad organizativa consignada en el *Certificado,* o
  - los datos de pertenencia al órgano administrativo *Suscriptor* del *Certificado,* o
  - cualquier otro dato que refleje o caracterice la relación de éste con la unidad organizativa u órgano de la administración consignado en el *Certificado.*

221. Las relaciones de la FNMT-RCM y el *Suscriptor* quedarán determinadas principalmente a los efectos del régimen de uso de los *Certificados* a través del documento relativo a las condiciones de utilización o, en su caso, contrato de emisión del *Certificado* y por la tipificación de los acuerdos o convenios o documento de relación entre la FNMT-RCM y el órgano, organismo o entidad pública.

222. El resto de la *Comunidad Electrónica* y los terceros regularán sus relaciones con la FNMT-RCM a través de la *DGPC*, y, en su caso, a través de estas *Políticas de Certificación y Prácticas de Certificación Particulares*. Todo ello, sin perjuicio de lo dispuesto en la normativa sobre firma electrónica y demás normativa que resulte de aplicación.

223. FNMT-RCM no será responsable de la comprobación de la pertenencia de la unidad organizativa a consignar en el *Certificado* al órgano de la administración *Suscriptora* del *Certificado* ni de la pertenencia del *Solicitante* a la unidad organizativa como máximo responsable de ésta, correspondiendo esta actividad y responsabilidad de comprobación a la *Oficina de Registro*. FNMT-RCM considerará representante del órgano, organismo o entidad de la administración *Suscriptora* del Certificado, salvo que sea informada de lo contrario al *Responsable de Operaciones de Registro* correspondiente.

224. FNMT-RCM no será responsable de la utilización de los *Certificados* emitidos bajo esta política cuando los representantes del *Suscriptor* del *Certificado* electrónico realicen actuaciones sin facultades o extralimitándose de las mismas.

### 14.1.5. Límites de uso de los Certificados de Sellos electrónicos

225. Constituyen límites de uso de este tipo de *Certificados* la creación de sellos electrónicos de Administración Pública, organismo o entidad de derecho público, de conformidad con la Ley 40/2015, y con la Ley 18/2011, de 5 de julio, para la identificación y autenticación del ejercicio de la competencia y en la actuación administrativa / judicial automatizada de la unidad organizativa perteneciente a una Administración, organismo o entidad pública.

226. La FNMT-RCM y la Administración, organismos y entidades podrán fijar en los acuerdos o convenios, o a través del documento de relación correspondiente o, si fuera procedente en la *Ley de Emisión* de estos *Certificados*, otros límites adicionales.

227. Para poder usar los *Certificados de Sello electrónico* dentro de los límites señalados y de forma diligente, se deberá previamente formar parte de la *Comunidad Electrónica*, y adquirir la condición de *Entidad Usuaria*.

228. En cualquier caso, si un tercero desea confiar en la firma electrónica realizada con uno de estos *Certificados* sin acceder a los servicios de comprobación de la vigencia de los *Certificados* emitidos bajo esta *Política de Certificación*, no se obtendrá cobertura de las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares*, y se carecerá de legitimidad alguna para reclamar o emprender acciones legales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado*.

229. Además, no se podrán emplear este tipo de *Certificados,* para:

- Firmar o sellar otro *Certificado*.
- Usos particulares o privados.
- Firmar o sellar software o componentes.
- Generar sellos de tiempo para procedimientos de *Fechado electrónico* sin autorización previa y expresa de la FNMT-RCM.
- Generar *Listas de Revocación* o prestar servicios de *OCSP.*
- Cualquier uso que exceda de la finalidad de este tipo de *Certificados* sin la autorización previa de la FNMT-RCM.

## 14.2. PRÁCTICAS DE CERTIFICACIÓN PARTICULARES PARA LOS CERTIFICADOS DE SELLO ELECTRÓNICO

230. La FNMT-RCM en su labor como *Prestador de Servicios de Confianza* y para demostrar la necesaria fiabilidad para la prestación de dichos servicios, cuenta con una *Declaración de Prácticas de Certificación* cuyo objeto es la información pública sobre las condiciones generales de prestación de los mismos.

231. En especial deberá tenerse presente, a efectos interpretativos del presente documento el apartado “Definiciones” del cuerpo principal de la *DGPC*.

232. El presente documento trae causa y forma parte integrante de la *Declaración de Prácticas de Certificación* de la FNMT-RCM y define el conjunto de prácticas particulares adoptadas por la FNMT-RCM como *Prestador de Servicios de Confianza* para la gestión del ciclo de vida de los *Certificados de Sello electrónico* de la Administración Pública, organismos públicos o entidades de derecho público, expedidos bajo la *Política de Certificación* identificada con el OID 1.3.6.1.4.1.5734.3.3.9.1.

### 14.2.1. Servicios de Gestión de las *Claves*

233. La FNMT-RCM no genera ni almacena las *Claves Privadas* asociadas a los *Certificados* expedidos bajo la presente *Política de Certificación*, que son generadas bajo el exclusivo control del *Responsable de Operaciones de Registro* o la persona autorizada por éste.

### 14.2.2. Gestión del ciclo de vida de los Certificados

#### *14.2.2.1. Registro de los Suscriptores*

234. Con carácter previo al establecimiento de cualquier relación institucional con los *Suscriptores*, la FNMT-RCM informa, a través de los medios y direcciones web citadas en estas *Prácticas de Certificación Particulares* y, subsidiariamente, en la *DGPC*, acerca de las condiciones del servicio, así como de las obligaciones, garantías y responsabilidades de las partes implicadas en la expedición y uso de los *Certificados* por ella emitidos en su labor como *Prestador de Servicios de Confianza*.

235. La FNMT-RCM, en su actividad como *Prestador de Servicios de Confianza,* a través de las *Oficinas de Registro,* procede a la identificación de los *Solicitantes* de los C*ertificados de Sello electrónico* de la Administración Pública, organismos y entidades de derecho público mediante aquellos procedimientos que así se dispongan para ello. FNMT-RCM considerará con competencia al efecto cualquier solicitud que venga realizada por el *Responsable de Operaciones de Registro* correspondiente, en su condición de representante del *Suscriptor*.

236. La FNMT-RCM recabará de los *Solicitantes* solo aquella información, recibida de la *Oficina de Registro*, que sea necesaria para la expedición de los *Certificados* y para la comprobación de la identidad, legitimidad y competencia de los representantes, almacenando la información legalmente exigida durante el periodo de quince (15) años, tratándola con la debida diligencia para el cumplimiento de la legislación nacional vigente en materia de protección de datos de carácter personal.

237. La FNMT-RCM no genera el par de *Claves* asociado a los *Certificados* expedidos bajo la presente *Política de Certificación*, poniendo todos los mecanismos necesarios durante el proceso de *Solicitud de Certificados* para posibilitar que el *Responsable de Operaciones de Registro* y/o el representante del *Suscriptor* se encuentran en posesión de la *Clave Privada* asociada a la *Clave Pública* que se certificará.

#### *14.2.2.2. Procedimiento de solicitud del Certificado*

238. A continuación se describe el procedimiento de solicitud del *Certificado* por el que se toma la denominación oficial de las unidades administrativas pertenecientes a la Administración, organismo o entidad pública, que serán los *Suscriptores* de los *Certificados de Sello*

*electrónico*, se toman los datos personales de los representantes de los *Suscriptores*, que tendrán legitimación y competencia suficientes para solicitar y obtener el *Certificado*, se confirma su identidad, vigencia del cargo o empleo y se formaliza, entre el representante del *Suscriptor* y la FNMT-RCM, el documento de condiciones de utilización o el contrato tipo de emisión, para la posterior expedición de un *Certificado de Sello electrónico*.

239. Se hace constar que FNMT-RCM, en función de la relación de *Solicitantes* habilitados remitida por la Administración, organismo o entidad pública, considerará, bajo responsabilidad de los correspondientes órganos, organismos y/o entidades que actuarán a través de las *Oficinas de Registro*, que dichos *Solicitantes* cumplen los requisitos establecidos en la presente Declaración y, por tanto, tienen la legitimidad y competencia necesarias para solicitar y obtener el *Certificado de Sello electrónico*. La FNMT-RCM presumirá con facultades y competencia suficientes a los representantes de los *Suscriptores* que tengan encomendada la responsabilidad de la *Oficina de Registro*.

240. Con carácter previo el *Solicitante* y el representante del *Suscriptor* deberán consultar la *DGPC* y las presentes *Políticas de Certificación y Prácticas de Certificación Particulares* en la dirección

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

con las condiciones de uso y obligaciones para las partes, pudiendo realizar las consultas que estimen oportunas sobre el alcance de esta Declaración; todo ello, sin perjuicio de que, con posterioridad, el representante del *Suscriptor* deba suscribir el documento de condiciones de utilización o si procede el contrato de emisión. En ningún caso la continuación del procedimiento de solicitud implicará la conclusión del proceso.

241. El *Solicitante*, como representante del *Suscriptor,* (o la persona autorizada por éste para este fin), que habitualmente será el *Responsable de Operaciones de Registro* correspondiente, genera las *Claves Pública* y *Privada* que serán vinculadas al *Certificado* y compone una solicitud electrónica del *Certificado*, que incluye la *Clave Pública*, generalmente en formato PKCS#10.

242. Dicho *Solicitante* se identifica, mediante un *Certificado de firma electrónica* de los admitidos para tal fin, en el *sitio web* de la FNMT-RCM, a través de la dirección

https://apuc20.cert.fnmt.es/PreregistroComponentes/indexCRDinamicos.jsp

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

244. La FNMT-RCM, tras comprobar que el *Solicitante* ha sido habilitado por el representante del *Suscriptor* para llevar a cabo dicha solicitud, le muestra un formulario en el que deberá introducir los datos del órgano *Suscriptor* para el cual se emitirá el *Certificado* y del que depende la unidad organizativa, así como los datos de la *persona física* en su condición de responsable de la custodia diligente de la *Clave privada* asociada al *Certificado* y la solicitud electrónica generada anteriormente. Toda esta información es firmada por el *Solicitante* con los *Datos de creación de firma* asociados a su *Certificado de firma electrónica* y remitida a la FNMT-RCM.

245. FNMT-RCM asignará e indicará al *Solicitante* un código de solicitud para su utilización posterior. Adicionalmente, el Solicitante suscribe las condiciones de utilización o, en su caso, contrato de solicitud del *Certificado*, cuya custodia recae en la *Oficina de Registro*.

246. Esta información no dará lugar a la generación de un *Certificado* por parte de la FNMT-RCM, en tanto que ésta no reciba la declaración responsable, en cuanto al cumplimiento de los procedimientos aquí descritos y la veracidad de los datos incluidos en la solicitud, firmada por el *Responsable de Operaciones de Registro*.

247. La FNMT-RCM, tras recibir esta información, comprobará la validez de la información de la solicitud firmada, así como la posesión y correspondencia de la pareja de *Claves* criptográficas asociadas al *Certificado de Sello electrónico* y el tamaño de las mismas.

*14.2.2.3. Extensión de la función de registro*

248. La FNMT-RCM, podrá acordar con las Administraciones, organismos y entidades públicas que así lo soliciten, la creación de *Oficinas de Registro* delegadas con el fin de centralizar la realización de los procedimientos de registro con destino a otras Administraciones, vinculadas o dependientes, que no dispongan de medios suficientes para hacerlo en aplicación de las leyes sobre racionalización del gasto.

*14.2.2.4. Emisión del Certificado de Sello electrónico*

249. La FNMT-RCM recibe la declaración responsable, en cuanto al cumplimiento de los procedimientos aquí descritos y la veracidad de los datos incluidos en la solicitud, firmada por el *Responsable de Operaciones de Registro*, y que incluye el código de solicitud. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

250. A continuación, la FNMT-RCM comprueba los datos que confirman la relación del representante con la Administración Pública, para proceder posteriormente a la emisión del *Certificado*.

251. La FNMT-RCM en ningún caso incluirá en un *Certificado* información distinta de la aquí mostrada, ni límites distintos a los previstos en los acuerdos, convenios y, en su caso, a los previstos en la *Ley de Emisión* correspondiente.

252. En cualquier caso, la FNMT-RCM actuará diligentemente para:

- Comprobar que el *Solicitante* del *Certificado* o el *Responsable de Operaciones de Registro* utilicen la *Clave Privada* correspondiente a la *Clave Publica* vinculada al *Certificado.*
- Lograr que la información incluida en el *Certificado* se base en la información proporcionada por el *Solicitante* y/o por el *Responsable de Operaciones de Registro* correspondiente.
- No ignorar hechos notorios que puedan afectar a la fiabilidad del *Certificado.*
- Lograr que el *DN* (nombre distintivo) asignado en el *Certificado* sea único en toda la *Infraestructura de Clave Pública* de la FNMT-RCM.

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

1. Composición de la estructura de datos que conforman el *Certificado de Sello electrónico.*

   Con los datos recogidos durante el proceso de solicitud del *Certificado*, se procede a componer el nombre distintivo (*DN*) conforme al estándar *X.500*, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades. No se contempla el uso de seudónimos como forma de identificación del *Suscriptor*.

   El atributo *CN* contiene la denominación del sistema o de la aplicación del proceso automático para el que se expide el *Certificado*.

2. Generación del *Certificado* conforme al Perfil del *Certificado de Sello electrónico*

   El formato del *Certificado de Sello electrónico* expedido por la FNMT-RCM bajo la presente *Política de Certificación*, en consonancia con la norma UIT-T X.509 versión 3 y de acuerdo con la normativa legalmente aplicable en materia de *Certificados Cualificados*, puede consultarse en la página http://www.cert.fnmt.es/dpcs/

*14.2.2.5. Información de la emisión del Certificado*

254. Una vez emitido el *Certificado*, FNMT-RCM envía una comunicación a la dirección de correo electrónico del responsable del sistema o de la aplicación del proceso automático para el que se expide el *Certificado,* anunciando que está disponible para su descarga.

*14.2.2.6. Descarga e instalación del Certificado*

255. En un plazo máximo de 72 horas desde la recepción en la FNMT – RCM de la documentación necesaria para realizar las comprobaciones ya comentadas de forma previa a la expedición del *Certificado*, la FNMT-RCM pondrá a disposición del *Solicitante* un mecanismo de descarga del *Certificado*, en la dirección de titularidad de la Administración u organismo, a través del siguiente enlace:

https://apuc20.cert.fnmt.es/PreregistroComponentes/indexCRDinamicos.jsp

256. En este proceso guiado se le pedirá al *Responsable de Operaciones de Registro* del ámbito del *Suscriptor* que introduzca el NIF del órgano, organismo o entidad pública con el que realizó el proceso de solicitud, así como el código de solicitud asignado al finalizar dicho proceso. Si el *Certificado* no ha sido aún generado por cualquier motivo, se le indicará este hecho en el momento que intente su descarga.

257. El *Certificado* puesto a disposición del *Personal al servicio de la Administración Pública* o de la *Oficina de Registro*, será introducido directamente en el soporte en el que se generaron las *Claves* durante el proceso de solicitud.

*14.2.2.7. Vigencia del Certificado de Sello electrónico*

**14.2.2.7.1. Caducidad**

258. Los *Certificados de Sello electrónico* emitidos por la FNMT-RCM tendrán validez durante un período de tres (3) años contados a partir del momento de la emisión del *Certificado*, siempre y cuando no se extinga su vigencia. Transcurrido este período y si el *Certificado*

sigue activo, caducará, siendo necesaria la emisión de uno nuevo en caso de que el *Suscriptor* desee seguir utilizando los servicios del *Prestador de Servicios de Confianza*.

#### 14.2.2.7.2. Extinción de la vigencia del Certificado

259. Los *Certificados de Sello electrónico* emitidos por la FNMT-RCM quedarán sin efecto en los siguientes casos:

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

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

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

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

260. A los efectos enumerados anteriormente, se hace constar que la solicitud de emisión de un *Certificado de Sello electrónico* emitido por la FNMT-RCM cuando exista otro vigente a favor del mismo *Suscriptor* y perteneciente a la misma *Ley de Emisión* no conllevará la revocación del primero obtenido.

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

### *14.2.2.8. Revocación del Certificado de Sello electrónico*

#### 14.2.2.8.1. Causas de revocación

262. Adicionalmente a lo previsto en el apartado "Extinción de la vigencia del *Certificado*" en relación con la solicitud de un *Certificado* existiendo otro en vigor a favor del mismo *Firmante* y mismo *Suscriptor* y perteneciente a la misma *Ley de Emisión*, serán causas de revocación de un *Certificado de Sello electrónico*:

a) La solicitud de revocación por parte de las personas autorizadas. En todo caso deberá dar lugar a esta solicitud:

- La pérdida del soporte del *Certificado*.
- La utilización por un tercero de la *Clave Privada* asociada al *Certificado*.
- La violación o puesta en peligro del secreto de la *Clave Privada* asociada al *Certificado*.
- La no aceptación de las nuevas condiciones que puedan suponer la emisión de nuevas *Declaraciones de Prácticas de Certificación*, durante el periodo de un mes tras su publicación.

b) Resolución judicial o administrativa que así lo ordene.

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

d) Terminación de la forma de representación del representante del *Suscriptor* del *Certificado.*

e) Incapacidad sobrevenida, total o parcial, del representante del *Suscriptor*.

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

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

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

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

263. 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.

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

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

265. Las actuaciones constitutivas de delito o falta de las que no tenga conocimiento la FNMT-RCM que se realicen sobre los datos o el *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.

#### 14.2.2.8.2. Efectos de la revocación

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

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

#### 14.2.2.8.3. Procedimiento para la revocación de Certificados

268. La solicitud de revocación de los *Certificados de Sello electrónico* podrá efectuarse durante el período de validez que consta en el *Certificado*.

269. La revocación de *Certificados* consiste en la cancelación de la garantía de identidad, autenticidad u otras propiedades del *Suscriptor* y sus representantes y su correspondencia con la *Clave pública* asociada. Implica, además de su extinción, la finalización de la relación y régimen de uso del *Certificado* con la FNMT-RCM

270. Estarán legitimados para solicitar la revocación de un *Certificado de Sello electrónico*, con base en la inexactitud de datos, variación de los mismos o cualquier otra causa a valorar por el *Suscriptor*:

- El órgano directivo de la Administración Pública, organismo público o entidad de derecho público, o personas en quien deleguen.
- La *Oficina de Registro*, —a través de su responsable— que esté designada a tal efecto, por la Administración, organismo o entidad de derecho público, *Suscriptora* del *Certificado* a revocar, cuando detecte que alguno de los datos consignados en el *Certificado*
  - es incorrecto, inexacto o haya variado respecto a lo consignado en el *Certificado,* o
  - la persona física, custodio del *Certificado* no se corresponda con el responsable máximo o designado de la unidad organizativa, órgano, organismo o entidad pública consignada en el *Certificado,* o
  - la unidad organizativa consignada en el *Certificado* no depende organizativamente del órgano, organismo o entidad pública a la que se ha expedido el *Certificado*

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

271. A continuación, se describe el procedimiento a observar por la *Oficina de Registro* por el que se formaliza la solicitud de revocación de un *Certificado*. En todo caso FNMT-RCM, presumirá la competencia y capacidad del *Solicitante* cuando se trate del *Responsable de Operaciones de Registro* correspondiente.

1. Personación del *Solicitante* ante la *Oficinas de Registro*

   Para revocar el *Certificado*, el *Solicitante* con capacidad y competencia suficientes, se personará ante una *Oficina de Registro* designada a tal efecto por el órgano, organismo o entidad *Suscriptora* del *Certificado* a revocar o se realizará directamente por el *Responsable de Operaciones de Registro*.

2. Comparecencia y documentación

   El *Solicitante* aportará los datos que se le requieran y que acrediten:

- su identidad personal,
- su condición de *Personal al servicio de la Administración Pública, Suscriptora* del *Certificado* o su condición de *Responsable de Operaciones de Registro*.
- su condición de máximo responsable o persona designada de la unidad organizativa consignada en el *Certificado* y dependiente de la administración *Suscriptora* del *Certificado* o de personal adscrito a la *Oficina de Registro* designada a tal efecto por el organismo o entidad *Suscriptora* del *Certificado* a revocar.

FNMT-RCM admitirá, en todo caso, la función e informe que realice la *Oficina de Registro* designada por la Administración. En el caso de que no se acrediten los puntos anteriores, la *Oficina de Registro* no procederá con la solicitud de revocación del *Certificado.*

3. Envío de la solicitud de revocación a la FNMT-RCM y tramitación

   Sin que existan causas notorias de falta de competencia del *Responsable de Operaciones de Registro* y/o una vez confirmada la identidad del *Solicitante*, vigencia de las condiciones exigidas a éste y suscrito el documento de solicitud de revocación, la *Oficina de Registro* procederá a validar los datos y a enviarlos a la FNMT-RCM para la revocación efectiva del *Certificado*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

   Dicho envío sólo se producirá si la *Oficina de Registro* tiene potestad para actuar como tal en nombre del órgano, organismo o entidad de la Administración Pública *Suscriptora* del *Certificado* y si éste es responsable o tiene competencia suficiente sobre la unidad organizativa consignada en el *Certificado.*

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

272. Adicionalmente, existe un servicio de atención telefónica, en horario 24 x 7, en el teléfono 902 200 616, al que se pueden dirigir las solicitudes de revocación. La comunicación quedará grabada y registrada, sirviendo de soporte y garantía de la aceptación de la solicitud de revocación solicitada.

273. Para solicitar una revocación telefónica de un *Certificado*, el *Solicitante* de la misma debe ser el representante del *Suscriptor*.

274. Una vez que la FNMT-RCM ha procedido a la revocación del *Certificado*, se publicará en el *Directorio* seguro la correspondiente *Lista de Certificados Revocados,* conteniendo el número de serie del *Certificado* revocado, así como la fecha, hora y la causa de revocación. El responsable del *Suscriptor* recibirá, a través de la dirección de correo electrónico consignada en la solicitud, la notificación del cambio de estado de vigencia del *Certificado*.

*14.2.2.9. Suspensión del Certificado de Sello electrónico*

275. No se contempla.

*14.2.2.10. Información del cambio de estado del Certificado*

276. Una vez se ha hecho efectiva la revocación del *Certificado,* FNMT-RCM envía una comunicación a la dirección de correo electrónico del responsable del sistema o de la aplicación del proceso automático para el que se expide el *Certificado,* informando del cambio de estado del *Certificado.*

*14.2.2.11. Renovación del Certificado Sello electrónico*

277. La renovación del *Certificado de Sello electrónico* se realiza siempre emitiendo nuevas claves, por lo que el proceso es realmente el mismo que el seguido para la obtención de un *Certificado* nuevo.

*14.2.2.12. Comprobación del estado del Certificado*

278. El *Suscriptor* del *Certificado,* las Administraciones, organismos y entidades usuarias pertenecientes a la *Comunidad Electrónica* y terceros que confían podrán realizar la comprobación del estado de un *Certificado* en la forma y condiciones que se expresan en este apartado.

279. El estado del *Certificado de Sello electrónico* se podrá comprobar bien a través del acceso a las *Listas de Revocación*, bien a través del *Servicio de información y consulta del estado de los certificados* a través de OCSP.

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

281. El funcionamiento del *Servicio de información y consulta del estado de los certificados* es el siguiente: el servidor OCSP recibe la petición OCSP efectuada por un *Cliente OCSP* y comprueba el estado de vigencia de los *Certificados* incluidos en la misma. En caso de que la petición sea válida, se emitirá una respuesta de OCSP informando acerca del estado en el que se encuentran en ese momento los *Certificados* incluidos en la petición. Dicha respuesta es firmada / sellada con los *Datos de Creación de Firma* / *Sello* de la FNMT-RCM garantizando así la integridad y la autenticidad de la información suministrada sobre el estado de revocación de los *Certificados* consultados.

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

## 15. TARIFAS

283. FNMT-RCM aplicará a las Administraciones Públicas las tarifas aprobadas por la Subsecretaría de la cual depende para la prestación de los servicios de confianza o, en su defecto, las tarifas acordadas en el convenio o encomienda de gestión formalizado para tal efecto.

## ANEXO I: IDENTIFICACIÓN DE CERTIFICADOS DE AUTORIDADES DE CERTIFICACIÓN

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

**Certificado de la Autoridad de Certificación "AC Administración Pública"**

Nombre distintivo: CN = AC Administración Pública, serialNumber = Q2826004J, OU = CERES, O = FNMT-RCM, C = ES

- Jerarquía SHA-1
  - Número de serie: 01
  - Período de validez desde: viernes, 21 de mayo de 2010
  - Período de validez hasta: sábado, 21 de mayo de 2022
  - Huellas digitales:
    - Huella digital (sha1):

      1C:5B:FA:A3:DD:E8:C5:A4:A9:09:D1:10:37:A5:0A:EC:0B:4B:21:EC
    - Huella digital (sha256):

      18:A4:3C:51:D0:81:74:C3:A6:D8:5F:1C:13:18:BD:29:09:75:3E:75:D9:1C:F6:59:9F:73:34:7B:00:70:28:90

- Jerarquía SHA-256
  - Número de serie: 02
  - Período de validez desde: viernes, 21 de mayo de 2010
  - Período de validez hasta: sábado, 21 de mayo de 2022
  - Huellas digitales:
    - Huella digital (sha1):

      73:20:B5:52:7A:A9:D4:B0:26:E8:0F:9F:7A:92:E8:A4:A4:A7:24:62
    - Huella digital (sha256):

      83:0F:F2:05:AE:69:48:50:59:C3:FB:23:76:A7:F2:F9:EE:1C:2A:61:DE:25:9D:D0:9D:0B:B6:AD:69:F8:88:32