ENCARGO A LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA (FNMT-RCM) CONSISTENTE EN LA PRESTACIÓN DE SERVICIOS ELECTRÓNICOS DE CONFIANZA A LA ADMINISTRACIÓN GENERAL DEL ESTADO Y A DETERMINADOS ORGANISMOS PÚBLICOS Y ENTIDADES DEPENDIENTES.

En Madrid, a 18 de febrero de 2021

Doña María del Pilar Paneque Sosa, Subsecretaria del Ministerio de Hacienda, en nombre y representación de la Administración General del Estado y actuando en virtud de las competencias atribuidas por el Real Decreto 689/2020, de 21 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y se modifica el Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales y la Orden HAC/316/2019, de 12 de marzo, de delegación de competencias y por la que se fijan los límites de las competencias de gestión presupuestaria y concesión de subvenciones y ayudas de los titulares de las Secretarías de Estado, formaliza el presente encargo a la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (en adelante, FNMT-RCM), para la prestación de servicios electrónicos de confianza a la Administración General del Estado, así como a determinados organismos públicos y entidades del sector público dependientes, de acuerdo con los siguientes,

ANTECEDENTES

PRIMERO. Que la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, establece las bases de regulación de la firma electrónica, su eficacia

jurídica y la prestación de servicios de certificación, tanto para el Sector público como el privado.

SEGUNDO. Que, de acuerdo con el artículo 2.1. g) de su Estatuto, aprobado por el Real Decreto 1114/1999, de 25 de junio, entre los fines de la FNMT-RCM se encuentra la prestación, en el ámbito de las Administraciones públicas y sus organismos públicos, vinculados o dependientes, de servicios de seguridad, técnicos y administrativos, en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT), así como la expedición, fabricación y suministro de los títulos o certificados de usuario o soportes en tarjeta necesarios a tal fin, de acuerdo con lo establecido en el citado artículo 81 de la Ley 66/1997 y en su normativa de desarrollo o, en su caso, en los términos que establezcan las disposiciones legales correspondientes.

TERCERO. Que la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, ha venido a establecer una regulación completa y sistemática de las relaciones entre las Administraciones y los administrados, que incluye los sistemas de identificación y firma electrónicas a utilizar, tanto por parte de los interesados en el procedimiento administrativo como de las Administraciones Públicas mientras que, por su parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ha establecido las bases de su funcionamiento electrónico.

A tal objeto, la FNMT-RCM viene prestando servicios técnicos y administrativos necesarios para la identificación y autenticación de los intervinientes en las comunicaciones electrónicas de las Administraciones Públicas, a través del uso de certificados de firma electrónica dirigidos tanto a los interesados en el procedimiento administrativo como a funcionarios y demás empleados públicos, así como certificados de sede electrónica y certificados de sello electrónico.

CUARTO. Que el Reglamento (UE) n.º 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),

establece las condiciones en que los Estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro, así como las normas para los servicios de confianza y un marco jurídico 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.

QUINTO. Que en aplicación de la disposición adicional sexta de la Ley 17/2012, de 27 de diciembre, de Presupuestos Generales del Estado para el año 2013 y del Informe elaborado por la Comisión para la Reforma de la Administraciones Públicas (CORA) en junio de 2013, la prestación de los servicios de certificación, firma y de administración electrónica que presta la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda en el ámbito de la Administración General del Estado se ha venido instrumentando a través de diversas Encomiendas de Gestión y Encargos a Medios Propios formalizadas por la Subsecretaría de Hacienda desde 2014.

SEXTO. Que, asimismo, de conformidad con la disposición adicional quincuagésimo quinta de la Ley 9/2017, de 8 de noviembre, de contratos del sector público, introducida por el Real Decreto-ley 11/2020, de 31 de marzo, por el que se adoptan medidas urgentes complementarias en el ámbito social y económico para hacer frente al COVID-19, establece en su apartado 5º que *la persona titular del Ministerio de Hacienda, en los supuestos y con el alcance subjetivo que determine, podrá realizarle encargos de forma centralizada a favor de aquellos entes, organismos y entidades para los que la FNMT-RCM sea medio propio conforme a las previsiones de la citada Ley 9/2017. Estos encargos se financiarán conforme a lo previsto en la disposición adicional undécima de la Ley 36/2014, de 26 de diciembre, de Presupuestos Generales del Estado para 2015 y en la disposición adicional vigésimo tercera de la ley 47/2003, de 26 de noviembre, General Presupuestaria*.

SÉPTIMO. Que, de acuerdo con la cláusula cuarta del Encargo a la FNMT-RCM consistente en la prestación de servicios electrónicos de confianza a la AGE y a determinados organismos públicos y entidades dependientes de 28 de

febrero de 2019, así como de su Adenda de Modificación y Prórroga del Encargo de 28 de febrero de 2020, la vigencia del mismo finaliza el 28 de febrero de 2021.

OCTAVO. Que la ejecución de los citados encargos ha puesto de manifiesto su utilidad como instrumento de simplificación administrativa, reducción de costes y homogenización de los servicios prestados por la FNMT-RCM al conjunto de la Administración General del Estado, así como la conveniencia de aprobar un nuevo texto que precise los servicios que, efectivamente, se financiarán con cargo al crédito aprobado en el subconcepto 22109 -*Labores Fábrica Nacional Moneda y Timbre*- del Servicio 01 –Dirección General de Racionalización y Centralización de la Contratación- de la Sección 10 –Contratación Centralizada-, programa presupuestario 923 R "Contratación Centralizada", de los Presupuestos Generales del Estado vigentes.

NOVENO. Que, de conformidad con el artículo 7.4.b) de la Orden HAC/316/2019, de 12 de marzo, de delegación de competencias y por la que se fijan los límites de las competencias de gestión presupuestaria y concesión de subvenciones y ayudas de los titulares de las Secretarías de Estado, por delegación del Ministro de Hacienda, corresponde a la persona titular de la Subsecretaría del Ministerio de Hacienda, la competencia para formalizar los encargos a que se refiere el artículo 32 de la Ley 9/2017, de 8 de noviembre de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, no delegada en otros órganos del Departamento.

DÉCIMO. Que la FNMT-RCM tiene, en virtud del artículo 3.2 de su Estatuto, la condición de medio propio y servicio técnico de la Administración General del Estado, así como de los organismos, entes y entidades del sector público estatal, sean de naturaleza jurídica pública o privada.

En consecuencia, en atención a las circunstancias y fundamentos expuestos, al amparo de lo dispuesto en el mencionado artículo 32 y en la disposición adicional quinquagésimo quinta de la Ley 9/2017, de 8 de noviembre de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo

2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, la Subsecretaria de Hacienda formaliza el presente encargo, con arreglo a las siguientes,

CLÁUSULAS

PRIMERA. OBJETO

Constituye el objeto del presente encargo la prestación de las actividades y servicios que se especifican en el anexo, por parte de la FNMT-RCM a solicitud de la Administración General del Estado y a los organismos y entidades del sector público vinculadas o dependientes de la misma incluidos en la cláusula segunda, y consistentes en:

a) Servicios técnicos, administrativos y de seguridad necesarios para garantizar la validez y eficacia de la emisión y recepción de comunicaciones y documentos producidos a través de técnicas y medios EIT (servicios de certificación y firma electrónica) en el ámbito competencial de los destinatarios del presente encargo, en las condiciones técnico-administrativas recogidas en el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, y sus normas de desarrollo, referidas en este encargo y detalladas en el capítulo I del anexo de la misma.

La FNMT-RCM proporcionará instrumentos de identificación, acreditación y firma para asegurar las comunicaciones en el ámbito EIT, como son los certificados de firma electrónica, a las personas físicas que actúan como interesados en el procedimiento administrativo de acuerdo con la normativa vigente y las cláusulas del presente encargo, con las administraciones destinatarias de los servicios previstos en aquél. A tal efecto, los Departamentos, organismos y entidades del sector público destinatarios de los servicios admiten los certificados electrónicos expedidos en virtud de del presente encargo por la FNMT-RCM, en calidad de Prestador Cualificado de Servicios de Confianza, como sistemas de identificación electrónica que permiten acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados en el procedimiento administrativo, así como la creación de firmas electrónicas.

Así mismo, la FNMT – RCM proporcionará certificados electrónicos de representante de persona jurídica, a solicitud de la Administración General del Estados o de los organismos y entidades del sector público vinculadas o dependientes de la misma incluidos en la cláusula segunda, como medio de identificación y firma electrónicas en su relación con el resto de Administraciones Públicas que los admitan para tales fines.

b) Servicios relativos a la identificación electrónica de las Administraciones Públicas y autenticación del ejercicio de su competencia, de conformidad con las Leyes 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, y normativa de desarrollo, en concreto, las actividades que se enumeran a continuación y en el capítulo II del anexo de este encargo.

La FNMT-RCM, a los efectos de lo dispuesto en las citadas Leyes 40/2015 y 18/2011 y sus normas de desarrollo, prestará los servicios comprendidos en el objeto de este encargo a Departamentos, organismos y entidades del sector público en los términos de las citadas Leyes y en los señalados en el capítulo II del anexo de este encargo, y con sujeción a lo establecido en la Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica, accesible en la dirección electrónica: http://www.cert.fnmt.es/dpcs/

Los servicios de identificación electrónica y autenticación de documentos electrónicos de las Administraciones Públicas se basarán en sistemas de identificación, firma y creación de sellos electrónicos en el ejercicio de la competencia en la actuación administrativa automatizada y en la actuación judicial automatizada. Dichos servicios se concretan en la expedición y gestión del ciclo de vida de los siguientes tipos de certificados electrónicos:

- Certificados de firma electrónica del personal al servicio de las Administraciones Públicas y Administración de Justicia.
- Certificados de firma electrónica con seudónimo del personal al servicio de las Administraciones Públicas.

- Certificados de firma electrónica con seudónimo del personal al servicio de la Administración de Justicia, específicamente aprobados por el Comité Técnico Estatal de la Administración Judicial Electrónica.
- Certificados de sello electrónico de Administración Pública, órgano, organismo o entidad de derecho público.
- Certificados para la identificación de sedes electrónicas.

Asimismo, la FNMT – RCM desarrollará soluciones de identificación y firma electrónicas en movilidad para los empleados al servicio de las Administraciones Públicas incluidas en el ámbito de aplicación del presente encargo.

c) La FNMT-RCM también prestará, a solicitud de los Departamentos, órganos, organismos y entidades del sector público, los siguientes servicios:

- Expedición de certificados de autenticación de sitio web, con los límites establecidos.
- Servicios de validación de certificados a través de la plataforma FNMT- RCM.
- Servicio de sellado de tiempo (creación de sellos cualificados de tiempo electrónicos).

Asimismo, podrán incorporarse al presente encargo, sin coste adicional, otros certificados electrónicos que desarrolle la FNMT – RCM con motivo de una sustitución de los certificados incluidos en la presente cláusula debido a exigencias de actualización normativa o tecnológica, siempre que resulten necesarios para la prestación por dicha Entidad de servicios de confianza y certificación electrónica a la Administración General del Estado y Organismos Públicos y entidades del sector público dependientes incluidos en la cláusula siguiente.

SEGUNDA. ÁMBITO DE APLICACIÓN

La FNMT-RCM prestará los servicios a que se refiere el presente encargo a los distintos Departamentos ministeriales, sus organismos autónomos, y a las siguientes entidades del sector público:

- Agencia Estatal de Administración Tributaria {AEAT).
- Agencia Estatal de Seguridad Aérea (AESA)-Dirección General de Aviación Civil.
- ENAIRE.
- RED.es
- Sociedad Estatal Aguas de las Cuencas Mediterráneas S.A. (ACUAMED).
- Agencia Estatal Boletín Oficial del Estado.
- Instituto Cervantes.
- Agencia Española de Protección de la Salud en el Deporte.

TERCERA. OBLIGACIONES DERIVADAS DE LA PRESTACIÓN EFECTIVA DE LOS SERVICIOS OBJETO DEL ENCARGO

1.- Para la prestación efectiva de los servicios objeto de este encargo la FNMT-RCM se compromete a:

- Aportar la infraestructura técnica, organizativa y de seguridad relacionada en el anexo de este encargo.
- Aportar los derechos de propiedad industrial e intelectual necesarios, garantizando su uso pacífico. La FNMT-RCM excluye cualesquiera licencias o sublicencias, a terceras partes o a los Departamentos, organismos y entidades del sector público destinatarios de los servicios del presente encargo para aplicaciones y sistemas de los mismos, o de terceros, distintas de las aportadas directamente por la FNMT-RCM, en virtud de este encargo.
- Prestar la asistencia técnica que se precise con objeto de facilitar la información necesaria para el buen funcionamiento de los sistemas, de conformidad con lo establecido en el anexo de este encargo.
- Actualizar tecnológicamente los sistemas de acuerdo con el estado de la técnica, así como mantener los servicios incluidos en el presente encargo conforme al Reglamento eIDAS, siempre que las disponibilidades presupuestarias de la FNMT-RCM lo permitan. Todo ello, sin perjuicio de la aprobación de los requisitos técnicos

correspondientes por la Secretaría General de Administración Digital o, en su caso, por el órgano competente.

- Emitir sellos de tiempo, según el estado de la técnica, en las comunicaciones electrónicas, informáticas y telemáticas que tengan lugar al amparo del presente encargo.

- Aportar la tecnología necesaria para que las obligaciones de los Departamentos, organismos y entidades del sector público destinatarios de los servicios del presente encargo puedan ser realizadas, en particular, las aplicaciones necesarias para la constitución de las Oficinas de Registro y la acreditación y la tramitación de las solicitudes relativas a los certificados electrónicos. Tales aplicaciones serán compatibles en función de los avances tecnológicos y el estado de la técnica.

- Tener disponible para consulta de los Departamentos, organismos y entidades del sector público destinatarios de los servicios y de los usuarios una Declaración de Prácticas de Certificación (DPC). Tal DPC, estará disponible en la dirección electrónica (URL) siguiente: http://www.cert.fnmt.es/dpcs

  Esta DPC podrá ser consultada por todos los interesados y podrá ser modificada por la FNMT-RCM, por razones legales o de procedimiento. Las modificaciones en la DPC serán comunicadas a los usuarios a través de su dirección electrónica: www.ceres.fnmt.es.

  Es necesario tener en cuenta, en todo caso, la parte general de la Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica y, para cada tipo de certificado o ámbito de actuación, su correspondiente Declaración de Políticas y Prácticas de Certificación Particulares aplicables específicamente.

- Asumir todas las obligaciones que resulten necesarias para la prestación de los servicios EIT, en especial, las establecidas por el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre

circulación de estos datos y por el que deroga la Directiva 95/46/CE (en lo sucesivo, Reglamento General de Protección de Datos) y las derivadas de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Mantener el secreto de las características técnicas de seguridad que deben reunir los productos, servicios y procedimientos aplicados, tanto en sus instalaciones y personal, como, en su caso, en las de entidades colaboradoras, aplicando, de conformidad con la normativa especial correspondiente y las normas de contratación aplicables a la entidad, las obligaciones de confidencialidad pertinentes, restringiendo la información y la publicidad de los diferentes elementos de seguridad, según los estándares aplicables y, en general, realizando la actividad encomendada implantando medidas especiales de seguridad, de conformidad con el estado de la técnica.

- Con el fin de que los certificados de servidor y de sede electrónica para la Administración General del Estado identifiquen adecuadamente a las respectivas sedes y portales frente a los ciudadanos, la FNMT-RCM realizará cuantas actuaciones resulten necesarias al objeto de mantener a sus autoridades de certificación dentro de la lista de confianza de los principales navegadores de internet y sistemas operativos de dispositivos móviles.

En cuanto a la prestación efectiva de los servicios de validación a través de la plataforma FNMT como parte integrante del servicio nacional de verificación de certificados, conjuntamente con la plataforma @firma de la AGE, la FNMT-RCM asume las siguientes obligaciones:

- Instalar en su infraestructura una copia de la plataforma federada de @firma con el objeto de preservar la total disponibilidad de los servicios ante fallos críticos en la infraestructura principal o de respaldar la plataforma @firma y ofrecer así las máximas garantías a la Administración General del Estado, así como con el fin de garantizar la compatibilidad, inmediatez en la actualización, contención del gasto y equidad en la evolución tecnológica.

- Ofrecer a través de la citada plataforma federada los mismos servicios de validación y verificación disponibles en la plataforma @firma de la AGE con equivalentes formas de invocación y comportamiento, con el objeto de asegurar la homogeneidad y ubicuidad en el uso de las plataformas por parte de los organismos usuarios.

- Adaptar de forma continua la citada plataforma según evolucione la plataforma @firma de la AGE conforme a las necesidades de los usuarios y a los obligados avances tecnológicos.

- Realizar una réplica periódica global de CRLs de certificados en la plataforma @firma de la AGE con el objeto de mantener la autonomía ante una contingencia con la plataforma propia de FNMT-RCM. Asimismo, asumirá que las réplicas de sus CRL en la plataforma @firma serán válidas hasta su fecha de caducidad o fecha estimada de nueva publicación, no siendo responsable dicha plataforma de las validaciones que se hagan con las CRL replicadas, aun en caso de existir versiones más actualizadas de las mismas a disposición de la FNMT-RCM.

- Realizar las pruebas de funcionamiento que sean precisas y las comprobaciones prácticas necesarias al objeto de asegurar la calidad, seguridad e interoperabilidad de los servicios y plataformas de validación referidos en este encargo.

En todo caso, los medios técnicos y tecnología empleados por la FNMT-RCM permitirán demostrar la fiabilidad del servicio de certificación electrónica, la constatación de la fecha y hora de expedición, suspensión o revocación de un certificado, la fiabilidad de los sistemas y productos (que contarán con la debida protección contra alteraciones y con los niveles de seguridad técnica y criptográfica idóneos dependiendo de los procedimientos donde se utilicen), la comprobación de la identidad del titular del certificado, a través de las Oficinas de Registro y acreditación autorizadas y, en su caso, -exclusivamente frente a la parte o entidad a través de la cual se ha identificado y registrado al titular del certificado- los atributos pertinentes, así como, en general, las actuaciones que resulten de aplicación de conformidad con la normativa

comunitaria o nacional correspondiente.

No obstante lo anterior, en la prestación de servicios del ámbito de las Leyes 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, las Oficinas de Registro, por las especialidades del derecho administrativo y de gestión y de conformidad con el artículo 11 del Real Decreto 1317/2001, de 30 de noviembre, por el que se desarrolla el artículo 81 de la ley 66/1997, en materia de prestación de servicios de seguridad en las comunicaciones de las Administraciones Públicas a través de técnicas y medios electrónicos, informáticos y telemáticos, con las Administraciones Públicas, no dependerán directamente de la FNMT-RCM sino del órgano u organismo público de origen, sin perjuicio de las funciones de comprobación, coordinación y control de gestión y de los protocolos de registro que realice la FNMT-RCM, en su condición de Prestador de Servicios de Certificación.

La FNMT-RCM se compromete, en el desarrollo y ejecución del presente encargo, a la aplicación, cuando sea procedente de acuerdo con el tipo de actividad realizada, de las disposiciones y recomendaciones relativas a los ámbitos normativos o programáticos sobre protección del medio ambiente, prevención de riesgos laborales, igualdad y no discriminación.

2.- En cuanto a los Departamentos, organismos y entidades del sector público destinatarios de los servicios del presente encargo, se comprometen a:

- Conservar las notificaciones, comunicaciones o documentación emitida y recibida por la FNMT-RCM en las transacciones relativas a la actividad de las oficinas de registro, durante el tiempo pertinente para hacer valer los derechos de las partes.
- Utilizar las aplicaciones proporcionadas por la FNMT-RCM para la provisión de los servicios de confianza, al objeto de garantizar la seguridad en el intercambio de información, mediante el cifrado de las comunicaciones emitidas y recibidas.
- Realizar las actividades de identificación previa a la obtención del certificado electrónico y, en su caso, de comprobación y suficiencia

de los atributos correspondientes, de los titulares de los certificados, así como del cargo y competencia de los firmantes correspondientes. Todo ello, a través de la Oficina de Registro y acreditación designada ante la FNMT-RCM, utilizando los procedimientos establecidos por esta entidad que figuran en la aplicación de Registro (aplicación Web) y de conformidad con las condiciones establecidas en las correspondientes DPC de la FNMT-RCM. Tales procedimientos son documentos sujetos a verificaciones y auditorías por lo que podrán ser modificados por la FNMT-RCM a los efectos de mejorar el servicio.

- Conservar, a su vez, durante el periodo de tiempo que defina la normativa aplicable, los formularios y documentos donde constan las condiciones para la solicitud, revocación y suspensión, en su caso, de certificados electrónicos emitidos por la FNMT-RCM en el ámbito de las Leyes 39/2015, de 1 de octubre, 40/2015, de 1 de octubre, y 18/2011, de 5 de julio, (certificados de usuario, de representante de personas jurídicas, de empleado público, de sede y de sello), así como su remisión electrónica a la FNMT-RCM, de conformidad con lo establecido en los citados procedimientos de registro.
- Velar frente a los usuarios, en calidad de encargados del tratamiento de datos de carácter personal, por el cumplimiento de las obligaciones que le correspondan en relación con la identificación, acreditación y registro de usuarios y de los funcionarios y empleados públicos, firmantes, así como de la recepción y tramitación de solicitudes de expedición, revocación y, en su caso, suspensión de cualesquiera certificados electrónicos previstos en este encargo y su anexo.

3.- Oficinas de Registro.

En relación a los servicios del artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas administrativas, fiscales y del orden social:

Los Departamentos, organismos y entidades del sector público destinatarios de los servicios del presente encargo podrán disponer

de una Oficina o red de Oficinas de Registro y Acreditación que deberán contar con los medios informáticos precisos para conectarse telemáticamente con la FNMT-RCM. En ellas, la acreditación e identificación de los solicitantes de los certificados exigirá la comprobación de su identidad y de su voluntad de que sea expedido un certificado electrónico y, en su caso, de las facultades de representación, competencia e idoneidad para la obtención del certificado correspondiente, y se verificará de conformidad y con pleno respeto a lo dispuesto en la normativa aplicable.

Estas Oficinas de Registro y acreditación se integrarán en la Red de Oficinas de Registro y acreditación a las que los ciudadanos pueden dirigirse para obtener un certificado electrónico expedido por la FNMT-RCM con observancia de lo dispuesto en la normativa aplicable. Las acreditaciones realizadas por las personas, entidades y corporaciones a que se refiere el apartado nueve del artículo 81 de la Ley 66/1997, de 30 de diciembre, citada, y por los diferentes órganos y organismos públicos de la Red de Oficinas de Registro y acreditación, surtirán plenos efectos y serán válidas para su aceptación por cualquier administración pública que admita los certificados emitidos por la FNMT-RCM.

En relación a los servicios de las Leyes 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia:

Las Oficinas de Registro de los Departamentos, órganos, organismos y entidades del sector público destinatarios de los servicios del presente Encargo, para el ámbito de las citadas Leyes 40/2015, de 1 de octubre, y 18/2011, de 5 de julio, son de orden interno de cada administración u organismo correspondiente.

Dichas Oficinas, determinarán la identidad y competencia de las Administraciones y la de los diferentes firmantes, de los certificados de conformidad con la DPC General y la específica Política y Prácticas de Certificación Particulares y procedimientos de registro de la

FNMT-RCM aplicables a los servicios de confianza en el ámbito de organización y funcionamiento de las administraciones públicas, sus organismos y entidades vinculadas o dependientes, disponibles para consulta en las Webs:

https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

https://www.cert.fnmt.es/registro-inicio.

A tal efecto, los Departamentos, organismos y entidades del sector público destinatarios de los servicios del presente encargo dispondrán de las Oficinas de Registro y acreditación que consideren necesarias y adecuadas para la acreditación de este tipo de certificados y deberán contar con los medios informáticos precisos para conectarse telemáticamente con la FNMT-RCM y realizar las solicitudes de emisión de los certificados. En las Oficinas de Registro, para acreditar e identificar a los titulares de los certificados, se exigirá la comprobación de su identidad, del cargo y de las facultades de representación, competencia e idoneidad para la obtención del certificado correspondiente y de la voluntad del titular del certificado, verificándose de conformidad y con pleno respeto a lo dispuesto en la normativa aplicable.

4.- Formularios.

Los formularios y condiciones de solicitud de emisión, revocación y, en su caso, suspensión de certificados se ajustarán a los procedimientos definidos en las Declaraciones de Prácticas de Certificación de la entidad, aplicable a cada tipo de certificado, accesible en las direcciones Webs citadas en el apartado anterior y en otras de la FNMT-RCM de acceso general.

CUARTA. SUBCONTRATACIÓN

De conformidad con lo establecido por la disposición final quinta del Real Decreto-Ley 36/2020, de 30 de diciembre**,** de medidas urgentes para la modernización de la Administración Pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia, a través de la cual, se modificó el

párrafo tercero de la letra b) del apartado 7 del artículo 32 de la Ley 9/2017, de Contratos del Sector Público, no resulta de aplicación al presente encargo, el límite a la subcontratación establecido en el párrafo primero de la letra b) del apartado 7 del artículo 32, de la citada Ley.

QUINTA. PLAZO DE DURACIÓN

El presente encargo entrará en vigor el 1 de marzo de 2021, extendiéndose su vigencia durante un año, hasta el 28 de febrero de 2022.

La duración del encargo se podrá prorrogar, antes de su vencimiento, por un plazo máximo de un año, siendo esta prórroga obligatoria para la FNMT-RCM.

SEXTA. RECEPCIÓN Y PAGO DEL SERVICIO

La FNMT-RCM tendrá derecho al abono de los trabajos efectivamente realizados, presentando las correspondientes facturas, expedidas de acuerdo con lo determinado en el Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación y en la Ley 25/2013, de 27 de diciembre de 2013, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público.

La compensación a percibir por la FNMT-RCM por la realización de los servicios objeto del presente encargo dirigido a los Departamentos, órganos, organismos y entidades del sector público previstos en la cláusula segunda será de 232.500 euros mensuales, de acuerdo con la Resolución de la Subsecretaria de Hacienda de 9 de febrero de 2021 por la que se fijan las tarifas de la FNMT-RCM para la prestación de los servicios electrónicos de confianza a la Administración General del Estado y a determinados organismos públicos y entidades dependientes.

El pago a realizar por el Ministerio de Hacienda a la FNMT-RCM por los servicios prestados en el marco del presente encargo se atenderá con cargo a la aplicación presupuestaria 10.01.923R.22109, con la siguiente distribución de anualidades:

- 2021: 8 meses por la tarifa mensual de 232.500 euros, resultando

un total de 1.860.000 euros.

- 2022: 4 meses por la tarifa mensual de 232.500 euros, resultando un total de 930.000 euros.

Los trabajos efectivamente realizados se facturarán cuatrimestralmente.

A efectos de la constatación de la prestación del servicio, la FNMT-RCM acompañará, a la factura correspondiente, de una certificación expedida por cada uno de los Departamentos, organismos y entidades del sector público destinatarios, y en la que se acredite tanto la realización de los mismos como la correspondiente conformidad con los servicios.

SÉPTIMA. RESPONSABILIDAD

La FNMT-RCM como prestador de los servicios citados en la cláusula primera y anexo, y los destinatarios de los servicios de confianza y encargados de las funciones de registro y acreditación en el procedimiento de identificación, acreditación y registro de los usuarios y, en su caso, la administración y firmantes, responderán, cada uno en el ámbito de sus respectivas funciones, de los daños y perjuicios que causara el funcionamiento del sistema de acuerdo con las reglas generales del ordenamiento jurídico que resultaran de aplicación y de conformidad con las obligaciones asumidas a través del presente encargo.

OCTAVA. RESOLUCIÓN Y EXTINCIÓN

El encargo podrá resolverse anticipadamente por parte de la Subsecretaría del Ministerio de Hacienda cuando la prestación del servicio por la FNMT-RCM no se ajuste a los términos establecidos en aquél o cuando así lo aconsejen los cambios normativos que afecten a los servicios de confianza y certificación electrónica que recibe la Administración General del Estado.

Será causa de extinción del encargo el cumplimiento del plazo previsto en la cláusula quinta *y* sus prórrogas.

La FNMT-RCM no podrá interrumpir el servicio o, en su caso, dejar de prestarlo por retrasos o falta de pago o, en los supuestos de finalización de la vigencia del encargo, cuando no estuvieran garantizados los

servicios de Administración Electrónica para los ciudadanos y empresas. En estos casos, la FNMT-RCM tendrá derecho a ser compensada por su actividad a través de los instrumentos presupuestarios que se determinen.

NOVENA. PROTECCIÓN DE DATOS

1. El régimen de protección de datos de carácter personal derivados de este encargo y de la actuación conjunta de los órganos incluidos en el mismo será el previsto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprobó el Reglamento de protección de datos de carácter personal.

Los ficheros de la FNMT-RCM se crearon por la Orden EHA/2357/2008, de 30 de julio, por la que se regulan los ficheros de datos de carácter personal de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (BOE núm. 190, de 7 de agosto), habiéndose creado un Registro de Actividades de Tratamiento y nombrado a un Delegado de Protección de Datos con el fin de dar cumplimiento al RGPD. Se puede consultar en: http://www.fnmt.es/rgpd

2. La comunicación de datos de carácter personal que los Departamentos, los organismos y entidades del sector público destinatarios de los servicios del presente encargo realicen a la FNMT-RCM sobre los datos de los empleados públicos de aquellos para la emisión de certificados de firma electrónica en el ámbito de las Leyes 40/2015, de 1 de octubre, y 18/2011, de 5 de julio, y con las obligaciones y pautas, para FNMT-RCM, establecidas en la Ley 66/1997, artículo 81), no requerirá consentimiento del interesado al estar, tal cesión o comunicación, amparada por el artículo 6.1.e) del Reglamento General de Protección de Datos, ya que tal comunicación resulta ineludible para que la FNMT RCM expida los citados certificados de firma electrónica.

3. Sin perjuicio de las cesiones de datos que por aplicación de la legislación de protección de datos de carácter personal se puedan realizar entre las Administraciones Públicas en el ejercicio de sus competencias, no tendrá carácter de comunicación de datos el acceso que, como responsable del tratamiento, pueda realizar la Subsecretaría del Ministerio de Hacienda y, en su caso, los Departamentos, organismos

y entidades del sector público destinatarios de los servicios sobre los datos de carácter personal que mantiene la FNMT-RCM, como responsable del fichero, sobre sus usuarios, personas físicas, con la finalidad de solicitar los servicios descritos en el presente encargo. Tales datos son los que figuran en el fichero regulado, en el número 5 del anexo de la citada Orden EHA/2357/2008 (ahora tratamiento nº 15 de su Registro de Actividades de Tratamiento).

Tampoco tendrá carácter de comunicación de datos el acceso que, como encargado del tratamiento, la FNMT-RCM pudiera realizar sobre los datos de carácter personal de la Subsecretaría del Ministerio de Hacienda responsable del fichero o la que se realizara sobre los datos que los órganos, organismos o entidades del sector público destinatarios de los servicios mantienen sobre sus usuarios personas físicas, con análoga finalidad de prestar los servicios descritos en este encargo.

De conformidad con el artículo 28 del Reglamento General de Protección de Datos, la FNMT-RCM, los Departamentos, organismos y entidades del sector público destinatarios de los servicios del presente encargo, en su calidad de encargados del tratamiento, asumirán, entre otras, las siguientes obligaciones:

- Tratarán los datos conforme a las instrucciones de la FNMT-RCM como responsable del fichero en lo que se refiere exclusivamente a hacer efectiva la realización de las actividades contempladas en este Convenio y, específicamente, la de remitir una copia del contrato de solicitud y conservar otra de las copias.

- No aplicarán o utilizarán los datos con un fin distinto al que figura en el presente encargo.

- No los comunicarán, ni siquiera para su conservación, a otras personas.

- Aplicarán medidas de seguridad acordes con el tipo de datos que traten (las que se establecen en la Orden EHA/2357/2008 anteriormente citada y en su Registro nº 15 de Actividades de Tratamiento).

- No almacenarán innecesariamente datos personales en los accesos

que se efectúen y, en caso de que se almacenen, una vez finalizado el presente encargo, destruirán o devolverán al responsable del fichero los datos y soportes donde figuren, levantando acta del tal destrucción o devolución. No obstante, y con el fin de preservar los derechos del encargado frente a posibles responsabilidades derivadas de su actuación, en el supuesto referido en este apartado, el encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

- Cumplimiento del resto de obligaciones establecidas en el Reglamento General de Protección de Datos.

En caso de que la FNMT-RCM, la Subsecretaría del Ministerio de Hacienda y los Departamentos, organismos o entidades del sector público incluidos en el ámbito subjetivo del encargo, destinen los datos manejados a otra finalidad, los comuniquen o los utilicen incumpliendo las estipulaciones de este encargo, serán considerados también responsables del tratamiento, respondiendo de las infracciones en que hubieran incurrido.

DÉCIMA. RÉGIMEN JURÍDICO.

La prestación de los servicios contemplados en el presente encargo y su anexo, en cuanto al contenido y características de los mismos, se realizará con sujeción a la regulación contenida en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, el artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social y su normativa de desarrollo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y 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, así como al resto de disposiciones que pudieran resultar de aplicación.

Este acuerdo es el instrumento jurídico por el que se regula el encargo que realiza la Subsecretaría del Ministerio de Hacienda a la FNMT-RCM, de acuerdo con el artículo 32 y la disposición adicional quinquagésimo quinta de

la Ley 9/2017, de 8 de noviembre de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, y con el artículo 3.2 del vigente Estatuto de esta entidad, aprobado por el Real Decreto 1114/1999, de 25 de junio, así como el resto de disposiciones que sean de aplicación.

UNDÉCIMA. RESOLUCIÓN DE INCIDENCIAS Y CONFLICTOS.

El cauce procedimental específico para la resolución de las incidencias y conflictos que pudieran surgir en cuanto a la interpretación, cumplimiento o ejecución de los servicios contemplados en este encargo, entre la FNMT-RCM y los Departamentos u organismos destinatarios de aquéllos, consistirá en la audiencia por escrito y una sola vez, de la FNMT-RCM y el Departamento u organismo concernido, por parte de la Subsecretaría de Hacienda, la cual, resolverá lo que proceda.

DUODÉCIMA. RÉGIMEN DE IMPUGNACIÓN.

Conforme establece el artículo 44.2 letra e) de la Ley 9/2017, de 8 de noviembre de Contratos del Sector Público, frente a la formalización de encargos a medios propios, en los casos de que estos no cumplan los requisitos legales, es susceptible de interponerse el correspondiente recurso especial en materia de contratación.

Madrid,

La Subsecretaria de Hacienda

María del Pilar Paneque Sosa

Recibí

La Directora General de la FNMT-RCM

Lidia Sánchez Milán

25703952A LIDIA SANCHEZ (R: Q2826004J)

Firmado digitalmente por 25703952A LIDIA SANCHEZ (R: Q2826004J)
Fecha: 2021.02.19 12:23:47 +01'00'

ANEXO - SERVICIOS A PRESTAR

CARACTERÍSTICAS TÉCNICAS DE LAS ACTIVIDADES A REALIZAR POR LA FNMT-RCM

CAPÍTULO I – SERVICIOS EIT

La FNMT-RCM prestará, en el ámbito de las Administraciones públicas y sus organismos públicos, vinculados o dependientes, servicios de seguridad, técnicos y administrativos, en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT), así como la expedición, fabricación y suministro de los títulos o certificados de usuario, de acuerdo con lo establecido en el artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social y en su normativa de desarrollo o, en su caso, en los términos que establezcan las disposiciones legales correspondientes.

En el ejercicio de las facultades derivadas de este apartado, la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda quedará sometida a lo dispuesto en la normativa que se cita en el párrafo anterior, sin perjuicio del resto de supuestos en que resulte de aplicación, de acuerdo con los artículos 103 y siguientes de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

A los efectos de lo dispuesto en el presente Anexo, cuando los términos comiencen con letra mayúscula y estén en cursiva, se atendrán al significado expresado en el apartado “Definiciones” de la Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica y, en su caso, las Declaraciones de Certificación Particulares dependientes de ésta.

Descripción de los servicios

La FNMT-RCM suministrará, a solicitud de los Departamentos, organismos y entidades del sector público destinatarios de los servicios del presente encargo, los *Certificados* que se relacionan en este apartado y que serán válidos como sistemas de identificación y de firma electrónicas, de conformidad con la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, basados en *Certificados electrónicos cualificados* que son admitidos en virtud de su

inclusión en las listas de servicios de confianza, (TSL, por sus siglas en inglés), conforme a las especificaciones técnicas recogidas en el Anexo de la Decisión de la Comisión 2009/767/CE, de 16 de octubre de 2009, por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las ventanillas únicas.

Como servicios de certificación asociados al uso de los *Certificados* por parte de sus titulares, la FNMT-RCM ofrecerá los siguientes servicios técnicos y que se describen en detalle en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica (DGPC) y la Declaración de Prácticas de Certificación Particulares* aplicables:

- Servicio de registro de usuarios.
- Servicio de emisión, revocación y en su caso, renovación y suspensión de certificados.
- Publicación de certificados revocados:
  - Publicación directa por parte de la FNMT en directorios seguros propios y con alta disponibilidad.
  - Publicación en directorios de otras entidades u organismos mediante replicación periódica.
- Registro de eventos significativos.
- Servicio continuo e ininterrumpido de atención a usuarios para la solicitud de revocación de certificados.
- Servicio de atención a usuarios que permitirá resolver cualquier duda o incidencia relativa a la validez o utilización de los certificados.

Relación de certificados incluidos

El formato de los certificados utilizados por la FNMT-RCM se basa en el definido por la Unión Internacional de Telecomunicaciones, sector de normalización de las telecomunicaciones, en la Recomendación UIT-T X.509, de 31 de marzo de 2000 o superiores (ISO/IEC 9594-8 de 2001). El

formato será el correspondiente a la versión 3 del certificado, especificado en esta norma.

- **Certificado electrónico cualificado de persona física**

Certificado electrónico cualificado que expide la FNMT-RCM a personas físicas.

OID de la política: 1.3.6.1.4.1.5734.3.10.1 (Política de Certificación de *Certificados de Persona Física*).

- **Certificado electrónico cualificado de representante de persona jurídica**

Certificado electrónico cualificado que expide la FNMT-RCM a personas físicas que actúan de representantes de personas jurídicas.

OID de la política: 1.3.6.1.4.1.5734.3.11.2 (Política de Certificación de *Certificados de Representante de Persona jurídica*).

- **Certificado electrónico cualificado de representante de entidad sin personalidad jurídica**

Certificado electrónico cualificado que expide la FNMT-RCM a personas físicas que actúan de representantes de entidades sin personalidad jurídica.

OID de la política: 1.3.6.1.4.1.5734.3.11.3 (Política de Certificación de *Certificados de Representante de Entidad sin personalidad jurídica*).

Estos certificados son expedidos como *Certificados Cualificados* conforme al Reglamento eIDAS.

Responsabilidad y obligaciones de las partes

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 de la Ley 6/2020, de 11 de noviembre,

reguladora de determinados aspectos de los servicios electrónicos de confianza, su reglamentación de desarrollo y en el Reglamento eIDAS.

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

- La Administración, organismos, entidades del sector público y privadas que admiten los *Certificados* como medios de identificación y/o firma electrónica.
- Oficinas de Registro que, a través del personal designado por la Administración competente, deben seguir los procedimientos establecidos por la FNMT-RCM en la *Declaración de Prácticas de Certificación* y en las *Políticas de Certificación* de aplicación, en el desempeño de sus funciones de gestión, expedición, renovación y revocación de *Certificados* y no salirse de dicho marco de actuación.
- Los *Titulares* del *Certificado*.
- FNMT-RCM, en cuanto *Prestador de Servicios de Confianza*.
- En su caso, resto de *Comunidad Electrónica* y terceros.

Obligaciones y responsabilidad del Prestador de Servicios de Confianza

Las obligaciones y responsabilidades de la FNMT-RCM, como *Prestador de Servicios de Confianza*, con el *Titular* del *Certificado* y el resto de miembros de la *Comunidad Electrónica*, quedarán determinadas principalmente por el documento relativo a las condiciones de utilización o el contrato de expedición del *Certificado* y, subsidiariamente, por las *Políticas y Prácticas de Certificación Particulares* y por la *DGPC*.

<u>*Con carácter previo a la emisión del Certificado.*</u>

a) Comprobar la identidad y circunstancias personales de los *Titulares* de *Certificados* con arreglo a lo dispuesto en las *Políticas y Prácticas de Certificación Particulares*. La FNMT-RCM podrá realizar estas comprobaciones mediante la intervención de *Oficinas de Registro* autorizadas o de terceros que ostenten facultades fedatarias.

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

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

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

e) Poner a disposición del Solicitante, y demás interesados, la Declaración de Prácticas de Certificación y cuanta información sea relevante para el desarrollo de los procedimientos relacionados con el ciclo de vida de los Certificados (http://www.ceres.fnmt.es).

Conservación de la información por la FNMT-RCM

a) Conservar toda la información y documentación relativa a cada Certificado, en las debidas condiciones de seguridad, durante el periodo legal establecido, de manera que puedan verificarse las firmas efectuadas con el mismo.

b) Mantener un repositorio seguro y actualizado de *Certificados* en el que se identifican los *Certificados* expedidos, así como su vigencia, incluyendo en forma de *Listas de Revocación* la identificación de los *Certificados* que hayan sido revocados o suspendidos. La integridad de este directorio se protegerá mediante la utilización de sistemas conformes con las disposiciones reglamentarias específicas que al respecto se dicten en España y, en su caso, en la UE.

c) Mantener un *Servicio de información y consulta sobre el estado de validez de los certificados*. Este servicio se describe en el Capítulo III del presente anexo.

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

e) Conservar las DPCs durante el periodo de tiempo exigible por la legislación vigente desde su modificación o derogación por publicación de una nueva DPC, en las debidas condiciones de seguridad.

Protección de los Datos de Carácter Personal

La FNMT-RCM se compromete a cumplir la legislación vigente en materia de Protección de Datos Personales, fundamentalmente, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, el Reglamento General de Protección de Datos, así como el resto de normas de aplicación.

Para informarse sobre la política de protección de datos seguida por la FNMT-RCM, y acerca del uso que de los datos se realiza, se puede consultar el apartado "Datos de Carácter Personal" de la *DGPC.*

Cese de la actividad de la FNMT-RCM como Prestador de Servicios de Confianza

A este respecto se puede consultar el apartado "Cese de la actividad del *Prestador de Servicios de Confianza*" de la *DGPC*.

Obligaciones y responsabilidad de las Oficinas de Registro

Los órganos, organismos y entidades del sector público destinatarios de los servicios de la presente encomienda que realicen las actividades de registro de los certificados electrónicos emitidos por la FNMT - RCM, lo harán de acuerdo con la *Declaración de Prácticas de Certificación* aplicable a cada tipo de certificado.

El registro de usuarios es el procedimiento a través del cual se identifica al solicitante de un certificado electrónico, se comprueba su personalidad y se constata su efectiva voluntad de que le sea emitido el certificado por la FNMT-RCM.

Este registro podrá ser realizado por la propia FNMT-RCM o cualquier otra Administración Pública y, en su caso, por las demás personas, entidades o corporaciones habilitadas a tal efecto por las normas que resulten de aplicación. En todo caso el registro se llevará a cabo según lo

dispuesto por la FNMT-RCM, al objeto de que este registro se realice de acuerdo con lo establecido por la normativa específica aplicable y homogéneamente en todos los casos. De igual manera será la FNMT-RCM, quien defina y aporte los medios necesarios para la realización de este registro.

En el caso de que el registro lo realizara una Administración Pública, distinta de la FNMT-RCM, la persona que se encargue de la actividad de registro ha de ser personal al servicio de la Administración Pública. En estos casos, la FNMT-RCM dará soporte a la implantación de las distintas oficinas de registro que se establezcan cuando fuere necesario, en los siguientes términos:

a) Aportación de la aplicación informática de registro.

b) Aportación de la documentación relativa a la instalación y manejo de la aplicación, así como toda aquella referente a los procedimientos y normas sobre el registro.

c) Registro y formación de los encargados del registro, lo que supone la emisión de un certificado emitido por la FNMT-RCM para cada encargado del registro, que permita garantizar la seguridad de las comunicaciones con la FNMT-RCM, incluyendo la firma electrónica de las solicitudes de registro.

d) Soporte técnico para facilitar la instalación y/o configuración de las aplicaciones de registro.

De forma adicional a las obligaciones y responsabilidades de las partes recogidas en la *Declaración de Prácticas de Certificación Particulares* y en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica (DGPC)*, las *Oficinas de Registro* tienen la obligación de:

i) Comprobar fehacientemente la identidad y cualesquiera circunstancias personales de los *Solicitantes* de los *Certificados* relevantes para el fin propio de estos, utilizando cualquiera de los medios admitidos en Derecho, y conforme a lo previsto en la *DGPC* y con carácter particular en la *Declaración de Prácticas de Certificación Particulares*. En el caso

particular de los *Certificados de Representante*, comprobar la identidad de la *Entidad representada*, así como la identidad, suficiencia del nombramiento o apoderamiento y cualesquiera circunstancias personales de los *Representantes* de los *Certificados* relevantes.

ii) Conservar toda la información y documentación relativa a los *Certificados*, cuya solicitud, revocación, y en su caso renovación y suspensión, gestiona durante el plazo de tiempo establecido en la legislación vigente.

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

iv) Comunicar a la FNMT-RCM, a través de los medios dispuestos para ello, cualquier evento relacionado con la gestión del ciclo de vida de los *Certificados* expedidos por la FNMT-RCM: solicitudes de expedición, renovación, etc.

v) Respecto de la extinción de la validez de los *Certificados:*

1. Comprobar diligentemente las causas de revocación y suspensión que pudieran afectar a la vigencia de los *Certificados*.

2. Comunicar a la FNMT-RCM de forma diligente las solicitudes de revocación y suspensión de los *Certificados*.

vi) Respecto de la Protección de Datos de Carácter Personal, será de aplicación lo dispuesto en el apartado correspondiente de la *DGPC.*

vii) Las *Oficinas de Registro*, a través del personal adscrito al servicio por relación laboral o funcionarial, deberán ejercer funciones públicas de acuerdo con la legislación específica aplicable a la FNMT-RCM.

En todo caso la FNMT-RCM podrá repetir contra la oficina de registro que hubiera realizado el procedimiento de identificación, iniciando las acciones correspondientes, si la causa del daño tuviera su origen en la actuación dolosa o culposa de ésta.

Obligaciones y responsabilidad de la Entidad usuaria y terceros que confían en los Certificados

Las *Entidades Usuarias*, los miembros de la *Comunidad Electrónica* y, en general, los terceros que confían en los *Certificados* tienen la obligación de:

- Verificar, con carácter previo a confiar en los *Certificados*, la *Firma electrónica* o el *Sello electrónico* del *Prestador de Servicios de Confianza* que expidió el *Certificado*.

- Verificar que el *Certificado* en el que está confiando continúa vigente y activo.

- Verificar el estado de los *Certificados* en la cadena de certificación, mediante los medios puestos a su disposición, como por ejemplo el *Servicio de información y consulta sobre el estado de validez de los certificados* de la FNMT-RCM.

- Comprobar las limitaciones de uso contenidas en el *Certificado* que se verifica.

- Conocer las condiciones de utilización del *Certificado* conforme a las *Políticas y Prácticas de Certificación Particulares* de aplicación.

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

Será responsabilidad de la *Entidad usuaria* y de los terceros que confíen en *Certificados* expedidos por la FNMT-RCM la verificación de las *Firmas electrónicas* de los documentos, así como de los *Certificados*, no cabiendo en ningún caso presumir la autenticidad de los documentos o *Certificados* sin dicha verificación.

No podrá considerarse que la *Entidad usuaria* ha actuado con la mínima diligencia debida si confía en una *Firma electrónica* basada en un *Certificado* emitido por la FNMT-RCM sin haber observado lo dispuesto en la *DGPC* y en la *Declaración de Prácticas de Certificación Particulares* y

comprobado que dicha *Firma electrónica* puede ser verificada por referencia a una *Cadena de certificación* válida.

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

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

CAPÍTULO II- SERVICIOS ADMINISTRACIÓN PÚBLICA (LEYES 40/2015 Y 18/2011)

La FNMT-RCM prestará a los Departamentos, organismos y entidades del sector público destinatarios de los servicios del presente encargo que lo soliciten, los servicios relativos a la identificación electrónica de las Administraciones Públicas y Administración de Justicia y autenticación del ejercicio de su competencia, de conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y 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 normativa de desarrollo, y en concreto, las actividades que se enumeran en este apartado.

Los servicios de identificación electrónica y autenticación de documentos electrónicos de las citadas Administraciones se basarán en sistemas de identificación, firma y creación de sellos electrónicos en el ejercicio de la competencia en la actuación administrativa automatizada y en la actuación judicial automatizada. Dichos servicios se concretan en la expedición y gestión del ciclo de vida de los siguientes tipos de certificados electrónicos:

Certificado de firma electrónica del personal al servicio de las Administraciones Públicas y la Administración de Justicia

Bajo la *Política de Certificación* de *Certificados de Firma electrónica del personal al servicio de la Administración Pública*, la FNMT-RCM expide los siguientes certificados cualificados conforme al Reglamento eIDAS, válidos como medios de firma electrónica de conformidad con las Leyes 40/2015 y 18/2011, que confirma de forma conjunta la identidad del *Firmante* (*personal al servicio de la Administración Pública*), y la identidad de la Administración, órgano, organismo o entidad de derecho público donde el *Firmante* ejerce sus competencias, presta sus servicios, o desarrolla su actividad.

- Certificado de firma electrónica del personal al servicio de la Administración Pública y de la Administración de Justicia.

(OID de la Política: 1.3.6.1.4.1.5734.3.17.2)

- *Certificado con seudónimo de firma electrónica del personal al servicio de las Administraciones Públicas.*

(OID de la Política: 1.3.6.1.4.1.5734.3.17.4)

- *Certificado con seudónimo de firma electrónica del personal al servicio de la Administración de Justicia*, específicamente aprobado por el Comité Técnico Estatal de la Administración Judicial Electrónica.

(OID de la política: 1.3.6.1.4.1.5734.3.17.3)

Estos *Certificados* se emiten por la FNMT-RCM por cuenta de la Administración Pública o de la Administración de Justicia correspondientes a las que la FNMT-RCM presta los servicios técnicos, administrativos y de seguridad necesarios como *Prestador de Servicios de Confianza*.

Dichos *Certificados* son expedidos 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 del sector público.

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 y/o Administración de Justicia.

Estos *Certificados* son expedidos a funcionarios, personal laboral, estatutario a su servicio y personal autorizado, al servicio de las Administraciones Públicas o de la Administración de Justicia, 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.

Las Administraciones solo podrán requerir certificados con seudónimo de firma electrónica del personal al servicio de la Administración Pública y de la Administración de Justicia para su uso en aquellas actuaciones que, realizadas por medios electrónicos, afecten a información clasificada, a la seguridad pública, a la defensa nacional o a otras actuaciones en las que esté legalmente justificado el anonimato para su realización.

Los *Certificados de Firma electrónica* que la FNMT – RCM expida haciendo uso de seudónimos, indicarán claramente esta característica, de conformidad con el Reglamento eIDAS y la normativa nacional aplicable.

En el procedimiento de acreditación de la identidad, como paso previo a la expedición de un *Certificado de Firma electrónica* 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.

Certificado de Sello electrónico de las Administraciones Públicas y Administración de Justicia

FNMT-RCM expide el *Certificado de Sello electrónico* en el ámbito de las Administraciones Públicas, la Administración de Justicia, organismos y entidades de derecho público, con la consideración de certificado reconocido o cualificado conforme al artículo 19 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, conforme a los artículos 40 y 42 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y conforme al artículo 19 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.

Los "*Certificados de Sello electrónico*" expedidos por la FNMT-RCM 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.*

El *Certificado de Sello electrónico* es expedido basándose 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 o de la Administración de Justicia de la que depende la unidad organizativa consignada en el *Certificado*.

Cada uno de los Departamentos, organismos y entidades del sector público destinatarios de los servicios del presente encargo podrá solicitar tantos *Certificados de Sello electrónico* como número de órganos o unidades funcionales disponga para el ejercicio de sus competencias.

Certificado de Sede electrónica de las Administraciones Públicas

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

FNMT-RCM expide el *Certificado de Sede electrónica* en el ámbito de las Administraciones Públicas, la Administración de Justicia, organismos y entidades de derecho público con la consideración de certificado reconocido o cualificado conforme a los artículos 17 y 18 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, conforme a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y 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.

El *Certificado de Sede electrónica* es expedido basándose en actuaciones de identificación y registro realizadas por las *Oficinas de Registro* designadas por el órgano, organismo o entidad de la Administración Pública o de la Administración de Justicia que tienen la titularidad, gestión y administración de la dirección electrónica de la *Sede electrónica*.

Cada uno de los Departamentos, organismos y entidades del sector público destinatarios de los servicios del presente encargo podrá solicitar

tantos *Certificados de Sede electrónica* como sedes y/o subsedes oficiales tenga o requiera para llevar a cabo el ejercicio de sus competencias.

Responsabilidad y obligaciones de las partes

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 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y su reglamentación de desarrollo.

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

- La Administración, organismos, entidades del sector público representadas a través de los diferentes órganos competentes que serán los *Suscriptores* de los certificados. Salvo indicación en contrario, corresponderá la representación a la Oficina de Registro correspondiente a través de su responsable.
- Oficinas de Registro, que, a través del personal designado por la Administración competente
- Los custodios y firmantes de los certificados.
- FNMT-RCM, en cuanto Prestador de Servicios de Confianza.
- En su caso, resto de Comunidad Electrónica y terceros.

El régimen de derechos y obligaciones de las Administraciones, organismos, entidades del sector público y la FNMT-RCM se regirá mediante el presente documento de formalización de encargo.

De forma adicional a las obligaciones y responsabilidades de las partes recogidas en la *Declaración de Prácticas de Certificación Particulares* y en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* (DGPC), las entidades del sector público *Suscriptoras*, representadas a través de los diferentes órganos competentes, actuando a través del *Responsable de la Oficina de Registro* para la emisión de este tipo de *Certificados*, tienen la obligación de:

- No realizar registros o tramitar solicitudes de *Certificados* por 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 identificativos y competenciales del *Suscriptor* del *Certificado* y del *Solicitante* del *Certificado* y verificar su correspondencia con el titular y contactos establecidos en las bases de datos correspondientes. El *Prestador de Servicios de Confianza*, a través del Responsable *de la Oficina 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*.

- Solicitar la revocación del *Certificado* cuando alguno de los datos que se refleje en el mismo sea incorrecto, inexacto o haya variado respecto a lo consignado en el *Certificado*, o sea de necesaria revocación por razones de seguridad.

Las relaciones de la FNMT-RCM y el *Suscriptor* y los usuarios de los certificados 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.

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 las *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.

CAPÍTULO III – OTROS SERVICIOS INCLUIDOS

Expedición de Certificados de Componente.

La FNMT-RCM suministrará a los Departamentos, organismos y entidades del sector público destinatarios de los servicios del presente encargo que lo requieran hasta un total de 5 certificados de componente emitidos por la *Autoridad de Certificación* denominada *AC Componentes Informáticos* y conforme a la *Política de Certificación* de *Certificados de componente* de la FNMT-RCM.

Entre la tipología de *Certificados de Componente*, se encuentran los siguientes:

- *Certificado SSL/TLS estándar:* es aquel que permite establecer comunicaciones seguras con sus clientes utilizando el protocolo SSL/TLS. Este tipo de certificados garantiza la identidad del dominio donde se encuentra su servicio Web.

- *Certificado wildcard:* Identifica todos los sub-dominios asociados a un dominio determinado, sin necesidad de adquirir y gestionar múltiples certificados electrónicos. Por ejemplo, el certificado wildcard emitido a "*.ejemplo.es" garantiza la identidad de dominios como compras.ejemplo.es, ventas.ejemplo.es o altas.ejemplo.es.

- *Certificado SAN:* El certificado de tipo SAN, también conocido como certificado multidominio, UC o Unified Communications Certificates, le permite securizar con un solo certificado hasta doce dominios diferentes.

- *Certificado de firma de código* este certificado permite firmar programas y componentes informáticos acreditando la identidad del autor y realizar de este modo distribuciones seguras a través de Internet.

- *Certificado de sello de entidad* es aquel que se utiliza habitualmente para establecer conexiones seguras entre componentes informáticos genéricos.

Servicios de validación de los certificados de la FNMT-RCM

El *Servicio de información y consulta sobre el estado de validez de los certificados* permite, tanto a los suscriptores como a los usuarios de los mismos, validar la vigencia de dichos certificados electrónicos. Por ser la piedra angular de cualquier operación relacionada con los certificados electrónicos (verificación de firma electrónica y autenticación de usuarios), es fundamental la prestación de este servicio en alta disponibilidad dentro de la Infraestructura de Clave Pública de la FNMT-RCM.

Debido a su criticidad, este servicio está disponible las 24 horas del día y todos los días del año, con una disponibilidad mínima de un 99%, tanto a través de Internet como a través de la red SARA. El centro de respaldo de la FNMT – RCM garantiza estos niveles de disponibilidad.

La consulta sobre el estado de validez de los certificados se puede realizar mediante tres vías diferentes:

- *Servicio de información y consulta sobre el estado de validez de los certificados* basado en el protocolo "Online Certificate Status Protocol" (OCSP).
- Consulta de las CRLs.
- Replicación diaria de las listas de certificados revocados desde la FNMT-RCM a petición del organismo.

Descripción del Servicio de información y consulta sobre el estado de validez de los certificados

El *Servicio de información y consulta sobre el estado de validez de los certificados* proporciona información "on-line" del estado de uno o varios certificados a través de un servidor de confianza denominado *OCSPResponder*.

El servicio OCSP se basa en mecanismos de solicitud/respuesta que pueden encapsularse en múltiples protocolos de comunicaciones a nivel de transporte, aunque el más utilizado es HTTP.

La especificación de OCSP se describe en el documento "RFC 6960 Internet Public Key Infrastructure Online Certificate Status Protocol –

OCSP" y establece la forma en que se deben componer tanto las peticiones como las respuestas OCSP.

Si la petición no es conforme a la RFC 6960, el *OCSPResponder* devolverá un mensaje de error. En otro caso, se devuelve una respuesta OCSP que irá firmada.

Las respuestas OCSP pueden ser de varios tipos. Para la verificación de la firma de la respuesta el cliente tiene que confiar en el certificado utilizado por el servidor OCSP para firmar, distribuido de forma previa por mecanismos seguros.

La respuesta OCSP contiene:

- Versión de la sintaxis de la respuesta.
- Nombre del responder (UTF8).
- Respuesta para cada uno de los certificados de la petición.
- OID del algoritmo de firma.
- Firma calculada a partir del hash de la respuesta.

Una respuesta OCSP está constituida por dos campos,

1. Un campo responseStatus que indica información sobre el estado del proceso de la petición realizada.

Los posibles valores del campo OCSPResponseStatus son:

0. El proceso de generación de la respuesta ha sido exitoso.

1. La petición (request) enviada por el cliente tiene una sintaxis incorrecta.

2. Error interno del responder, servidor OCSP no está disponible por problemas internos, debe realizarse la consulta a otro responder.

3. Se debe realizar de nuevo la petición, el servidor está disponible, pero ha habido problemas temporales en el servidor OCSP.

4. La petición del cliente tiene que estar firmada.

5. El cliente no está autorizado para realizar este tipo de consultas al servidor.

2. La respuesta OCSP. Los clientes OCSP deben de ser capaces de recibir y procesar respuestas de este tipo. La información que guarda la respuesta es:

- responderID que es el identificador del servidor OCSP.
- producedAt que es la fecha en que el responder ha firmado la respuesta.
- responses con la información del estado de los certificados que el cliente quiere verificar, este campo devolverá la siguiente información de cada certificado.
- certID: identificador del certificado.
- certStatus: estado del certificado resultante de la verificación del mismo (puede tomar tres posibles valores: good, revoked con información de revocación o unknown).
- thisUpdate con la fecha de actualización de la información contra la que se ha verificado el certificado.

La URL de acceso al servicio OCSP se incluye, en cada certificado emitido, en el campo "Acceso a información de Autoridad (AIA)".

1. AC RAIZ. FNMT-RCM:
http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder
2. AC Subordinada Administración Pública:
http://ocspap.cert.fnmt.es/ocspap/OcspResponder
3. AC Subordinada Componentes Informáticos:
http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder
4. AC Subordinada Representación:
http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder
5. AC Subordinada Usuarios:
http://ocspusu.cert.fnmt.es/ocspusu/OcspResponder
6. AC FNMT Clase 2:
http://ocsp2.cert.fnmt.es/ocsp2/OcspResponder

Descripción del Servicio de Consulta del estado del Certificado mediante consulta de CRLs

Las listas de certificados revocados, o CRLs, contienen los números de serie de aquellos certificados que han sido revocados por algún motivo antes de su fecha de caducidad. El formato de CRLs viene establecida en la RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

La FNMT-RCM permitirá el acceso a los directorios LDAP a las administraciones, organismos y entidades del sector público destinatarios de los servicios del presente encargo que lo soliciten, con el objetivo de que los organismos puedan comprobar si un certificado está revocado.

Para los certificados de todas las CAs se utilizan CRLs fraccionadas; por cada 750 certificados se genera una nueva CRL. Por ejemplo, al emitir el certificado 1 se genera la CRL1. En ella se reserva espacio para incluir la información de revocación de los 750 primeros certificados. Al emitir el certificado 751 se crea la CRL2 donde se almacenará el estado de revocación de los siguientes 750 certificados.

Este acceso está restringido a sólo lectura y búsqueda, pudiendo utilizar como clave de búsqueda cualquier información contenida en una entrada de un usuario.

1. AC RAIZ. Accesos:

- ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint

- http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

2. AC Subordinada Administración Pública. Accesos:

- ldap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,CN=AC%20Administraci%F3n%20P%FAblica,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

- http://www.cert.fnmt.es/crlsacap/ CRL<xxx*>.crl

3. AC Subordinada Componentes Informáticos. Accesos:

- ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>,OU=AC%20Componentes%20Informaticos,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

- http://www.cert.fnmt.es/crlscomp/CRLxxx*.crl

4. AC Subordinada Representación

- ldap://ldaprep.cert.fnmt.es/CN=CRL<xxx>,OU=AC%20Representacion,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

- http://www.cert.fnmt.es/crlsrep/CRLnnn.crl

5. AC Subordinada Usuarios

- ldap://ldapusu.cert.fnmt.es/CN=CRL<xxx*>, CN=AC%20FNMT%20Usuarios,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

*xxx: número entero identificador de la CRL (CRL particionadas)

Réplica de Directorio

A petición de la administración, organismo o entidad destinataria de los servicios del presente encargo, la FNMT-RCM podrá publicar externamente las listas de certificados revocados en los directorios de dicho organismo. Las mismas irán firmadas / selladas con la clave privada del certificado de la FNMT-RCM emitido al respecto para ese fin.

Este servicio no incluye licencias de software en el cliente, la instalación ni el mantenimiento, que serán por cuenta del organismo que los solicite.

El directorio y su contenido no podrán ser cedidos a terceros bajo ningún concepto, y deberá ser protegido contra todo acceso de entidades ajenas.

Servicio de Sellado de Tiempo

La FNMT-RCM, es un *Prestador de Servicios de Confianza*, entre los que se incluye el *Sellado de Tiempo* o *creación de sellos cualificados de tiempo electrónicos*, conforme al Reglamentos elDAS, cuyo objeto es dar fe de la existencia de un conjunto de datos en un instante determinado en la línea de tiempo. Para ello utiliza como fuente de información temporal vinculada al Tiempo Universal Coordinado (UTC) la proporcionada por la Sección de Hora del Real Instituto y Observatorio de la Armada (ROA) en San Fernando, mediante el acuerdo alcanzado entre dicha Entidad y la FNMT-RCM para la sincronización continua de sus sistemas. El ROA tiene como misión el mantenimiento de la unidad básica de tiempo, declarado a efectos legales como Patrón Nacional de dicha unidad, así como el mantenimiento y difusión oficial de la escala "Tiempo Universal Coordinado" (UTC -ROA), considerada a todos los efectos como la base de la hora legal en todo el territorio español (Real Decreto 1308/1992, de 23 octubre 1992).

El Sistema de Sincronismo con el Real Observatorio de la Armada (SS-ROA) instalado en el Centro de Proceso de Datos (CPD) de la FNMT-RCM tiene como objetivo proporcionar una fuente de referencia temporal trazable a la escala de tiempo UTC (ROA), para la prestación del *Servicio de Sellado de Tiempo* de la FNMT-RCM.

Dicho sistema produce una serie de ficheros que contienen los datos de los seguimientos efectuados en un día y son utilizados por el ROA para elaborar los informes de diferencia de fase del patrón con la escala UTC (ROA).

La precisión declarada para la sincronización de la TSU con UTC es de 100 milisegundos, cumpliendo así sobradamente con los requisitos del estándar europeo [ETSI EN 319 421]. Por tanto, el *Servicio de Sellado de Tiempo* de la FNMT-RCM no expedirá ningún *Sello de tiempo electrónico* durante el periodo de tiempo en el que existiera un desfase mayor de 100 milisegundos entre los relojes de la TSU y la fuente de tiempo UTC del ROA.

La FNMT-RCM suministrará a los Departamentos, organismos y entidades del sector público destinatarios de los servicios del presente encargo que así lo soliciten el acceso a este servicio de *Sellado de Tiempo*.

Tanto las peticiones de *Sellado de Tiempo* como las respuestas se gestionarán conforme a lo descrito en la recomendación RFC 3161.

Las respuestas de la *Autoridad de Sellado de Tiempo*, del tipo "application/timestamp- reply", irán firmadas con un certificado con un tamaño de claves RSA de 3072 bits y algoritmo de firma SHA-256 y podrá validarse mediante cualquiera de los métodos de validación de los certificados que la FNMT-RCM pone a disposición de los usuarios y terceras partes que confían en los certificados y que se describe en el apartado anterior.