ENCOMIENDA DE GESTIÓN QUE «INSTITUTO MUNICIPAL DE INNOVACIÓN DEL AYUNTAMIENTO DE PALMA» REALIZA A LA «FÁBRICA NACIONAL DE MONEDA Y TIMBRE - REAL CASA DE LA MONEDA», PARA LA EJECUCIÓN DE ACTIVIDADES DE CARÁCTER MATERIAL Y TÉCNICO CON EL FIN DE EXTENDER DE LOS SERVICIOS PÚBLICOS ELECTRÓNICOS

En Madrid, a 23 de agosto de 2022

R E U N I D O S

De una parte, don/doña _Adrián García Campos_ en nombre y representación de Instituto Municipal de Innovación del Ayuntamiento de Palma en virtud de las competencias atribuidas por el _artículo 17 de los Estatutos y en cumplimiento de los acuerdos adoptados por el Consejo Rector en sesión de día _28_ de _septiembre_ de _2018_, y por la Junta de Gobierno de Palma en sesión de día 3 de octubre de 2018, con domicilio institucional en _calle Joan Maragall, 3 (07006, Palma)_ y NIF _P5790001A_.

Y de otra parte, doña Mª Isabel Valldecabres Ortiz, Directora General de la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda, nombrada por Real Decreto 726/2021, de 3 de agosto (BOE 185, de 4 de agosto), en nombre y representación de este Entidad, según el artículo 19.2 del Real Decreto 1114/1999, de 25 de junio, por el que sea aprueba el Estatuto de la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (BOE núm. 161, de 7 de julio) con domicilio institucional en Madrid, calle Jorge Juan, 106 y NIF Q2826004J.

Ambas partes, reconociéndose respectivamente capacidad legal y competencia suficientes para formalizar la presente Encomienda,

E X P O N E N

I. En el ámbito de identificación electrónica de los interesados en un procedimiento, los arts. 9 y 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, establecen que, entre otros sistemas utilizados por los interesados y admitidos por las Administraciones Públicas "los interesados podrán identificarse electrónicamente (…) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la 'Lista de confianza de prestadores de servicios de certificación".

Esta Lista de confianza se elabora según lo previsto en la Decisión de Ejecución (UE) 2015/1505 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza. La Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM) es uno de los prestadores de servicios de certificación incluidos en esta Lista de confianza gestionada por el Ministerio de Asuntos Económicos y Transformación Digital (Secretaría de Estado de Digitalización e Inteligencia Artificial - SGAD).
https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/Prestadores.aspx

Por otro lado, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece el funcionamiento electrónico del sector público siendo lo habitual la utilización de los medios electrónicos por las Administraciones públicas, como la firma y sedes electrónicas, el intercambio electrónico de datos en entornos cerrados de comunicación y

la actuación administrativa automatizada. Se establece asimismo la obligación de que las Administraciones Públicas se relacionen entre sí por medios electrónicos, previsión que se desarrolla posteriormente en el título referente a la cooperación interadministrativa mediante una regulación específica de las relaciones electrónicas entre las Administraciones. Para ello, también se contempla como nuevo principio de actuación la interoperabilidad de los medios electrónicos y sistemas y la prestación conjunta de servicios a los ciudadanos.

El Capítulo V del Título Preliminar de la Ley 40/2015, de 1 de octubre, regula, específicamente, el funcionamiento electrónico del sector público, integrado por la Administración General del Estado, las Administraciones de las Comunidades Autónomas, las Entidades que integran la Administración Local y el Sector Público Institucional.

El Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, desarrolla y concreta las previsiones legales, antes esbozadas, con el fin, entre otros aspectos, de facilitar a los agentes involucrados en el uso de medios tecnológicos su utilización efectiva, aclarando y precisando, al mismo tiempo, aquellas materias reguladas en estas leyes que permiten un margen de actuación reglamentaria. La Agenda España Digital 2025 contiene un eje estratégico específico sobre la Transformación Digital del Sector Público, cuya plasmación se concreta en el cumplimiento de un conjunto de medidas entre las que se encuentra la mejora del marco regulatorio de la Administración digital y el Plan de Recuperación, Transformación y Resiliencia (España Puede) incluye entre sus diez políticas palanca de reforma estructural para un crecimiento sostenible e inclusivo, lograr una Administración modernizada a través de su digitalización, tanto a nivel transversal como en ámbitos estratégicos.

En relación con la materia de esta encomienda de gestión, el Real Decreto 203/2021, de 30 de marzo, desarrolla la actividad de identificación electrónica de las Administraciones Públicas y la autenticación del ejercicio de su competencia, que comprende la identificación de las sedes electrónicas y sedes asociadas, la identificación mediante sello electrónico basado en certificado electrónico cualificado, los sistemas de firma electrónica para la actuación administrativa automatizada, la identificación y firma del personal al servicio de las Administraciones Públicas (incluidos los certificados de empleado público con número de identificación profesional y con seudónimo) y también regula la identificación y firma de los interesados y su representación.

II. La realización material de estas actividades está regulada por el Reglamento (UE) 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 la que se deroga la Directiva 1999/93/CE.

En el ámbito del derecho interno sobre esta materia, se ha aprobado la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. La función de esta Ley es complementar al Reglamento europeo en aquellos aspectos concretos que no han sido armonizados y cuyo desarrollo su prevé en los ordenamientos de los diferentes Estados miembros, cuyas disposiciones han de ser interpretadas de acuerdo con él.

En relación con la actividad y efectos de los sistemas de identificación y demás servicios, la Disposición adicional segunda de esta Ley 6/2020, de 11 de noviembre, establece que todos los sistemas de identificación, firma y sello electrónico previstos en la Ley 39/2015, de 1 de octubre, y en la Ley 40/2015, de 1 de octubre, tendrán plenos efectos jurídicos.

III. Como regulación especial de la FNMT-RCM, incorporada al artículo 2 de su Estatuto, se aprobó y mantiene su vigencia, el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, bajo el título "*Prestación de servicios de seguridad por la Fábrica Nacional de Moneda y Timbre para las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos*", faculta a la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM) 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 (apartado 1º), y le habilita, tras la modificación operada por la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, previa formalización del correspondiente convenio (u otro instrumento de relaciones), a prestar a las personas, entidades y corporaciones que ejerzan funciones públicas los citados servicios y a su participación en los trámites de identificación y registro.

El Real Decreto 1317/2001, de 30 de noviembre, por el que se desarrolla el artículo 81, antes citado, regula el régimen de prestación de servicios de seguridad por la FNMT-RCM en la emisión y recepción de comunicaciones y escritos a través de medios y técnicas electrónicas, informáticas y telemáticas. Su artículo 6, faculta a la FNMT-RCM para establecer los términos que deben regir la prestación de sus servicios en relación con las comunicaciones empleando técnicas y medios electrónicos, informáticos y telemáticos, así como la colaboración mutua en materia de registro y acreditación (tanto de los interesados como de la propia institución y sus empleados).

La FNMT-RCM, desde mediados de los años noventa, ha desarrollado, mejorado y actualizado diversas infraestructuras de clave pública (PKI), que cubren las necesidades de la Ley 39/2015, de 1 de octubre, y Ley 40/2015, de 1 de octubre, soluciones que son potencialmente extensibles a otras Administraciones Públicas, Entes, Entidades y resto de órganos y poderes del Estado. Estas PKI se han puesto en marcha obedeciendo a los siguientes criterios:

- Aprovechamiento de la experiencia acumulada en el proyecto de Certificación Española CERES, que constituye el núcleo de la infraestructura de clave pública.
- Reducción de riesgos en la consolidación de la "Administración sin papeles".
- Economía de medios, derivada de la experiencia acumulada y transferencia de tecnologías entre Administraciones Públicas.
- Reutilización de tecnologías, equipamientos, tarjetas y aplicaciones actualmente en uso.

IV. El artículo 11 de la Ley 40/2015, de 1 de octubre, dispone que la realización de actividades de carácter material o técnico de la competencia de los órganos administrativos o de las Entidades de Derecho Público podrá ser encomendada a otros órganos o Entidades de Derecho Público de la misma o de distinta Administración, siempre que entre sus competencias estén esas actividades, por razones de eficacia o cuando no se posean los medios técnicos idóneos para su desempeño. Por medio del presente instrumento, se pretende encomendar a la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda la realización de las actividades necesarias para el cumplimiento de los fines del encomendante.

Dado que es de interés de Instituto Municipal de Innovación del Ayuntamiento de Palma garantizar que los interesados puedan relacionarse a través de medios electrónicos, así como poder identificarse y establecer comunicaciones con los interesados y otras administraciones, y que la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda está en disposición de realizar las actividades técnicas y de seguridad relativas a la certificación, firma electrónica y resto de actuaciones previstas en este documento, según

sus fines institucionales; se establece por Instituto Municipal de Innovación del Ayuntamiento de Palma encomendar a la FNMT-RCM su realización sobre la base de las siguientes

CLÁUSULAS

PRIMERA. OBJETO

Constituye la finalidad de esta Encomienda de Gestión la realización, por parte de la FNMT-RCM a Instituto Municipal de Innovación del Ayuntamiento de Palma, de actividades de carácter material o técnico con el fin de que sea posible el ejercicio de las funciones y competencias de la parte encomendante. Estas actividades permitirán la creación de un marco de actuación institucional que facilite el impulso de servicios públicos electrónicos de Instituto Municipal de Innovación del Ayuntamiento de Palma, a través de la extensión a su ámbito de competencia, de las actividades de Plataforma Pública de Certificación y de servicios electrónicos, informáticos y telemáticos desarrollados por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM) para su uso por las diferentes Administraciones.

En particular, la actividad de la FNMT-RCM comprenderá:

1. La extensión de la Plataforma Pública de Certificación mediante la implementación de las actividades que al efecto se enumeran en los Capítulos I y III, del Anexo I, de esta Encomienda, tanto para identificación de las Administraciones Públicas, como de los ciudadanos. En especial, se realizarán las siguientes actividades de carácter material o técnico:

1.1.- Expedición y gestión del ciclo de vida de certificados de usuario para personas físicas, a través de la AC USUARIOS. Mantenimiento de las Plataformas seguras de gestión de certificados.

1.2.- Expedición y gestión del ciclo de vida de certificados recogidos en la Ley 40/2015, de 1 de octubre, y mantenimiento de las Plataformas seguras de gestión de certificados: Certificados de Personal, Certificados de Sede Electrónica (autenticación de sitio Web) y Certificados de Sello Electrónico de Administración Pública (según apartado 3, siguiente).

También podrá integrar a petición de Instituto Municipal de Innovación del Ayuntamiento de Palma cualquiera, o la totalidad, de las funcionalidades y actividades que se enumeran en el Capítulo II, del mismo Anexo I, de esta Encomienda.

2. Reconocimiento y validación de certificados a través de la Plataforma de Validación Multi-AC de la FNMT-RCM, que es plenamente interoperable y redundante respecto de la plataforma de verificación de la Administración General del Estado.

3. La FNMT-RCM también podrá realizar, con carácter instrumental de las anteriores y previa petición de Instituto Municipal de Innovación del Ayuntamiento de Palma, las siguientes actividades adicionales:

- Emisión de Sellos de Tiempo en las comunicaciones electrónicas, informáticas y telemáticas que tengan lugar al amparo del presente documento, previa petición de Instituto Municipal de Innovación del Ayuntamiento de Palma, a través de la Infraestructura Pública de Sellado de Tiempo de la FNMT-RCM, sincronizada mediante

convenio con el Real Instituto y Observatorio de la Armada (ROA), como órgano competente del mantenimiento del Patrón Hora en España.

- 5 Certificados de componente (según las características del Anexo II).

SEGUNDA. ÁMBITO SUBJETIVO DE APLICACIÓN

1. Dentro del ámbito de aplicación subjetivo de esta Encomienda es el Ayuntamiento de Palma, sus órganos, unidades administrativas y organismos autónomos dependientes.
Organismos autónomos:

- IMI (Institut Municipal d'Innovació de Palma)
- IME (Institut Municipal de l'Esport)
- PalmaActiva
- PMEI (Patronat Municipal d'Escoles d'Infants)
- PMH-RIBA (Patronat Municipal de l'Habitatge)

2. No podrán adherirse a la presente Encomienda, los organismos y entidades dependientes de la encomendante.

TERCERA. ACTIVIDADES A DESARROLLAR

De acuerdo con el régimen de competencias y funciones propias de cada parte, corresponde a la FNMT-RCM, de acuerdo con lo dispuesto en el objeto de esta Encomienda y en la normativa referida en el mismo, la puesta a disposición de Instituto Municipal de Innovación del Ayuntamiento de Palma, de la Plataforma Pública de Certificación desarrollada para el funcionamiento de la Administración Electrónica, para ofrecer seguridad en la utilización de instrumentos de identificación electrónica por parte de los interesados y de las administraciones y otros entes del Estado. Estas Plataformas, junto con otras funcionalidades adicionales, como el Sellado de Tiempo, permiten, a la FNMT-RCM, la realización de las actividades de carácter material y técnico en el ámbito de la securización de las comunicaciones, de la certificación y firma electrónica, cumpliendo con su mandato de extensión de la Administración Electrónica.

De otra parte, corresponde a Instituto Municipal de Innovación del Ayuntamiento de Palma la realización de las actuaciones administrativas y el desarrollo de sus funciones y competencias dirigidas a la implementación de las Plataformas en sus procedimientos. Para la adecuada consecución del objeto de esta Encomienda, las partes han de desplegar una serie de actuaciones:

1. La FNMT-RCM, realizará las siguientes actividades:

1.1. De carácter material, administrativo y técnico:

- Aportar la infraestructura técnica y organizativa adecuada para procurar la extensión e implementación de las Plataformas, con las funcionalidades previstas para el desarrollo de las relaciones administrativas de los ciudadanos, a través de sistemas EIT y de conformidad con lo contenido en los Anexos y el estado de la técnica.

- Aportar los derechos de propiedad industrial e intelectual necesarios para tal implementación, garantizando su uso pacífico. La FNMT-RCM, excluye cualesquiera licencias o sublicencias, a terceras partes o a Instituto Municipal de Innovación del Ayuntamiento de Palma para aplicaciones y sistemas de Instituto Municipal de Innovación del Ayuntamiento de Palma o de terceros, distintas de las aportadas para ser utilizadas, en calidad de usuarios, directamente por la FNMT-RCM, en virtud de esta Encomienda.

- Asistencia técnica, de conformidad con lo establecido en los Anexos, con objeto de facilitar a Instituto Municipal de Innovación del Ayuntamiento de Palma la información necesaria para el buen funcionamiento de los sistemas.

- Actualización tecnológica de los sistemas, de acuerdo con el estado de la técnica y los Esquemas Nacionales de Interoperabilidad y Seguridad, sin perjuicio de la aprobación de los requisitos técnicos correspondientes por la Comisión de Estrategia TIC o, en su caso, por el órgano competente.

- Aportar la tecnología necesaria para que las obligaciones de Instituto Municipal de Innovación del Ayuntamiento de Palma puedan ser realizadas; en particular las aplicaciones necesarias para la constitución de las Oficinas de Registro y Acreditación y la tramitación de las solicitudes de emisión de certificados electrónicos.

- Emisión de informes, a petición de Instituto Municipal de Innovación del Ayuntamiento de Palma acreditativos de las actividades realizadas por la FNMT-RCM.

- Tener disponible para consulta de Instituto Municipal de Innovación del Ayuntamiento de Palma y de los usuarios una Declaración de Prácticas de Certificación o del Servicio de Confianza (DPC), que contendrá, al menos, las especificaciones establecidas en el Reglamento (UE) 910/2014 y en la Ley 6/2020, de 11 de noviembre. La DPC y demás información de interés, estará disponible en la dirección electrónica (URL) siguiente:
  https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

  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 avisos en su dirección electrónica.

  En relación con la DPC y sus anexos es necesario tener en cuenta la Declaración de Prácticas de Certificación General y las Políticas y Prácticas de Certificación Particulares para cada tipo de certificado o ámbito de los mismos.

- En todo caso, los medios técnicos y tecnología empleados por la FNMT-RCM permitirán demostrar la fiabilidad de la actividad 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 (los cuáles contarán con la debida protección contra alteraciones, así como 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, los que resulten de aplicación de conformidad con la normativa comunitaria o nacional correspondiente.

No obstante lo anterior, en la realización de actuaciones del ámbito de la Ley 40/2015, las Oficinas de Registro (por las especialidades de gestión y del derecho administrativo, y de conformidad con el artículo 11 del Real Decreto 1317/2001, de 30 de noviembre) no dependerán directamente de la FNMT-RCM sino del órgano, organismo o entidad de la que orgánicamente dependan, sin perjuicio de las funciones de comprobación, coordinación, control de gestión y de los protocolos y directrices sobre registro y acreditación que realice la FNMT-RCM, en su condición de Prestador de Servicios de Confianza.

La FNMT-RCM se compromete, en el desarrollo y ejecución de la Encomienda 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.

1.2. De desarrollo de las facultades establecidas en su normativa específica, realizando su actividad en los términos y con los efectos previstos en el Real Decreto 1317/2001, de 30 de noviembre, en especial:

- Funciones de comprobación, coordinación y control de las Oficinas de Registro y Acreditación, sin perjuicio de su dependencia, orgánica y funcional, de la Administración u organismo público a que pertenezcan.

- Resolución de los recursos y reclamaciones de competencia de la FNMT-RCM derivadas de la actividad convenida.

- Comunicación al Ministerio de Hacienda, a efectos de coordinación e interoperabilidad, para el desarrollo de la administración electrónica y acceso electrónico de los ciudadanos a los servicios públicos.

- *Medidas de Seguridad*. La FNMT-RCM adoptará medidas en orden a 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, los Esquemas Nacionales de Seguridad e Interoperabilidad y las normas sobre contratación pública, así como las obligaciones de confidencialidad pertinentes establecidas y reguladas en su Estatuto, restringiendo la información y la publicidad de los diferentes elementos de seguridad, según los estándares aplicables y, en general, realizando la actividad encargada implantando medidas especiales de seguridad, de conformidad con el estado de la técnica.

2. Instituto Municipal de Innovación del Ayuntamiento de Palma, para una adecuada funcionalidad de los sistemas, realizará las siguientes actuaciones:

- Actividades de autoridad de registro, con las actuaciones establecidas en el siguiente apartado, consistentes en la identificación previa a la obtención del certificado electrónico y, en su caso, de comprobación y suficiencia de los atributos

correspondientes, cargo y competencia de los firmantes/custodios, a través de la Oficina de Registro acreditada ante la FNMT-RCM.

- Reconoce el carácter universal de los certificados de firma electrónica que expide la FNMT-RCM.

- Resolver los recursos y reclamaciones de su competencia.

3. Régimen de las Oficinas de Registro y Acreditación:

- General: El número y ubicación de las Oficinas de Registro y Acreditación de Instituto Municipal de Innovación del Ayuntamiento de Palma, será el que se recoge en el Anexo II de esta Encomienda. En tales oficinas se llevarán a cabo las actividades de identificación, recepción y tramitación de solicitudes de expedición de certificados electrónicos. Cualquier modificación o alteración de dicha relación o de la ubicación de las Oficinas deberá ser comunicada a la FNMT-RCM, que deberá aceptar su alta o modificación, quien dará la oportuna difusión para mantener permanentemente actualizada la relación de la red de Oficinas de Registro y Acreditación para la obtención de certificados electrónicos en los términos previstos en el Real Decreto 1317/2001, de 30 de noviembre y resto de normativa aplicable.

  Las aplicaciones informáticas necesarias para llevar a cabo las actividades de acreditación e identificación serán facilitadas por la FNMT-RCM. Tales aplicaciones serán tecnológicamente compatibles en función de los avances tecnológicos y el estado de la técnica y contarán con sistemas para asegurar la confidencialidad y seguridad de las comunicaciones.

  Las solicitudes de emisión y revocación y/o suspensión, en su caso, de certificados se ajustarán a los modelos establecidos por la FNMT-RCM y a la Declaración de Prácticas de Certificación de la Entidad accesible como en la dirección:

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

- Para actuaciones en el ámbito del artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social: Instituto Municipal de Innovación del Ayuntamiento de Palma dispondrá de Oficina u Oficinas de Registro y Acreditación que deberán contar con los medios informáticos y sistemas de seguridad precisos para conectarse telemáticamente con la FNMT-RCM, previa aceptación de las condiciones de uso del sistema de registro. En ellas, la acreditación e identificación de los solicitantes de los certificados de ciudadanos 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, verificándose de conformidad y con pleno respeto a lo dispuesto en la normativa aplicable.

  Las acreditaciones realizadas surtirán plenos efectos y serán válidas para su aceptación por cualquier Administración Pública u otra entidad que admita los certificados emitidos por la FNMT-RCM.

- Para actuaciones en el ámbito de la Ley 40/2015, de 1 de octubre: Las Oficinas de Registro y Acreditación de Instituto Municipal de Innovación del Ayuntamiento de

Palma dependerán orgánica y funcionalmente de éste (sin perjuicio de las funciones de comprobación, coordinación y control de la FNMT-RCM) y determinarán la identidad y competencia de la propia Instituto Municipal de Innovación del Ayuntamiento de Palma y la de los diferentes usuarios (firmantes/custodios) designados por la Administración titular de los certificados, de conformidad con la DPC General y las Políticas y Prácticas de Certificación Particulares de Administración Pública, disponibles para consulta en la Web: ***https://www.sede.fnmt.gob.es/dpcs/acap*** correspondientes a los certificados y sistemas de firma electrónica de este ámbito de aplicación y con los formularios y condiciones de utilización de cada tipo de certificado.

A tal efecto, Instituto Municipal de Innovación del Ayuntamiento de Palma dispondrá de las Oficinas de Registro y Acreditación que considere necesarias 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, previa aceptación de las condiciones de uso del sistema de registro. En estas Oficinas de Registro, donde se acreditarán e identificarán a los titulares y custodios 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.

CUARTA. FINANCIACIÓN

Las partes de esta Encomienda asumirán, cada una, los costes por la actividad desplegada en el mismo de acuerdo con sus competencias. No obstante, Instituto Municipal de Innovación del Ayuntamiento de Palma asume la obligación de financiar las actuaciones específicas desarrolladas por la FNMT-RCM, en el marco competencial de actuación de la administración encomendante, teniendo en cuenta que la actividad de la FNMT-RCM está orientada a costes y su régimen se establece en el Estatuto de la Entidad y en la Ley.

1. REEMBOLSO DE GASTOS POR LA REALIZACIÓN DE ACTIVIDADES EN MATERIA DE CERTIFICACIÓN ELECTRÓNICA. La FNMT-RCM como compensación por las actividades, de carácter material o técnico, realizadas según el Capítulo I (Servicios EIT), en el Capítulo II (Servicios Avanzados) y en el Capítulo III (Servicios AP) del Anexo I, a Instituto Municipal de Innovación del Ayuntamiento de Palma percibirá, anualmente, la cantidad total de catorce mil novecientos sesenta y cuatro Euros (14.964,00€), impuestos no incluidos. En caso de que el período inicial de duración de la Encomienda sea inferior a un año, la cantidad anterior se prorrateará, reduciéndose proporcionalmente.

Si hubiera petición expresa, por parte de Instituto Municipal de Innovación del Ayuntamiento de Palma de extensión de otras actividades o funcionalidades, entre las recogidas en los Capítulos II y III, del Anexo II, la cantidad anterior quedaría incrementada por el importe correspondiente que se dedujera de la aplicación de las tablas, contenidas en dicho Anexo II, de la presente Encomienda.

2. REEMBOLSO EN AÑOS SUCESIVOS. En caso de prórroga de la Encomienda, se aplicará el mismo criterio en función de las compensaciones a percibir, actividades solicitadas y duración de las prórrogas.

3. FACTURACIÓN. La financiación de las actividades técnicas realizadas por la FNMT-RCM (que incluirá, en su caso, las actuaciones adicionales solicitadas), se efectuará al comienzo

de la realización de tales actividades y en cada anualidad. En función del tipo de prestación (suministros o servicios), a las cantidades finales acordadas entre las partes como financiación de las actividades, se aplicará el IVA legalmente vigente en cada momento.

El abono de las facturas se realizará, en un plazo no superior a treinta días de la fecha de factura, mediante transferencia bancaria a la cuenta de la FNMT-RCM:

- CCC: 0182 2370 49 0208501334
- IBAN: ES28 0182 2370 4902 0850 1334
- Código BIC: BBVAESMM,

Las facturas de la FNMT-RCM se emitirán a nombre de:

Denominación: _Institut Municipal d'Innovació de Palma_
Calle: _Joan Maragall, 3_
Población: _Palma_
Provincia: _Islas Baleares_
NIF: _P5790001A_
Departamento o persona de contacto: _Servicios Corporativos_
Datos para facturación electrónica (en su caso): _Código LA0001354 para Órgano Gestor, Oficina Contable y Unidad Tramitadora_

QUINTA. PLAZO DE DURACIÓN

Esta Encomienda entrará en vigor el día 16 de abril de 2022, y su duración se extenderá hasta el día 15 de abril de 2026.

SEXTA. REVISIÓN

Las partes podrán proponer la revisión o actualización de la Encomienda en cualquier momento de su vigencia, a efectos de incluir las modificaciones que resulten pertinentes.

SÉPTIMA. COMISIÓN

A instancia de cualquiera de las partes, podrá constituirse una Comisión Mixta con funciones de vigilancia y control, así como de resolución de cuestiones derivadas de los problemas de interpretación y cumplimiento de la presente Encomienda. Esta Comisión tendrá carácter de órgano colegiado y en sus funciones se regirá por lo establecido en la Ley 40/2015, de 1 de octubre.

OCTAVA. RESPONSABILIDAD

La FNMT-RCM, como prestador de las actividades descritas en la presente Encomienda, y Instituto Municipal de Innovación del Ayuntamiento de Palma, como destinatario de las mismas y encargado de las funciones incluidas en el procedimiento de identificación, acreditación y registro de los usuarios y, en su caso, de las administraciones y firmantes/custodios, responderán, cada una 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 de la presente Encomienda.

La FNMT-RCM, dado el mandato legal de extensión de estos servicios y actividades, limita su responsabilidad, siempre que su actuación o la de sus empleados no se deba a dolo o negligencia grave, hasta un importe anual de esta Encomienda incrementado en un 10% como máximo.

NOVENA. RESOLUCIÓN Y EXTINCIÓN

Causas de resolución. La FNMT-RCM estará obligada a la realización de las actividades previstas en esta Encomienda, a tenor de lo dispuesto en la legislación citada en este documento, por tanto, la Encomienda podrá resolverse, por parte de Instituto Municipal de Innovación del Ayuntamiento de Palma cuando existiera manifiesta falta de calidad en la realización de las actividades, por parte de la FNMT-RCM, o incumplimiento grave de las obligaciones de ésta en el desarrollo de su actuación.

La FNMT-RCM podrá instar la resolución de la Encomienda por falta de pago del precio acordado, por falta de consignación presupuestaria / reserva de crédito o por incumplimiento grave de las obligaciones que corresponden a Instituto Municipal de Innovación del Ayuntamiento de Palma.

Causas de extinción. Serán causas de extinción:

- El cumplimiento del plazo previsto en este documento y, en su caso, sus prórrogas.
- El mutuo acuerdo de las partes.

DÉCIMA. PROTECCIÓN DE DATOS

RÉGIMEN. El régimen de protección de datos de carácter personal derivado de esta Encomienda y de la actuación conjunta de las partes, será el previsto en 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 se deroga la Directiva 95/46/CE (Reglamento general de protección de datos - RGPD); en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), y en el Real Decreto 1720/2007, de 21 de diciembre, en lo que no se oponga a las normas antes citadas.

La FNMT-RCM ha creado un Registro de Actividades de Tratamiento y nombrado a un Delegado de Protección de Datos, con el fin de adaptarse al RGPD, que pueden consultarse en: http://www.fnmt.es/rgpd Instituto Municipal de Innovación del Ayuntamiento de Palma ha creado un Registro de Actividades de Tratamiento y nombrado a un Delegado de Protección de Datos, con el fin de adaptarse al RGPD, que pueden consultarse en: http://www.

COMUNICACIÓN DE DATOS. La comunicación de datos de carácter personal que Instituto Municipal de Innovación del Ayuntamiento de Palma realice a la FNMT-RCM sobre los datos de los empleados públicos de aquélla para la emisión de certificados de firma electrónica en el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (y, en su caso, en el del art. 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social), cuenta con el consentimiento del interesado que ha aceptado las condiciones de emisión del certificado al solicitar el mismo y ha sido informado sobre las finalidades del tratamiento de sus datos, sobre los posibles destinatarios y del resto de finalidades e información establecidos en las normas de aplicación (RGPD, art. 13 y

LOPDGDD, art. 11), según consta en el Registro de Actividades de Tratamiento antes señalado (Tratamiento nº 15).

Todo ello de conformidad con el art. 6.1. del RGPD, existiendo un interés legítimo de la Entidad ya que, además, tal comunicación resulta ineludible para que la FNMT-RCM expida los certificados de firma electrónica a los empleados de Instituto Municipal de Innovación del Ayuntamiento de Palma y, en su caso, a terceros.

ACCESO A LOS DATOS POR CUENTA DE TERCEROS (ENCARGADO DEL TRATAMIENTO).

En términos generales y de conformidad con el art. 11.2 de la Ley 40/2015, de 1 de octubre, la FNMT-RCM como entidad encomendada tendrá la condición de encargado del tratamiento de los datos de carácter personal a los que pudiera tener acceso en ejecución de la encomienda de gestión, siéndole de aplicación lo dispuesto en la normativa de protección de datos de carácter personal.

De manera específica, dados los mecanismos de gestión de la Plataforma de Registro y Acreditación, el encomendante también tendrá carácter de encargado del tratamiento en relación con el de acceso a datos personales si actuara como Oficina de Registro y Acreditación, por cuenta de la FNMT-RCM, de conformidad con los siguientes criterios y condiciones:

1) No tendrá carácter de comunicación de datos el acceso que Instituto Municipal de Innovación del Ayuntamiento de Palma, en calidad de Oficina de Registro y Acreditación de la FNMT-RCM, realice sobre los datos de carácter personal que la FNMT-RCM mantiene, como Responsable del tratamiento, sobre sus usuarios, personas físicas, con la finalidad de solicitar los servicios EIT en el ámbito del art. 81 de la Ley 66/1997, de 30 de diciembre, descritos en este documento. Tales datos son los que figuran en el tratamiento nº 15 del Registro de Actividades de Tratamiento (RAT) de la FNMT-RCM, descrito en el enlace anterior.

2) Por tanto, y de conformidad con el artículo 28 del RGPD, Instituto Municipal de Innovación del Ayuntamiento de Palma actuará en calidad de Encargado del tratamiento por cuenta de la FNMT-RCM y asumirá las obligaciones que se establecen en esta condición y en la legislación de aplicación.

3) Las actuaciones concretas que sobre el Tratamiento nº 15 del RAT de la FNMT-RCM que Instituto Municipal de Innovación del Ayuntamiento de Palma realizará sobre los datos serán los siguientes:

☒	Recogida	☒	Registro
☒	Estructuración	☒	Modificación
☒	Conservación	☒	Extracción
☒	Consulta	☐	Comunicación
☐	Difusión	☒	Interconexión
☒	Cotejo	☒	Limitación
☒	Supresión	☐	Destrucción
☐	Otros…	☐	Otros…

4) El Encargado del tratamiento, respecto de su actuación en esta Encomienda, se obliga a:

a) Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de esta Encomienda. En ningún caso, podrá utilizar los datos para fines propios.

b) Tratar los datos de acuerdo con las instrucciones del Responsable del tratamiento. Si el Encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el Encargado informará inmediatamente al Responsable.

c) Adoptar las medidas de seguridad que exige el Reglamento de desarrollo de la LOPD, el RGPD y las recomendaciones de la AEPD. Las medidas de seguridad se determinan en función del nivel de seguridad de los ficheros de la FNMT-RCM antes comunicadas y en función del modo y lugar de acceso a los datos personales por los Encargados.

Las medidas de seguridad implantadas para el tratamiento podrán ser objeto de modificación, supresión y/o novación en aras a dar cumplimiento a las exigencias que impone el Reglamento General de Protección de Datos y resto de normativa vigente relacionada. Al efecto se llevará a cabo una evaluación de riesgos, y evaluación de impacto y/o consulta previa, si procediera, en la que se determinará si se precisa implementar otras medidas más adecuadas para garantizar la seguridad del tratamiento, las cuales deberán ser adoptadas, documentando todo lo actuado. En cualquier caso, podrán acordarse aquellas que se establezcan en códigos de conducta, sellos, certificaciones o cualquier norma o estándar internacional actualizado de cumplimiento de protección de datos y seguridad de la información, a que el Responsable o Encargado se hallen adheridos.

Todo el personal al que el Encargado proporcione acceso a los datos personales deberá ser informado, de forma expresa, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

d) Llevar por escrito y estar disponible, un Registro Actividades de Tratamiento efectuados por cuenta del Responsable, que contenga (en su caso): las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas;

En ese registro, también se incluirá una descripción general de las medidas técnicas, organizativas y de seguridad relativas a:

- La seudonimización y el cifrado de datos personales (en su caso).
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

e) No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del Responsable del tratamiento, en los supuestos legalmente admitidos.

Si el Encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al Responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

f) No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del Encargado. El

Encargado podrá comunicar los datos a otros encargados del tratamiento del mismo Responsable, previo consentimiento y de acuerdo con las instrucciones del Responsable, indicando los tratamientos que se pretenden subcontratar e identificando, de forma clara e inequívoca, la empresa subcontratista y sus datos de contacto.

En caso de que el Responsable autorice la subcontratación de los servicios por parte del Encargado, éste se compromete a trasladar las obligaciones de este contrato a los subencargados.

g) Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud de la presente Encomienda, incluso después de que finalice el objeto del mismo.

h) Mantener a disposición del Responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i) Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j) Asistir al Responsable del tratamiento en la respuesta al ejercicio de los derechos de:

1. Acceso, rectificación, supresión y oposición
2. Limitación del tratamiento
3. Portabilidad de datos
4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

k) Si procede, designar un delegado de protección de datos y comunicar su identidad y datos de contacto al Responsable.

l) Devolver al Responsable los datos de carácter personal que hayan sido objeto de tratamiento. En todo caso, el encargado podrá conservar debidamente bloqueados aquellos datos que sean necesarios, en tanto pudieran derivarse responsabilidades de su relación con el Responsable del tratamiento.

5) El Responsable del tratamiento, respecto de su actuación en esta Encomienda, se obliga a:

a) Facilitar al Encargado el acceso a los datos que forman parte de sus ficheros o entregárselos del modo que resulte oportuno para la correcta prestación del servicio.

b) Informar conforme a la normativa a los interesados cuyos datos sean objeto de tratamiento y haber obtenido de los mismos lícitamente su consentimiento expreso o contar con motivos legítimos y acreditables para el mismo.

c) Tener establecida la base legal que legitima el tratamiento.

d) Disponer de mecanismos sencillos para que los interesados puedan ejercitar sus derechos.

e) Contar con análisis de riesgos, con un registro de los tratamientos y evaluaciones de impacto si fuera necesario por la naturaleza de los datos tratados.

f) Tener habilitadas las medidas de seguridad adecuadas para salvaguardar los datos en la transmisión de los datos al Encargado.

g) Nombrar un delegado de protección de datos en los casos que fuera obligatorio y comunicar su identidad al encargado. Actualmente y a la fecha de suscripción del presente contrato los datos del Delegado de Protección de Datos nombrado por la FNMT-RCM son los siguientes:

Delegado de Protección de Datos de la FNMT-RCM
Email: dpd@fnmt.es
Dirección: Calle Jorge Juan 106, CP: 28009 Madrid

En lo no previsto en este documento será de aplicación, en todo caso, la normativa vigente en materia de protección de datos personales.

UNDÉCIMA. DERECHO APLICABLE Y RESOLUCIÓN DE CONFLICTOS

La presente Encomienda la realiza Instituto Municipal de Innovación del Ayuntamiento de Palma a la FNMT-RCM, de conformidad con el artículo 11 de la Ley 40/2015, de 1 de octubre, tiene naturaleza administrativa, y se regirá por lo expresamente pactado por las partes en este documento, por las normas citadas en el mismo y, en su defecto, por las normas de derecho administrativo que resulten de aplicación.

Sin perjuicio de la facultad de las partes de constituir la Comisión Mixta establecida en la cláusula séptima, la realización de actividades previstas en esta Encomienda y Anexos, en cuanto al contenido y características de los mismos, se realizará con sujeción a la regulación contenida en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas; en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza; en 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.

Las partes se comprometen a resolver de mutuo acuerdo las incidencias que pudieran surgir en su interpretación y cumplimiento. Las cuestiones litigiosas que se suscitaran entre las partes durante el desarrollo y ejecución del mismo, se someterán, en caso de que sea de aplicación su intervención, al Servicio Jurídico del Estado y, en caso contrario, a la jurisdicción contencioso-administrativa, conforme a lo dispuesto en la Ley reguladora de la misma.

DUODÉCIMA. – EFICACIA

De conformidad con el artículo 11 de la Ley 40/2015, de 1 de octubre, esta Encomienda surtirá efectos desde el momento de su firma y, para su plena eficacia, se publicará en el Boletín Oficial del Estado, o en el Boletín oficial de la Comunidad Autónoma o en el de la Provincia, según la Administración a que pertenezca el órgano encomendante.

Y, en prueba de conformidad, ambas partes suscriben la presente Encomienda y todos sus Anexos, en el lugar y fecha indicados en el encabezamiento.

INSTITUTO MUNICIPAL DE INNOVACIÓN DEL AYUNTAMIENTO DE PALMA *Presidente*	**FÁBRICA NACIONAL DE MONEDA Y TIMBRE - REAL CASA DE LA MONEDA** 25388473S MARIA ISABEL VALLDECABRES (R: Q2826004J) Firmado digitalmente por 25388473S MARIA ISABEL VALLDECABRES (R: Q2826004J) Fecha: 2022.09.08 11:44:17 +02'00'
Adrián García Campos	*Isabel Valldecabres Ortiz*

ANEXO I

CAPITULO I - SERVICIOS EIT

La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT-RCM), como prestador de servicios de certificación, emitirá para todo aquel usuario que lo solicite un conjunto de certificados, denominado "Certificado Básico" o "Título de Usuario", que permite al Titular del mismo comunicarse con otros usuarios, de forma segura.

El formato de los certificados utilizados por la FNMT-RCM se basa en el definido por la Unión Internacional de Telecomunicaciones, sector de normalización de las telecomunicaciones, en la Recomendación UIT-T X.509, de 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

El certificado será válido para el uso con protocolos de comunicación estándares de mercado, tipo SSL, TLS, etc.

Como servicios de certificación asociados para el uso de los certificados por parte de sus titulares, la FNMT-RCM ofrecerá los siguientes servicios técnicos:

- registro de usuarios
- emisión, revocación y archivo de certificados de clave pública
- publicación de certificados y del Registro de Certificados
- registro de eventos significativos

GENERACIÓN Y GESTIÓN DE CLAVES

Generación y gestión de las claves

En el procedimiento de obtención de certificados, la FNMT-RCM desarrollará los elementos necesarios para activar, en el puesto del solicitante, el software que genere a través de su navegador web, un par de claves, pública y privada, que le permitirá firmar e identificarse, así como proteger la seguridad de sus comunicaciones a través de mecanismos de cifrado.

Las claves privadas serán utilizadas bajo el control del software de navegación web del que disponga el propio usuario, enviando todas las claves públicas a la FNMT-RCM con el fin de integrarlas en un certificado.

Las claves privadas de firma, permanecerán siempre bajo el control exclusivo de su titular, y guardadas en el soporte correspondiente, no guardándose copia de ellas por la FNMT-RCM.

La FNMT-RCM garantizará que el usuario, Titular del certificado, puede tener el control exclusivo de las claves privadas correspondientes a las claves públicas que se consignan en el certificado, mediante la obtención de las pruebas de posesión oportunas, a través de la adjudicación del número de identificación único.

Archivo de las claves públicas

Las claves públicas de los usuarios permanecerán archivadas, por si fuera necesario su recuperación, en archivos seguros, tanto física como lógicamente, durante un periodo no menor de 15 años.

Exclusividad de las claves

Las claves privadas son exclusivas para los Titulares de los certificados y son de uso personal e intransferible.

Las claves públicas son exclusivas para los Titulares de los certificados, independientemente del soporte físico donde estén almacenadas y protegidas.

Renovación de claves

La FNMT-RCM identifica una relación uno a uno entre la clave pública de un usuario y su certificado de clave pública, no previéndose utilizar distintos certificados para una misma clave. Es por esto que las claves se renovarán con los certificados cuando dicha renovación esté contemplada en la normativa específica aplicable.

REGISTRO DE USUARIOS

Registro de usuarios

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 Básico" o "Título de Usuario" 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 homogéneo 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.

Identificación de los solicitantes de los certificados, comprobación de su personalidad y constatación de su voluntad.-

La identificación de los solicitantes de los certificados en las oficinas de registro y la comprobación de su personalidad se hará mediante la exhibición del Documento Nacional de Identidad, Pasaporte u otros medios admitidos en derecho.

En el acto de registro, el personal encargado de las oficinas de acreditación constatará que el solicitante tiene la voluntad de solicitar que le sea emitido un certificado electrónico por la FNMT-RCM y que éste reúne los requisitos exigidos por el ordenamiento jurídico.

En caso de que solicite un certificado de persona jurídica, será de aplicación el procedimiento de verificación de la identidad del solicitante y de comprobación de los datos de constitución de la persona jurídica y de la suficiencia, extensión y vigencia de las facultades de representación del solicitante que se establece en el apartado 4 del Artículo 7 de la Ley 6/2020, de 11 de noviembre. El detalle del procedimiento figura en la Declaración de Prácticas de Certificación: https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

Necesidad de presentarse en persona

El procedimiento de registro requiere presencia física del interesado para formalizar el procedimiento de registro en la oficina de acreditación. No obstante, serán válidas y se dará el curso correspondiente a las solicitudes de emisión de certificados electrónicos cumplimentadas según el modelo aprobado por la FNMT – RCM para este fin siempre que la firma del interesado haya sido legitimada notarialmente en los términos señalados en el referido modelo.

Necesidad de confirmar la identidad de los componentes por la FNMT-RCM

Si se trata de solicitudes relativas a certificados electrónicos a descargar en un servidor u otro componente, la FNMT-RCM requerirá la aportación de la documentación necesaria que le acredite como responsable de dicho componente y, en su caso, la propiedad del nombre del dominio o dirección IP. (Certificado de componente no es un certificado reconocido ni se recoge en la legislación española)

Incorporación de la dirección de correo electrónico del titular al certificado

En su caso, la incorporación de la dirección de correo electrónico del titular al certificado se realizará a los efectos de que el certificado pueda soportar el protocolo S/MIME en el caso de que la aplicación utilizada por el usuario así lo requiera.

Cuando la dirección del correo electrónico del titular del certificado conste en una de las extensiones del propio certificado, ni la FNMT–RCM, como firmante y responsable del mismo, ni el_____ como encargado del registro de usuarios responden de que esta dirección esté vinculada con el titular del certificado.

Obtención del "Certificado Básico" o "Título de usuario"

Para la obtención de este certificado, así como para su revocación o suspensión, el solicitante deberá observar las normas y procedimientos desarrollados a tal fin por la FNMT-RCM de conformidad con la normativa vigente aplicable.

EMISIÓN, REVOCACIÓN Y ARCHIVO DE CERTIFICADOS DE CLAVE PÚBLICA

Emisión de los certificados

La emisión de certificados supone la generación de documentos electrónicos que acreditan la identidad u otras propiedades del usuario y su correspondencia con la clave pública asociada; del mismo modo, la emisión de los certificados implica su posterior envío al directorio de manera que sea accesible por todas las personas interesadas en hacer uso de sus claves públicas.

La emisión de certificados por parte de la FNMT-RCM, sólo puede realizarla ella misma, no existiendo ninguna otra entidad u organismo con capacidad de emisión de estos certificados.

La FNMT–RCM, por medio de su firma electrónica, garantizará los certificados, así como la verificación de la identidad y cualesquiera otras circunstancias personales de sus titulares. Por otro lado, y con el fin de evitar la manipulación de la información contenida en los certificados, la FNMT-RCM utilizará mecanismos criptográficos para asegurar la autenticidad e integridad de dicho certificado.

La FNMT - RCM, una vez emitido el certificado, lo publicará y mantendrá una relación de certificados emitidos durante todo el periodo de vida del mismo en un servicio de acceso telemático, universal, en línea y siempre disponible.

La FNMT-RCM garantiza para un certificado emitido:

a) Que el usuario dispone de la clave privada correspondiente a la clave pública del certificado, en el momento de su emisión.
b) Que la información incluida en el certificado se basa en la información proporcionada por el usuario.
c) Que no omite hechos conocidos que puedan afectar a la fiabilidad del certificado

Aceptación de certificados

✓ Para que un certificado sea publicado por la FNMT-RCM, ésta comprobará previamente:

a) Que el signatario es la persona identificada en el certificado
b) Que el signatario tiene un identificativo único
c) Que el signatario dispone de la clave privada

✓ El Instituto Municipal de Innovación del Ayuntamiento de Palma garantizará que, al solicitar un certificado electrónico, su titular acepta que:

a) La clave privada con la que se genera la firma electrónica corresponde a la clave pública del certificado.
b) Únicamente el titular del certificado tiene acceso a su clave privada.
c) Toda la información entregada durante el registro por parte del titular es exacta.
d) El certificado será usado exclusivamente para fines legales y autorizados y de acuerdo con lo establecido por la FNMT-RCM.
e) El usuario final del certificado no es un Prestador de Servicios de Certificación y no utilizará su clave privada asociada a la clave pública que aparece en el certificado para firmar otros certificados (u otros formatos de certificados de clave pública), o listados de certificados, como un Prestador de Servicios de Certificación o de otra manera.

- ✓ El Instituto Municipal de Innovación del Ayuntamiento de Palma garantizará que, al solicitar un certificado electrónico, su titular asume las siguientes obligaciones sobre su clave privada:

  a) A conservar su control.
  b) A tomar las precauciones suficientes para prevenir su pérdida, revelación, modificación o uso no autorizado.

Al solicitar el certificado, el titular deberá prestar su conformidad con los términos y condiciones de su régimen y utilización.

Revocación y suspensión de certificados electrónicos

La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, dejará sin efecto los certificados electrónicos otorgados a los usuarios cuando concurra alguna de las siguientes circunstancias:

a) Solicitud de revocación del usuario, por la persona física o jurídica representada por éste o por un tercero autorizado.
b) Resolución judicial o administrativa que lo ordene.
c) Fallecimiento o extinción de la personalidad del usuario o incapacidad sobrevenida.
d) Finalización del plazo de vigencia del certificado.
e) Pérdida o inutilización por daños en el soporte del certificado.
f) Utilización indebida por un tercero.
g) Inexactitudes graves en los datos aportados por el usuario para la obtención del certificado.
h) Cualquier otra prevista en la normativa vigente.

La extinción de la eficacia de un certificado producirá efectos desde la fecha en que la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda tuviera conocimiento cierto de cualquiera de los hechos determinantes de la extinción previstos en el apartado anterior y así lo haga constar en su Registro de certificados. En el supuesto de expiración del período de validez del certificado, la extinción surtirá efectos desde que termine el plazo de validez.

La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda podrá suspender temporalmente la eficacia de los certificados si así lo solicita el usuario o lo ordena una autoridad judicial o administrativa, o cuando existan dudas razonables, por parte de cualquier usuario público, sobre la vigencia de los datos declarados y su verificación requiera la presencia física del interesado. En este caso, la FNMT-RCM podrá requerir, de forma motivada, su comparecencia ante la oficina de acreditación donde se realizó la actividad de identificación previa a la obtención del certificado o, excepcionalmente, ante otra oficina de acreditación al efecto de la práctica de las comprobaciones que procedan. El incumplimiento de este requerimiento por un periodo de 10 días podrá dar lugar a la revocación del certificado.

La suspensión de los certificados surtirá efectos en la forma prevista para la extinción de su vigencia.

La extinción de la condición de usuario público se regirá por lo dispuesto en la presente Orden de encargo o lo que se determine, en su caso, por la normativa vigente o por resolución judicial o administrativa.

Comunicación y publicación en el Registro de Certificados de circunstancias determinantes de la suspensión y extinción de la vigencia de un certificado ya expedido.

La FNMT-RCM suministrará a el Instituto Municipal de Innovación del Ayuntamiento de Palma los mecanismos de la transmisión segura para el establecimiento de un servicio continuo e ininterrumpido de comunicación entre ambas a fin de que, por medios telemáticos o a través de un centro de atención telefónica a usuarios, se ponga de inmediato en conocimiento de la FNMT-RCM cualquier circunstancia de que tenga conocimiento y que sea determinante para la suspensión, revocación o extinción de la vigencia de los certificados ya expedidos, a fin de que se pueda dar publicidad de este hecho, de manera inmediata, en el directorio actualizado de certificados. a que se refiere el apartado 4 del artículo 9de la Ley 6/2020, de 11 de noviembre, de Servicios electrónicos de confianza,

La FNMT-RCM pondrá a disposición de los titulares de los certificados un centro de atención de usuarios que permitirá resolver cualquier duda o incidencia relativa a la validez o utilización de los certificados.

Además el citado centro de atención a los usuarios permitirá resolver cualquier duda o incidencia relativa a la validez o utilización de los certificados.

El Instituto Municipal de Innovación del Ayuntamiento de Palma y la FNMT-RCM responderán de los daños y perjuicios causados por cualquier dilación que les sea imputable en la comunicación y publicación en el Registro de Certificados, respectivamente, de las circunstancias de que tengan conocimiento y que sean determinantes de la suspensión, revocación o extinción de un certificado expedido.

PUBLICACION DE CERTIFICADOS DE CLAVE PÚBLICA Y REGISTRO DE CERTIFICADOS

-Publicación de certificados de clave pública

La FNMT-RCM publicará los certificados emitidos en un directorio seguro.

Cuando el certificado sea revocado, temporal o definitivamente, este será publicado en el Registro de certificados que incluirá una lista de certificados revocados, comprensiva de los certificados expedidos por la FNMT-RCM cuya vigencia se ha extinguido o suspendido al menos hasta un año después de su fecha de caducidad.

Esta publicación puede ser:

a) Publicación directa por parte de la FNMT-RCM.- Esta operación la realiza la FNMT-RCM a través de la publicación en un directorio propio. La actualización en el directorio seguro de las listas de revocación se realizará de forma continuada.
   La consulta de este directorio se realizará en línea, por acceso directo del usuario. Este servicio permite la disponibilidad continua y la integridad de la información almacenada en el directorio. Las listas de revocación serán firmadas con la clave privada de firma de la FNMT-RCM.
b) Publicación en directorios externos.- La FNMT-RCM podrá publicar externamente, en directorios públicos ofrecidos por otras entidades u Organismos, mediante replicación periódica o en línea, tanto certificados como listas de certificados

revocados. Estas listas, al igual que las publicadas internamente, irán firmadas con la clave privada de firma de la FNMT-RCM.

Frecuencia de la publicación en directorios externos

La publicación en directorios externos a la FNMT-RCM podrá ser realizada periódicamente o en línea, en función de los requerimientos de la entidad u Organismo que ofrezca el directorio.

Control de acceso

En la publicación directa por parte de la FNMT-RCM, el acceso al directorio se realizará con autenticación previa. Este acceso estará restringido a sólo lectura y búsqueda, pudiendo utilizar como clave de búsqueda cualquier información contenida en una entrada de un usuario.

En cuanto a las listas de revocación, tanto las publicadas interna como externamente, el acceso será público y universal, para verificar este hecho.

REGISTRO DE EVENTOS SIGNIFICATIVOS

Tipos de eventos registrados

La FNMT-RCM registrará todos aquellos eventos relacionados con sus servicios que puedan ser relevantes con el fin de verificar que todos los procedimientos internos necesarios para el desarrollo de la actividad se desarrollan de acuerdo a la normativa legal aplicable y a lo establecido en el Plan de Seguridad Interna, y permitan detectar las causas de una anomalía detectada.

Todos los eventos registrados son susceptibles de auditarse por medio de una auditoría interna o externa.

Frecuencia y periodo de archivo de un registro de un evento

La frecuencia de realización de las operaciones de registro dependerá de la importancia y características de los eventos registrados (bien sea para salvaguardar la seguridad del sistema o de los procedimientos), garantizando siempre la conservación de todos los datos relevantes para la verificación del correcto funcionamiento de los servicios.

El periodo de archivado de los datos correspondientes a cada registro dependerá asimismo de la importancia de los eventos registrados.

Archivo de un registro de eventos

La FNMT-RCM realizará una grabación segura y constante de todos los eventos relevantes desde el punto de vista de la seguridad y auditoría (operaciones realizadas) que vaya realizando, con el fin de reducir los riesgos de vulneración, mitigar cualquier daño que se produjera por una violación de la seguridad y detectar posibles ataques.

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

La FNMT-RCM mantendrá archivados todos los eventos registrados más importantes, manteniendo su accesibilidad, durante un periodo nunca inferior a 15 años.

En el caso del archivo histórico de los certificados, éstos permanecerán archivados durante al menos 15 años.

Datos relevantes que serán registrados

Serán registrados los siguientes eventos relevantes:

a) La emisión y revocación y demás eventos relevantes relacionados con los certificados.
b) Todas las operaciones referentes a la firma de los certificados por la FNMT-RCM.
c) Las firmas y demás eventos relevantes relacionados con las Listas de Certificados revocados.
d) Todas las operaciones de acceso al archivo de certificados.
e) Eventos relevantes de la generación de claves.
f) Todas las operaciones del servicio de archivo de claves y del acceso al archivo de claves propias expiradas.
g) Todas las operaciones relacionadas con la recuperación de claves.

Las funciones de administración y operación de los sistemas de archivado y auditoría de eventos serán siempre encomendadas a personal especializado de la FNMT-RCM.

Protección de un registro de actividad

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

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

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

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

La FNMT-RCM garantiza la existencia de copias de seguridad de todos los registros auditados.

CAPITULO II - SERVICIOS AVANZADOS

Certificados de componente

La FNMT-RCM emite certificados de componente genérico, de servidor y de firma de código, por lo que se hereda la confianza que representa la FNMT-RCM como Autoridad de Certificación instalada en los navegadores principales.

- *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 sello de entidad* es aquel que se utiliza habitualmente para establecer conexiones seguras entre componentes informáticos genéricos. Su flexible configuración permite dotarle de diferentes usos:

  Autenticación de componentes informáticos de una Entidad en su acceso a servicios informáticos, o a otras infraestructuras tecnológicas, con acceso restringido o identificación de cliente.
  Intercambio de mensajes o datos cifrados con garantías de confidencialidad, autenticación e integridad.

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.

CAPITULO III - SERVICIOS ADMINISTRACIÓN PÚBLICA (LEY 40/2015)

Servicio de Validación del Certificado de la AC Administración Pública/Sector Público

Para comprobar la validez del certificado de la Autoridad de Certificación de la Administración Pública/Sector Público, se ha dispuesto dos mecanismos para la descarga de la CRL asociada a dicho certificado. Ambos, se encuentran disponibles en el propio certificado de la AC, como CRLDistributionPoints y son, por este orden:

- **LDAP**

Localización del servicio ldap para la descarga de la CRL de la AC RAIZ de la FNMT-RCM:

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

Este servicio ldap se prestará en su versión 3, en modo binario, estando disponible en el puerto estándar para el servicio ldap (389), y sin requerir ningún tipo de autenticación.

La prestación del servicio será de carácter universal y sin control de acceso, teniendo únicamente la restricción de poder descargarse una única crl en cada conexión realizada que en este caso solo existe una CRL, la ARL.

El acceso a este servicio estará disponible a través de Internet así como a través de la Red SARA.

La CRL emitida para esta infraestructura tendrá un periodo de validez de 3 meses y se publicará 10 días antes de su caducidad y, en cualquier caso, siempre que se revoque algún certificado emitido por la AC RAIZ de la FNMT-RCM.

La FNMT-RCM se reserva el derecho a bloquear el acceso a aquellas direcciones IP para las que se observe un uso indebido o abusivo de este servicio.

- **HTTP**

Localización del servicio http para la descarga de la CRL de la AC RAIZ de la FNMT-RCM:

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

La CRL emitida para esta infraestructura tendrá un periodo de validez de 3 meses y se publicará 10 días antes de su caducidad y, en cualquier caso, siempre que se revoque algún certificado emitido por la AC RAIZ de la FNMT-RCM.

La prestación del servicio será de carácter universal, gratuito, y sin control de acceso, teniendo únicamente la restricción de poder descargarse una única crl en cada conexión realizada.

El acceso a este servicio estará disponible a través e Internet así como a través de la Red SARA.

La FNMT-RCM se reserva el derecho a bloquear el acceso a aquellas direcciones IP para las que se observe un uso indebido o abusivo de este servicio.

Servicio de Validación de Certificados de Entidad Final para Administración Pública

El servicio de Validación de Certificados para la infraestructura Administración Pública, se prestará mediante los siguientes servicios:

- Servicio de descarga de CRLs de AC Administración Pública/Sector Público mediante protocolo LDAP.
- Servicio de descarga de CRLs de AC Administración Pública mediante protocolo http.

La disponibilidad de múltiples servicios para la validación de certificados, proporciona compatibilidad total con las distintas necesidades de las aplicaciones en las que deberán integrarse los certificados de Entidad Final emitidos por la infraestructura de la Administración Pública.

Servicio de descarga de CRLs mediante protocolo LDAP

Este servicio será de carácter universal, anónimo, gratuito y si ningún tipo de autenticación, de tal forma que cualquier cliente podrá descargarse la CRL para poder validar un certificado de Entidad Final emitido por la AC Administración Pública/Sector Público.

Este servicio se prestará desde la siguiente URL en el puerto estándar ldap 389:

ldap://ldapape.cert.fnmt.es/CN=CRLnnn,OU=AC APE/SP, O=FNMT-RCM, C=ES ?certificateRevocationList ?base ?objectclass=cRLDistributionPoint

Este punto de distribución de CRLs, irá insertado en todos los certificados de Entidad Final emitidos por la AC de la Administración Pública/Sector Público, siendo en cada caso CRLnnn el número de CRL que le corresponde a dicho certificado.

El acceso a este servicio estará disponible a través de Internet así como a través de la Red SARA.

La FNMT-RCM se reserva el derecho a bloquear el acceso a aquellas direcciones IP para las que se observe un uso indebido o abusivo de este servicio.

Servicio de descarga de CRLs mediante protocolo HTTP.

Este servicio será de carácter universal, anónimo, gratuito y si ningún tipo de autenticación, de tal forma que cualquier cliente podrá descargarse la CRL para poder validar un certificado de Entidad Final emitido por la AC Administración Pública/Sector Público.

Este servicio se prestará desde la siguiente URL en el puerto estándar http 80:

http://www.cert.fnmt.es/crlsape/CRLnnn.crl

http://www.cert.fnmt.es/crlssp/CRLnnn.crl

Este punto de distribución de CRLs, irá insertado en todos los certificados de Entidad Final emitidos por la AC de la Administración Pública, siendo en cada caso CRLnnn el número de CRL que le corresponde a dicho certificado al igual que el anteriormente descrito.

El acceso a este servicio estará disponible a través de Internet así como a través de la Red SARA.

La FNMT-RCM se reserva el derecho a bloquear el acceso a aquellas direcciones IP para las que se observe un uso indebido o abusivo de este servicio.

CERTIFICADO DE FIRMA ELECTRONICA DEL PERSONAL AL SERVICIO DE LAS ADMINISTRACIONES PÚBLICAS Y CERTIFICADO DE FIRMA ELECTRÓNICA DEL PERSONAL AL SERVICIO DE LAS ADMINISTRACIONES PÚBLICAS CON SEUDÓNIMO

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 Cualificado de Servicios de Confianza.

El certificado para personal al servicio de la Administración Pública es desarrollado por la FNMT-RCM mediante una infraestructura PKI específica y ad hoc, basada en actuaciones de identificación y registro realizadas por la red de Oficinas de Registro designadas por el órgano, organismo o entidad Suscriptora del certificado. Los "Procedimientos 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.

Son expedidos por la FNMT-RCM como Prestador Cualificado de Servicios de Confianza cumpliendo con los criterios establecidos en la Ley 6/2020, de 11 de noviembre, citada y en la normativa técnica EESSI, concretamente de conformidad con el estándar europeo 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". Estos certificados electrónicos son emitidos exclusivamente al personal al servicio de la Administración, y por tanto no se emiten al público general.

Los certificados de firma electrónica del personal al servicio de la Administración Pública son cualificados 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. Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza (TSL, por sus siglas en inglés) de España, a través del enlace https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl..

El tamaño de las claves RSA relativas al certificado raíz de la Autoridad de certificación que emite los certificados electrónicos es actualmente de 4.096 bits.

El tamaño de las claves RSA relativas a los certificados electrónicos cualificados para identificar a los empleados públicos es actualmente de 2.048 bits.

El algoritmo de cifrado de todos los certificados emitidos es de SHA-265.

FNMT-RCM no regula el uso de este certificado, dado que se establece en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y demás legislación aplicable, limitándose a crear una infraestructura técnica a disposición de la Administración, Organismo o Entidad pública titular correspondiente. Asimismo, todas aquellas circunstancias y requisitos referentes a los usuarios, por la propia naturaleza de los certificados de empleado público, serán controlados, exclusivamente, por la Administración,

informando a la FNMT-RCM de su alteración o modificación; todo ello, a través de las Oficinas de Registro habilitadas por las Administraciones, Organismos y Entidades públicas.

Las Administraciones sólo 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.

El perfil del certificado es el descrito en las declaraciones de prácticas de certificación.

Servicio de firma electrónica centralizada para empleados públicos (firma en la nube)

La AC Sector Público expide certificados de firma electrónica centralizada para funcionarios, personal laboral, estatutario a su servicio y personal autorizado, al servicio de la Administración Pública, órgano, organismo público o entidad 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 certificado de firma electrónica centralizada para empleados públicos es un certificado cualificado para la creación de firmas electrónicas avanzadas generadas en un dispositivo de creación de firma remoto, en un entorno seguro y confiable. Esto es, la generación de las Claves pública y privada no se realiza directamente en el navegador de Internet del Firmante o en otro dispositivo en su poder, sino que se generan y se almacenan en un entorno seguro perteneciente a la FNMT-RCM. Para proveer este servicio, se ha integrado en la infraestructura de la FNMT-RCM, el módulo TrustedX eIDAS de Safelayer.

El Certificado de firma electrónica centralizada para empleado público, confirma de forma conjunta, la identidad del personal al servicio de las Administraciones Públicas, y al suscriptor del certificado, que es el órgano, organismo o entidad de la Administración Pública, donde dicho personal ejerce sus competencias, presta sus servicios, o desarrolla su actividad.

Asimismo, la firma electrónica se realiza de forma centralizada, garantizándose en todo momento el control exclusivo del proceso de firma por parte del Personal al servicio de la Administración al que se le ha expedido el Certificado. El acceso a las claves privadas del firmante se llevará a cabo garantizando siempre un Nivel de Aseguramiento ALTO (usuario+password + 2º factor de autenticación OTP).

Las funcionalidades y propósitos del Certificado de firma electrónica centralizada para empleado público permiten garantizar la autenticidad, integridad y confidencialidad de las comunicaciones. La expedición y firma del Certificado se realizará por la "AC Sector Público" subordinada de la "AC Raíz" de la FNMT-RCM.

Los Certificados de firma electrónica centralizada para empleado público expedidos por la FNMT-RCM tendrán validez durante un periodo máximo de tres (3) años contados a partir del momento de la expedición del Certificado, siempre y cuando no se extinga su vigencia. Transcurrido este periodo y si el Certificado sigue activo, caducará, siendo necesaria la expedición de uno nuevo en caso de que se desee seguir utilizando los servicios del Proveedor de Servicios de Confianza.

La longitud de la clave utilizada en la "AC Sector Público" es de 2048 bits y en la "AC Raíz" es de 4096 bits.

La validación del estado de vigencia de este tipo de certificados se puede comprobar a través del servicio de información y consulta del estado de los Certificados que provee la FNMT – RCM mediante el protocolo OCSP, disponible en la ubicación especificada en el propio certificado.

SELLO ELECTRÓNICO CUALIFICADO DE LAS ADMINISTRACIONES PÚBLICAS

Certificado cualificado de Sello electrónico para 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.

Se expiden de conformidad con el estándar europeo 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".

Los certificados de sello electrónico son cualificados 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. Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza (TSL, por sus siglas en inglés) de España, a través del enlace https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl.

La duración de los mismos se establece en 1 año y la longitud de clave RSA en 2.048 bits. Cuentan con servicio validación mediante OCSP, de libre acceso por parte de cualquier interesado, operativo las 24 horas del día, todos los días del año, y cuya URL, accesible desde internet, se refleja en los propios certificados.

FNMT-RCM no regula el uso de este certificado, dado que se establece en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y demás legislación aplicable, limitándose a crear una infraestructura técnica a disposición de los usuarios y custodios de la Administración, Organismo o Entidad pública titular del certificado, propietario o responsable de la unidad administrativa y del componente informático correspondiente. Asimismo, todas aquellas circunstancias y requisitos referentes a los usuarios y custodios, por la propia naturaleza de los certificados de Sello electrónico de las AA.PP., serán controlados, exclusivamente, por la Administración, informando a la FNMT-RCM de su alteración o modificación; todo ello, a través a través de las Oficinas de Registro habilitadas por las Administraciones, Organismos y Entidades públicas.

El perfil del certificado es el descrito en las declaraciones de prácticas de certificación.

CERTIFICADOS CUALIFICADOS DE AUTENTICACIÓN DE SITIOS WEB PARA SEDE ELELCTRÓNICA DE LAS ADMINISTRACIONES ELECTRONICAS

Certificados para la identificación de sedes electrónicas de la administración pública, organismos y entidades públicas vinculadas o dependientes emitidos por la FNMT – RCM bajo la denominación de certificados administración.

Se expiden de conformidad con los estándares europeos:

- ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates"
- ETSI EN 319 412-4 "Certificate profile for web site certificates".

Adicionalmente, cumplen con todos los requisitos establecidos por el CA/Browser Forum en sus especificaciones:

- "Baseline requirements for the issuance and management of publicly Trusted Certificates".
- "Guidelines for the issuance and management of extended validation certificates".

Estos certificados se expiden como cualificados 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, de conformidad con los estándares europeos ETSI EN 319 411-1 "Policy and Security Requirements for Trust Services Providers issuing certificates- General Requirements. Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza (TSL, por sus siglas en inglés) de España, a través del enlace https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl.

La duración de los mismos se establece en 1 año y la longitud de la clave ECC (Elliptic Curve Criptography) es de 384 bits. La utilización de la más moderna tecnología criptográfica de curvas elípticas, en sustitución de la anterior tecnología basada en el algoritmo RSA, ha permitido reducir considerablemente la longitud de la clave, manteniendo e incluso superando las características de seguridad (una clave ECC de 384 bits es equivalente a una clave RSA de aproximadamente 7680 bits1), lo que asegura operaciones criptográficas más rápidas y eficaces en entornos más seguros todavía.

Estos certificados cuentan con servicio de validación mediante OCSP, de libre acceso por parte de cualquier interesado, operativo las 24 horas del día, todos los días del año, y cuya URL, accesible desde internet, se refleja en los propios certificados.

FNMT-RCM no regula el uso de este certificado, dado que se establece en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y demás legislación aplicable, limitándose a crear una infraestructura técnica a disposición de los usuarios y custodios de la Administración, Organismo o Entidad pública titular de la Sede electrónica correspondiente. Asimismo, todas aquellas circunstancias y requisitos referentes a los usuarios y custodios, por la propia naturaleza de los certificados para la identificación de Sedes electrónicas, serán controlados, exclusivamente, por la Administración, informando a la FNMT-RCM de su alteración o modificación; todo ello, a través a través de las Oficinas de Registro habilitadas por las Administraciones, Organismos y Entidades públicas.

El perfil del certificado es el descrito en las declaraciones de prácticas de certificación.

ANEXO II

CAPITULO I - SERVICIOS EIT

1. Precio anual de los servicios

Se establece un precio fijo para los servicios EIT de 1.764,00 Euros al año, impuestos no incluidos.

Se establece un precio fijo de 78,00 euros/año por cada registrador adicional.

2. Soporte Técnico

El coste del soporte técnico especializado realizado por parte de personal de la FNMT-RCM será de 122,64 Euros/hora.

En el caso en que el soporte técnico se preste en las instalaciones del conviniente, a la tarifa anterior le serán añadidos los gastos derivados de la estancia fijados en 204,38 Euros/día por persona, más los derivados del desplazamiento y pernocta.

3. Condiciones

A todas las cantidades expuestas en el capítulo I del presente Anexo habrá que añadirlas el IVA legalmente establecido.

CAPITULO II - SERVICIOS AVANZADOS

1. **Certificados de componente**

El precio anual establecido en el apartado I del Capítulo III de este anexo de precios incluye la emisión de un número máximo de 5 certificados de componente (SSL, Sello de entidad, Wildcard).

El precio de los certificados de componentes adicionales será el estipulado en el apartado correspondiente de la página web de Ceres:

www.cert.fnmt.es/catalogo-de-servicios/certificados-electronicos

2. **Servicio de Sellado de Tiempo**

El precio anual establecido en el apartado I del Capítulo III de este anexo de precios incluye la prestación de este servicio.

CAPITULO III - SERVICIOS ADMINISTRACIÓN PÚBLICA (LEY 40/2015)

1. Certificados para los servicios del ámbito de la Ley 40/2015

El precio anual para los servicios del ámbito de la Ley 40/2015 asciende a 13.200,00 Euros/año impuestos no incluidos, incluye la emisión de todos certificados de empleado público que el conviniente requiera (sw, con seudónimo y firma centralizada), 1 certificado de sede electrónica y 3 certificados de sello electrónico.

2. Condiciones

A todas las cantidades expuestas en el capítulo III del presente Anexo habrá que añadirlas el IVA legalmente establecido.

3. Condiciones

A todas las cantidades expuestas en el capítulo II del presente Anexo habrá que añadirlas el IVA legalmente establecido.