Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

Ajuntament de Palma
Secretaria General del Ple
REGISTRE DE CONVENIS I PROTOCOLS
Data 0 8 FEB. 2019
Nº Ordre 1634

Institut Municipal d'Innovació de Palma

CONVENIO DE COLABORACIÓN INTERADMINISTRATIVA ENTRE LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA Y EL INSTITUTO MUNICIPAL DE INNOVACIÓN DEL AYUNTAMIENTO DE PALMA PARA LA EXTENSIÓN DE LOS SERVICIOS PÚBLICOS ELECTRÓNICOS.

En Madrid, a ____ de - 3 OCT. 2018 de 20__

REUNIDOS

De una parte, don Adrián García Campos, Concejal del Area de Economía, Hacienda y Innovación i Presidente del Instituto Municipal de Innovación del Ayuntamiento de Palma en nombre y representación del Instituto Municipal de Innovación, 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 del día 28 de Septiembre de 2018 y por la Junta de Gobierno de Palma en sesión del día 3 de Octubre de 2018

Y de otra, Don Jaime Sánchez Revenga, como Director General, cargo para el que fue nombrado por el Real Decreto 286/2012, de 27 de enero, BOE núm. 24 de 28 de enero de 2012, en nombre y representación de la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT – RCM), según resulta del artículo 19 de su Estatuto, siendo esta entidad Organismo Público, Entidad Pública Empresarial, teniendo su domicilio institucional en Madrid, calle Jorge Juan número 106 y código de identificación Q28/26004 – J.

Ambas partes, reconociéndose respectivamente capacidad legal y competencia suficientes para formalizar el presente Convenio,

EXPONEN

PRIMERO. - La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que para el funcionamiento de las Administraciones Públicas la utilización de los medios electrónicos ha de ser lo habitual (firma y sedes electrónicas, el intercambio electrónico de datos en entornos cerrados de comunicación y la actuación administrativa automatizada mediante sello electrónico).

Por su parte, la Ley 59/2003, de 19 de diciembre, de firma electrónica, establece las bases de regulación de la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación, tanto para el sector público como el privado. El artículo 4 de esta Ley establece el empleo de la firma electrónica en el ámbito de las Administraciones Públicas, para que, con el objetivo básico de salvaguardar las garantías de cada procedimiento, se puedan establecer condiciones adicionales.

La disposición adicional cuarta de la Ley 59/2003, antes citada, constata la especialidad en la regulación que afecta a la actividad de la FNMT-RCM, al señalar que, lo dispuesto en esa Ley se entiende sin perjuicio de lo establecido en el artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social.

SEGUNDO. - El citado artículo 81 de la Ley 66/1997, de 30 de diciembre, y la normativa de desarrollo prevista en el Real Decreto 1317/2001, de 30 de noviembre, facultan a la FNMT-RCM para que, mediante convenio de colaboración, extienda la utilización de la Plataforma Pública de Certificación mediante técnicas y medios electrónicos, informáticos y telemáticos (EIT), a las Administraciones, organismos y entidades públicas en el actual marco de impulso de la Administración electrónica, tal y como se desprende de las modificaciones introducidas en el referido artículo 81 por las Leyes 55/1999, 14/2000, 44/2002, 53/2002 y 59/2003.

TERCERO. - La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, reconoció el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos y los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa en las relaciones entre las Administraciones Públicas, partiendo de un principio general de cooperación entre administraciones para el impulso de la administración electrónica. También se regulan las relaciones de los ciudadanos con las administraciones con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas derogó, con efectos 2 de octubre de 2016, la Ley 11/2007, de 22 de junio. Esta Ley consolida el derecho de los ciudadanos a relacionarse, preferentemente por medios electrónicos, con las administraciones públicas admitiendo diversos sistemas electrónicos para identificación y firma por parte de los interesados, siendo, no obstante, obligatoria la utilización de medios electrónicos para trámites administrativos a determinados colectivos (personas jurídicas, entidades sin personalidad jurídica, profesionales colegiados, etc.), según las normas de desarrollo.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, antes mencionada, recoge, con las adaptaciones necesarias, las normas hasta ahora contenidas en la Ley 11/2007, de 22 de junio, en lo relativo al funcionamiento electrónico del sector público, y algunas de las previstas en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la anterior. La Ley establece que la utilización de los medios electrónicos ha de ser lo habitual, 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.

CUARTO. - La FNMT-RCM ha desarrollado, desde 1999, 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.

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 existente con CERES y transferencia de tecnologías entre Administraciones Públicas.
- Reutilización de tecnologías, equipamientos, tarjetas y aplicaciones actualmente en uso.

QUINTO. - Por otra parte, el Real Decreto 589/2005, de 20 de mayo, por el que se reestructuran los órganos colegiados responsables de la Administración electrónica, estableció, en su Disposición adicional cuarta, que la prestación de los servicios de certificación y firma electrónica realizados por la FNMT-RCM en el ámbito público, se desarrollarán de acuerdo con las normas que le son de aplicación y tendrá la consideración de proyecto de interés prioritario. Este Real Decreto fue derogado por el Real Decreto 806/2014, de 19 de septiembre, sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus Organismos Públicos, que mantiene, en su artículo 11, este tipo de proyectos cuando tengan como objetivo la colaboración y cooperación con las comunidades autónomas y los entes que integran la Administración local y la Unión Europea en materia de Administración digital.

SEXTO. - El régimen de colaboración administrativa entre la FNMT-RCM y el Instituto Municipal de Innovación del Ayuntamiento de Palma en cuanto al ejercicio de las respectivas competencias se ha instrumentado tradicionalmente y sin discontinuidad del servicio durante los últimos 8 años a través del clásico Convenio, que correspondería a lo que actualmente de forma análoga se recoge en los artículos 47 y siguientes y la Disposición adicional séptima, de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que dispone que la Administración General y los Organismos públicos, vinculados o dependientes de la misma, podrán celebrar convenios de colaboración (en este caso interadministrativos) con los órganos correspondientes de las Administraciones de las Comunidades Autónomas para la utilización de medios, servicios y recursos en el ejercicio de competencias propias o delegadas. Todo ello en relación con el artículo 57 y concordantes de la Ley 7/1985, de 2 de abril, de Bases de Régimen Local.

De acuerdo con lo expuesto, ambas partes formalizan la presente encomienda de gestión intrumentada también en forma de Convenio de Colaboración Interadministrativa, según se recoge en el artículo 11 de la referida Ley 40/2015, conformidad con las siguientes

CLÁUSULAS

PRIMERA. - OBJETO

Constituye la finalidad de este Convenio de Colaboración, la creación del marco de actuación institucional entre las dos partes firmantes, que permita el impulso de servicios públicos electrónicos y el cumplimiento de los derechos de acceso electrónico de los ciudadanos a los servicios públicos reconocidos en la Ley 39/2015 y 40/2015, ambas de 1 de octubre, a través de la extensión al ámbito de competencias del Instituto Municipal de Innovación del Ayuntamiento de Palma de la Plataforma Pública de Certificación y de servicios electrónicos, informáticos y telemáticos desarrollada por la 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 este Convenio, tanto para identificación de las Administraciones Públicas, como de los ciudadanos (según las leyes citadas).

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

1.2. - Hasta 5 certificados de Representante de Persona Jurídica para el Instituto Municipal de Innovación del Ayuntamiento de Palma emitidos por la AC Representación.

1.3. - Expedición y gestión del ciclo de vida de certificados recogidos en la Ley 40/2015, de 1 de octubre:

Ilimitados certificados de Empleado Público y certificados de Empleado Público con Seudónimo

1 Certificados de Sede Electrónica (autenticación de sitio Web)

3 Certificados de Sello Electrónico de Administración Pública.

1.4. - Expedición y gestión del ciclo de vida de 5 certificados de componente y firma de código, recogidos en el Capítulo II del Anexo I,

2. - Emisión de Sellos de Tiempo en las comunicaciones electrónicas, informáticas y telemáticas que tengan lugar al amparo del presente Convenio, 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.

SEGUNDA. - ÁMBITO DE APLICACIÓN

El ámbito de aplicación del presente Convenio es el Ayuntamiento de Palma, sus órganos, unidades administrativas y organismos autónomos dependientes.

TERCERA. - ACTIVIDAD DE LAS PARTES

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 este Convenio y en la normativa referida en el mismo, la puesta a disposición del Instituto Municipal de Innovación del Ayuntamiento de Palma de la Plataforma Pública de Certificación desarrollada para la Administración Electrónica, para ofrecer seguridad en la utilización de instrumentos de identificación electrónica por parte de los ciudadanos. 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, con efectos en el ámbito público y para todos los ciudadanos del territorio nacional que opten por el acceso electrónico a través de esta Entidad, cumpliendo, por tanto, 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 competencias dirigidas a la implementación de las Plataformas en sus procedimientos, extendiéndose a la identificación y registro de sus empleados, así como, en su caso, la acreditación y valoración de la identidad y capacidad, de los ciudadanos, que ejerzan los derechos de acceso electrónico a los Servicios Públicos de Instituto Municipal de Innovación del Ayuntamiento de Palma y el resto de actividades recogidas en este Convenio.

Para la adecuada consecución del objeto de este Convenio, las partes han de desplegar una serie de actuaciones de colaboración, que son:

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

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 el objeto, 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 al Instituto Municipal de Innovación del Ayuntamiento de Palma, para aplicaciones y sistemas del 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 este Convenio.
- Asistencia técnica, de conformidad con lo establecido en los Anexos, con objeto de facilitar al 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 del 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 del Instituto Municipal de Innovación del Ayuntamiento de Palma y de los Juzgados, Tribunales y, en su caso, órganos administrativos y/o supervisores competentes, acreditativos de la actividad realizada por la FNMT-RCM en virtud del presente Convenio.
- Tener disponible para consulta del Instituto Municipal de Innovación del Ayuntamiento de Palma y de los usuarios una Declaración de Prácticas de Certificación (DPC), que contendrá, al menos, las especificaciones establecidas en el artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica. Tal DPC, 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 la dirección Web de la FNMT. 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.

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 Dirección General de Tecnologías de la Información y las Comunicaciones a los efectos de coordinación e interoperabilidad correspondientes para el desarrollo de la Administración electrónica.

2. - El Instituto Municipal de Innovación del Ayuntamiento de Palma realizará las siguientes actuaciones:

2.1- De carácter administrativo y de desarrollo de sus competencias:

- Emitir, cuando proceda, el recibo de presentación firmado electrónicamente, donde se haga constancia expresa de la fecha y hora de recepción de las comunicaciones recibidas, de conformidad con lo dispuesto en la normativa aplicable.
- Conservar las notificaciones, comunicaciones o documentación emitida y recibida en las transacciones y actos durante el tiempo pertinente.
- Cifrar las comunicaciones emitidas y recibidas.
- Realizar las actividades de autoridad de registro 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.
- Reconocer el carácter universal de los certificados de firma electrónica que expide la FNMT-RCM y que, por tanto, servirán para las relaciones jurídicas que mantengan los usuarios con las diferentes Administraciones públicas y, en su caso, en el ámbito privado que admitan la utilización de estos certificados, en sus registros, procedimientos y trámites. De esta forma, los certificados que haya expedido o expida la FNMT-RCM, para otros órganos, organismos y administraciones en el ámbito público de actuación, podrán ser utilizados por los usuarios en sus relaciones con el Instituto Municipal de Innovación del Ayuntamiento de Palma_ cuando así lo admita el ordenamiento jurídico.
- Resolver los recursos y reclamaciones de su competencia.

Régimen de las Oficinas de Registro y Acreditación.

* General

El número y ubicación de las Oficinas de Registro y Acreditación donde se llevarán a cabo las actividades de identificación, recepción y tramitación de solicitudes de expedición de certificados electrónicos será informado a la FNMT – RCM, así como cualquier modificación o alteración de dicha relación o de la ubicación de las Oficinas.

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.

Las solicitudes de emisión y revocación y/o suspensión, en su caso, de certificados se ajustarán a los modelos aprobados por la FNMT – RCM y a los procedimientos recogidos en 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 los servicios del artículo 81 de la Ley 66/1997,

El Instituto Municipal de Innovación del Ayuntamiento de Palma dispondrá de Oficina u Oficinas de Registro y Acreditación que deberán contar con los medios informáticos precisos para conectarse telemáticamente con la FNMT-RCM. En ellas, la acreditación e identificación de los solicitantes de los certificados de persona física 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.

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

* Para los servicios de la Ley 40/2015.

Las Oficinas de Registro y Acreditación del Instituto Municipal de Innovación del Ayuntamiento de Palma para el ámbito de la Ley 40/2015, dependerán orgánica y funcionalmente de esta Administración (sin perjuicio de las funciones de comprobación,

coordinación y control de la FNMT-RCM) y determinarán la identidad y competencia del propio Instituto Municipal de Innovación del Ayuntamiento de Palma y la de los diferentes usuarios (firmantes/custodios) designados por la Administración suscriptora 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/normativa/declaracion-de-practicas-de-certificacion

A tal efecto, el Instituto Municipal de Innovación del Ayuntamiento de Palma dispondrá de la/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. 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 este Convenio asumirán cada una los costes por la actividad desplegada en el mismo de acuerdo con sus competencias.

No obstante, el Instituto Municipal de Innovación del Ayuntamiento de Palma asume la obligación de financiar las actuaciones desarrolladas por la FNMT-RCM, desarrolladas específicamente para la Instituto Municipal de Innovación del Ayuntamiento de Palma en el marco competencial de actuación de esta administración, de conformidad con lo que se relaciona a continuación:

1. - REEMBOLSO DE GASTOS POR COLABORACIÓN ADMINISTRATIVA EN MATERIA DE CERTIFICACIÓN ELECTRÓNICA.

La FNMT-RCM, como compensación por su actividad de extensión de la Administración Electrónica desarrollada según las condiciones del presente Convenio percibirá la cantidad de sesenta y cinco mil euros (65.000,00€/ año), impuestos no incluidos. Siendo el IVA de aplicación un 21% de dicho importe (13.650,00 Euros), la compensación anual es de cincuenta y cinco mil setecientos cuarenta y cuatro con sesenta y cinco céntimos (78.650,00 Euros), IVA incluido.

Tanto durante el primer año, como en el de los siguientes, si hubiera petición expresa, por parte del Instituto Municipal de Innovación del Ayuntamiento de Palma, de extensión de otras funcionalidades de entre las recogidas en el Anexo I, la cantidad anterior quedaría incrementada por el importe correspondiente que se dedujera de la

aplicación de las tablas del Anexo II, de Precios y Plan de Implantación, del presente Convenio.

2. - FACTURACIÓN. La FNMT-RCM, podrá realizar facturaciones semestrales contra certificaciones o autorizaciones parciales conformadas por el Instituto Municipal de Innovación del Ayuntamiento de Palma mediante el prorrateo de la cantidad anual a abonar pudiendo, además, liquidar en tales facturas mensuales aquellos servicios adicionales solicitados. El abono de las facturas se realizará mediante transferencia bancaria a la cuenta de la FNMT-RCM: (Código Cuenta : 0182 2370 49 0208501334 IBAN : ES28 0182 2370 4902 0850 1334 Código BIC: BBVAESMM), en un plazo no superior a treinta días de la fecha de factura.

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

Denominación: Instituto Municipal de Innovación del Ayuntamiento de Palma
Domicilio: C/ Joan Maragall, 3
Población: Palma
Provincia: Illes Balears
NIF: P5790001A

Departamento o persona de contacto / Teléfono: José Llull Pastor /971 46 6000 ext. 3066

3. - SERVICIOS DE VALIDACIÓN

De conformidad con el artículo 24.4 del "REGLAMENTO (UE) nº 910/2014 del PARLAMENTO EUROPEO y del CONSEJO, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE", la puesta a disposición de la información sobre el estado de validez de los certificados reconocidos o cualificados, que emita la FNMT-RCM, no tendrán coste para las Administraciones Públicas.

4. - ACTUALIZACIÓN IMPORTES. Si el presente Convenio se prorrogase y no se hubiera establecido el importe del reembolso de gastos a percibir, por la FNMT-RCM en las siguientes anualidades, el importe anual de cada una de las prórrogas y de los importes consignados en el Convenio y Anexos, se actualizará mediante la aplicación, al importe anual anterior, de la variación del 85% del Índice de Precios de Consumo, IPC (índice general interanual), publicado y producido durante los doce meses anteriores a la fecha en que se produzca la actualización.

QUINTA. - PLAZO DE DURACIÓN

El presente Convenio entrará en vigor el día 16 de abril de 2018 y su duración se extenderá hasta el 15 de abril de 2022, teniendo en cuenta lo establecido en la cláusula duodécima.

El régimen de colaboración administrativa prevista en este Convenio más allá de su duración inicial solo podrá realizarse por nuevo Convenio.

SEXTA. - REVISIÓN

Las partes podrán proponer la revisión del Convenio en cualquier momento de su vigencia, a efectos de incluir, de mutuo acuerdo, 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 del presente Convenio.

OCTAVA. - RESPONSABILIDAD

La FNMT-RCM y el Instituto Municipal de Innovación del Ayuntamiento de Palma a los efectos previstos en el objeto de este Convenio, responderán cada una en el ámbito de sus respectivas funciones y competencias, en relación con los daños y perjuicios que causara el funcionamiento del sistema de acuerdo con las reglas generales del ordenamiento jurídico que resultaran de aplicación y de conformidad con las obligaciones asumidas a través del presente Convenio.

La FNMT-RCM, dado el mandato legal de extensión de los servicios, limita su responsabilidad, siempre que su actuación o la de sus empleados no se deba a dolo o negligencia grave, hasta un importe anual del presente Convenio incrementado hasta un 10% como máximo.

NOVENA. - RESOLUCIÓN Y EXTINCIÓN DEL CONVENIO

El Convenio podrá resolverse a instancia de la parte perjudicada, cuando existieran incumplimientos graves de las respectivas obligaciones atribuidas en este instrumento.

La FNMT-RCM podrá instar la resolución del Convenio por el incumplimiento grave de las obligaciones correspondientes al Instituto Municipal de Innovación del Ayuntamiento de Palma, en especial, por el incumplimiento de las obligaciones de reembolso de gastos previstas.

Por su parte, el Instituto Municipal de Innovación del Ayuntamiento de Palma podrá instar la resolución cuando la FNMT-RCM realizara su actividad de carácter material y técnico con manifiesta falta de calidad.

Causas de extinción. Serán causas de extinción:

- El cumplimiento del plazo previsto en el convenio y sus prórrogas.

- El mutuo acuerdo de las partes.

DÉCIMA- PROTECCIÓN DE DATOS PERSONALES

La FNMT-RCM publica toda la información relativa a datos de carácter personal, para su consulta por parte de las partes interesadas, en el siguiente sitio web:

http://www.fnmt.es/rgpd

Plan de privacidad

El tratamiento de datos de carácter personal que realiza la FNMT-RCM cumple con lo dispuesto 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, en adelante RGPD), así como con los requisitos que sean de aplicación por normativa nacional específica en esta materia.

Información tratada como privada

La FNMT-RCM considera como privada toda la información personal sobre las personas físicas usuarias de los servicios de confianza que no deba ser incorporada en los certificados y en los mecanismos que utiliza el Servicio de información y consulta sobre el estado de validez de los certificados.

En todo caso, es considerada información privada toda información personal recabada en los procesos de solicitud, renovación y revocación de certificados electrónicos (con la salvedad indicada en el siguiente apartado), las claves privadas que obrasen en poder del Prestador de Servicios de Confianza, así como toda aquella claramente identificada como tal.

La FNMT-RCM aplica las salvaguardas apropiadas para proteger la información privada.

Información no considerada privada

No se considera información privada aquella que se incorpora a los certificados electrónicos, la información relativa al estado de vigencia de los mismos, la fecha de inicio de dicho estado (activo, revocado, caducado…), así como el motivo que provocó el cambio de estado. Por tanto, los Certificados electrónicos, las Listas de Certificados Revocados y cualquier contenido de los mismos no es considerada información privada.

Responsabilidad de proteger la información privada

La FNMT-RCM adopta las medidas de seguridad requeridas de conformidad con el RGPD en cuanto al acceso y tratamiento que realiza sobre los datos personales de solicitantes y suscriptores de los Certificados.

Las medidas técnicas y organizativas se establecerán teniendo en cuenta el coste de la técnica, los costes de aplicación, así como la naturaleza, el alcance, el contexto y los fines del tratamiento y los riesgos para los derechos y libertades.

Delegado de Protección de Datos

El RGPD establece la obligación de designar un Delegado de Protección de Datos (DPD) a toda autoridad u organismo del sector público que lleve a cabo tratamiento de datos personales. Los datos de contacto del DPD de la FNMT-RCM están publicados en el sitio web referenciado en el primer punto del presente apartado "9.4 Protección de datos personales". Dichos datos de contacto incluyen la dirección de correo electrónico a la que los interesados pueden dirigir todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos, de conformidad con el artículo 38.4 del RGPD.

Registro de actividades de tratamiento

La FNMT-RCM cuenta con un registro de las actividades de tratamiento que realiza bajo su responsabilidad, entre los que se encuentra el de "gestión de la PKI" relativo a la actividad que realiza esta Entidad como Prestador de Servicios de Confianza. Dicho registro incluye, para cada tratamiento identificado, la siguiente información:

a. Finalidad
b. Entidad responsable
c. Categorías de datos personales
d. Quién proporciona los datos
e. Quién es el afectado de los datos personales
f. Quiénes son los encargados del tratamiento

g. Comunicaciones de datos
h. Transferencias internacionales de datos
i. Plazo de supresión
j. Medidas de seguridad

El documento de Registro de actividades de tratamiento puede consultarse en el sitio web referenciado en el primer punto del presente apartado "9.4 Protección de datos personales".

Derechos de los interesados

Los interesados podrán ejercer los derechos de acceso, rectificación, supresión, limitación de tratamiento, oposición y portabilidad de los datos, conforme a lo establecido en los artículos 15 a 22 del RGPD, dirigiéndose al responsable del tratamiento por vía electrónica, a través de la sede electrónica de la FNMT-RCM, o presencialmente a través del Registro General de dicha Entidad.

Cooperación con las Autoridades

La FNMT-RCM cooperará con la Agencia Española de Protección de Datos cuando sea requerida.

Notificación de violaciones de seguridad

La FNMT-RCM notificará a la Agencia Española de Protección de Datos (AEPD) cualquier violación de seguridad1 en materia de datos personales, sin dilación posible y, en todo caso, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella, siempre que esta sea susceptible de constituir un riesgo para los derechos las libertades de las personas físicas afectadas.

En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la AEPD se complementará con una notificación dirigida a estos últimos, al objeto de permitirles la adopción de medidas para protegerse de sus consecuencias.

Aviso y consentimiento para usar información privada

La obtención de información privada de las personas físicas en los procesos ligados al ciclo de vida de los Certificados (solicitud, acreditación de la identidad, renovación, revocación…) se realizará, en cualquier caso, previa obtención del consentimiento de dichas personas de forma inequívoca, es decir, mediante una manifestación del interesado o mediante una clara acción afirmativa.

[1] Según el RGPD, violación de seguridad de los datos incluye todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Divulgación conforme al proceso judicial o administrativo

La FNMT-RCM no divulgará datos personales, salvo petición por parte de las autoridades administrativas o judiciales.

Otras circunstancias de divulgación de información

No estipuladas.

UNDÉCIMA. - DERECHO APLICABLE Y RESOLUCIÓN DE CONFLICTOS

Sin perjuicio de la facultad de las partes de constituir la Comisión Mixta establecida en la cláusula octava, la colaboración administrativa prevista en este Convenio 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; la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público; la Ley 59/2003, de 19 de diciembre, de firma electrónica; 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, así como el resto de disposiciones que sean de aplicación.

El presente Convenio tiene naturaleza administrativa y se regirá por lo expresamente pactado por las partes en este instrumento, por las normas citadas en el mismo y, en su defecto, por las normas de derecho administrativo que resulten de aplicación. 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. - APROBACIÓN, INICIO DE LA ACTIVIDAD INFORMACIÓN Y PUBLICACIÓN

El presente Convenio surtirá efectos desde el momento de su firma previa aprobación o siempre que sea ratificado, según proceda, por el Consejo de Administración de la FNMT-RCM. En caso de ratificación, la FNMT-RCM, comunicará al Instituto Municipal de Innovación del Ayuntamiento de Palma tal hecho para su constancia y efectos.

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

FÁBRICA NACIONAL DE MONEDA Y TIMBRE – REAL CASA DE LA MONEDA	**INSTITUTO MUNICIPAL DE INNOVACIÓN DEL AYUNTAMIENTO DE PALMA**
Director General	***Presidente***
Fdo.: Jaime Sánchez Revenga	*Fdo.: Adrián García Campos*

ÍNDICE DE ANEXOS

ANEXO I

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

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 artículo 13 de la Ley 59/2003, de 19 de diciembre. 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 Instituto Municipal de Innovación del Ayuntamiento de Palma 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 publica 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 el presente Convenio 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 al 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 artículo 18 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

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 para servidor o componente y firma de código.

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 de Microsoft.

- *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.

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

Servicio de Validación del Certificado de la AC Administración Pública

Para comprobar la validez del certificado de la Autoridad de Certificación de la Administración Pública, 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, gratuito, 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 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.

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

ldap://ldapape.cert.fnmt.es/CN=CRLnnn,OU=AC APE, 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, 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.

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

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

SERVICIO CUALIFICADO DE SELLADO DE TIEMPO

El servicio de Sellado de Tiempo, se prestará a través de:

Internet: https://qtsa.cert.fnmt.es

Intranet de la Administración Pública española (Red Sara): https://10.121.8.115

El sellado de tiempo es un método para probar que un conjunto de datos (datum) existió antes de un momento dado y además que ningún bit de estos datos ha sido modificado desde entonces.

Además, el sellado de tiempo proporciona un valor añadido a la utilización de firma digital ya que ésta por si sola no proporciona ninguna información acerca del momento de creación de la firma. Los certificados digitales utilizados por el algoritmo de la firma digital tienen un periodo de validez y por lo tanto, la firma sin el fechado digital, pasada la validez del certificado, siempre puede ser repudiada.

Para asociar los datos con un específico momento de tiempo es necesario utilizar una Autoridad de Sellado (TSA - Time Stamp Authority) como tercera parte de confianza.

Tipo de sello de tiempo electrónico y uso

El servicio cualificado de Sellado de Tiempo es ofrecido por la Autoridad de Sellado de Tiempo de la FNMT-RCM como Prestador de Servicios de Confianza y de conformidad con el Reglamento (UE) No 910/2014 del Parlamento Europeo y la norma técnica de aplicación ETSI EN 319 421 y RFC 3161.

- Son sellados con los Datos de Creación de Sello de la FNMT-RCM y los algoritmos utilizados son SHA-256 y RSA 3072

- El tiempo de vigencia de los Datos de Creación de Sello que la FNMT-RCM utiliza para ofrecer el servicio cualificado de sellado de tiempo es hasta el 3/3/2022.

El cliente de Sellado que el usuario debe montar se atendrá a la especificación recogida en la ETSI EN 319 422.

Límites de uso

La precisión declarada para la sincronización de la TSU con UTC es de 50 milisegundos, cumpliendo así sobradamente con los requisitos del estándar europeo [ETSI EN 319 421]. Por tanto, el Servicio cualificado de Sellado de Tiempo de la FNMT-RCM no expedirá ningún Sello cualificado de tiempo electrónico durante el periodo de tiempo en el que existiera un desfase mayor de 50 milisegundos entre los relojes de la TSU y la fuente de tiempo UTC del Real Observatorio de la Armada (ROA).

La FNMT – RCM registra y mantiene archivados aquellos eventos significativos necesarios para verificar la actividad de este servicio de confianza durante un periodo nunca inferior a 15 años, conforme a la legislación aplicable.

Protocolo

La TSA centraliza la emisión de certificados temporales. El papel que jugará esta entidad será producir, almacenar, verificar y renovar los certificados temporales. La TSA será una tercera parte de confianza (TTP), siendo su firma sobre el certificado temporal suficiente para probar la validez de éste.

Este protocolo permite el sellado de tiempo de cualquier tipo de información digital, y protege la confidencialidad de los datos fechados.

El usuario del servicio de sellado de tiempo debe ser poseedor de un certificado emitido por la Autoridad de Certificación de esta FNMT y que deberá ser solicitado por el usuario o parte autorizada.

La TSA hace uso de un certificado exclusivamente emitido para labores de sellado de tiempo, es decir, en su certificado está presente críticamente la extensión "extendedKeyUsage", cuyo valor es id-kp-timestamping.

Solicitud de sellado de tiempo

Una vez que el usuario dispone de un certificado X.509 y su correspondiente clave privada podrá realizar peticiones de sellado de tiempo. El proceso para realizar una petición de sellado es el siguiente:

1. El usuario selecciona el fichero electrónico del cual se solicitará el sellado a la TSA.

2. La aplicación cliente compone un resumen (hash) del contenido de ese fichero.

3. El usuario selecciona la política de servicio que desea, el número de referencia, la versión,...

4. La aplicación cliente compone una petición de fechado digital y la envía vía HTTPS.

Respuesta de sellado de tiempo

Una vez que la TSA haya recibido la solicitud de sellado y la haya aceptado, procederá a devolver a la aplicación cliente la respuesta de sellado o Response vía HTTPS. Este Response es un objeto que contiene un campo obligatorio que es el estado de la operación y en caso de que se haya realizado satisfactoriamente contiene además un objeto CMS SignedData, que es la firma del objeto que contiene toda la información del certificado de tiempo. El cliente podrá optar por almacenar directamente ese Response, validándolo previamente o también podrá optar por realizar la verificación del mismo, en caso de que no haya habido errores. Para ello:

1. La aplicación cliente recompone el objeto Response, extrayendo el estado de la operación, y si éste es GRANTED se puede extraer también el objeto CMS SignedData.

2. La aplicación cliente recompone el objeto CMS SignedData, extrayendo los datos firmados y verificando que la firma es correcta, haciendo uso del certificado de la TSA incluido en el objeto CMS.

3. Se obtienen los certificados incluidos en el objeto CMS y se hace "path validation".

4. La aplicación cliente obtendrá los datos de sellado del token.

Estándares aplicables

La definición del servicio de Sellado de Tiempo está basada en las especificaciones del estándar IETF-PKIX RFC-3161 – "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)" y la correspondiente norma ISO 18014-2, en la cual la FNMT-RCM ha participado como elaboradores de la misma.

A continuación se describen brevemente algunos de los puntos del mencionado estándar que tienen mayor impacto en la definición de la solución final del servicio.

El estándar RFC3161 define entre otros, el formato de la solicitud de un sellado de tiempo y de la respuesta generada por la TSA. También establece los diferentes requerimientos de seguridad que debería cumplir una TSA.

Uno de estos requerimientos, es que todos los sellados de tiempo generados por la TSA deben estar firmados digitalmente por ella con la clave privada de un certificado digital válido emitido especialmente para este propósito.

Por otro lado el mencionado estándar especifica que los sellados de tiempo (tokens) generados por la TSA no pueden incluir ninguna identificación del cliente que ha solicitado la operación. Como consecuencia, no es necesario que los mensajes de solicitud de sellado de tiempo que recibe la TSA contengan algún tipo de autenticación del cliente.

El estándar enumera diferentes mecanismos de transporte para mensajes de TSA. Ninguno de estos métodos es obligatorio; todos ellos son opcionales e incluso se contempla la posibilidad de soportar en un futuro nuevos mecanismos. Los mecanismos que especifican el documento RFC3161 son:

- Protocolo utilizando correo electrónico
- Protocolo basado en la utilización de FTP
- Protocolo basado en sockets utilizando el puerto IP 318
- Protocolo vía http/ssl.

También hay que recalcar que el estándar solamente define la operación de solicitud de sellado de tiempo y de la respuesta correspondiente, dejando otros tipos de operaciones, como por ejemplo la validación del sellado, sin ninguna especificación, aunque se deba realizar la implementación de este tipo de operaciones.

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 59/2003, de 19 de diciembre, 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.

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 Administración Pública 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 Administración Pública" 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 Administración Pública" 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 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 3 años 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.

SEDES ELECTRÓNICAS 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.

Estos certificados se expiden 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.

Emitidos en conformidad con los "Requisitos base para la emisión y gestión de certificados de confianza", requisitos establecidos por la entidad CA/Browser fórum.

La duración de los mismos se establece en 2 años 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 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

PRECIOS Y PLAN DE IMPLANTACIÓN

CAPITULO I - SERVICIOS EIT

1. Precio anual de los servicios

Se establece un precio fijo para los servicios EIT de 65.000,00 Euros al año, impuestos no incluidos.

2. Soporte Técnico

El coste del soporte técnico 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. Réplica de Directorio para los servicios EIT

El precio anual establecido en el apartado 1 del Capítulo 1 del presente Anexo de Precios incluye la réplica diaria de las listas de certificados revocados desde la FNMT-RCM a las instalaciones del conviniente por redes públicas. Este precio incluye la licencia de uso del directorio X.500 InJoin Directory Server de Critical Path en las propias instalaciones del cliente.

Este servicio no incluye la instalación ni el mantenimiento, que serán por cuenta del conviniente.

El directorio y su contenido no podrá ser cedido a terceros bajo ningún concepto, y deberá ser protegido contra todo acceso por entidades ajenas al conviniente, incluyendo el acceso de consulta.

4. Condiciones

A todas las cantidades expuestas en este capítulo I se les añadirá el IVA legalmente establecido.

CAPITULO II - SERVICIOS AVANZADOS

1. Certificados para servidor o componente y firma de código.

El precio anual establecido en el apartado 1 del Capítulo I del presente Anexo de Precios incluye un número máximo de 5 certificados de componente (certificados de autenticación de sitios web o Sello de Entidad).

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

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

2. Condiciones

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

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

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

El precio anual establecido en el apartado 1 del Capítulo I del presente Anexo de Precios incluye los servicios del ámbito de la Ley 11/2007, y la emisión de 1 certificado de sede electrónica y 3 certificados de sello electrónico para actuaciones automatizadas, así como los todos certificados de empleado público, con y sin seudónimo, y de firma centralizada para empleado público que el conviniente requiera.

El precio de los certificados adicionales tanto de sede (emitido por 2 años) como de sello (emitido por 3 años) será de 620,00€ y 690,00€ Euros por cada unidad respectivamente.

2. Servicio de autoridad de Sellado de Tiempo para Administración Pública

El precio anual de los servicios del ámbito de la Ley 40/2015 establecido en el apartado 1 del capítulo III del presente Anexo II de Precios incluye el servicio de Sellado de Tiempo para Administración Pública junto con un certificado de firma electrónica necesario para la suscripción de las peticiones de sellados. La FNMT-RCM no aceptará certificados de firma electrónica de Prestadores de Servicios de Certificación no reconocidos por la propia FNMT-RCM.

3. Condiciones

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