

### III. OTRAS DISPOSICIONES

## AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

- 13421** *Resolución de 1 de octubre de 2017, de la Agencia Española de Protección de Datos, por la que se publica la encomienda de gestión a la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, para la prestación de servicios técnicos y de seguridad aplicables a la certificación y firma electrónica y en el ámbito de la Administración electrónica.*

En cumplimiento con lo previsto en el artículo 11.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, procede la publicación en el «Boletín Oficial del Estado» de la Encomienda de Gestión de la Agencia Española de Protección de Datos a la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

Madrid, 1 de octubre de 2017.–La Directora de la Agencia Española de Protección de Datos, Mar España Martí.

**ENCOMIENDA DE GESTIÓN DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS A LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA, PARA LA PRESTACIÓN DE SERVICIOS, TÉCNICOS Y DE SEGURIDAD, APLICABLES A LA CERTIFICACIÓN Y FIRMA ELECTRÓNICA Y EN EL ÁMBITO DE LA ADMINISTRACIÓN ELECTRÓNICA**

En Madrid, a 1 de octubre de 2017.

#### REUNIDOS

De una parte, doña Mar España Martí, en nombre y representación de la Agencia Española de Protección de Datos –en adelante AEPD– (entidad con NIF Q2813014D y domicilio social en calle Jorge Juan, número 6, 28001 Madrid), en su calidad de Directora de la misma, nombrada por Real Decreto 715/2015 de 24 de julio («BOE» del 25) y haciendo uso de las facultades que tiene conferidas por los artículos 12 y 13 del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

Y, de otra parte, don Jaime Sánchez Revenga, como Director General, cargo para el que fue nombrado por el Real Decreto 286/2012, de 27 de enero («BOE» número 24 del 28), 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 número de identificación fiscal: Q28/26004J.

La entidad está regulada por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y por su Estatuto, aprobado por el Real Decreto 1114/1999, de 25 de junio; estando adscrita a la Subsecretaría de Hacienda y Función Pública, en virtud del artículo 18.11.b) del Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas (ahora de Hacienda y Función Pública).

Ambas partes, reconociéndose la capacidad legal y competencia necesarias para formalizar la presente Encomienda de Gestión,

## EXPONEN

Primero.

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, como la imposición de fechas electrónicas sobre los documentos de la misma naturaleza, que integren un expediente administrativo.

En este ámbito, ha de tenerse en cuenta la efectiva aplicación, desde el 1 de julio de 2016, del «Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE», que es de directa aplicación en los Estados miembros, siendo necesario, para adaptarse a este Reglamento, ajustar y modificar las legislaciones interiores de los países miembros en esta materia, como la propia Ley 59/2003, de firma electrónica.

La disposición adicional cuarta de la Ley 59/2003, constata la especialidad en la regulación que afecta a la actividad de la FNMT-RCM, al referir 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, faculta a la FNMT-RCM para prestar los servicios técnicos y administrativos necesarios para garantizar la seguridad, validez y eficacia en la emisión y recepción de comunicaciones y documentos a través de técnicas electrónicas, informáticas y telemáticas (EIT), entre otros, entre las personas físicas y jurídicas con la Administración General del Estado y con los organismos públicos vinculados o dependientes de ella y de estos sujetos públicos entre sí. Tal artículo, modificado y ampliado mediante las Leyes 55/1999, 14/2000, 44/2002, 53/2002 y 59/2003, trae causa del mandato para el impulso del empleo y la aplicación de técnicas y medios EIT, en el desarrollo de la actividad y el ejercicio de las competencias de las Administraciones Públicas, según estableció el artículo 45.1 de la derogada Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y que ahora se regula en los artículos 17, 26 y 27 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Este mismo artículo 81, en su apartado cinco, señala que, con la finalidad de extender los servicios dados por la FNMT-RCM, que sería el ámbito de este instrumento, la Entidad podrá celebrar convenios con las diferentes Administraciones públicas, entidades y organismos públicos vinculados o dependientes, constituyendo, el referido artículo 81 y legislación de desarrollo antes citada, norma especial.

En relación con las actividades de identificación y registro, la FNMT-RCM, podrá celebrar convenios con personas, entidades y corporaciones que ejerzan funciones públicas, en los que se establezcan las condiciones en las que éstas puedan participar en tales actividades.

Tercero.

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

convenir con las entidades incluidas en su ámbito de aplicación, entre las que se encuentra la AEPD, los términos que deben regir la prestación de sus servicios en relación con las comunicaciones empleando técnicas y medios electrónicos, informáticos y telemáticos.

Cuarto.

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, reconoce a los ciudadanos de su derecho a relacionarse preferentemente y de forma electrónica con las Administraciones Públicas, con el fin de contribuir a la extensión y consolidación de la administración electrónica. Para ello, la FNMT-RCM en colaboración con las diferentes administraciones públicas, presta servicios técnicos y administrativos necesarios para la identificación y autenticación de los intervinientes en las comunicaciones electrónicas de las administraciones públicas, a través del uso de certificados de firma electrónica dirigida a funcionarios y demás empleados públicos, certificados de sede electrónica y certificados de sello electrónico para la actuación administrativa automatizada, en los que las administraciones y organismos actúan, en sus registros y sedes electrónicas, a través de las oficinas de registro propias encargadas de acreditar y constatar los requisitos y condiciones especiales de utilización de estos servicios de certificación electrónica a prestar por la FNMT-RCM.

La Ley 39/2015, de 1 de octubre, y el Real Decreto 1671/2009 de 6 de noviembre (que desarrollaba la derogada Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos y que mantiene parcialmente su vigencia en virtud de la disposición derogatoria única de la Ley 39/2015, de 1 de octubre, y la disposición derogatoria única de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público) facilitan a los ciudadanos la efectiva realización de los derechos reconocidos en la Ley, a través del triple objetivo del Real Decreto: evitar que la nueva regulación imponga una renovación que impida la pervivencia de técnicas de gran arraigo; facilitar la implantación y adaptación de las organizaciones a las nuevas funciones y procedimientos e impedir que la opción rígida de determinadas soluciones dificulte la incorporación futura de nuevos servicios y aplicaciones. Este Real Decreto, en los Capítulos I y II de su Título VI, regula la materia relativa a los documentos electrónicos y sus copias, en especial, documentos administrativos electrónicos, archivo electrónico de documentos, expediente electrónico y digitalización.

Por su parte, 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.

Quinto.

De acuerdo con lo establecido en los artículos 4.1.n) y 24.6 del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el Texto Refundido de la Ley de

Contratos del Sector Público, la Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014 y con las acotaciones y aclaraciones de la numerosa jurisprudencia del Tribunal de Justicia de las Comunidades Europeas, están excluidos de la aplicación del Real Decreto Legislativo 3/2011 los negocios jurídicos en cuya virtud se encargue una determinada prestación a una entidad que tenga atribuida la condición de medio propio y servicio técnico del poder adjudicador correspondiente, como la FNMT-RCM que, según su estatuto, es medio propio de la Administración General del Estado, ya que realiza la parte esencial de su actividad con esta administración que mantiene un control análogo al que ejerce sobre sus propios servicios, por lo que a la FNMT-RCM se le pueden conferir encomiendas de gestión de conformidad con los artículos antes citados.

Sexto.

La Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda es una entidad pública empresarial dependiente de la Administración General del Estado y se encuentra adscrita al Ministerio de Hacienda y Administraciones Públicas (ahora Hacienda y Función Pública), a través de la Subsecretaría de este departamento, que ejerce la dirección estratégica y el control de eficacia de la entidad.

El artículo 2 del Estatuto de la FNMT-RCM, aprobado mediante el Real Decreto 1114/1999, de 25 de junio, reconoce y establece, como uno de sus fines (fijados por el artículo 81, citado en el expositivo segundo), la prestación –en el ámbito de las administraciones públicas, o sus organismos públicos, vinculados o dependientes– de servicios de seguridad, técnicos y administrativos, en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT) así como la expedición, fabricación y suministro de títulos o certificados de usuario (y sus soportes), de acuerdo con lo que determinen las disposiciones legales correspondientes.

Por su parte, el apartado 7 del artículo 2 y el apartado 2 del artículo 3 de su Estatuto, según redacción dada por el artículo único del Real Decreto 336/2014, de 25 de junio, configura a la FNMT-RCM como medio propio y servicio técnico de la Administración General del Estado, así como de los organismos, entes y entidades del sector público estatal, sean de naturaleza jurídica pública o privada, en los términos del citado Real Decreto Legislativo 3/2011, de 14 de noviembre, TRLCSP y de su Estatuto.

Séptimo.

La AEPD, en el marco de desarrollo de sus competencias, presta determinados servicios soportados por técnicas y medios electrónicos, informáticos y telemáticos aplicados a determinados procedimientos administrativos. Estos servicios deben contar con las debidas garantías de seguridad conformes con las disposiciones legales y en orden a garantizar la validez y eficacia de la emisión y recepción de comunicaciones y documentos producidos a través de técnicas y medios EIT. Por otra parte también se requiere la identificación electrónica de la AEPD y autenticación del ejercicio de su competencia, de conformidad con la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.

Octavo.

Que, en virtud de las razones ahora expuestas, se ha considerado que las relaciones administrativas, prestacionales y de colaboración entre la AEPD y la FNMT-RCM, se instrumenten a través de una encomienda de gestión, al margen de una relación estrictamente contractual, en la que la propia administración realiza sus funciones con sus propios medios, o los de entidades sobre las que la administración, que efectúa la encomienda, ostenta un control análogo al que ejerce sobre sus propios servicios (medios propios y servicios técnicos). Todo ello, de acuerdo con lo dispuesto en los artículos 4.1.n) y 24.6 del Real Decreto Legislativo 3/2011, citado, y la normativa europea.

Estando ambas partes interesadas en procurar la máxima extensión de la administración electrónica para facilitar a los ciudadanos y Administraciones las relaciones administrativas a través de las técnicas y medios electrónicos, informáticos y telemáticos (EIT), y de conformidad con lo previsto en este expositivo, se procede a la formalización de la presente Encomienda de Gestión con arreglo a las siguientes

### CLÁUSULAS

#### Primera. *Objeto.*

1.1 Constituye el objeto de la presente Encomienda de Gestión la prestación, por parte de la FNMT-RCM a la AEPD, de las siguientes actividades:

a) Servicios técnicos, administrativos y de seguridad necesarios para garantizar la validez y eficacia de la emisión y recepción de comunicaciones y documentos producidos a través de técnicas y medios EIT en el ámbito de actuación de la AEPD, en las condiciones técnico-administrativas que, en las cláusulas siguientes, se estipulan y se detallan en el Capítulo I, del anexo I, de esta Encomienda de Gestión.

b) Servicios relativos a la identificación electrónica de las administraciones públicas y autenticación del ejercicio de su competencia, de conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y, en concreto, las actividades que se enumeran en la siguiente cláusula y en el Capítulo III, del anexo I, de esta Encomienda de Gestión.

1.2 La FNMT-RCM también prestará a petición de la AEPD cualquiera, o la totalidad, de los servicios avanzados o especiales o suministros que, al efecto, se enumeran en el Capítulo II, del mismo anexo I, de esta Encomienda de Gestión.

#### Segunda. *Prestaciones y ámbito de aplicación.*

##### 2.1 Para servicios del ámbito del artículo 81.

La FNMT-RCM prestará servicios EIT a las personas que tengan la condición de usuarios de acuerdo con la normativa vigente y las cláusulas de esta Encomienda de Gestión, cuando los usuarios se relacionen con la AEPD en el marco de sus respectivas competencias. A tal efecto, la AEPD asume que los certificados (títulos de usuario) que expida la FNMT-RCM son universales 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 igual 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 la AEPD cuando así lo admita el ordenamiento jurídico.

Concretamente, las actividades a desplegar son:

##### 2.2 Para servicios del ámbito de la Ley 40/2015.

La FNMT-RCM, a los efectos de lo dispuesto en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, prestará los servicios en los términos de la citada Ley y en los señalados en el Capítulo III, del Anexo I de esta Encomienda, y con sujeción a lo establecido en la Declaración de Prácticas de Certificación, accesibles en la dirección electrónica: <http://www.cert.fnmt.es/dpcs>, los siguientes servicios de identificación electrónica y autenticación de documentos electrónicos de las administraciones públicas:

- Número ilimitado de Certificados de Empleado Público.
- 1 Certificado de Sede Electrónica (autenticación de sitio web).
- 3 Certificados de Sello Electrónico de Administración Pública.



– Emisión de Sellos de Tiempo en las comunicaciones electrónicas, informáticas y telemáticas que tengan lugar al amparo de la presente encomienda, previa petición de la AEPD 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.

– Emisión de 5 certificados de componente (wildcard, SAN multidominio, sello de entidad, firma de código).

La AEPD conoce el texto de dicha declaración general de prácticas de servicios de confianza que se contiene en este momento en la página web de la FNMT.

2.3 Las condiciones económicas de las actividades a desarrollar en relación con servicios, actividades o suministros especificados en esta cláusula, se detallan en el apartado 2 del anexo II de Precios y Plan de Implantación.

2.4 El ámbito de aplicación de esta Encomienda será la AEPD, sus órganos y unidades administrativas. No forman parte de la presente Encomienda, los organismos y entidades de derecho público o privado, integrantes del Sector Público Institucional, dependientes de la Administración contratante.

*Tercera. Obligaciones de las partes para la prestación efectiva de los servicios objeto de la encomienda.*

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

- Aportar la infraestructura técnica, organizativa y de seguridad relacionada en los anexos I y II de esta Encomienda.
- Aportar los derechos de propiedad industrial e intelectual necesarios, garantizando su uso pacífico. La FNMT-RCM, excluye cualesquiera licencias o sublicencias, a terceras partes o la AEPD para aplicaciones y sistemas de la AEPD, o de terceros, distintas de las aportadas directamente por la FNMT-RCM, en virtud de este documento.
- Prestar la asistencia técnica que se precise con objeto de facilitar a la AEPD la información necesaria para el buen funcionamiento de los sistemas, de conformidad con lo establecido en los anexos de esta Encomienda.
- Actualizar tecnológicamente los sistemas, de acuerdo con el estado de la técnica y las disponibilidades presupuestarias de la FNMT-RCM, sin perjuicio de la aprobación de los requisitos técnicos correspondientes por La Comisión de Estrategia TIC o, en su caso, por el órgano competente.
- Emitir sellos de tiempo en las comunicaciones electrónicas, informáticas y telemáticas que tengan lugar al amparo de la presente Encomienda de Gestión, previa petición de la AEPD.
- Aportar la tecnología necesaria para que las obligaciones de la AEPD, puedan ser realizadas; en particular, las aplicaciones necesarias para la constitución de las Oficinas de Registro y acreditación y la tramitación de las solicitudes relativas a los certificados electrónicos. Tales aplicaciones serán compatibles en función de los avances tecnológicos y el estado de la técnica.
- Tener disponible para consulta de la AEPD y de los usuarios una Declaración de Prácticas de Certificación (DPC), referida en la cláusula segunda apartado 2.2, 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: <http://www.cert.fnmt.es/dpcs>. Esta DPC, podrá ser consultada por todos los interesados y podrá ser modificada por la FNMT-RCM, por razones legales o de procedimiento. Las modificaciones en la DPC serán comunicadas a los usuarios a través de su dirección electrónica: [www.ceres.fnmt.es](http://www.ceres.fnmt.es).
- Cuando las modificaciones practicadas en cualquiera de las Declaraciones de Prácticas de Certificación y Políticas de Certificación afecten directamente a los derechos y obligaciones de la AEPD, o bien restrinjan el ámbito de aplicación de los Certificados, la

FNMT-RCM notificará al interesado con una antelación mínima de treinta (30) días a la entrada en vigor de los cambios, con la finalidad que la AEPD adopte la decisión que a su derecho convenga.

- Es necesario tener en cuenta, en todo caso, la parte general de esta DPC y, para cada tipo de certificado o ámbito de actuación, sus Anexos, que constituyen las Políticas y Prácticas de Certificación Particulares aplicables específicamente.
- Emisión de informes, a petición de la AEPD y de los Juzgados, Tribunales y, en su caso, órganos administrativos y/o supervisores competentes, acreditativos de la actividad de certificación realizada por la FNMT-RCM en aplicación de esta Encomienda.

En todo caso, los medios técnicos y tecnología empleados por la FNMT-RCM permitirán demostrar la fiabilidad del servicio de certificación electrónica, la constatación de la fecha y hora de expedición, suspensión o revocación de un certificado, la fiabilidad de los sistemas y productos (que contarán con la debida protección contra alteraciones, 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, las actuaciones que resulten de aplicación de conformidad con la normativa comunitaria o nacional correspondiente.

No obstante lo anterior, en la prestación de servicios del ámbito de la Ley 40/2015, las Oficinas de Registro, por las especialidades del derecho administrativo y de gestión y de conformidad con el artículo 11 del Real Decreto 1317/2001, de 30 de noviembre, no dependerán directamente de la FNMT-RCM sino del órgano u organismo público de origen, sin perjuicio de las funciones de comprobación, coordinación y control de gestión y de los protocolos de registro que realice la FNMT-RCM, en su condición de Prestador de Servicios de Certificación.

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

2. Por su parte, la AEPD se compromete a:

- Emitir 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 durante el tiempo pertinente para hacer valer los derechos de las partes.
- Cifrar las comunicaciones emitidas y recibidas.
- Realizar las actividades de identificación previa a la obtención del certificado electrónico y, en su caso, de comprobación y suficiencia de los atributos correspondientes, de los titulares de los certificados, así como del cargo y competencia de los firmantes/custodios correspondientes. Todo ello, a través de la Oficina de Registro y acreditación designada ante la FNMT-RCM, utilizando los procedimientos establecidos por esta Entidad, que figuran en la aplicación de Registro (aplicación Web) y en la DPC de la FNMT-RCM. Tales procedimientos, son documentos sujetos a verificaciones y auditorías por lo que podrán ser modificados por la FNMT-RCM a los efectos de mejorar el servicio.
- Conservar, a su vez, durante al menos quince años, los formularios y documentos donde constan las condiciones para la solicitud, revocación y suspensión, en su caso, de certificados electrónicos emitidos por la FNMT-RCM en el ámbito de la Ley 40/2015 (empleado público, sede y sello), así como su remisión electrónica a la FNMT-RCM, de conformidad con lo establecido en los procedimientos de registro que constan en la URL citada en el apartado anterior o la que la sustituya.

La AEPD se compromete, en el desarrollo y ejecución de la presente 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.

### 3. Oficinas de Registro.

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

Para los servicios del artículo 81 de la Ley 66/1997.

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

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

Para los servicios de la Ley 40/2015.

Las Oficinas de Registro de la AEPD, para el ámbito de la Ley 40/2015, son de orden interno de cada administración u organismo correspondiente y determinarán la identidad y competencia de las Administraciones y la de los diferentes firmantes/custodios designados por las administraciones, entidades y organismos vinculados o dependientes suscriptores de los certificados, de conformidad con la DPC General y la específica Política y Prácticas de Certificación particulares de Administración Pública, disponibles para consulta en la Web: <http://www.cert.fnmt.es/dpcs>.

A tal efecto, la AEPD dispondrá de las Oficinas de Registro y acreditación que considere necesarias y adecuadas para la acreditación de este tipo de certificados y deberán contar con los medios informáticos precisos para conectarse telemáticamente con la FNMT-RCM y realizar las solicitudes de emisión de los certificados. En las Oficinas de Registro, para acreditar e identificar a los titulares 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. *Plazo de duración.*

La presente Encomienda de Gestión entrará en vigor el día de su firma y tendrá una duración anual. El pago de dicha anualidad se dividirá entre los ejercicios presupuestarios 2017 y 2018 proporcionalmente al período ejecutado en cada año.

La duración de la Encomienda se podrá prorrogar anualmente si así lo acordara expresamente la AEPD antes de su vencimiento, siendo esta prórroga asumida por la FNMT-RCM.

En virtud del artículo 11.3 de la Ley 40/2015 la presente Encomienda de Gestión deberá publicarse en el «Boletín Oficial del Estado» para su eficacia.

La contratación de las actividades previstas en esta Encomienda, más allá de su duración inicial y, en su caso, su prórroga o sus prórrogas, solamente podrá realizarse por nueva Encomienda.

#### Quinta. *Régimen de prestación de los servicios.*

##### Ámbito objetivo.

La prestación de los servicios EIT a que se refiere la cláusula primera, se realizará atendiendo a lo establecido en los Capítulos I y II del anexo I, para los servicios relativos al artículo 81 de la Ley 66/1997, y atendiendo a lo establecido en el Capítulo III, del anexo I, para los servicios relativos al ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

A tal efecto, ambas partes se comprometen a asumir las obligaciones necesarias a este fin. Igualmente, la AEPD se obliga a velar frente a los usuarios por el cumplimiento de las obligaciones que le correspondan como encargada de la identificación, acreditación y registro de usuarios y de los funcionarios y empleados públicos, firmantes/custodios, así como de la recepción y tramitación de solicitudes de expedición, revocación y, en su caso, suspensión de cualesquiera certificados electrónicos previstos en esta Encomienda de Gestión y sus anexos.

##### Medidas de seguridad.

La FNMT-RCM se compromete a adoptar cuantas medidas sean necesarias 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 Instrucciones Internas de Contratación de la entidad, así como las obligaciones de confidencialidad pertinentes, restringiendo la información y la publicidad de los diferentes elementos de seguridad, según los estándares aplicables y, en general, realizando la actividad encomendada implantando medidas especiales de seguridad, de conformidad con el estado de la técnica.

#### Sexta. *Tarifas y condiciones de pago.*

1. Tarifas en materia de certificación electrónica sobre la base del artículo 81 (ciudadanos/empresas).

En caso de ser solicitada la activación de estos servicios de forma expresa por parte de la AEPD, la FNMT-RCM, como compensación por las actividades desarrolladas, percibirá por su actividad de extensión de la Administración Electrónica en la AEPD (según el Capítulo I, del anexo I, y calculada de acuerdo con el artículo 30 del Estatuto de la FNMT-RCM), la cantidad de mil euros (1.000,00 €/ año), impuestos no incluidos.

Tanto durante el primer año, como en el de las eventuales prórrogas, si hubiera petición expresa, por parte de la AEPD, de extensión de otras funcionalidades de entre las recogidas en el Capítulo II, del anexo I, la cantidad anterior quedaría incrementada por el

importe correspondiente que se dedujera de la aplicación de las tablas de los Capítulos I y II, del anexo II, de Precios y Plan de Implantación, de la presente encomienda.

2. Tarifas en materia de intermediación administrativa sobre la base de la Ley 40/2015 (empleado/sede/sello).

La FNMT-RCM, como compensación por las actividades desarrolladas, percibirá por su actividad de extensión de la Administración Electrónica en la AEPD dentro del ámbito de la Ley 40/2015 recogida en el Capítulo III del anexo I, la cantidad de diez mil euros al año (10.000,00 €/año), impuestos no incluidos.

Tanto durante el primer año, como en el de las eventuales prórrogas, si hubiera petición expresa, por parte de la AEPD, de extensión de otras funcionalidades de entre las recogidas en el Capítulo III, del anexo I, la cantidad anterior quedaría incrementada por el importe correspondiente que se dedujera de la aplicación de las tablas del Capítulo III del anexo II, de Precios y Plan de Implantación, de la presente encomienda.

3. Reembolso total.

La cantidad total de compensación, a la FNMT-RCM, por aplicación de la Encomienda en un año asciende a 10.000,00 euros/año, impuestos no incluidos. Siendo el IVA de aplicación un 21% de dicho importe (2.100,00 euros), la compensación anual es de 12.100,00 euros, IVA incluido.

En caso de ser solicitada la activación de los servicios del artículo 81 de forma expresa de forma expresa por parte de la AEPD, la cantidad total de compensación, a la FNMT-RCM, por aplicación de la encomienda en un año asciende a trece mil trescientos diez euros al año (13.310,00 €/año), impuestos incluidos.

Esta cantidad se obtiene de la suma de las cantidades establecidas en los apartados 1 y 2 anteriores, sin perjuicio de su incremento por petición de funcionalidades adicionales.

La contraprestación a percibir por la FNMT-RCM en las siguientes anualidades serán:

- Para el ejercicio 2017, de 2.500,00 euros, IVA no incluido.
- Para el ejercicio 2018, de 7.500,00 euros, IVA no incluido.

Estos pagos se realizarán con cargo a la aplicación presupuestaria 13.301.135M.227.06.

En caso de sucesivas prórrogas, se aplicará el mismo criterio en función de las compensaciones a percibir, servicios solicitados y prórrogas de la Encomienda.

4. Consideración de las contraprestaciones.

Las contraprestaciones establecidas en esta Encomienda y sus anexos, tienen la consideración de tarifas a los efectos previstos en el artículo 24.6 párrafo segundo, del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el Texto Refundido de la Ley de Contratos del Sector Público, una vez sea autorizada la formalización de la presente Encomienda por el órgano directivo de adscripción de la FNMT-RCM, de conformidad con lo dispuesto en el artículo 3.2 del Estatuto de esta entidad. No obstante, la FNMT-RCM quedará obligada a aceptar cualesquiera otras tarifas que sean impuestas por la Subsecretaría de Hacienda y Administraciones Públicas, en cuanto órgano directivo de adscripción de la entidad, en relación con el número de administraciones destinatarias, de las disponibilidades presupuestarias y del volumen de los servicios prestados, teniendo en cuenta la equiparación entre el coste del producto o servicio y el precio a repercutir, el cual comprenderá necesariamente un porcentaje de beneficio industrial, que podrá oscilar en función de los volúmenes contratados u otras circunstancias objetivamente atendibles de acuerdo con los mercados correspondientes.

5. Facturación.

La FNMT-RCM, podrá realizar facturaciones trimestrales contra certificaciones o autorizaciones parciales conformadas por la AEPD, mediante el prorrateo de la cantidad

anual a abonar pudiendo, además, liquidar en tales facturas mensuales aquellos servicios adicionales o avanzados solicitados. 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:

- Código Cuenta: 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: Agencia Española de Protección de Datos.

Calle: Jorge Juan, 6.

Población: Madrid.

Provincia-CP: Madrid-28001.

NIF/CIF: Q2813014D.

Departamento o persona de contacto / Teléfono: Área de Contratación - 913991207.

6. Servicios de validación (Leyes 39/2015 y 40/2015).

De conformidad con el artículo 24.4 del «Reglamento (UE) número 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.

Séptima. *Revisión y comisión de seguimiento.*

Sin perjuicio de lo dispuesto a efectos de actualización de las condiciones económicas de las actividades encomendadas, las partes podrán proponer la revisión de esta Encomienda en cualquier momento de su vigencia, a efectos de incluir, de mutuo acuerdo, las modificaciones que resulten pertinentes.

A petición de cualesquiera de las partes podrá crearse una comisión mixta para el examen, seguimiento, coordinación de la Encomienda y, en su caso, adhesiones, así como para plantear propuestas de modificación y de resolución de conflictos.

Octava. *Responsabilidad.*

La FNMT-RCM como prestador de los servicios citados en la cláusula primera y Anexos, y la AEPD como destinatario de los servicios de certificación y firma electrónica y encargado de las funciones de registro y acreditación en el procedimiento de identificación, acreditación y registro de los usuarios y, en su caso, 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 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 de la presente 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 la presente Encomienda de Gestión, en su condición de medio propio y servicio técnico de la Administración General del Estado, a tenor de lo dispuesto en el artículo 24.6 del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se

aprueba el Texto Refundido de la Ley de Contratos del Sector Público y en el artículo 3.2 de su Estatuto, por lo que no podrá instar ninguna de las siguientes causas de resolución sin la autorización previa del órgano directivo de adscripción de la entidad.

La Encomienda de Gestión podrá resolverse por parte de la AEPD y, en su caso, de los organismos que estén adheridos, cuando existiera manifiesta falta de calidad del servicio, por parte de la FNMT-RCM, o incumplimiento grave de las obligaciones de ésta en el desarrollo de su actividad. La resolución de un organismo adherido o del firmante principal de la Encomienda, no supondrá la resolución en nombre del resto de organismos que tengan personalidad jurídica independiente de su órgano de adscripción o vinculación.

La FNMT-RCM podrá instar, previa autorización de su órgano de adscripción, 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 la AEPD.

Causas de extinción. Serán causas de extinción:

- El cumplimiento del plazo previsto en la Encomienda y 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 de gestión y de la actuación conjunta de las partes, será el previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y en su reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre. Los ficheros de la FNMT-RCM son de titularidad pública y su creación se ha realizado por disposición general publicada en el «BOE» (Orden EHA/2357/2008, de 30 de julio, por la que se regulan los ficheros de datos de carácter personal de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, «BOE» número 190, de 7 de agosto).

Los ficheros de la AEPD, serán de titularidad pública y su creación, modificación o supresión se realizará por disposición general, de conformidad con la Ley.

Comunicación de datos.—La comunicación de datos de carácter personal que la AEPD 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 (y, en su caso, en el de la Ley 66/1997, art. 81), no requerirá consentimiento del interesado al estar, tal cesión o comunicación, amparada por el artículo 11.2.c) de la Ley Orgánica 15/1999, ya que tal comunicación resulta ineludible para que la FNMT-RCM expida los certificados de firma electrónica a los empleados de la AEPD.

Acceso a los datos por cuenta de terceros (encargado del tratamiento).—No tendrá carácter de comunicación de datos el acceso que la AEPD, 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 fichero, sobre sus usuarios, personas físicas, con la finalidad de solicitar los servicios EIT en el ámbito del artículo 81 de la Ley 66/1997, descritos en la presente Encomienda. Tales datos son los que figuran en el fichero regulado, en el número 5 del anexo de la citada Orden EHA/2357/2008, o la que modifique o sustituya.

De conformidad con el artículo 12 de la LOPD, la AEPD, actuará en calidad de encargado del tratamiento, por cuenta de la FNMT-RCM, y asumirá las siguientes obligaciones:

- Tratará los datos conforme a las instrucciones de la FNMT-RCM como responsable del fichero y que se refiere exclusivamente a hacer efectiva la realización de las actividades contempladas en esta Encomienda y, específicamente, la de remitir una copia del contrato de solicitud y conservar otra de las copias.
- No aplicará o utilizará los datos con un fin distinto al que figura en la presente Encomienda y sus anexos.

- No los comunicará, ni siquiera para su conservación, a otras personas.
- Aplicará medidas de seguridad acordes con el tipo de datos que traten (las que se establecen en la Orden EHA/2357/2008, citada, o la que modifique o sustituya).
- No almacenará innecesariamente datos personales en los accesos que se efectúen y en caso de que se almacenen, una vez finalizada la presente Encomienda, destruirá o devolverá al responsable del fichero los datos y soportes donde figuren, levantando acta del tal destrucción o devolución. No obstante, y con el fin de preservar los derechos del encargado frente a posibles responsabilidades derivadas de su actuación, en el supuesto referido en este apartado, el encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

En caso que la AEPD y los organismos o entidades que estén adheridos, destinen los datos manejados a otra finalidad, los comuniquen o los utilicen incumpliendo las estipulaciones de esta Encomienda, serán considerados también responsables del tratamiento, respondiendo de las infracciones en que hubieran incurrido.

*Undécima. Régimen jurídico y resolución de conflictos.*

La prestación de los servicios contemplados en la presente Encomienda de Gestión y sus anexos, en cuanto al contenido y características de los mismos, se realizará con sujeción a la regulación contenida en 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, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y el resto de disposiciones citadas en el expositivo así como a las disposiciones que sean de aplicación y en su caso, cuantas disposiciones se dictaran, durante la vigencia de la Encomienda y que afectaran a su objeto.

Este instrumento jurídico formalizado mediante una Encomienda de Gestión es realizado por la AEPD a la FNMT-RCM, de acuerdo con los artículos 4.1.n) y 24.6 del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el Texto Refundido de la Ley de Contratos del Sector Público, con el artículo 3.2 del vigente Estatuto de esta entidad, aprobado por el Real Decreto 1114/1999, de 25 de junio y modificado por el Real Decreto 199/2009, de 23 de febrero; el Real Decreto 390/2011, de 18 de marzo, y el Real Decreto 336/2014, de 9 de mayo, así como el resto de disposiciones que sean de aplicación.

Las partes se comprometen, a través de la comisión prevista en la cláusula séptima, a resolver de mutuo acuerdo las incidencias que pudieran existir en la interpretación y cumplimiento de esta Encomienda. Las cuestiones litigiosas que, no obstante, surjan entre las partes se someterán a la Ley 52/1997, de 27 de noviembre, y normas de desarrollo y, en cualquier caso, a la jurisdicción contencioso-administrativa, conforme a lo dispuesto en su Ley reguladora.

*Duodécima. Coordinación administrativa.*

FNMT-RCM procederá a informar de la formalización y, en su caso, extinción de la prestación a que se refiere la presente Encomienda al Ministerio de Hacienda y Función Pública y a la Dirección de Tecnologías de la Información y Comunicaciones, así como a los demás órganos competentes, a los efectos de coordinación e interoperabilidad correspondientes para el desarrollo de la Administración electrónica y el acceso electrónico de los ciudadanos a los Servicios Públicos.

Y, en prueba de conformidad, ambas partes suscriben la presente Encomienda de Gestión y todos sus anexos, en el lugar y fecha indicados en el encabezamiento.—Por la Agencia Española de Protección de Datos, la Directora, Mar España Martí.—Por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, el Director General, Jaime Sánchez Revenga.



## ÍNDICE DE ANEXOS

Anexo I. Características técnicas de las actividades a realizar por la FNMT-RCM.

- Capítulo I. Servicios EIT.
- Capítulo II. Servicios avanzados.
- Capítulo III. Servicios AP (Ley 40/2015).

Anexo II. Tarifas y plan de implantación.

### ANEXO I

#### Servicios a prestar

##### CAPÍTULO 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 la AEPD 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:

- Que el usuario dispone de la clave privada correspondiente a la clave pública del certificado, en el momento de su emisión.
- Que la información incluida en el certificado se basa en la información proporcionada por el usuario.
- 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:

- Que el signatario es la persona identificada en el certificado.
- Que el signatario tiene un identificativo único.
- Que el signatario dispone de la clave privada.

La AEPD garantizará que, al solicitar un certificado electrónico, su titular acepta que:

- La clave privada con la que se genera la firma electrónica corresponde a la clave pública del certificado.
- Únicamente el titular del certificado tiene acceso a su clave privada.
- Toda la información entregada durante el registro por parte del titular es exacta.
- El certificado será usado exclusivamente para fines legales y autorizados y de acuerdo con lo establecido por la FNMT-RCM.
- 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.

La AEPD garantizará que, al solicitar un certificado electrónico, su titular asume las siguientes obligaciones sobre su clave privada:

- A conservar su control.
- 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:

- Solicitud de revocación del usuario, por la persona física o jurídica representada por éste o por un tercero autorizado.
- Resolución judicial o administrativa que lo ordene.
- Fallecimiento o extinción de la personalidad del usuario o incapacidad sobrevenida.
- Finalización del plazo de vigencia del certificado.
- Pérdida o inutilización por daños en el soporte del certificado.
- Utilización indebida por un tercero.
- Inexactitudes graves en los datos aportados por el usuario para la obtención del certificado.
- 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 encomienda 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 la AEPD 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.

La AEPD 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.

#### *Publicación 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.

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

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

### CAPÍTULO 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=E S?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 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 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 de Sellado de Tiempo para Administración Pública.

El servicio de Sellado de Tiempo, se prestará a través de la URL.

`https://apuseg.cert.fnmt.es/TimeStampAPE/TimeStampServer`

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.

Este servicio es una Autoridad de Sellado de Tiempo compatible con IETF RFC 3161, y las peticiones realizadas serán del tipo «application/timestamp-query» utilizando método POST.

La referencia temporal utilizada como fuente de tiempo de dicha Autoridad de Sellado de Tiempo, se basa en el Sistema de Sincronismo Real Observatorio de la Armada instalado en el CPD de la Fábrica Nacional de Moneda. Este sistema tiene como objetivo proporcionar una fuente de referencia temporal trazable a la escala de tiempo UTC (ROA).

Las respuestas de la Autoridad de Sellado de Tiempo, del tipo «application/timestamp-reply», irán firmadas con un certificado emitido por la infraestructura Administración Pública, con un tamaño de claves RSA de 2048 y algoritmo de firma SHA-256.

El certificado de firma de las respuestas de la Autoridad de Sellado de Tiempo podrá validarse mediante cualquiera de los métodos expuestos en el apartado anterior.

El servicio está basado en el «appliance» Time Stamp Server de la empresa nCipher.

El acceso a este servicio será universal y dispondrá de visibilidad a través de Internet así como a través de la Red SARA con la única restricción comentada del control de dirección IP.

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 electrónica del personal al servicio de las administraciones públicas.

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.

La infraestructura de servicios de certificación y firma electrónica de la FNMT-RCM permite diferentes usos y funcionalidades:

1) Uso principal. El uso principal del certificado de empleado público es la identificación electrónica y autenticación conjunta de la administración, organismo o entidad pública actuante en el ejercicio de sus competencias y de la identidad, cargo o empleo del personal a su servicio.

Este certificado es la certificación electrónica emitida por la FNMT-RCM que vincula al Firmante con unos Datos de verificación de Firma y confirma, de forma conjunta:

a) La identidad del Firmante y custodio de las Claves (personal al servicio de las Administraciones Públicas que realiza firmas electrónicas utilizando el Certificado en nombre de la Administración actuante), número de identificación personal, cargo, puesto de trabajo y/o condición de autorizado y

b) Al Suscriptor del Certificado, que es el órgano, organismo o entidad de la Administración Pública, bien sea ésta General, autonómica, local o institucional, donde ejerce sus competencias, presta sus servicios, o desarrolla su actividad.

2) Otros usos. Este certificado podrá ser utilizado por el personal para actuaciones funcionariales, administrativas o laborales, relacionadas con los diferentes derechos y obligaciones del personal al servicio de las Administraciones Públicas en el ámbito de su Administración, Organismo o Entidad pública de dependencia o, en su caso, con el resto del Sector Público.

3) Uso no autorizado. El personal usuario no está autorizado para utilizar estos certificados para usos distintos a los establecidos en los apartados 1) y 2) anteriores.

4) Marco legislativo. El uso del certificado de empleado público se realizará en el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y de



conformidad con las competencias de la Administración, Organismo o Entidad pública actuante y de las facultades conferidas a su personal (independientemente de su condición: funcionarial, laboral, estatutaria, etc.) en virtud de su nombramiento, designación, contrato o instrumento jurídico que regule su relación con tales Administraciones.

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

Sello electrónico de las Administraciones Públicas.

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.

La infraestructura de servicios de certificación y firma electrónica de la FNMT-RCM permite diferentes usos y funcionalidades:

Uso principal. El uso principal del Certificado para la actuación administrativa automatizada» con el concepto de sello electrónico, es vincular unos Datos de verificación de Firma a:

Los datos identificativos y de autenticación de determinada Administración, organismo o entidad y sus respectivas unidades organizativas (unidad que se realiza la actuación administrativa automatizada: área, sección, departamento y

La persona física responsable de la correspondiente Oficina de Registro y/o representante de la Administración, organismo o entidad Suscriptora del Certificado y, en su caso, el personal en quien se delegue a efectos de la actuación administrativa automatizada.

2) Uso no autorizado. El usuario y/o custodio no está autorizado para utilizar estos certificados para usos distintos a los establecidos en el apartado 1) anterior.

3) Marco legislativo. El uso del certificado de Sello electrónico de las AA.PP. se realizará en el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y de conformidad con las competencias de la unidad perteneciente a la Administración, Organismo o Entidad pública titular de la misma y de la infraestructura que alberga el certificado de Sello electrónico de las AA.PP.

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

Sedes electrónicas de las Administraciones Electrónicas.

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.

La infraestructura de servicios de certificación y firma electrónica de la FNMT-RCM permite diferentes usos y funcionalidades:

1) Uso principal. El uso principal del certificado es la identificación de Sedes electrónicas y establecimiento de comunicaciones seguras con dichas Sedes. Los certificados para la identificación de Sedes electrónicas son aquellos certificados expedidos por la FNMT-RCM y que vinculan unos Datos de verificación de Firma a los datos identificativos de una sede electrónica en la que existe una persona física que actúa como firmante o custodio de la clave y el Suscriptor del Certificado que es la administración, organismo o entidad pública a la que pertenece y que es titular de la dirección electrónica y dominio a través de la que se accede a la sede electrónica. Esta persona física es la que tiene el control sobre dicho Certificado y los Datos de creación y verificación de firma y es responsable de su custodia de forma diligente.

2) Uso no autorizado. El usuario y/o custodio no está autorizado para utilizar estos certificados para usos distintos a los establecidos en el apartado 1) anterior.

3) Marco legislativo. El uso del certificado para la identificación de Sedes electrónicas, se realizará en el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y de conformidad con las competencias de la administración, organismo o entidad pública titular del dominio y de la infraestructura que alberga la sede electrónica.

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

Nota sobre prestación de los servicios:

Los servicios contemplados en el presente anexo I, que preste la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, se realizarán de conformidad con lo establecido en la legislación aplicable a los mismos y los acuerdos, encomiendas, convenios o contratos que suscriba la FNMT-RCM con las diferentes administraciones públicas o con personas o entidades privadas.

## ANEXO II

### Precios y plan de implantación

#### CAPÍTULO I

#### Servicios EIT

##### 1. Precio anual de los servicios.

Se establece un precio fijo para los servicios EIT, en caso de ser solicitada su activación de forma expresa por parte de la AEPD, de 1.000,00 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 conviniante, 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.

Se establece un precio de 20.539,66 €/año por la réplica diaria de las listas de certificados revocados desde la FNMT-RCM a las instalaciones del conviniante 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 conviniante.

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 conviniante, incluyendo el acceso de consulta.

#### 4. Condiciones.

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

### CAPÍTULO II

#### Servicios avanzados

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

El precio anual establecido en el apartado 1 del Capítulo III del presente anexo de precios incluye un número máximo de 5 certificados de componente (certificado SSL, SSL plus, Sello de Entidad o de firma de código).

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](http://www.cert.fnmt.es/catalogo-de-servicios/certificados-electronicos)

##### 2. Condiciones.

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

### CAPÍTULO 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 10.000,00 Euros/año impuestos no incluidos, incluye 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 que el conviniente requiera.

El precio de los certificados adicionales será de 807 euros y 690 euros para los certificados de sede electrónica y sello electrónico, 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 añadirles el IVA legalmente establecido.

#### *Plan de Implantación (Tentativo)*

Entrega de documentación y productos.

- Aportación de manuales de uso e instalación de los productos.
- Aportación del software y documentación técnica, incluyendo ejemplos de aplicación.

Acreditación de encargados de acreditar.

- Relación de oficinas de acreditación, incluyendo su denominación y dirección postal completa y dirección IP.

- Relación del número de puestos por oficina de acreditación.
- Selección de los encargados de acreditar.
- Relación de encargados de acreditar por puesto, incluyendo su nombre y apellidos, NIF, y dirección postal completa.
- Calendario de implantación de las oficinas de acreditación.
- Formación de los encargados de acreditar.
- Acreditación de encargados de acreditar, equipo lógico (software) y manuales.
- Constitución de las oficinas y comienzo de la acreditación de usuarios.

Implantación de aplicativos.

- Aportación de la documentación necesaria para la emisión de los certificados de servidor o componente y las claves a firmar.
- Emisión de certificados de firma de código y de servidor o componente necesarios, Definición de los servicios a prestar.
- Calendario de puesta en marcha de las aplicaciones.
- Soporte técnico a la implantación por la FNMT.

Comunicación a los usuarios de los nuevos servicios.

- Envío de correo electrónico, comunicando los nuevos servicios disponibles, a los usuarios activos con dirección de correo electrónico.
- Redacción conjunta de nota de prensa y envío a los medios.
- Publicación de servicios en el apartado de Colaboraciones del web de la FNMT.