TÍTULO: Resolución de 28 de marzo de 2012 por la que se publica el Acuerdo de 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 de firma electrónica y en el ámbito de la Administración electrónica

REGISTRO *NORM@DOC*:	30163
BOMEH:	19/2012
PUBLICADO EN:	BOE n.º 99 de 25 de abril de 2012
Disponible en:	ADMINISTRACIÓN ELECTRÓNICA
VIGENCIA:	En vigor a los 20 días de su publicación
DEPARTAMENTO EMISOR:	Ministerio de Fomento
ANÁLISIS JURÍDICO:	
MATERIAS:	Administración electrónica Firma electrónica

Con fecha 15 de noviembre se ha suscrito el Acuerdo por el que se instrumenta una Encomienda de gestión de la Comisión Nacional del Sector Postal (CNSP) a la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM) para la prestación de servicios técnicos y de seguridad aplicables a la certificación de firma electrónica y en el ámbito de la Administración electrónica.

En cumplimiento de lo dispuesto en el apartado 3 del artículo 15 de la Ley 30/1992, de 26 de noviembre, de Régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y, de conformidad con las competencias conferidas a esta Presidencia en virtud de las competencias/facultades atribuidas por Ley 23/2007, de 8 de octubre y de su nombramiento, realizado mediante Real Decreto 924/2010, de 16 de julio,

RESUELVE:

Proceder a la publicación en el «Boletín Oficial del Estado» del citado Acuerdo, que se incorpora como anexo a esta Resolución.

ANEXO I

Acuerdo por el que se instrumenta la encomienda de gestión por parte de la Comisión Nacional del Sector Postal 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 de firma electrónica y en el ámbito de la Administración electrónica

En Madrid, a 15 de noviembre de 2011.

REUNIDOS

De una parte, doña Rosa Isabel Aza Conejo en nombre y representación de La Comisión Nacional del Sector Postal (en adelante CNSP), en virtud de las competencias/facultades atribuidas por Ley 23/2007, de 8 de octubre y de su nombramiento, realizado mediante Real Decreto 924/2010, de 16 de julio.

Y de otra, don Ángel Esteban Paúl, Director general de la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM), actuando en representación de esta Entidad Pública Empresarial, en virtud de las competencias que le atribuye el artículo 19 del Estatuto de la Entidad, aprobado por el Real Decreto 1114/1999, de 25 de junio (BOE de 7 de julio), y de su nombramiento, realizado mediante el Real Decreto 1869/2008, de 8 de noviembre, (BOE de 11 de noviembre).

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.

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 establece el artículo 45.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Este mismo artículo 81, en su apartado dos, habilita la prestación, por la FNMT-RCM, de los servicios antes señalados, a las Comunidades Autónomas, entidades locales, organismos públicos y entidades de derecho público, vinculadas o dependientes de ellas, siempre que, previamente, se hayan formalizado los convenios o acuerdos procedentes. Y, 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 CNSP, 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 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, determina el reconocimiento a los ciudadanos de su derecho a relacionarse telemática y electrónicamente con las Administraciones Públicas, con el fin de contribuir a la consolidación de la Administración Electrónica, sin perjuicio de la aplicación de los plazos de implantación que figuran en la propia norma. 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 11/2007 ha sido desarrollada parcialmente por el Real Decreto 1671/2009, de 6 de noviembre, en el ámbito de la Administración General del Estado, como un complemento necesario para la facilitar a los ciudadanos la efectiva realización de los derechos reconocidos en la Ley. Este Real Decreto persigue el triple objetivo: 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 servicio y aplicaciones.

Por otra parte, el Real Decreto 1671/2009, establece que la plataforma de verificación de certificados (la denominada validación o consulta sobre la vigencia de certificados de firma electrónica) desarrollada por la FNMT-RCM, se integrará en el sistema nacional de verificación de certificados.

La Orden PRE/878/2010, de 5 de abril, (como desarrollo del artículo 38 del Real Decreto 1671/2009 antes citado) atribuye al Ministerio de la Presidencia la titularidad de la plataforma de notificaciones electrónicas y dirección electrónica habilitada, que se encuentra a disposición de los órganos y organismos públicos, vinculados o dependientes de la AGE, que no hayan establecido sistemas de notificación propios, con el fin de realizar notificaciones electrónicas a los ciudadanos. Los certificados emitidos y el servicio de información sobre el estado de validez de un certificado –servicios prestados por la FNMT-RCM– permiten asegurar las comunicaciones, identificar y autenticar a los emisores y receptores de las comunicaciones realizadas a través del servicio de dirección electrónica habilitada.

Quinto.

De acuerdo con lo establecido en los artículos 4.1.n) y 24.6 de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, la Directiva 2004/18/CE del Parlamento Europeo y del Consejo, de 31 de marzo de 2004 y con las acotaciones y aclaraciones de la numerosa jurisprudencia del Tribunal de Justicia de las Comunidades Europeas, están excluidos de la aplicación de la Ley 30/2007 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 Economía y Hacienda, 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

Modificado por los Reales Decretos 199/2009 y 390/2011., 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 199/2009, de 23 de febrero, configura a la FNMT-RCM, como medio propio y servicio técnico de la Administración General del Estado en los términos de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público y de su Estatuto.

Séptimo.

Expositivo a cumplimentar por la CNSP. En este punto se hace La Comisión Nacional del Sector Postal está creada por la Ley 23/2007, de 8 de octubre, como organismo regulador del sector postal, con el objeto de velar por su transparencia y buen funcionamiento y por el cumplimiento de las exigencias de la libre competencia y se configura como un organismo público, con personalidad jurídica propia y plena capacidad de obrar, de los previstos en la Ley 2/2011, de Economía Sostenible.

El Real Decreto 1920/2009, de 11 de diciembre, por el que se aprueba el Reglamento de desarrollo general de la Ley 23/2007, de 8 de octubre, de creación de la Comisión Nacional del Sector Postal, dispone en su artículo 56 que:

«*La Comisión Nacional del Sector Postal dispondrá de un sitio en Internet de conformidad con lo establecido en la disposición adicional cuarta de la Ley 23/2007, de 8 de octubre y al objeto de cumplir con las previsiones establecidas en la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.*

En el sitio de Internet estarán accesibles, al menos, la estructura y composición de los órganos de la Comisión, el Reglamento Interno de Funcionamiento, las Circulares emitidas, así como todos los informes realizados por la

Comisión para el cumplimiento de sus objetivos y funciones y aquellos que prevea, en cada momento, así como los objetivos anuales o el Plan Estratégico de la Comisión.

El sitio deberá servir de soporte para la divulgación de los objetivos de la Comisión, de los derechos de los usuarios en relación con las competencias de la Comisión, así como plataforma para poder presentar «on line» cualquier consulta, queja o reclamación, debiendo respetar, en todo caso, lo establecido en la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.»

Octavo.

Que, en virtud de las razones ahora expuestas, se ha considerado que las relaciones administrativas, prestacionales y de colaboración entre la CNSP 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 de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público.

Estando ambas partes interesadas en procurar la máxima extensión de la Administración Electrónica para facilitar a los ciudadanos 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. Constituye el objeto de la presente Encomienda de Gestión la prestación, por parte de la FNMT-RCM a la CNSP, de los siguientes servicios:

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 CNSP, 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 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, 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.

2. La FNMT-RCM también prestará a petición de la CNSP los servicios avanzados o especiales que, al efecto, se enumeran en el Capítulo II, del mismo Anexo I, de esta Encomienda de Gestión.

Adicionalmente, y a petición de la CNSP, la FNMT – RCM proveerá los siguientes servicios:

– Tarjetas criptográficas (*según apartado 2.3, de la cláusula segunda*).

– Certificados de software y componentes.

Segunda. 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 CNSP en el marco de sus respectivas competencias.

A tal efecto, la CNSP 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 CNSP cuando así lo admita el ordenamiento jurídico.

2.2 Para servicios del ámbito de la Ley 11/2007. La FNMT-RCM, a los efectos de lo dispuesto en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, prestará 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:

Certificado de firma electrónica del personal al servicio de las Administraciones Públicas (con soporte en tarjeta criptográfica).

Certificados de Sello electrónico de Administración Pública, órgano, organismo o entidad de derecho público.

Certificado para la identificación de Sedes electrónicas.

2.3 Soporte de los Certificados-Títulos de usuario. Tanto para los servicios del artículo 81, como para los de la Ley 11/2007, la FNMT-RCM suministrará, a petición de la CNSP, tarjetas criptográficas como soporte de los certificados del personal al servicio de las Administraciones Públicas y los que tecnológicamente las admitan y que también podrán servir como medio de identificación, de entrada y presencia, de sus funcionarios y empleados. Todo ello, sin perjuicio de la prestación de una serie de infraestructuras que, adecuadamente integradas, permitan cumplir los mandatos de la legislación citada en el expositivo de la presente Encomienda.

2.4 Extensión del ámbito de aplicación. La presente Encomienda de Gestión no aplicará la capacidad para adherirse a la misma, de los organismos y entidades públicas dependientes de la Administración contratante, de haberlos, siendo por ello inoperante el contenido de lo establecido en la cláusula Octava.

2.5 Servicios avanzados o especiales de los señalados en el apartado 2, de la cláusula primera.

Estos servicios podrán prestarse tanto en el ámbito del artículo 81 de la Ley 66/1997, como en el de la Ley 11/2007 y se caracterizan por ser complementarios de los servicios básicos señalados en el apartado 1, de la cláusula primera.

Las condiciones económicas de las actividades a desarrollar en relación con estos servicios se detallan en el Anexo IV de Precios y Plan de Implantación, comprendiendo solo los servicios detallados en el apartado 2, de la cláusula Primera de esta Encomienda.

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 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 a la CNSP para aplicaciones y sistemas de la CNSP, 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 CNSP 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 el Consejo Superior de Administración Electrónica 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 CNSP.

Aportar la tecnología necesaria para que las obligaciones de la CNSP, 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 CNSP 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: http://www.cert.fnmt.es/dpcs.

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

Es necesario tener en cuenta, en todo caso, la parte general de 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.

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 11/2007, 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 CNSP 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 11/2007 (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 CNSP 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 la que se recoge en el Anexo II de esta Encomienda de Gestión. Cualquier modificación o alteración de dicha relación o de la ubicación de las oficinas deberá ser comunicada a la FNMT-RCM, quien dará la oportuna difusión para mantener permanentemente actualizada la relación de la red de Oficinas de Registro y acreditación para la obtención de certificados electrónicos en los términos previstos en el Real Decreto 1317/2001, de 30 de noviembre y resto de normativa aplicable.

Para los servicios del artículo 81 de la Ley 66/1997. La CNSP dispondrá de una red de Oficinas de Registro y acreditación que deberán contar con los medios informáticos precisos para conectarse telemáticamente con la FNMT-RCM. En ellas, la acreditación e identificación de los solicitantes de los certificados exigirá la comprobación de su identidad y de su voluntad de que sea expedido un certificado electrónico y, en su caso, de las facultades de representación, competencia e idoneidad para la obtención del certificado correspondiente, y se verificará de conformidad y con pleno respeto a lo dispuesto en la normativa aplicable.

Estas Oficinas de Registro y acreditación de la CNSP, 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 11/2007. Las Oficinas de Registro de la CNSP, para el ámbito de la Ley 11/2007, 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 titulares de los certificados, de conformidad con la DPC General y la específica Política y Prácticas de Certificación particulares AP, aplicable a este tipo de sistemas, disponibles para consulta en la web:

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

correspondientes a los certificados y sistemas de firma electrónica de este ámbito de aplicación y con los formularios y condiciones de utilización de cada tipo de certificado (Anexo III).

A tal efecto, la CNSP 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.

4. Formularios. Los formularios y condiciones de solicitud de emisión y revocación y/o suspensión, en su caso, de certificados se ajustarán a los modelos recogidos en el Anexo III y a la Declaración de Prácticas de Certificación de la Entidad, aplicable a cada tipo de certificados, accesible en la dirección web citada en el párrafo anterior.

Cuarta. Plazo de duración.

La presente Encomienda de Gestión entrará en vigor el día de su firma y se extenderá hasta el 31 de diciembre de 2012, por lo que abarcará los siguientes ejercicios presupuestarios: 2011 y 2012.

La duración de la Encomienda se podrá prorrogar por años naturales si así lo acordara expresamente la CNSP antes de su vencimiento, dentro de los plazos legales, siendo esta prórroga asumida por la FNMT-RCM.

La contratación de los servicios previstos 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 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

A tal efecto, ambas partes se comprometen a asumir las obligaciones necesarias a este fin. Igualmente, la CNSP 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 y las Instrucciones Internas de Contratación de la Entidad, las obligaciones de confidencialidad pertinentes, restringiendo la información y la publicidad de los diferentes elementos de seguridad, según los estándares aplicables y, en general, realizando la actividad encomendada implantando medidas especiales de seguridad, de conformidad con el estado de la técnica.

Sexta. Tarifas y condiciones de pago.

1. Tarifas por los servicios FNMT. La FNMT-RCM percibirá, por los servicios recogidos en el Capítulo I, del Anexo I (Servicios EIT), y por los servicios recogidos en el Capítulo III del mismo Anexo I (Servicios AP), prestados a la CNSP la cantidad de diez mil doscientos sesenta y seis euros/año (10.266,00 €/año), IVA incluido.

En caso de que el período inicial de duración de la Encomienda sea inferior a un año, la cantidad anterior se prorrateará, reduciéndose proporcionalmente a su duración inicial.

Si hubiera petición expresa de servicios avanzados de los recogidos en el apartado 2.5 de la cláusula Segunda y en el Capítulo II del Anexo I (Servicios avanzados), hecha por la CNSP, la cantidad anterior quedaría incrementada por el importe correspondiente que se dedujera de la aplicación de las tablas del Anexo IV, de Tarifas y Plan de Implantación, de esta Encomienda.

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

Para el ejercicio 2011, de 885,50 euros, IVA incluido.

Para el ejercicio 2012, de 10.266,00 euros, IVA incluido.

Existe certificación de crédito y propuesta y autorización de gasto con fecha 15 de noviembre de 2011 para los ejercicios 2011 y 2012 por un importe de 885,50 euros y de 10.266,00 euros respectivamente.

2. Actualización IPC de la contraprestación. En caso de que no se determinara la contraprestación para la segunda y siguientes anualidades, éstas se actualizarán aplicando la variación del 85% del IPC (índice general interanual) publicado en los doce meses anteriores, de acuerdo con el índice aprobado por el INE, tomando como referencia el del año de la firma de esta Encomienda de Gestión.

3. 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, de la Ley 30/2007, de 30 de octubre, 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 Economía de Hacienda, 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.

4. Facturación. La FNMT-RCM podrá realizar facturaciones trimestrales contra certificaciones parciales conformadas por la CNSP, 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: Comisión Nacional del Sector Postal

Calle: Zurbano, 7

Población: Madrid

Provincia – CP: Madrid - 28010

NIF/CIF: Q2801807E

Departamento o persona de contacto: Gerencia. Pedro Martínez Milla.

Teléfono: 91 348 98 12.

Referencia: Certificaciones firma electrónica.

5. Coste de los servicios de validación (Ley 11/2007). De conformidad con el artículo 21.1 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, la puesta a disposición de la información sobre el estado de validez de los certificados reconocidos, que emita la FNMT-RCM en el ámbito de esta Ley, 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. Extensión de los servicios a otros organismos y entidades públicas vinculadas o dependientes.

La FNMT-RCM no extenderá la prestación de los servicios a que se refiere esta Encomienda de Gestión a organismos y entidades públicas vinculadas o dependientes de la Administración que realiza la presente Encomienda.

Novena. Responsabilidad.

La FNMT-RCM como prestador de los servicios citados en la cláusula primera y Anexos, y la CNSP 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.

Décima. 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 de la Ley 30/2007 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 CNSP 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 CNSP o a los organismos que estén adheridos y que figuran en las cláusulas de esta Encomienda de Gestión y sus Anexos. La resolución frente a un organismo adherido o al firmante principal de la Encomienda, no supondrá la resolución con el resto de organismos que tengan personalidad jurídica independiente de su órgano de adscripción o vinculación.

Causas de extinción. Serán causas de extinción:

El cumplimiento del plazo previsto en la Encomienda y sus prórrogas.

El mutuo acuerdo de las partes.

Undécima. Protección de datos.

Régimen. El régimen de protección de datos de carácter personal derivado de este Convenio 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 n.º 190, de 7 de agosto).

Los ficheros de la CNSP, 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 CNSP 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 11/2007 (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 CNSP.

Acceso a los datos por cuenta de terceros (encargado del tratamiento). No tendrá carácter de comunicación de datos el acceso que la CNSP, 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 art. 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.

De conformidad con el artículo 12 de la LOPD, la CNSP, 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 este Convenio 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 el presente Convenio 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).

No almacenará innecesariamente datos personales en los accesos que se efectúen y en caso de que se almacenen, una vez finalizado el presente Convenio, 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 CNSP 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.

Duodécima. 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 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, 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 Acuerdo es el instrumento jurídico por el que se regula la Encomienda de Gestión que realiza la CNSP a la FNMT-RCM, de acuerdo con los artículos 4.1.n) y 24.6 de la Ley 30/2007, de 30 de octubre, del 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 y el Real Decreto 390/2011, de 18 de marzo, 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.

Decimotercera. 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 a los Ministerios de Economía y Hacienda y de Política Territorial y Administración Pública, 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.

– Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda.

El Director General Ángel Esteban Paúl. La Presidenta de la Comisión Nacional del Sector Postal, Rosa Isabel Aza Conejo.

ÍNDICE DE ANEXOS

ANEXO I

Servicios a prestar

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

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 las 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:

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

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 trascrito en el Anexo III de la presente Encomienda 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. No es preceptiva la incorporación de la dirección de correo electrónico del titular al certificado si bien se hará constar en él en el caso en que el titular aporte dicha dirección en el momento del registro.

Esta incorporación 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 CNSP 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.

La CNSP 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.

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

a) A conservar su control.

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

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

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

a) Solicitud de revocación del usuario, por la persona física o jurídica representada por éste o por un tercero autorizado.

b) Resolución judicial o administrativa que lo ordene.

c) Fallecimiento o extinción de la personalidad del usuario o incapacidad sobrevenida.

d) Finalización del plazo de vigencia del certificado.

e) Pérdida o inutilización por daños en el soporte del certificado.

f) Utilización indebida por un tercero.

g) Inexactitudes graves en los datos aportados por el usuario para la obtención del certificado.

h) Cualquier otra prevista en la normativa vigente.

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

La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda podrá suspender temporalmente la eficacia de los certificados si así lo solicita el usuario o lo ordena una autoridad judicial o administrativa, o cuando existan dudas razonables, por parte de cualquier usuario público, sobre la vigencia de los datos declarados y su verificación requiera la presencia física del interesado. En este caso, la FNMT-RCM podrá requerir, de forma motivada, su comparecencia ante la oficina de acreditación donde se realizó la actividad de identificación previa a la obtención del certificado o,

excepcionalmente, ante otra oficina de acreditación al efecto de la práctica de las comprobaciones que procedan. El incumplimiento de este requerimiento por un periodo de 10 días podrá dar lugar a la revocación del certificado.

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

La extinción de la condición de usuario público se regirá por lo dispuesto en la presente 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 CNSP 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 CNSP 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 en que ofrece acceso a:

Listas de certificados revocados. La actualización en el directorio seguro de los certificados se hará de la siguiente forma:

Los certificados revocados, en el momento de producir efectos la revocación.

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.

Tanto los certificados como 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 en función del tipo de usuario, de forma que:

a) Los órganos de la Administración General del Estado, así como los organismos públicos vinculados o dependientes de ella, tendrán acceso a todos los certificados sin ninguna restricción en cuanto a la información contenida en el directorio. El acceso 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.

b) Las Comunidades Autónomas, las Entidades Locales, así como los Organismos Públicos vinculados o dependientes de ellas, tendrán igualmente acceso a todos los certificados sin ninguna restricción en cuanto a la información contenida en el directorio. El acceso 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.

c) Los operadores y administradores de la infraestructura y los módulos internos, tendrán acceso a toda la información existente en el directorio, pudiendo realizar todo tipo de operaciones en función del perfil definido previamente por el Plan de Seguridad Integral. Este acceso se realizará con autenticación previa.

d) El resto de los usuarios, tendrán el acceso restringido a su propio certificado, y a los de los órganos de la Administración General del Estado, y organismos públicos vinculados o dependientes de ella, y a los de las Comunidades Autónomas, las entidades locales y las entidades de Derecho público vinculadas a ellas. El acceso será solamente de lectura, no pudiendo realizar operaciones para añadir, borrar, modificar o hacer listados de entrada en el directorio.

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

Validación de certificados vía OCSP

Consulta del estado de validez de certificados vía OCSP (ON-Line certificate status protocol)

Introducción.

Uno de los usos de los certificados electrónicos por parte de terceras personas es la verificación de firmas electrónicas efectuadas por el titular del certificado. Sin embargo, aunque la firma electrónica de un determinado documento sea verificada y sea correcta, puede que el poseedor haya invalidado ese certificado con anterioridad a la realización de esa firma. Este proceso, efectuado a petición del propio titular, se denomina revocación del certificado y siempre que se verifique una firma se debe comprobar la validez del certificado del firmante.

Uno de los usos de los certificados electrónicos por parte de terceras personas es la verificación de firmas electrónicas efectuadas por el usuario del certificado. Sin embargo, la firma electrónica de un determinado documento ha de ser verificada en el momento de su utilización, ya que puede que el usuario haya invalidado ese certificado con anterioridad a la realización de esa firma (revocación/suspensión del certificado) o se haya producido la caducidad del mismo por las causas legales correspondientes. Por tanto, es necesario que siempre que se utilice un certificado para generar una firma electrónica se debe comprobar, en tiempo real, la validez de dicho certificado del firmante.

Para realizar esta comprobación existen varios métodos:

Comprobación de CRLs: cuando se solicita la revocación de un certificado, la CA emite y firma una CRL en la que se incluyen los certificados revocados. El usuario que desee verificar el estado de un certificado deberá acceder al directorio donde se publican las CRLs y comprobar si en la CRL que corresponda se encuentra ese certificado.

Verificación OCSP: la verificación OCSP se realiza accediendo al servicio de OCSP. Este servicio abstrae al usuario del acceso al directorio y de la comprobación de la CRL, devolviendo al usuario el estado del certificado objeto de consulta tras una petición de verificación.

Procedimiento.

Básicamente el procedimiento podrá realizarse de la siguiente manera, sin perjuicio de otras opciones posibles, según las condiciones técnicas del servicio:

Un usuario, persona física, que dispone de un certificado electrónico «Clase 2» de la FNMT-RCM desea acceder a los servicios electrónicos del Ministerio de Sanidad y Consumo utilizando, como medio de identificación, su certificado.

El usuario accede a la página web o a las aplicaciones con conexión a Internet del Ministerio de Sanidad y Consumo con el fin de utilizar los servicios electrónicos disponibles, utilizando la identificación que proporciona el certificado emitido por la FNMT-RCM a través de la firma electrónica que genera.

Simultáneamente el sistema del Ministerio de Sanidad y Consumo solicita la validación (OCSP) del certificado al servidor de la FNMT-RCM, el cual le devuelve la información precisa sobre la vigencia, o no, del certificado. En caso de que el certificado esté suspendido o revocado, rechazará la petición de acceso impidiendo continuar con la gestión.

En caso de que el certificado esté vigente y sea válido, el sistema permitirá el acceso a los servicios del Ministerio de Sanidad y Consumo finalizando, en este momento, los servicios prestados por la FNMT-RCM.

Descripción del servicio.

El servicio de consulta del estado de validez de certificados vía OCSP se basa en una arquitectura cliente-servidor. El usuario solicitante de la verificación de un certificado vía OCSP será el que haga uso de la aplicación cliente y la autoridad de validación OCSP hará las labores de servidor.

Servidor OCSP Responder.

El servidor de OCSP (OCSP responder) comprueba la firma de la petición OCSP efectuada por un cliente OCSP registrado en el sistema (base de datos de clientes de los cuales se admiten peticiones) y verifica el estado de los certificados objeto de consulta incluidos en dicha petición. En caso de que la firma de la petición OCSP sea inválida (certificado revocado o caducado, por ejemplo), la petición se rechaza y se retorna al cliente OCSP una respuesta negativa. En la respuesta de OCSP se informará del estado en el que se encuentran los certificados en ese momento.

Las librerías utilizadas son de BouncyCastle (http://www.bouncycastle.org/).

OCSP Cliente.

Herramienta cliente para hacer peticiones de OCSP. Se pueden utilizar los productos del mercado. La FNMT-RCM facilitará una relación con productos de libre distribución, pero en ningún caso suministrará un OCSP cliente, pues se pueden encontrar con facilidad en el mercado de forma estándar.

Los intercambios de información entre las partes cliente y servidor OCSP se ajustarán a las estructuras definidas por el estándar RFC 2560, correspondiente a la norma de OCSP (Online Cetificate Status Protocol) de IETF-PKIX.

Una petición de OCSP contiene los siguientes datos:

Versión del protocolo.

Identificador/es del/los certificado/s a verificar.

Extensiones.

Firma.

Cuando se recibe la petición, el servidor de OCSP determina si el mensaje está correctamente formado y contiene la información necesaria para poder componer una respuesta satisfactoria.

Todas las respuestas proporcionadas por el servidor de OCSP deben ser firmadas digitalmente, y además deben componer los siguientes campos:

Versión de la respuesta.

Nombre del OCSP Responder.

Respuestas para cada uno de los certificados.

Extensiones opcionales.

OID del algoritmo de firma.

Firma.

La respuesta para cada uno de los certificados consiste en:

Identificador del certificado.

Estado del certificado.

Intervalo de validez de la respuesta.

Extensiones opcionales.

El estado de un certificado puede ser:

Good.

Revoked.

Unknown.

CAPÍTULO III

Servicios administración pública (Ley 11/2007)

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 e 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 de AC Administración Pública 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 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 descarga de CRLs de AC Administración Pública 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 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 Autoridad de Fechado Digital (TSA) para Administración Pública

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

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

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 Fechado Digital 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 Fechado Digital, 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 Fechado Digital, 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 Fechado Digital 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 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos 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 a su titular (la Administración, Órgano, Organismo o Entidad pública) con unos datos de verificación de firma y confirma: (1) 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), su número de identificación personal, cargo, puesto de trabajo y/o condición de autorizado, y (2) al titular del certificado, que es el Órgano, Organismo o Entidad de la Administración pública, bien sea ésta General, Autonómica, Local o Institucional.

2) Otros usos. Este certificado podrá ser utilizado por el personal (firmante/custodio) 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 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos 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 donde figura en soporte tarjeta criptográfica y en soporte software.

Sello electrónico de las administraciones públicas

FNMT-RCM no regula el uso de este certificado, dado que se establece en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos 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:

1) Uso principal. El uso principal del certificado de Sello electrónico de las AA.PP. es la identificación y autenticación del ejercicio de la competencia en la actuación administrativa automatizada y la autenticación de

documentos y actuaciones de la Administración, Organismo o Entidad pública titular del mismo. Los certificados de Sello electrónico de las AA.PP. son aquellos certificados expedidos por la FNMT-RCM que vinculan unos datos de verificación de firma a los datos identificativos y de autenticación de determinada Administración, Organismo o Entidad pública y sus respectivas unidades organizativas (unidad que realiza la actuación administrativa automatizada a través de componentes informáticos —área, sección, departamento—) y vinculan a la persona física responsable de la Oficina de Registro y/o representante de la Administración, Organismo o Entidad titular del certificado en quien se delegue y que actuarán como custodios del certificado y sus claves.

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 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos 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 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos 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 (1) los datos identificativos de una Sede electrónica en la que existe una persona física que actúa como custodio del certificado y sus claves y (2) el titular del certificado que es la Administración, Organismo o Entidad pública a la que pertenece y que es, además, titular de la dirección electrónica, dominio e infraestructura a través de la que se accede a la Sede electrónica.

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 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos 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

Oficinas de Registro y Acreditación.

Capítulo I. Procedimientos de registro (URL del Área de Registro).

Capítulo II. Listado de las oficinas de registro.

Con expresión concreta de las Oficinas de Acreditación, su relación, su denominación, la dirección postal correspondiente, la dirección IP.

Oficina de Registro en:

Pz./C:

Dirección I.P.:

ANEXO III

Formularios y condiciones de uso

Capítulo I. Formularios y condiciones clase 2.

Capítulo II. Formularios y condiciones administración pública.

ANEXO IV

Precios y plan de implantación

CAPÍTULO I

Servicios EIT

1. Precio anual de los servicios. Se establece un precio fijo para los servicios EIT y servicios del ámbito de la Ley 11/2007, de diez mil doscientos sesenta y seis euros al año (10.266,00 €/año), incluidos impuestos, cantidad a la que se le repercutirá anualmente la variación por repercusión del 85% del IPC anual.

2. Constitución de las oficinas de acreditación para los servicios EIT. Podrán implantarse cuantas oficinas de acreditación se estime conveniente por parte de la CNSP.

El precio para la constitución de oficinas de acreditación adicionales a la oficina central, se establece en:

32,75 euros por puesto de acreditación. Este precio incluye el software de acreditación.

41,06 euros cada persona encargada de acreditación autorizada. Este precio incluye la emisión de una tarjeta por cada persona y su formación en las instalaciones de la FNMT-RCM.

En el caso en que la formación 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.

En el caso de que fuese personal de la FNMT-RCM quien se encargara del registro, sería necesario valorar los recursos necesarios, en función de los requerimientos del Organismo solicitante.

3. Soporte Técnico.

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

b) 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.

4. 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 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 podrán ser cedidos a terceros bajo ningún concepto, y deberá ser protegido contra todo acceso por entidades ajenas al conviniente, incluyendo el acceso de consulta.

5. Condiciones. Todas las cantidades anteriormente expuestas que supongan pagos fijos anuales se incrementarán a partir de la primera anualidad, aplicando la variación del 85% del IPC publicado en los doce meses anteriores, de acuerdo con el índice aprobado por el I.N.E., tomando como referencia el del año de la firma de la Encomienda de Gestión.

Todas las cantidades expuestas anteriormente en este capítulo I incluyen el IVA legalmente establecido.

CAPÍTULO II

Servicios avanzados

1. Certificados para servidor o componente y firma de código. El precio anual de los servicios esenciales establecido en el apartado 1 del Capítulo I del presente Anexo de Precios incluye un total de 2 certificados de servidor, de componente o de firma de código.

El precio de los certificados adicionales será de 902,70 Euros por cada año de certificado de servidor o componente y de certificado de firma de código siendo emitidos todos ellos por cuatro años.

Certificado de servidor es aquel que permite identificar un servidor web o una URL

Certificado de firma de código es aquel que permite firmar código ejecutable como applets de Java.

2. Tarjetas criptográficas. En el caso de que el certificado solicitado, requiera que el soporte del mismo sea una tarjeta criptográfica, el coste de las mismas será de 15,88 euros por cada una de ellas. Este coste podrá variar dependiendo de las características de las mismas y el número de ellas solicitado. El coste estimado contempla el plástico con su formato estándar y definido por la FNMT-RCM, la personalización de la misma y su envío al titular del certificado. Para estas variaciones de formato o cantidad consultar la siguiente tabla.

A partir de 1.000 unidades se pueden solicitar variaciones sobre el modelo original diseñado por la FNMT-RCM. Para estas variaciones de formato o cantidad consultar la siguiente tabla.

Precios tarjeta criptográfica FNMT-RCM

Año 2011

Cantidad	Tarjeta base	Tarjeta con Pin y CD individual	Sobrecoste Mifare	Tarjeta 4+4	Tarjeta genérica	Panel de firma
100	10,52	11,47	2,20 €	–	11,02	–
300	10,01	10,96	1,62 €	–	10,52	–
500	9,16	10,11	1,50 €	–	10,34	–
1.000	6,02	6,97	1,40 €	10,17	7,60	0,07
2.000	5,64	6,59	1,40 €	7,85	6,40	0,04
3.000	5,42	6,37	1,40 €	6,90	–	0,03
5.000	4,80	5,75	1,40 €	5,63	–	0,03
10.000	4,62	5,57	1,40 €	5,04	–	0,03
15.000	4,35	5,30	1,40 €	4,62	–	0,03
25.000	4,26	5,21	1,40 €	4,43	–	0,03
50.000	3,98	4,93	1,40 €	4,08	–	0,03
100.000	3,95	4,90	1,40 €	4,01	–	0,03

• Precios unitarios en euros.

• La columna Tarjeta Base incluye tarjeta blanca laminada, con banda magnética HICO y chip 80 KB preparada para la carga de certificados.

• La columna Tarjeta con PIN y Código de Desbloqueo individual, corresponde a tarjeta base, incluyendo carrier genérico de FNMT-RCM y sobre blanco, cuyo incremento es de 0,95 euros por unidad.

• La columna Sobrecoste Mifare, corresponde al incremento por incluir chip Mifare de 1 KB y que habría que sumar a la columna que corresponda.

• La columna Tarjeta 4+4 incluye los mismos elementos de la Tarjeta Base pero con impresión en cuatricromía en anverso y reverso.

• La columna Tarjeta Genérica incluye tarjeta impresa con la imagen genérica de la FNMT-RCM, banda magnética HICO y chip 80 KB preparada para la carga de certificados.

• Si la tarjeta lleva panel de firma, se sumará la columna Panel de firma.

• Si la tarjeta incluye Holograma Ceres, el precio se incrementará en 0,50 euros por unidad.

• Si un pedido estuviese entre dos cantidades, siempre se aplicará el precio de la cantidad inmediatamente inferior.

• Transporte e impuestos no incluidos.

3. Validación de certificados vía OCSP. Consulta del estado de validez de certificados vía OCSP (on-line certificate status protocol).

Servicio de validación de certificados vía OCSP: Queda incluido en las condiciones económicas de la presente Encomienda la prestación sin costo del presente servicio.

4. Condiciones. Todas las cantidades anteriormente expuestas que supongan pagos fijos anuales se incrementarán a partir de la primera anualidad, aplicando la variación del 85% del IPC publicado en los doce meses anteriores, de acuerdo con el índice aprobado por el I.N.E., tomando como referencia el del año de la firma de la Encomienda de Gestión.

A todas las cantidades expuestas en el presente capítulo II excepto las de su apartado 1 habrá que añadirlas el IVA legalmente establecido.

CAPÍTULO III

Servicios administración pública (Ley 11/2007)

1. Certificados de *sede electrónica* y de *sello electrónico* para actuaciones automatizadas para los servicios del ámbito de la Ley 11/2007.

El precio anual de los servicios del ámbito de la Ley 11/2007 establecido en el apartado 1 del Capítulo I del presente Anexo IV de Precios incluye 1 certificado de sede y 1 certificado de sello.

El precio de los certificados adicionales tanto de *sede* como de *sello* será de 900,00 Euros por cada unidad y año de certificado siendo emitidos todos ellos por tres años.

2. Servicio de autoridad de fechado digital (TSA) para Administración Pública.

El precio anual de los servicios del ámbito de la Ley 11/2007 establecido en el apartado 1 del cap. I del presente Anexo IV de Precios incluye el servicio de autoridad de fechado digital (TSA) para Administración Pública junto con un certificado de firma electrónica (emitido por tres años) 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. Servicio de autoridad de fechado digital (TSA) para Administración Pública.

La FNMT - RCM emitirá certificados de empleado público a la CNSP hasta un máximo de 25 certificados.

4. Condiciones. Todas las cantidades anteriormente expuestas que supongan pagos fijos anuales se incrementarán a partir de la primera anualidad, aplicando la variación del 85% del IPC publicado en los doce meses anteriores, de acuerdo con el índice aprobado por el I.N.E., tomando como referencia el del año de la firma de la Encomienda de Gestión.

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

Aportación del software de verificación de listas de revocación.

Aportación del software de firma.

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, entrega de tarjetas, equipo lógico (software), lectores 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.

Evaluación de la conformidad de cumplimiento del punto 1.2 relativa a extensión de los servicios.

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 Colabora.