III. OTRAS DISPOSICIONES

MINISTERIO DE SANIDAD Y POLÍTICA SOCIAL

21109 *Resolución de 2 de diciembre de 2009, del Instituto de Mayores y Servicios Sociales, 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.*

Con fecha 25 de noviembre se ha suscrito el Acuerdo por el que se instrumenta una Encomienda de gestión del Instituto de Mayores y Servicios Sociales (IMSERSO) 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 Dirección General por el Real Decreto 1226/2005, de 13 de octubre, resuelve:

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

Madrid, 2 de diciembre de 2009.–La Directora General del Instituto de Mayores y Servicios Sociales, Pilar Rodríguez Rodríguez.

ANEXO I

Acuerdo por el que se instrumenta la Encomienda de gestión por parte del Instituto de Mayores y Servicios Sociales 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 25 de noviembre de 2009.

REUNIDOS

De una parte, doña Pilar Rodríguez Rodríguez en nombre y representación del Instituto de Mayores y Servicios Sociales (en adelante IMSERSO), en virtud del nombramiento por Real Decreto 1455/2008, de 29 de agosto.

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,

cve: BOE-A-2009-21109

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 el IMSERSO, los términos que deben regir la prestación de sus servicios en relación con las comunicaciones empleando técnicas y medios electrónicos, informáticos y telemáticos.

Por su parte, el Real Decreto 209/2003, de 21 de febrero, regula los registros y las notificaciones telemáticas y la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos y establece una regulación específicamente dirigida al desarrollo e implantación de la administración electrónica dentro de la Administración General del Estado. Este Real Decreto modifica el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas para la Administración General del Estado y el Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro.

La Orden PRE/1551/2003, de 10 de junio, desarrolla la disposición final primera del antes citado Real Decreto 209/2003, de 21 de febrero, estableciendo los requisitos de autenticidad, integridad, disponibilidad y confidencialidad de los dispositivos y aplicaciones

cve: BOE-A-2009-21109

de registro y notificación, así como los protocolos y criterios técnicos a los que deben sujetarse y las condiciones que ha de reunir el órgano, organismo o entidad habilitada para la prestación del servicio de dirección electrónica única así como las condiciones de su prestación.

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.

Hasta que se produzca el desarrollo reglamentario de esta Ley, los Reales Decretos citados anteriormente seguirán en vigor siempre que no contradigan o se opongan a lo establecido en la Ley 11/2007, de 22 de junio.

Quinto.–El artículo 15, de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, establece que la realización de actividades de carácter material, técnico o de servicios de la competencia de los órganos administrativos o de las Entidades de derecho público podrá ser encomendada a otros órganos o Entidades de la misma o de distinta Administración, por razones de eficacia o cuando no se posean los medios técnicos idóneos para su desempeño; todo ello, sin que el hecho de encomendar los servicios correspondientes supongan cesión de titularidad de la competencia ni de los elementos sustantivos de su ejercicio, siendo responsabilidad del órgano o Entidad encomendante dictar cuantos actos o resoluciones de carácter jurídico den soporte o en los que se integre la concreta actividad material objeto de encomienda.

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, reconoce y establece, como uno de los fines de la Entidad (fijados por el citado artículo 81 de la Ley 66/1997), 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 usuarios (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.–El IMSERSO, en el marco de desarrollo de sus competencias, presta determinados servicios soportados por técnicas y medios electrónicos, informáticos y telemáticos aplicados a determinados procedimientos administrativos. Estos servicios deben contar con las debidas garantías de seguridad conformes con las disposiciones legales y en orden a garantizar la validez y eficacia de la emisión y recepción de comunicaciones y documentos producidos a través de técnicas y medios EIT. Por otra

cve: BOE-A-2009-21109

parte también se requiere la identificación electrónica del IMSERSO 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.

Octavo.–Que, en virtud de las razones ahora expuestas, se ha considerado que las relaciones administrativas, prestacionales y de colaboración entre el IMSERSO 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 el artículo 15, de la citada Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo común y los artículos 4.1.n) y 24.6 de la Ley 30/2007, de 30 de octubre.

Se hace constar que el presente documento se aprobó como documento tipo por el Consejo de Administración de la FNMT-RCM, el cual será elevado a la Subsecretaría de Economía y Hacienda, a través del citado Consejo, con el fin de que sea confirmado por el órgano de adscripción de la FNMT-RCM, de conformidad con el artículo 3, apartado 2, del Estatuto de esta Entidad.

Estando ambas partes interesadas en procurar la máxima extensión de la prestación de estos servicios 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 al IMSERSO, 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 del IMSERSO, 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 del IMSERSO cualquiera, o la totalidad, de los servicios avanzados o especiales que, al efecto, se enumeran en el capítulo II, del mismo anexo I, de esta Encomienda de Gestión.

Segunda. *Ámbito de aplicación.*

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 el IMSERSO en el marco de sus respectivas competencias. A tal efecto, el IMSERSO 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.

cve: BOE-A-2009-21109

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 el IMSERSO cuando así lo admita el ordenamiento jurídico.

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.ceres.fnmt.es/index.php?cha=cit&sec=3&page=197&lang=es

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.

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 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.

Extensión del ámbito de aplicación.–Podrán adherirse a la presente Encomienda, los organismos y entidades públicas dependientes de la Administración contratante, de conformidad con lo establecido en la cláusula octava.

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 necesaria infraestructura técnica, organizativa y de seguridad.

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 al IMSERSO para aplicaciones y sistemas del IMSERSO, 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 al IMSERSO la información necesaria para el buen funcionamiento de los sistemas.

Actualizar tecnológicamente los sistemas, de acuerdo con el estado de la técnica, 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 del IMSERSO.

Aportar la tecnología necesaria para que las obligaciones del IMSERSO, 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.

cve: BOE-A-2009-21109

Tener disponible para consulta del IMSERSO 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.ceres.fnmt.es/index.php?cha=cit&sec=3&page=197&lang=es

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, no dependerán directamente de la FNMT-RCM sino del órgano u organismo público de origen, sin perjuicio del control de gestión y protocolos de registro que realice la FNMT-RCM, en su condición de Prestador de Servicios de Certificación.

2. Por su parte, el IMSERSO 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 el la URL www.imserso.es 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.

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.

cve: BOE-A-2009-21109

Para los servicios del artículo 81 de la Ley 66/1997.–El IMSERSO 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 del IMSERSO, 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 del IMSERSO, 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 Declaración de Prácticas Certificación APE aplicable a este tipo de sistemas, disponibles para consulta en la Web:

http://www.ceres.fnmt.es/index.php?cha=cit&sec=3&page=197&lang=es

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, el IMSERSO 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 2011.

La duración de la Encomienda podrá prorrogarse, por años naturales, hasta dos ejercicios más si así lo acordara expresamente el IMSERSO antes de su vencimiento, siendo estas prórrogas asumidas por la FNMT-RCM.

La contratación de los servicios previstos en esta Encomienda, más allá de su duración inicial y, en su caso, las dos posibles prórrogas, solamente podrá realizarse por nueva Encomienda.

cve: BOE-A-2009-21109

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, el IMSERSO 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. *Precio y condiciones de pago.*

Precio total.–La contraprestación a percibir por la FNMT-RCM sobre las actividades realizadas en esta Encomienda de Gestión asciende a la cantidad de noventa y ocho mil cuatrocientos veintitrés euros al año (98.423,00 €/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.

El precio total se imcrementará por el suministro de 1.000 tarjetas con chip de 32 Kb preparadas para generar y usar los certificados digitales con impresión de cuatricromía en anverso y reverso, con el chip de proximidad Mifare para control de accesos y personalización con foto por termoimpresión por importe de diecisiete mil quinientos cincuenta euros con ochenta céntimos (17.550,86 €), 700 tarjetas se suministraran en el ejercicio 2010 y 300 en el ejercicio 2011.

La distribución por anualidades IVA incluido será la siguiente:

Para el ejercicio 2010, de 102.506,67 euros (11 mensualidades + 700 tarjetas).
Para el ejercicio 2011, de 103.688,27 euros.(12 mensualidades + 300 tarjetas).
Para el ejercicio 2012, de 8.201,92 euros (mensualidad diciembre 2011).

Para los sucesivos años de vida de la Encomienda la cantidad a percibir por la FNMT-RCM sobre las actividades realizadas en esta Encomienda de Gestión será actualizada por aplicación de la variación del 85% del IPC (índice general interanual) publicado en los doce meses anteriores de acuerdo con el índice aprobado por el INE.

Existe reserva de crédito en la aplicación presupuestaria 3591 227.82 para los ejercicios 2010, 2011 y 2012.

Este precio se obtiene sumando los importes recogidos en los apartados 1 y 2 siguientes, al que podrán añadirse partidas por servicios avanzados.

1. Precios por servicios EIT - artículo 81 (Ciudadanos / Empresas / Serv. Adicionales).–La FNMT-RCM percibirá, por los servicios esenciales EIT, recogidos en el capítulo I, del anexo I, prestados al IMSERSO la cantidad de ochenta y seis mil ochocientos veintitrés euros al año (86.823,00 €/año), incluidos impuestos cantidad que se incrementará a partir de la primera anualidad de vida de la Encomienda, aplicando la variación del 85%del IPC (índice general

cve: BOE-A-2009-21109

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. La aplicación de este precio se establece en el capítulo I del anexo IV, de la presente Encomienda.

Si hubiera petición expresa de servicios avanzados de los recogidos en el capítulo II del anexo I, hecha por el IMSERSO la cantidad anterior quedaría incrementada por el importe correspondiente que se dedujera de la aplicación de las tablas del capítulo II del anexo IV, de Precios y Plan de Implantación, de la presente Encomienda.

2. Precios por Servicios Ley 11/2007 (Empleado / Sede / Sello / Tarjetas / Serv. Adicionales).–La FNMT-RCM percibirá, por los servicios de la Ley 11/2007, recogidos en el capítulo III del anexo I, prestados al IMSERSO la cantidad de once mil seiscientos euros al año (11.600,00 €/año) (IVA incluido) cantidad que se incrementará a partir de la primera anualidad de vida de la Encomienda, 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. La aplicación de este precio se establece en las tablas de los capítulos I, y III del anexo IV, de esta Encomienda.

Si hubiera petición expresa de servicios de los recogidos en el capítulo III del anexo I, hecha por el IMSERSO, la cantidad anterior quedaría incrementada por el importe correspondiente que se dedujera de la aplicación de las tablas del capítulo II del anexo IV, de Precios y Plan de Implantación, de esta Encomienda.

3. Actualización de precios.–En caso de que se produzcan prórrogas de la Encomienda y no se fije el precio de las mismas o se acuerde su actualización, todos los precios de cada una de las prórrogas correspondientes, 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.

4. Consideración de los precios.–Los precios establecidos 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 función del número de administraciones destinatarias, de las disponibilidades presupuestarias y del volumen de los servicios prestados.

5. Facturación.–La FNMT-RCM, podrá realizar facturaciones mensuales contra certificaciones parciales conformadas por el IMSERSO, 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 IMSERSO. Área de Informática.
Calle Avenida de la Ilustración s/n con vta a Ginzo de Limia, 58.
Población Madrid.
Provincia – CP 28029 Madrid.
NIF/CIF Q2827004I.
Persona de contacto/Teléfono: Antonio Sánchez Burgos / 913638505.
Referencia: Encomienda FNMT.

cve: BOE-A-2009-21109

6. 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 del firmante.*–La FNMT-RCM extenderá la prestación de los servicios a que se refiere esta Encomienda de Gestión a solicitud de cualesquiera organismos y entidades públicas vinculadas o dependientes de la Administración que realiza la presente Encomienda. Esta solicitud se instrumentará a través del protocolo de adhesión a la Encomienda, según el modelo del anexo V.

FNMT-RCM quedará vinculada por la solicitud de adhesión, siempre que se cumplan las siguientes dos condiciones:

a) Que esta Entidad cuente con las capacidades presupuestarias y productivas necesarias y

b) Que, por parte del organismo o entidad que se adhiera, exista reserva de crédito o asignación presupuestaria suficiente para la prestación de los servicios en cada ejercicio y así se refleje en el citado protocolo de adhesión.

Novena. *Responsabilidad.*–La FNMT-RCM como prestador de los servicios citados en la cláusula primera y anexos, y el IMSERSO 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 del IMSERSO 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 adherente 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

cve: BOE-A-2009-21109

corresponden al IMSERSO 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 adherente 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 derivados de esta Encomienda 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 serán de titularidad pública y su creación, modificación o supresión se ha realizado por disposición general publicada en el «Boletín Oficial del Estado» (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 del IMSERSO y, en su caso, de los organismos o entidades que se adhieran, serán de titularidad pública y su creación, modificación o supresión se realizará por disposición general, de conformidad con la Ley.

Acceso a los datos por cuenta de terceros.–Sin perjuicio de las cesiones de datos que por aplicación de la legislación de protección de datos de carácter personal se puedan realizar entre las Administraciones Públicas en el ejercicio de sus competencias, no tendrá carácter de comunicación de datos el acceso que el IMSERSO y los organismos y entidades que se adhieran, puedan realizar sobre los datos de carácter personal que mantiene la FNMT-RCM, como responsable del fichero, sobre sus usuarios, personas físicas, con la finalidad de solicitar los servicios descritos en la presente Encomienda. Tales datos son los que figuran en el fichero regulado, en el número 5 del anexo de la Orden EHA/2357/2008, citada en el apartado anterior.

Tampoco tendrá carácter de comunicación de datos el acceso que la FNMT-RCM pudiera realizar sobre los datos de carácter personal que, como responsable del fichero, el IMSERSO y los organismos o entidades que estén adheridos mantienen sobre sus usuarios personas físicas, con la finalidad de prestar los servicios descritos en esta Encomienda.

De conformidad con el artículo 12 de la LOPD, la FNMT-RCM, el IMSERSO y los organismos o entidades que estén adheridos, en su calidad de encargados del tratamiento, asumirán las siguientes obligaciones:

Únicamente tratarán los datos conforme a las instrucciones del responsable del fichero y que se refiere exclusivamente a hacer efectiva la realización de los servicios contemplados en esta Encomienda.

No aplicarán o utilizarán los datos con un fin distinto al que figura en la presente Encomienda y sus anexos.

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

Aplicarán medidas de seguridad acordes con el tipo de datos que traten.

No almacenarán innecesariamente datos personales en los accesos que se efectúen y en caso de que se almacenen, una vez finalizado el presente Contrato, destruirán o devolverán al responsable del fichero los datos y soportes donde figuren, levantando acta del tal destrucción o devolución.

cve: BOE-A-2009-21109

En caso de que la FNMT-RCM, el IMSERSO 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 el IMSERSO 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 y el Estatuto de la FNMT-RCM, así como el resto de disposiciones de aplicación.

El IMSERSO tendrá, en cuanto encomendante, la facultad de dictar cuantos actos y resoluciones fueran necesarias para el desarrollo de la actividad material y técnica encomendada a la FNMT-RCM, de acuerdo con lo dispuesto en el artículo 15, apartado 2, de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en su caso normativa especial correspondiente.

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. *Información y publicación.*–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 la Presidencia, 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.

La presente Encomienda de Gestión, será objeto de publicación en los términos previstos por la normativa aplicable.

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.–Imserso, la Directora General del Imserso, Pilar Rodríguez Rodríguez.

ÍNDICE DE ANEXOS

cve: BOE-A-2009-21109

ANEXO I

Servicios a prestar

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

CAPITULO I

Servicios EIT

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

El formato de los certificados utilizados por la FNMT-RCM se basa en el definido por la Unión Internacional de Telecomunicaciones, sector de normalización de las telecomunicaciones, en la Recomendación UIT-T X.509, de 31 de marzo de 2000 o superiores (ISO/IEC 9594-8 de 2001). El formato será el correspondiente a la Versión 3 del certificado, especificado en esta norma.

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

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

Registro de usuarios.
Emisión, revocación y archivo de certificados de clave pública.
Publicación de certificados y del Registro de Certificados.
Registro de eventos significativos.

Generación y gestión de claves

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

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

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

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

cve: BOE-A-2009-21109

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/content/pages_std/docs/00034_cit_obtain_cert_0000000000%20-%20Declaracion%20de%20Practicas%20de%20Certificacion.pdf

cve: BOE-A-2009-21109

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 el IMSERSO 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.

cve: BOE-A-2009-21109

Aceptación de certificados.–Para que un certificado sea publicado por la FNMT-RCM, ésta comprobará previamente:

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

El IMSERSO garantizará que, al solicitar un certificado electrónico, su titular acepta que:

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

El IMSERSO 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

cve: BOE-A-2009-21109

otra oficina de acreditación al efecto de la práctica de las comprobaciones que procedan. El incumplimiento de este requerimiento por un periodo de diez 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 al IMSERSO los mecanismos de la transmisión segura para el establecimiento de un servicio continuo e ininterrumpido de comunicación entre ambas a fin de que, por medios telemáticos o a través de un centro de atención telefónica a usuarios, se ponga de inmediato en conocimiento de la FNMT-RCM cualquier circunstancia de que tenga conocimiento y que sea determinante para la suspensión, revocación o extinción de la vigencia de los certificados ya expedidos, a fin de que se pueda dar publicidad de este hecho, de manera inmediata, en el directorio actualizado de certificados a que se refiere el artículo 18 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

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

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

El IMSERSO 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.

cve: BOE-A-2009-21109

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.

cve: BOE-A-2009-21109

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 quince años.

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

Datos relevantes que serán registrados.–Serán registrados los siguientes eventos relevantes:

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

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

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

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

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

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

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

CAPITULO II

Servicios avanzados

Servicio de fechado digital

Introducción

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

cve: BOE-A-2009-21109

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

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

Protocolo

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

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

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

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

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

1. El usuario selecciona el fichero electrónico del cual se solicitará el sellado a la TSA.
2. La aplicación cliente compone un resumen (hash) del contenido de ese fichero.
3. El usuario selecciona la política de servicio que desea, el número de referencia, la versión,...
4. La aplicación cliente compone una petición de fechado digital y la envía vía HTTPS.

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

1. La aplicación cliente recompone el objeto Response, extrayendo el estado de la operación, y si éste es GRANTED se puede extraer también el objeto CMS SignedData.
2. La aplicación cliente recompone el objeto CMS SignedData, extrayendo los datos firmados y verificando que la firma es correcta, haciendo uso del certificado de la TSA incluido en el objeto CMS.
3. Se obtienen los certificados incluidos en el objeto CMS y se hace «path validation».
4. Si el cliente lo ha seleccionado se realiza la verificación OCSP (On-line Certificate Status Protocol) de los certificados, para así comprobar el estado de revocación de esos certificados.
5. La aplicación cliente obtendrá los datos de sellado del «token».

cve: BOE-A-2009-21109

Estándares aplicables

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

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

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

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

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

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

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

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

El estándar RFC 2630 define el formato usado para la encapsulación de datos firmados, cifrados, resumidos o para la autenticación de mensajes arbitrarios. La RFC 2630 deriva del PKCS#7 versión 1.5 (RFC 2315).

Dentro de la iniciativa EESSI se ha recogido la anterior normativa a través de la ETSI TS 101 861, según se ha extraído en el presente texto.

Estructuras de datos

Las estructuras de datos utilizadas en el protocolo son las siguientes:

```
TimeStampRequest::= SEQUENCE {
version                 Integer {v1(1)},
messageImprint          MessageImprint,
reqPolicy               PolicyInformation OPTIONAL,
nonce                           Integer OPTIONAL,
certReq                 BOOLEAN DEFAULT FALSE,
extensions              [0] IMPLICIT Extensions OPTIONAL }
TimeStampResp::= SEQUENCE {
status                          PKIStatusInfo,
timeStampToken          TimeStampToken OPTIONAL }
TSTInfo::= SEQUENCE {
version                 INTEGER {v1(1)},
policy                          TSAPolicyId,
messageImprint          MessageImprint,
serialNumber                    INTEGER
```

cve: BOE-A-2009-21109

genTime	GeneralizedTime,
accuracy	Accuracy OPTIONAL,
ordering	BOOLEAN DEFAULT FALSE,
nonce	INTEGER OPTIONAL,
tsa	[0] GeneralName OPTIONAL,
extensions	[1] IMPLICIT Extensions OPTIONAL }

Fuente de tiempo

La fuente de tiempo segura es un servicio que proporciona el instante exacto en el momento en el que se realiza la petición.

Las fuentes de tiempo utilizadas por la Autoridad de Fechado Digital es el ROA.

Una vez recibida la fuente de tiempo distribuye la referencia temporal a la Autoridad de Fechado Digital haciendo uso del protocolo NTP (Network Time Protocol) con una precisión de entre uno (1) y diez (10) milisegundos.

Actualización tecnológica

La FNMT someterá el servicio a la actualización tecnológica constante que permita que la disponibilidad del servicio y el acceso al mismo cumpla en todo momento los criterios técnicos iniciales así como aquellos que fruto de los avances tecnológicos o del desarrollo normativo, le sean de aplicación.

Dicha actualización se realizará, tratando de evitar en la medida de lo posible, el cambio en los procedimientos seguidos hasta la fecha de la actualización por los titulares.

La FNMT notificará a los titulares con 2 meses de antelación las actualizaciones que pudieran causar modificaciones en los procedimientos de acceso a la dirección o de consulta del contenido depositado.

Prácticas del servicio

La declaración detallada de prácticas del servicio se publicará en la dirección electrónica de la FNMT y podrá ser variada sin previo aviso. La variación no limitará el servicio.

CAPITULO III

Servicios APE (Ley 11/2007)

Servicio de Validación del Certificado de la AC APE.–Para comprobar la validez del certificado de la Autoridad de Certificación de la APE, 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.

cve: BOE-A-2009-21109

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 APE.–El servicio de Validación de Certificados para la infraestructura APE, se prestará mediante los siguientes servicios:

Servicio de descarga de CRLs de AC APE mediante protocolo LDAP.
Servicio de descarga de CRLs de AC APE 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 del APE.

Servicio de descarga de CRLs de AC APE 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 APE.

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 del APE, 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 APE 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 APE.

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 del APE, siendo en cada caso CRLnnn el número de CRL que le corresponde a dicho certificado al igual que el anteriormente descrito.

cve: BOE-A-2009-21109

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

http://tsaape.cert.fnmt.es/ TSS/HttpTspServer.

Este servicio NO requerirá autenticación de cliente, pero si será necesario que el organismo que desee utilizarlo, nos proporcione la IP con la que accederá a dicho servicio para tener control de su actividad y será necesaria su autorización por parte de la FNMT-RCM antes de poder realizar peticiones.

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 APE, 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.

cve: BOE-A-2009-21109

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.

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

cve: BOE-A-2009-21109

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:

IMSERSO
Pz. / C
Dirección I.P.:

ANEXO III

Formularios y condiciones de uso

Capítulo I. Formularios y condiciones clase 2.
Capítulo II. Formularios y condiciones APE.

cve: BOE-A-2009-21109

ANEXO IV

Precios y plan de implantación

CAPITULO I

Servicios EIT

1. Precio anual de los servicios.–Se establece un precio fijo para los servicios EIT, impuestos incluidos, de 86.823,00 €/año, cantidad a la que se le repercutirá anualmente la variación por repercusión del 85% del IPC anual.

Se establece un precio fijo para los servicios del ámbito de la Ley 11/2007, incluidos impuestos, de 11.600,00 €/año, cantidad a la que se le repercutirá anualmente la variación por repercusión del 85% del IPC anual.

Este importe no incluye la extensión del servicio del ámbito de la Ley 11/2007 a los Organismos que se adhieran a la presente Encomienda de Gestión.

2. Constitución de las oficinas de acreditación para los servicios EIT.–Podrán implantarse cuantas oficinas de acreditación se estime conveniente por parte del IMSERSO, las cuales deberán hacerse públicas, indicando su dirección postal y horario de atención al público, en la dirección www._____

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

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

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

5. Condiciones.–Todas las cantidades anteriormente expuestas que supongan pagos fijos anuales se incrementarán a partir de la primera anualidad, aplicando la variación 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.

cve: BOE-A-2009-21109

CAPITULO 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 4 certificados de servidor o componente y 1 de firma de código.

El precio de los certificados adicionales será de 875,11 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. Fechado Digital para los servicios EIT.–El precio anual de los servicios esenciales establecido en el apartado 1 del capítulo I del presente anexo de Precios incluye el alta y mantenimiento de este servicio en los términos que exactamente se indican en el siguiente párrafo y la realización de todos los sellados de tiempo durante el primer año de vigencia de la Encomienda de Gestión, transcurrido el cual sin haberse hecho uso de los mismos, parcialmente o en su totalidad, no será posible su convalidación para los sucesivos periodos anuales.

El precio de este servicio, adquirido de forma independiente, se facturará por dos conceptos:

a) Por alta y mantenimiento del sistema: Este concepto es de 5.000 euros. Este precio incluye las librerías necesarias para el uso de la aplicación (y el mantenimiento de las mismas), pero no los posibles desarrollos que haya que realizar y 50.000 sellados anuales los cuales han de consumirse en el plazo máximo de una anualidad lo que, de no hacerlo, no los hace acumulables para los años posteriores. Su abono es anual.

b) Por un coste variable que establece por el número de los sellados realizados en el plazo de una anualidad cuya cifra acumulada supere la cantidad de 50.000, sin mayor límite, a razón de 0,05 €/sellado.

3. 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:

cve: BOE-A-2009-21109

PRECIOS TARJETA CRIPTOGRÁFICA FNMT-RCM
AÑO 2.009

CANTIDAD	TARJETA BASE	SOBRECOSTE MIFARE	TARJETA 4+4	TARJETA GENÉRICA	PANEL DE FIRMA
100	11,47 €	5,45 €	-------	11,97 €	------
300	10,96 €	4,72 €	-------	11,47 €	------
500	10,11 €	3,51 €	-------	11,29 €	------
1.000	6,97 €	3,05 €	11,12 €	8,55 €	0,07
2.000	6,59 €	2,75 €	8,80 €	7,35 €	0,04
3.000	6,37 €	2,55 €	7,85 €	------	0,03
5.000	5,75 €	2,32 €	6,58 €	------	0,03
10.000	5,57 €	2,01 €	5,99 €	------	0,03
15.000	5,30 €	1,57 €	5,57 €	------	0,03
25.000	5,21 €	1,41 €	5,38 €	------	0,03
50.000	4,93 €	1,21 €	5,03 €	------	0,03
100.000	4,90 €	1,16 €	4,96 €	------	0,03

- Precios unitarios en euros.
- La columna **Tarjeta Base** incluye tarjeta blanca laminada, con banda magnética HICO y chip 32 KB preparada para la carga de certificados.
- 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, holograma FNMT, panel de firma y chip 32 KB preparada para la carga de certificados.
- Si la tarjeta lleva panel de firma, se sumará la columna **Panel de firma**.
- En todos los casos, la tarjeta lleva **PIN y Código de Desbloqueo individual**, incluyendo carrier genérico de FNMT-RCM y sobre blanco, sin sobrecoste adicional.
- Si un pedido estuviese entre dos cantidades, siempre se aplicará el precio de la cantidad inmediatamente inferior.
- Transporte e impuestos no incluidos.

cve: BOE-A-2009-21109

4. Condiciones.–Todas las cantidades anteriormente expuestas que supongan pagos fijos anuales se incrementarán a partir de la primera anualidad, aplicando la variación 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.

CAPITULO III

Servicios APE (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 3 certificados 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 APE.–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 el servicio de autoridad de fechado digital (TSA) para APE, 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. Condiciones.–Todas las cantidades anteriormente expuestas que supongan pagos fijos anuales se incrementarán a partir de la primera anualidad, aplicando la variación del IPC 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 la Encomienda de Gestión.

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

ANEXO V

Modelo de protocolo de adhesión

PROTOCOLO DE ADHESIÓN DE ____ (DEPARTAMENTO, ÓRGANO, ORGANISMO O ENTIDAD) ____ A LA ENCOMIENDA SUSCRITA EL __ (FECHA) __ ENTRE _____ Y LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA, PARA LA PRESTACIÓN DE SERVICIOS, TÉCNICOS Y DE SEGURIDAD, APLICABLES A LA CERTIFICACIÓN Y FIRMA ELECTRÓNICA EN EL ÁMBITO DE LA ADMINISTRACIÓN ELECTRÓNICA.

En Madrid, a ____ de _____ de _____

REUNIDOS

De una parte, don/doña _____, en su calidad de _____, en nombre y representación de _____, en virtud de las competencias atribuidas por _____.

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).

cve: BOE-A-2009-21109

Ambas partes, reconociéndose competencia y capacidad legal necesaria para formalizar el presente Protocolo de Adhesión,

EXPONEN

Primero.–El _____ y la FNMT-RCM suscribieron, con fecha _____, una Encomienda de Gestión para la prestación, por parte de ésta, de servicios de certificación y firma electrónica según se estipula en las cláusulas de esta Encomienda de Gestión y sus anexos y que, de conformidad con su objeto, son: (1) servicios técnicos, administrativos y de seguridad para garantizar la validez y eficacia en la emisión y recepción de comunicaciones y documentos producidos a través de técnicas y medios EIT en el ámbito de actuación de este IMSERSO y en el de las administraciones que se adhieran a la citada Encomienda de Gestión; y (2) la prestación de los 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.

Segundo.–La cláusula octava de la referida Encomienda de Gestión expresa que la FNMT-RCM prestará los servicios referidos en el mismo a cualesquiera Departamentos ministeriales, Órganos, Organismos y Entidades públicas, vinculadas o dependientes de la Administración General del Estado, instrumentándose mediante el Protocolo de Adhesión que figura anexo a la citada Encomienda de Gestión. Lo que viene a ejecutarse en este acto.

Tercero.–A los efectos previstos en el expositivo anterior, el ___(departamento, órgano, organismo o entidad)____ ha considerado, previa aprobación del órgano competente, adherirse a la referida Encomienda de Gestión expresado en el expositivo Primero, para lo cual suscribe, conjuntamente con la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, el presente Protocolo de Adhesión, con arreglo a las siguientes

CLÁUSULAS

Primera.–A través del presente Protocolo y de conformidad con lo anteriormente manifestado, ____(departamento, órgano, organismo o entidad)____ se adhiere a la «Encomienda de Gestión entre el _____ y la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, para la prestación de servicios técnicos y de seguridad aplicables a la certificación y firma electrónica en el ámbito de la Administración Electrónica», suscrita con fecha _____, expresando que lo conoce y acepta en toda su extensión. Una copia del mismo se incorpora a este Protocolo como anexo.

A partir de la entrada en vigor del presente Protocolo, ____(departamento, órgano, organismo o entidad)____, se considera parte de la Encomienda de Gestión citada en el párrafo anterior, en calidad de parte destinataria de los servicios y asume los derechos y obligaciones contenidos en el mismo, siendo, la FNMT-RCM, el prestador de los servicios y actividades contenidas en la citada Encomienda de Gestión. En consecuencia, ____(departamento, órgano, organismo o entidad)____, acepta los mismos derechos y obligaciones que, en esta Encomienda de Gestión, ostenta el _____.

Segunda.–La presente adhesión se realiza sobre la base de lo previsto en la cláusula octava de la Encomienda de Gestión del que trae causa el presente Protocolo.

Tercera.–El precio total máximo que ____(departamento, órgano, organismo o entidad)____ abonará a la FNMT-RCM por los servicios y demás actividades expresadas en la Encomienda de Gestión desde la entrada en vigor de esta adhesión, hasta el 31 de diciembre de _____, asciende a la cantidad de _____ euros (_____€), incluidos impuestos.

(Este precio se obtiene de prorratear, dado que la duración de la presente adhesión es inferior a un año, el precio total máximo anual, que asciende a _____ euros al año (_____€/año), incluidos impuestos).

La formación del precio actual y futuro, así como la fijación o actualización de precios por anualidades, en caso de existir prórrogas de la adhesión, y el resto de cuestiones económicas de las relaciones entre la FNMT-RCM y ____(departamento, órgano, organismo

cve: BOE-A-2009-21109

o entidad)____, se regirán por lo establecido en el anexo Económico del presente Protocolo y, subsidiaria y supletoriamente, por el anexo V de la Encomienda de Gestión (Precios y Plan de Implantación), hasta tanto no se aprueben las tarifas por parte de la Subsecretaría de Economía y Hacienda como órgano de adscripción de la FNMT-RCM (cláusula octava de la Encomienda de Gestión).

Existe consignación presupuestaria (n.º _____) para la contraprestación de los servicios efectuados por la FNMT-RCM. En caso de producirse prórrogas, el ____ (departamento, órgano, organismo o entidad)____ se compromete a realizar las correspondientes consignaciones presupuestarias.

Cuarta.–El establecimiento de Oficinas de Registro y Acreditación, por parte de ___ (departamento, órgano, organismo o entidad)___, se realizará de conformidad con lo dispuesto en la Encomienda de Gestión y sus anexos, debiendo, las partes, informarse recíprocamente de la creación de las mismas y de sus datos identificativos, a los efectos de la necesaria coordinación administrativa.

Quinta.–La información sobre las adhesiones producidas y las relaciones administrativas entre las administraciones que formen parte de la Encomienda de Gestión se regirán por lo establecido en la cláusula decimocuarta de la Encomienda de Gestión, por la legislación específica aplicable a la administración electrónica y por el resto de normativa que sea de aplicación. La FNMT-RCM informará, a través de su Consejo de Administración, al _____ de las adhesiones que se produzcan.

Sexta.–Quedan subsistentes y sin alteración alguna, las condiciones que integran la Encomienda de Gestión suscrita entre el _____ y la FNMT-RCM con fecha _____, a excepción de lo expresamente recogido en el presente instrumento.

Séptima.–Este Protocolo entrará en vigor el día de su firma y se extenderá hasta el 31 de diciembre de _____, aplicándose el régimen de prórrogas contemplado en la cláusula sexta de la Encomienda de Gestión del que trae causa esta adhesión.

Y, en prueba de conformidad, ambas partes suscriben el presente documento, por duplicado, en el lugar y fecha indicado en el encabezamiento.

FÁBRICA NACIONAL DE MONEDA Y TIMBRE -REAL CASA DE LA MONEDA, Fdo.: Ángel Esteban Paúl; ____(DEPARTAMENTO, ÓRGANO, ORGANISMO O ENTIDAD)____, Fdo.: _____

ANEXO DEL PROTOCOLO DE ADHESIÓN

COPIA DE LA ENCOMIENDA ENTRE _____ Y LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA, PARA LA PRESTACIÓN DE SERVICIOS TÉCNICOS Y DE SEGURIDAD APLICABLES A LA CERTIFICACIÓN Y FIRMA ELECTRÓNICA EN EL ÁMBITO DE LA ADMINISTRACIÓN ELECTRÓNICA.

ANEXO ECONÓMICO DEL PROTOCOLO DE ADHESIÓN

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.

cve: BOE-A-2009-21109

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 Colaboraciones del web de la FNMT.

cve: BOE-A-2009-21109