

Fundamentos jurídicos

Primero.—Resultan de aplicación para la resolución del expediente: el artículo 34 de la Constitución Española, que reconoce el derecho a fundar para fines de interés general. La Ley 50/2002, de 26 de diciembre, de Fundaciones. El Reglamento de Fundaciones de Competencia Estatal, aprobado por Real Decreto 1337/2005, de 11 de noviembre (BOE de 22 de noviembre). El Reglamento del Registro de Fundaciones de Competencia Estatal, aprobado por Real Decreto 384/1996, de 1 de marzo (BOE de 29 de marzo).

La Orden APA/1603/2005, de 17 de mayo (BOE de 2 de junio), en virtud de la cual se delegan en el Secretario General Técnico del Departamento las competencias relativas al Protectorado de Fundaciones que corresponden al Ministro.

Segundo.—La Ley 50/2002, de 26 de diciembre, de Fundaciones, establece que se inscribirán en el Registro, entre otros actos, la constitución de la fundación, la modificación o nueva redacción de los Estatutos, el nombramiento, revocación, sustitución, suspensión y cese, por cualquier causa, de los miembros del patronato y otros órganos creados por los Estatutos, y las delegaciones y apoderamientos generales concedidos por el patronato y la extinción de estos cargos.

Tercero.—Según las disposiciones transitorias cuarta de la Ley de Fundaciones y única del Reglamento del Registro de Fundaciones de competencia estatal, hasta tanto no entre en funcionamiento dicho Registro, subsistirán los actualmente existentes, por lo que procede la inscripción de la Fundación Para la Defensa de la Calidad de los Alimentos en el Registro de Fundaciones del Ministerio de Agricultura, Pesca y Alimentación.

Por todo lo cual, este Ministerio ha resuelto:

Primero.—Aceptar la documentación de la Fundación para la Defensa de la Calidad de los Alimentos, domiciliada en Madrid, cuyo fin de interés general es promover la defensa de la calidad de los alimentos en todos sus ámbitos, pasando este Departamento a ejercer el Protectorado sobre la misma.

Segundo.—Ordenar la inscripción de la denominada Fundación para la Defensa de la Calidad de los Alimentos, de ámbito estatal, con domicilio en Madrid, calle Lope de Vega, número 27, en el Registro de Fundaciones del Ministerio de Agricultura, Pesca y Alimentación, bajo el número 1/2007.

Tercero.—Registrar sus Estatutos.

Cuarto.—Registrar la composición del Patronato.

Quinto.—Notificar a los interesados a los efectos previstos en el artículo 58.2 de la Ley 30/1992, de 26 de noviembre de Régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, modificada por la Ley 4/1999, de 13 de enero.

Madrid, 17 de julio de 2007.—La Ministra de Agricultura, Pesca y Alimentación, P. D. (Orden APA/1603/2005, de 17 de mayo), el Secretario General Técnico del Ministerio de Agricultura, Pesca y Alimentación, Juan José Granado Martín.

MINISTERIO DE LA PRESIDENCIA

14778 *RESOLUCIÓN de 19 julio de 2007, de la Subsecretaría, por la que se dispone la publicación del Acuerdo de encomienda de gestión por el Ministerio de Medio Ambiente a la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, para la prestación de servicios de certificación de firma electrónica y otros servicios relativos a la administración electrónica.*

La Subsecretaría del Ministerio de Medio Ambiente y el Director General de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda han suscrito, con fecha 28 de junio de 2007, un Acuerdo de encomienda de gestión para la prestación de servicios de certificación de firma electrónica y otros servicios relativos a la Administración electrónica.

Para general conocimiento, se dispone su publicación como anejo a la presente Resolución.

Madrid, 19 de julio de 2007.—El Subsecretario de la Presidencia, Luis Herrero Juan.

ANEJO**Acuerdo por el que se instrumenta la encomienda de gestión por parte del Ministerio de Medio Ambiente a la Fábrica Nacional de la Moneda y Timbre-Real Casa de la Moneda, para la prestación de servicios de certificación de firma electrónica y otros servicios relativos a la Administración electrónica**

En Madrid, a 28 de junio de 2007.

REUNIDOS

De una parte, Concepción Toquero Plaza, en nombre y representación del Ministerio de Medio Ambiente en virtud de nombramiento efectuado por Real Decreto 718/2003, de 19 de abril (BOE de 20 de abril), actuando la competencia delegada por el titular del departamento mediante Orden MAM/224/2005, de 28 de enero (BOE núm. 35, correspondiente al 10 de febrero 2005) del Ministerio de Medio Ambiente.

Y de otra, Sixto Heredia Herrera, 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 aprobado por Real Decreto 1114/1999, de 25 de junio y de su nombramiento mediante el Real Decreto 802/2004, de 23 de abril (BOE de 24 de abril).

Reconociéndose ambas partes la capacidad legal necesaria para formalizar la presente Encomienda de Gestión,

EXPONEN

Primero.—La Ley 59/2003, de 19 de diciembre, de firma electrónica, establece las bases de regulación de la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación, tanto para el sector público como el privado. El artículo 4 de esta Ley, establece el empleo de la firma electrónica en el ámbito de las Administraciones Públicas, para que, con el objetivo básico de salvaguardar las garantías de cada procedimiento, se puedan establecer condiciones adicionales, como la imposición de fechas electrónicas sobre los documentos de la misma naturaleza, que integren un expediente administrativo.

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

Segundo.—El citado artículo 81 de la Ley 66/1997, de 30 de diciembre, faculta a la FNMT-RCM para prestar los servicios técnicos y administrativos necesarios para garantizar la seguridad, validez y eficacia en la emisión y recepción de comunicaciones y documentos a través de técnicas electrónicas, informáticas y telemáticas (EIT), entre otros, entre las personas físicas y jurídicas con la Administración General del Estado y con los organismos públicos vinculados o dependientes de ella. 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 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuando sea de aplicación.

Asimismo, el 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.

En relación con las actividades de identificación y registro, la FNMT-RCM, podrá celebrar convenios o acuerdos 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 a convenir con las entidades incluidas en su ámbito de aplicación, entre las que se encuentra el Ministerio de Medio Ambiente, los términos que deben regir la prestación de sus servicios en relación con las comunicaciones empleando técnicas y medios electrónicos, informáticos y telemáticos.

Como desarrollo de los artículos 38.9, 45 y 59.3 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, (según los apartados añadidos —al primer y tercer de los artículos citados por la Ley 24/2001, de 27 de diciembre—), se

aprobó el Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos, que establece una regulación específicamente dirigida al desarrollo e implantación de la administración electrónica dentro de la Administración del Estado; que 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, estableciendo los requisitos de autenticidad, integridad, disponibilidad y confidencialidad de los dispositivos y aplicaciones 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.—El artículo 2 del Estatuto de la FNMT-RCM, aprobado por Real Decreto 1114/1999, de 25 de junio, reconoce como fines de la Entidad 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 través de técnicas y medios electrónicos, informáticos y telemáticos (EIT) así como la expedición, fabricación y suministro de títulos o certificados de usuarios, de acuerdo con lo que establezcan las disposiciones legales correspondientes.

Quinto.—El Ministerio de Medio Ambiente tiene entre sus objetivos el agilizar y simplificar la tramitación de los procedimientos administrativos en las materias de su competencia. Una de las medidas encaminadas a ese objetivo ha de ser la progresiva introducción de la «firma electrónica avanzada», destinada a facilitar a los ciudadanos sus relaciones con los Servicios públicos, así como a posibilitar la tramitación telemática de los procedimientos. Para ello, se considera necesaria la suscripción de la presente Encomienda de Gestión.

Sexto.—Que, en virtud de las razones ahora expuestas, no resulta conveniente, por razones de seguridad y para facilitar a los ciudadanos las relaciones administrativas, que la colaboración entre el Ministerio de Medio Ambiente (Registros Telemáticos/otros servicios) y la FNMT-RCM (Entidad Pública adscrita al Ministerio de Economía y Hacienda) se instrumente a través de los diferentes tipos contractuales previstos en la legislación de contratos de las administraciones públicas, por tratarse de actuaciones entre instituciones públicas que ejercen sus respectivas competencias y facultades (registro telemático/firma electrónica). En este sentido, se considera que esta coactuación administrativa debe formalizarse —en esta fase— a través del instrumento jurídico de la encomienda de gestión, al margen de una relación estrictamente contractual. Todo ello, de acuerdo con lo dispuesto en las siguientes disposiciones: artículo 15, de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo común; artículo 3.1.1), del R.D. Legislativo 2/2000, de 16 de junio, por el que se aprueba el Texto Refundido de la Ley de Contratos de las Administraciones Públicas y, finalmente, artículo 3.4, último párrafo, del Real Decreto 1.114/1999, de 25 de junio, por el que se adapta la Fábrica Nacional de Moneda y Timbre a la ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, se aprueba su Estatuto y se acuerda su denominación como Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

Séptimo.—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 el apartado cinco del artículo 81 de la Ley 66/1997, de 30 diciembre, en redacción dada por la Disposición adicional vigésima sexta de la Ley 14/2000, de 29 de diciembre, de medidas fiscales, administrativas y del orden social, se procede a la formalización del presente Acuerdo 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 Ministerio de Medio Ambiente, de los servicios técnicos, administrativos y de seguridad necesarios 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 en el ámbito de actuación del Ministerio de Medio Ambiente con las condiciones técnico-administrativas que en las cláusulas siguientes se estipulan.

2. En particular, la FNMT-RCM prestará los servicios necesarios para que el Ministerio de Medio Ambiente pueda habilitar sistemas de registro telemático y otros instrumentos de relaciones administrativas, utilizando

técnicas o medios EIT, ofreciendo autenticidad, integridad, conservación y, en su caso, recepción de las comunicaciones mediante «firma electrónica avanzada» cuando los usuarios utilicen los certificados emitidos por la FNMT-RCM y, en concreto, prestará los servicios que al efecto se enumeran en el capítulo I del anexo I de esta Encomienda de Gestión.

También prestará a petición del Ministerio de Medio Ambiente cualquiera, o la totalidad, de los servicios avanzados que al efecto se enumeran en el capítulo II del mismo anexo I de esta Encomienda de Gestión.

Segunda. *Ámbito de aplicación.*—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 Sistema de Registro Telemático (ESTELA), el Sistema para la Gestión del Dominio Público Marítimo Terrestre (DUNA), el Sistema para la Gestión de los Recursos Administrativos y Responsabilidad Patrimonial (EDICTA), el Sistema para la Gestión de las Evaluaciones de Impacto Ambiental (Planes y Proyectos) (SABIA), el Sistema para la Gestión de las Figuras Parlamentarias (ÁGORA) y el Sistema de Registro de Aguas, todos ellos pertenecientes al Ministerio de Medio Ambiente en el marco de sus respectivas competencias. A tal efecto, el Ministerio de Medio Ambiente asume que los certificados (títulos de usuario) que expida la FNMT-RCM son universales y que por tanto servirán para las relaciones jurídicas que al efecto mantengan los usuarios con las diferentes Administraciones públicas y, en su caso, en el ámbito privado que admitan la utilización de estos certificados, en sus registros, procedimientos y trámites.

De igual forma los certificados que haya expedido o expida la FNMT-RCM, en el ámbito público de actuación, podrán ser utilizados por los usuarios en sus relaciones con el Sistema de Registro Telemático (ESTELA), el Sistema para la Gestión del Dominio Público Marítimo Terrestre (DUNA), el Sistema para la Gestión de los Recursos Administrativos y Responsabilidad Patrimonial (EDICTA), el Sistema para la Gestión de las Evaluaciones de Impacto Ambiental (Planes y Proyectos) (SABIA), el Sistema para la Gestión de las Figuras Parlamentarias (ÁGORA) y el Sistema de Registro de Aguas, todos ellos pertenecientes al Ministerio de Medio Ambiente cuando así lo admita el ordenamiento jurídico.

Tercera. *Obligaciones de las partes para la prestación efectiva de los servicios objeto de la encomienda de gestión.*—1. Para la prestación efectiva de los servicios objeto de la Encomienda de Gestión, la FNMT-RCM se compromete a:

Aportar la infraestructura técnica y organizativa que a tal efecto, se requiera.

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 Ministerio, para aplicaciones y sistemas del Ministerio de Medio Ambiente 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 Ministerio de Medio Ambiente la información necesaria para el buen funcionamiento de los sistemas.

Actualizar tecnológicamente los sistemas, de acuerdo con el estado de la técnica, así como de conformidad con los requisitos técnicos que, en su caso, pudiera establecerse por el Consejo Superior de Administración Electrónica o 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, a petición del Ministerio de Medio Ambiente.

Aportar la tecnología necesaria para que las obligaciones de la otra Parte firmante de la Encomienda de Gestión, puedan ser realizadas; en particular las aplicaciones necesarias para la implantación de la «firma electrónica avanzada» en la que se utilicen los certificados electrónicos expedidos por la FNMT-RCM, la constitución de las oficinas de acreditación y la tramitación de las solicitudes de emisión de certificados electrónicos.

Tener disponible para consulta del Ministerio de Medio Ambiente y de los usuarios una Declaración de Prácticas de Certificación (DPC), que contendrá, al menos, las especificaciones establecidas en el artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica. Tal DPC, estará disponible en la dirección electrónica (URL) siguiente:

http://www.cert.fnmt.es/content/pages_std/docs/00034_cit_obtain_cert_0000000000%20-%20Declaracion%20de%20Practicas%20de%20Certificacion.pdf

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 serán comunicadas a los usuarios a través de avisos en su dirección electrónica.

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 produc-

tos, los cuáles contarán con la debida protección contra alteraciones, así como con los niveles de seguridad técnica y criptográfica idóneos dependiendo de los procedimientos donde se utilicen, la comprobación de la identidad del titular del certificado y, en su caso, y exclusivamente frente a la parte o entidad a través de la cual se ha identificado y registrado al titular del certificado, los atributos pertinentes, así como, en general, los que resulten de aplicación de conformidad con la normativa comunitaria o nacional correspondiente.

La FNMT-RCM comunicará al Ministerio de Medio Ambiente, con al menos un mes de anterioridad a su aplicación, las modificaciones que haya de realizar en la prestación de sus servicios. Si estas modificaciones fueran sustanciales y no se llegara a un acuerdo sobre el alcance o las repercusiones de las mismas, el Ministerio de Medio Ambiente podrá resolver la presente Encomienda de Gestión.

Igualmente, la FNMT-RCM deberá comunicar al Ministerio de Medio Ambiente, con al menos un mes de anticipación, el cese de la prestación de los servicios y actuaciones previstos en esta Encomienda de Gestión, lo que dará lugar, al cumplirse tal fecha, a que quede sin efecto, sin perjuicio de las indemnizaciones que por tal causa pudieran derivarse.

2. Por su parte, el Ministerio de Medio Ambiente se compromete a:

Emitir, cuando proceda, el recibo de presentación, en su caso 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.

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, en calidad de Oficina de Acreditación la FNMT-RCM.

Aceptar la plena validez de los certificados electrónicos expedidos por la FNMT-RCM para la presentación de documentos a través de Internet y, en general, para la tramitación a través de técnicas E.I.T., de las solicitudes y demás escritos o manifestaciones que realicen los usuarios en el curso de aquellos procedimientos en los que el Ministerio haya acordado la admisibilidad de su tramitación mediante estas técnicas E.I.T.

Sin perjuicio de lo anterior, el Ministerio de Medio Ambiente aceptará los certificados electrónicos expedidos por otros prestadores de servicios de certificación, siempre que por los mismos se cumplan los requisitos normativos y técnicos de aplicación, de acuerdo con el principio de «neutralidad tecnológica».

Ajustar sus actuaciones a las previsiones, normativas y técnicas que sean de aplicación en materia de E.I.T., en general y de «firma electrónica avanzada» en particular, coordinándose a tal fin, cuando ello sea necesario, con la FNMT-RCM.

Realizar las actividades de identificación previa a la obtención del certificado electrónico de la FNMT-RCM y, en su caso, las de comprobación de la suficiencia de los atributos correspondientes.

A tal efecto, determinará las Unidades Administrativas del Departamento que realizarán las funciones de acreditación, que deberán contar con los medios informáticos precisos para conectarse telemáticamente con la FNMT-RCM. La acreditación e identificación de los solicitantes de los certificados de esas Unidades exigirá la comprobación de su identidad y de su voluntad de que les sea expedido un certificado electrónico, y se verificará de conformidad y con pleno respeto a lo dispuesto en la normativa aplicable.

Antes del inicio de la prestación del servicio, el Ministerio comunicará a la FNMT-RCM la Unidad que, en sus servicios centrales, realizará estas funciones de oficina de acreditación, con su denominación, dirección postal y dirección IP. La misma tendrá el carácter de «oficina central de acreditación del Ministerio de Medio Ambiente».

Con posterioridad, comunicará también aquellas otras Unidades del Departamento, que realizarán estas funciones. El Ministerio comunicará también cualquier modificación o alteración de los datos de cada una de ellas.

Las solicitudes de emisión y revocación y/o suspensión, en su caso, de certificados se ajustarán a los modelos recogidos en el Anexo III.

Cuarta. *Precio y condiciones de pago.*—La FNMT-RCM percibirá, por los servicios EIT prestados a los Sistemas de Registro Telemático (ESTELA), para la Gestión del Dominio Público Marítimo Terrestre (DUNA), para la Gestión de los Recursos Administrativos y Responsabilidad Patrimonial (EDICTA), para la Gestión de las Evaluaciones de Impacto Ambiental (Planes y Proyectos) (SABIA), para la Gestión de las Figuras Parlamentarias (ÁGORA) y de Registro de Aguas todos ellos pertenecientes al Ministerio de Medio Ambiente la cantidad de cuatrocientos noventa y un mil treinta y cuatro euros al año, (491.034,00 € al año), IVA incluido, cantidad que se incrementará 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 del contrato. La aplicación de este precio se establece en los Capítulos I y II del Anexo IV.

Si hubiera petición expresa de servicios avanzados hecha por el Ministerio de Medio Ambiente la cantidad anterior quedaría incrementada por el importe correspondiente que de la aplicación de las tablas del Capítulo II del Anexo IV de Precios y Plan de Implantación de la presente Encomienda de Gestión se dedujera, lo que requerirá la fiscalización de la oportuna addenda.

La FNMT-RCM, podrá realizar certificaciones parciales conformadas por el Ministerio de Medio Ambiente, mediante el prorrateo de la cantidad anual a abonar por el Ministerio de Medio Ambiente, pudiendo, además, liquidar en tales facturas aquellos servicios adicionales solicitados. El abono de las facturas se realizará mediante transferencia bancaria a la cuenta de la FNMT-RCM.

En caso de que se produzcan prórrogas de la presente Encomienda de Gestión, se registrará en las mismas condiciones de la actual.

Quinta. *Régimen de prestación de los servicios.*—La prestación de los servicios EIT a que se refiere la cláusula primera, se realizará atendiendo a lo establecido en el Anexo I.

A tal efecto, ambas partes se comprometen a asumir las obligaciones necesarias a este fin. Igualmente, el Ministerio de Medio Ambiente se obliga a velar frente a los usuarios por el cumplimiento de las obligaciones que le correspondan en cuanto a la identificación y/o registro de usuarios, y a la recepción y tramitación de solicitudes de expedición, revocación y, en su caso, suspensión de certificados electrónicos.

Sexta. *Plazo de duración.*—La Encomienda de Gestión entrará en vigor el día de su firma y se extenderá durante dos años a contar desde la fecha de su firma. Se producirá la prórroga automática del mismo, si no mediara denuncia de ninguna de las partes con un mes de antelación a su vencimiento inicial o al de cualquiera de sus prórrogas.

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

Séptima. *Responsabilidad.*—La FNMT-RCM como prestador de los servicios citados en la cláusula primera, y el Ministerio de Medio Ambiente como usuario público del sistema y participe en el procedimiento de identificación y registro de los usuarios, 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 de Gestión.

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

Octava. *Resolución.*—Sin perjuicio de lo dispuesto en la cláusula Tercera, la Encomienda de Gestión podrá resolverse por parte del Ministerio de Medio Ambiente 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 FNMT-RCM podrá instar la resolución de la Encomienda de Gestión por falta de pago del precio convenido o por incumplimiento grave de las obligaciones que corresponden al Ministerio de Medio Ambiente y que figuran en las cláusulas de ésta Encomienda de Gestión.

Novena. *Protección de datos.*—El régimen de protección de datos de carácter personal derivados de ésta Encomienda de Gestión y de la actuación conjunta de ambas partes será el previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en su normativa de desarrollo. Los ficheros serán de titularidad pública y su creación, modificación o supresión se realizará por disposición general publicada en el Boletín Oficial del Estado, (Para la FNMT-RCM: Orden del Ministerio de Economía de 11 de diciembre de 2001, BOE de 28 de diciembre).

Décima. *Derecho aplicable.*—La prestación de los servicios de certificación contemplados en la presente Encomienda de Gestión 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, así como a las disposiciones que sean de aplicación y en su caso, cuantas disposiciones se dictaren, durante la vigencia de la Encomienda de Gestión y que afectaren al objeto del mismo.

Undécima. *Régimen jurídico y de resolución de conflictos.*—Esta Encomienda de Gestión es el instrumento jurídico por el que se regula la encomienda de gestión descrita a la FNMT-RCM, de acuerdo con el artículo 3.1.1), del Texto Refundido de la Ley de Contratos de las Administraciones Públicas.

Las cuestiones litigiosas que puedan surgir en la interpretación, modificación, efectos o resolución de esta Encomienda de Gestión, serán

resultas de mutuo acuerdo y, en su caso y una vez agotada la vía administrativa, por la Jurisdicción Contencioso-Administrativa, de conformidad con su ley reguladora.

Duodécima. *Inicio de la prestación.*—El presente Convenio surtirá efectos desde el momento de su firma, previa aprobación o siempre que sea ratificado, según proceda, por el Consejo de Administración de la FNMT-RCM, iniciándose la prestación del servicio el día de su firma. En caso de ratificación, la FNMT-RCM, comunicará al Ministerio de Medio Ambiente tal hecho para su debida constancia.

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.

ANEXO I

Servicios a prestar

CAPÍTULO I

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

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

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

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

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

Generación y gestión de claves

Generación y gestión de las claves.

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

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

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

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

Archivo de las claves públicas.

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

Exclusividad de las claves.

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

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

Renovación de claves.

La FNMT-RCM identifica una relación uno a uno entre la clave pública de un usuario y su certificado de clave pública, no previéndose utilizar

distintos certificados para una misma clave. Es por esto que las claves se renovarán con los certificados cuando dicha renovación esté contemplada en la normativa específica aplicable.

Registro de usuarios

Registro de usuarios.

El registro de usuarios es el procedimiento a través del cual se identifica al solicitante de un certificado electrónico, se comprueba su personalidad y se constata su efectiva voluntad de que le sea emitido el «Certificado Básico» o «Título de Usuario» por la FNMT-RCM.

Este registro podrá ser realizado por la propia FNMT-RCM o cualquier otra Administración pública y, en su caso, por las demás personas, entidades o corporaciones habilitadas a tal efecto por las normas que resulten de aplicación. En todo caso el registro se llevará a cabo según lo dispuesto por la FNMT-RCM, al objeto de que este registro se realice de acuerdo con lo establecido por la normativa específica aplicable y homogéneo en todos los casos. De igual manera será la FNMT-RCM, quien defina y aporte los medios necesarios para la realización de este registro.

En el caso de que el registro lo realizara una Administración Pública, distinta de la FNMT-RCM, la persona que se encargue de la actividad de registro ha de ser personal al servicio de la Administración Pública. En estos casos la FNMT-RCM, dará soporte a la implantación de las distintas oficinas de registro que se establezcan cuando fuere necesario, en los siguientes términos:

- a) Aportación de la aplicación informática de registro.
- b) Aportación de la documentación relativa a la instalación y manejo de la aplicación, así como toda aquella referente a los procedimientos y normas sobre el registro.
- c) Registro y formación de los encargados del registro, lo que supone la emisión de un certificado emitido por la FNMT-RCM para cada encargado del registro, que permita garantizar la seguridad de las comunicaciones con la FNMT-RCM, incluyendo la firma electrónica de las solicitudes de registro.

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

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

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

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 transcrito en el anexo III de la presente Encomienda de Gestión 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.

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 Ministerio de Medio Ambiente como encargado del registro de usuarios responden que esta dirección esté vinculada con el titular del certificado.

Obtención del «Certificado Básico» o «Título de usuario».

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

Emisión, revocación y archivo de certificados de clave pública

Emisión de los certificados.

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

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

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

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

La FNMT-RCM garantiza para un certificado emitido:

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

Aceptación de certificados.

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

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

El Ministerio de Medio Ambiente garantizará que, al solicitar un certificado electrónico, su titular acepta que:

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

El Ministerio de Medio Ambiente garantizará que, al solicitar un certificado electrónico, su titular asume las siguientes obligaciones sobre su clave privada:

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

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

Revocación y suspensión de certificados electrónicos.

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

- Solicitud de revocación del usuario, por la persona física o jurídica representada por éste o por un tercero autorizado.
- Resolución judicial o administrativa que lo ordene.
- Fallecimiento o extinción de la personalidad del usuario o incapacidad sobrevenida.

- Finalización del plazo de vigencia del certificado.
- Pérdida o inutilización por daños en el soporte del certificado.
- Utilización indebida por un tercero.
- Inexactitudes graves en los datos aportados por el usuario para la obtención del certificado.
- Cualquier otra prevista en la normativa vigente.

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

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

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

La extinción de la condición de usuario público se registrará por lo dispuesto en la presente Encomienda de Gestión 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 Ministerio de Medio Ambiente 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 con disponibilidad de 24 horas durante los 365 días del año para la recepción, y en su caso tramitación de solicitudes de revocación de certificados vigentes siguiendo un protocolo de identificación telefónica.

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 Ministerio de Medio Ambiente 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 directorio actualizado 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 directorio actualizado 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 tal forma que:

Para los certificados revocados, la actualización sea hecha en el momento de producir efectos la revocación.

La actualización en el directorio seguro de las listas de revocación se realizará de forma continuada.

La consulta de este directorio se realizará en línea, por acceso directo del usuario. Este servicio permite la disponibilidad continua y la integridad de la información almacenada en el directorio.

Tanto los certificados como las listas de revocación serán firmadas con la clave privada de firma de la FNMT-RCM.

b) **Publicación en directorios externos.**—La FNMT-RCM podrá publicar externamente, en directorios públicos ofrecidos por otras entidades u Organismos, mediante replicación periódica o en línea, tanto certificados como listas de certificados revocados. Estas listas, al igual que las publicadas internamente, irán firmadas con la clave privada de firma de la FNMT-RCM.

Frecuencia de la publicación en directorios externos.

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

Control de acceso.

En la publicación directa por parte de la FNMT-RCM, el acceso al directorio se realizará en función del tipo de usuario, de forma que:

a) Los órganos de la Administración General del Estado, así como los organismos públicos vinculados o dependientes de ella, tendrán acceso a todos los certificados sin ninguna restricción en cuanto a la información contenida en el directorio. El acceso se realizará con autenticación previa. Este acceso estará restringido a sólo lectura y búsqueda, pudiendo utilizar como clave de búsqueda cualquier información contenida en una entrada de un usuario.

b) Las Comunidades Autónomas, las Entidades Locales, así como los Organismos Públicos vinculados o dependientes de ellas, tendrán igualmente acceso a todos los certificados sin ninguna restricción en cuanto a la información contenida en el directorio. El acceso se realizará con autenticación previa. Este acceso estará restringido a sólo lectura y búsqueda, pudiendo utilizar como clave de búsqueda cualquier información contenida en una entrada de un usuario.

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

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

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

Registro de eventos significativos

Tipos de eventos registrados.

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

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

Frecuencia y periodo de archivo de un registro de un evento.

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

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

Archivo de un registro de eventos.

La FNMT-RCM realizará una grabación segura y constante de todos los eventos relevantes desde el punto de vista de la seguridad y auditoría (operaciones realizadas) que vaya realizando, con el fin de reducir los

riesgos de vulneración, mitigar cualquier daño que se produjera por una violación de la seguridad y detectar posibles ataques.

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

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

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

Datos relevantes que serán registrados.

Serán registrados los siguientes eventos relevantes:

a) La emisión y revocación y demás eventos relevantes relacionados con los certificados.

b) Todas las operaciones referentes a la firma de los certificados por la FNMT-RCM.

c) Las firmas y demás eventos relevantes relacionados con las Listas de Certificados Revocados.

d) Todas las operaciones de acceso al archivo de certificados.

e) Eventos relevantes de la generación de claves.

f) Todas las operaciones del servicio de archivo de claves y del acceso al archivo de claves propias expiradas.

g) Todas las operaciones relacionadas con la recuperación de claves.

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

Protección de un registro de actividad.

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

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

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

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

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

CAPÍTULO II

Servicio de Notificaciones Electrónicas

La Fábrica Nacional de Moneda y Timbre como prestador de servicios técnico de apoyo a la notificación electrónica dispone de un servicio regulado por la siguiente legislación:

Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social (art. 81).

Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos (que modificó los Reales Decretos 263/1996, y 772/1991).

Orden PRE/1551/2003, de 10 de junio, por la que se desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

El servicio será conforme con los criterios recogidos en dicha legislación así como en el marco de los criterios de seguridad, normalización y conservación a los que se refiere el Real Decreto 263/1996, de 16 de febrero, a los requisitos de autenticidad, integridad, disponibilidad y confidencialidad de los dispositivos y aplicaciones de registro y notificación, así como los protocolos y criterios técnicos a los que deben sujetarse.

Dichos criterios de seguridad, normalización y conservación han sido objeto de informe favorable del Consejo Superior de Informática y para el impulso de la Administración Electrónica.

Descripción del servicio.

El servicio de notificaciones es un servicio de web mail con acuse de recibo, cuyo acceso se realizará mediante identificación por procedimien-

tos de firma electrónica. El servicio provee a los notificadotes de un sistema de no repudio en destino.

Las notificaciones practicadas serán selladas y custodiadas electrónicamente. Las especificaciones del servicio de sellado de tiempo son las que se recogen en este mismo anexo y están basadas en las especificaciones del estándar RFC3161 –«Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)». Las especificaciones del servicio de custodia son las que se recogen en este mismo anexo.

El servicio de notificación electrónica se podrá complementar adicionalmente con un servicio de notificación tradicional para completar una solución de correo mixto.

Acceso al servicio.

El servicio será accesible a través de Internet por el cliente siempre que esté dado de alta en el sistema y esté en posesión de un certificado de verificación de firma electrónica emitido por la Fábrica Nacional de Moneda y Timbre, válido y no revocado así como de su correspondiente clave privada, lo que le permitirá identificarse mediante el uso de firma electrónica.

Las especificaciones de los certificados de verificación de firma electrónica son las que se recogen en el Capítulo I de este mismo anexo y están basadas en un certificado reconocido según la Recomendación UIT-T X.509, de 31 de Marzo de 2000 o superiores (ISO/IEC 9594-8 de 2001) de acuerdo con lo previsto en la legislación de firma electrónica.

El acceso a los servicios contará con las debidas medidas de confidencialidad de modo que solo los clientes sean capaces de practicar notificaciones a las direcciones electrónicas. Dichas medidas de confidencialidad podrán al menos cifrar la información mediante el uso de alguno de los protocolos de comunicación estándares SSL, TLS, AES o similares, con una clave simétrica de intercambio de datos de al menos 128 bits mediante el uso de los algoritmos de cifrado más habituales.

La solicitud de acceso a los servicios se realizará por medios electrónicos y mediante firma electrónica. La FNMT guardará la firma generada así como la prueba sellada de tiempo que permita confirmar la identidad del cliente así como su solicitud y el momento de la realización. De igual manera, la solicitud de baja en el servicio se realizará mediante los mismos procedimientos de firma y sellado de tiempo.

La FNMT guardará prueba firmada y con sello de tiempo de cada notificación practicada y pondrá dicha información a disposición del notificador, del notificado así como de las autoridades competentes de acuerdo a la legislación aplicable.

La FNMT, como prestador del servicio y a los únicos efectos de dar fe de lo acontecido, tendrá un acceso limitado a las notificaciones practicadas. Dicho acceso limitado no permitirá en ningún caso, a ningún empleado o colaborador externo de la FNMT, a título individual, el acceso a las notificaciones. El procedimiento de acceso se regulará en los procedimientos de seguridad internos y estará basado en un sistema de concurrencia de al menos 4 personas, con carácter ejecutivo dentro de la FNMT. Todo acceso será anotado en un libro de control de accesos donde se hará constar al menos, la fecha, la hora, el motivo justificado del acceso así como los intervinientes y su cualificación.

Práctica de notificaciones.

Una Entidad Cliente podrá solicitar el servicio de Notificación para enviar a los ciudadanos una información determinada, la cual quedará depositada en la dirección electrónica única (DEU) de estos. Esta notificación puede ser el envío de un fichero, de un texto o ambos (fichero y texto).

A continuación se presenta el flujo de datos correspondiente a esta operación:

El cliente solicita el servicio de Notificación enviando el mensaje *requestNotification*

El servicio de Notificación realiza la autenticación y autorización de la solicitud.

Gestor Transaccional almacena el documento en la base de datos, quedando éste bajo custodia hasta la fecha de expiración de la custodia.

Gestor Transaccional genera y envía al cliente el mensaje de respuesta *returnNotification*.

Gestor Transaccional genera y envía el mensaje de correo electrónico con la notificación. Adicionalmente y de manera opcional puede mandar un mensaje a diversos destinatarios informando de que la notificación se ha llevado a cabo.

En caso que se informe el teléfono móvil de los ciudadanos y el flag de envío SMS esté marcado, a la vez de enviar el e-mail informando de la notificación, se enviará un SMS al teléfono móvil con la misma información (sin firmar).

El envío del e-mail informando de la recepción de la notificación, puede ser parametrizable para que se puedan llevar a cabo en periodos de baja actividad del Sistema (por ejemplo por la noche). En este caso, se

dejará parametrizable la hora de inicio y fin del proceso de envío de estos e-mails con el aviso de las notificaciones.

También cabe la posibilidad de que este proceso se fuerce cuando se procese el servicio, pasando automáticamente al servidor de correo un lote con los destinatarios.

Descripción de las notificaciones.

Contenido del mensaje de petición de notificación *requestNotification*:

Identificador de Contrato.

Tipo de operación.

Nombre del documento (en caso que contenga documento).

Documento.

Lista con los destinatarios de e-recibo (e-mail).

Texto para la notificación (cuerpo del mensaje).

Indicador de número de días para considerar rechazada la notificación.

Flag para pedir acuse de recibo de notificación accedida.

Flag para envío SMS.

Lista con los NIF's de los ciudadanos a notificar.

E-mail's de los ciudadanos a notificar.

Teléfono móvil de los ciudadanos a notificar.

Certificado digital del cliente.

Firma digital del cliente sobre el mensaje.

Contenido del mensaje de respuesta *returnNotification*:

Información sobre el resultado de la petición y posibles causas del problema si éste aparece.

Firma digital del servicio de notificación de la FNMT-RCM.

Prestaciones adicionales del sistema.

Los organismos o empresas pueden enviar los mensajes en batch, de tal modo que no tienen que teclearlos, y en un formato que al menos debe tener: NIF destinatario, mensaje firmado en PKCS#7, id organismo o empresa enviante.

Internamente los mensajes se guardan cifrados incluso para el administrador de la base de datos mediante un sistema de criptografía simétrica (3DES).

El concepto de dirección electrónica no es el de cuenta de correo, sino que el servicio estará accesible en la URL («<http://www.cert.fnmt.es/clase2/notificacionesmain.htm>») a través de la opción «Acceso a su buzón de notificaciones».

La autenticación de los destinatarios que acceden a coger el correo sea mediante SSL con certificado usuario de la FNMT-RCM.

Es parametrizable. Automáticamente a los x días de no recepción se pueden imprimir los mensajes que no se hayan leído.

El sistema de fechado digital que se emplea es el de la FNMT-RCM-CERES.

Dispone de un sistema de aviso mediante ficheros o consulta para que el organismo que envía pueda saber el estado de su envío.

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.

Servicio de Custodia de documentos electrónicos.

La Fábrica Nacional de Moneda y Timbre como prestador de servicios de custodia de documentos electrónicos dispone de un servicio regulado por la siguiente legislación:

Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico

El servicio será conforme con los criterios recogidos en dicha legislación así como en el marco de los criterios de seguridad, normalización y conservación a los que se refiere el Real Decreto 263/1996, de 16 de febrero, a los requisitos de autenticidad, integridad, disponibilidad y confidencialidad de los dispositivos y aplicaciones de registro y notificación, así como los protocolos y criterios técnicos a los que deben sujetarse.

Dichos criterios de seguridad, normalización y conservación han sido objeto de informe favorable del Consejo Superior de Administración Electrónica.

La custodia de las transacciones y documentos electrónicos es un factor importante en el desarrollo de las relaciones electrónicas entre partes ya que permiten dotar a las mismas de seguridad jurídica preventiva preconstituyendo tanto una prueba testimonial como documental de la realización de la transacción entre las partes.

Este sistema de custodia facilita la captura de cualquier transacción electrónica que se haya realizado en Internet proporcionando a la misma seguridad jurídica, esto es, garantizando que ninguna de las partes puede alterar a futuro el contenido de lo acordado.

Asimismo, como usuario informático en muchos momentos se hace necesario disponer de un almacenamiento de ficheros, formularios etc. que quede fuera de los avatares a los que nuestro propio PC pueda verse sometido, esto es, contar con un archivo seguro y remoto.

Descripción del servicio.

El servicio de custodia de documentos electrónicos es un servicio, cuyo acceso se realizará mediante identificación por procedimientos de firma electrónica. El servicio provee a los clientes de un sistema de depósito de documentos electrónicos realizado por un tercero capaz de dar fe de la existencia y contenido del documento.

Acceso al servicio.

El servicio será accesible a través de Internet por el cliente siempre que esté dado de alta en el sistema y esté en posesión de un certificado de verificación de firma electrónica emitido por la Fábrica Nacional de Moneda y Timbre, válido y no revocado así como de su correspondiente clave privada, lo que le permitirá identificarse mediante el uso de firma electrónica.

Las especificaciones de los certificados de verificación de firma electrónica son las que se recogen en el Capítulo I de este mismo anexo y están basadas en un certificado reconocido según la recomendación UIT-T X.509, de 31 de marzo de 2000 o superiores (ISO/IEC 9594-8 de 2001) de acuerdo con lo previsto en la legislación de firma electrónica.

El acceso a los servicios contará con las debidas medidas de confidencialidad de modo que solo los clientes o quienes estos designen sean capaces de almacenar documentos electrónicos y tener acceso a ellos. Dichas medidas de confidencialidad podrán al menos cifrar la información mediante el uso de alguno de los protocolos de comunicación estándares SSL, TLS, AES o similares, con una clave simétrica de intercambio de datos de al menos 128 bits mediante el uso de los algoritmos de cifrado más habituales.

La solicitud de acceso a los servicios se realizará por medios electrónicos y mediante firma electrónica. La FNMT guardará la firma generada así como la prueba sellada de tiempo que permita confirmar la identidad del cliente así como su solicitud y el momento de la realización. De igual manera, la solicitud de baja en el servicio se realizará mediante los mismos procedimientos de firma y sellado de tiempo.

La FNMT custodiará el documento durante el tiempo acordado y dará prueba firmada de su existencia al depositante, a quien el depositante designe así como de las autoridades competentes de acuerdo a la legislación aplicable.

La FNMT, como prestador del servicio y a los únicos efectos de dar fe de lo acontecido, tendrá un acceso limitado a los documentos. Dicho acceso limitado no permitirá en ningún caso, a ningún empleado o colaborador externo de la FNMT, a título individual, el acceso a los documentos. El procedimiento de acceso se regulará en los procedimientos de seguridad internos y estará basado en un sistema de concurrencia de al menos 4 personas, con carácter ejecutivo dentro de la FNMT. Todo acceso será anotado en un libro de control de accesos donde se hará constar al menos, la fecha, la hora, el motivo justificado del acceso así como los intervinientes y su cualificación.

Depósito de documentos.

Una Entidad Cliente podrá solicitar el depósito de documentos electrónicos que se realizará en las instalaciones al efecto de la FNMT. Dicho servicio podrá ser limitado en función del volumen de los documentos a depositar.

A continuación se presenta el flujo de datos correspondiente a esta operación.

El cliente solicita la custodia enviando el mensaje requestTimeStampWithCustody

El servicio de Custodia realiza la autenticación y autorización de la solicitud.

El Gestor Transaccional realiza una petición de fechado digital al módulo Servidor de Fechado Digital.

El Servidor de Fechado Digital genera un fechado digital estándar y lo almacena en la base de datos.

El Servidor de Fechado Digital envía el fechado al Gestor Transaccional. Gestor Transaccional almacena el documento en la base de datos, quedando éste bajo custodia hasta la fecha de expiración de la custodia.

Gestor Transaccional genera y envía al cliente el mensaje de respuesta returnTimeStampWithCustody.

Gestor Transaccional genera y envía el mensaje de correo electrónico informativo sobre la operación realizada a todos los destinatarios especificados en el mensaje de solicitud (opcional).

Cuando se envía una petición de fechado al servidor de TSA, es obligatorio enviar el hash del documento. En el caso de solicitud de fechado, el servidor no dispone del documento, es por eso que el hash lo tiene generar el Cliente, pero en el caso de custodia, el Cliente envía el documento a la aplicación por lo tanto se puede generar el hash en los servidores, quitando de esta forma carga de proceso a la aplicación Cliente.

Es por eso que para el caso de custodia, el mensaje que sale del API Cliente no incluye el hash del documento y será la aplicación de Custodia quien al recibir el mensaje generará el hash utilizando el documento contenido en el mensaje y construirá el mensaje completo para el servidor de fechado.

De igual forma que en el punto anterior, este fechado digital se tendrá que guardar automáticamente en una ruta de la máquina definida para tal efecto cambiando el nombre del token de manera adecuada para que sea fácil reconocerlo y poderlo asociar al documento original (nombre_del_documento_origen.fecha_de_la_peticion.token.der).

Descripción de los mensajes.

Contenido del mensaje de petición de custodia de un documento requestTimeStampWithCustody:

Identificador de Contrato.

Tipo de operación.

Nombre del documento.

Huella digital del documento (hash del documento) calculado en el Cliente.

Campo libre.

Documento cifrado con la clave simétrica.

Clave simétrica cifrada con la clave pública.

Lista con los destinatarios de e-recibo.

Tipo de identificador para cada destinatario.

Identificación para cada componente de la lista con los destinatarios de e-recibo.

Certificado digital del cliente.

Firma digital del cliente sobre el mensaje.

Contenido del mensaje de respuesta returnTimeStampWithCustody:

Información sobre el resultado de la petición y posibles causas del problema si éste aparece.

Fechado digital

Referencia de custodia.

Firma digital del mensaje.

Recuperación de un documento en custodia.

Un documento bajo custodia podrá ser consultado o recuperado posteriormente por parte del cliente que lo entregó en custodia.

El cliente solicita la recuperación de un documento en custodia enviando el mensaje getDocument.

El servicio de custodia realiza la autenticación y autorización de la solicitud.

El Gestor Transaccional obtiene de la base de datos el fechado digital y el documento custodiado

El Gestor Transaccional verifica si el fechado digital recibido en el mensaje de solicitud getDocument corresponde al documento y el fechado digital recuperado de la base de datos de Custodia. Esta verificación consta de las siguientes fases:

Verificación la firma digital del fechado digital recibido.

Validación del fechado digital con el documento recuperado de la base de datos.

Validación que la fecha de expiración de la custodia no haya sido superada.

En caso de una verificación correcta el Gestor Transaccional descifra el documento custodiado.

Gestor Transaccional genera y envía al cliente el mensaje de respuesta returnDocument.

Descripción de los mensajes.

Contenido del mensaje de petición de recuperación de documento bajo custodia getDocument:

Identificador de Contrato.
Tipo de operación.
Fechado digital.
Certificado digital del cliente.
Firma digital del cliente.

Contenido del mensaje de respuesta de petición de recuperación del documento returnDocument:

Información sobre el resultado de la petición y posibles causas del problema si éste aparece.

Nombre del documento.
El documento bajo custodia cifrado con la clave simétrica.
Clave simétrica cifrada con la clave pública del cliente.
Fechado digital.
Firma digital del mensaje.

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.

Servicio de dirección electrónica.

La Fábrica Nacional de Moneda y Timbre como de dirección electrónica pondrá a disposición de todo usuario que lo solicite una dirección en Internet que permitirá a su titular recibir las notificaciones reguladas por la siguiente legislación.

Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social.

Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

Orden PRE/1551/2003, de 10 de junio, por la que se desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

El servicio será conforme con los criterios recogidos en dicha legislación así como en el marco de los criterios de seguridad, normalización y conservación a los que se refiere el Real Decreto 263/1996, de 16 de febrero, a los requisitos de autenticidad, integridad, disponibilidad y confidencialidad de los dispositivos y aplicaciones de registro y notificación, así como los protocolos y criterios técnicos a los que deben sujetarse.

Dichos criterios de seguridad, normalización y conservación han sido objeto de informe favorable del Consejo Superior de Informática y para el impulso de la Administración Electrónica.

Acceso a la dirección electrónica.

La dirección electrónica será accesible a través de Internet por el titular siempre que esté en posesión de un certificado de firma electrónica emitido por la Fábrica Nacional de Moneda y Timbre, válido y no revocado así como de su correspondiente clave privada, lo que le permitirá identificarse mediante el uso de firma electrónica.

Las especificaciones de los certificados de verificación de firma electrónica son las que se recogen en el Capítulo I de este mismo anexo y están basadas en un certificado reconocido según la Recomendación

UIT-T X.509, de 31 de Marzo de 2000 o superiores (ISO/IEC 9594-8 de 2001) de acuerdo con lo previsto en la legislación de firma electrónica.

El acceso a los servicios contará con las debidas medidas de confidencialidad de modo que solo el titular sea capaz de ver la información disponible en su dirección electrónica. Dichas medidas de confidencialidad podrán al menos cifrar la información mediante el uso de alguno de los protocolos de comunicación estándares SSL, TLS, AES o similares, con una clave simétrica de intercambio de datos de al menos 128 bits mediante el uso de los algoritmos de cifrado mas habituales.

La solicitud de acceso a los servicios se realizará por medios electrónicos y mediante firma electrónica. La FNMT guardará la firma generada así como la prueba sellada de tiempo que permita confirmar la identidad del solicitante así como su solicitud y el momento de la realización. De igual manera, la solicitud de baja en el servicio se realizará mediante los mismos procedimientos de firma y sellado de tiempo.

Las especificaciones del servicio de sellado de tiempo son las que se recogen en este mismo anexo y están basadas en las especificaciones del estándar RFC3161 –«Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)».

La FNMT guardará prueba firmada y con sello de tiempo de cada acceso realizado a la dirección electrónica y pondrá dicha información a disposición de su titular así como a disposición de las entidades notificadoras así como de las autoridades competentes de acuerdo a la legislación aplicable.

La FNMT, como prestador del servicio y a los únicos efectos de dar fe de lo acontecido, tendrá un acceso limitado a los contenidos de la dirección electrónica. Dicho acceso limitado no permitirá en ningún caso, a ningún empleado o colaborador externo de la FNMT, a título individual, el acceso a la dirección electrónica. El procedimiento de acceso a la dirección electrónica se regulará en los procedimientos de seguridad internos y estará basado en un sistema de concurrencia de al menos 4 personas, con carácter ejecutivo dentro de la FNMT. Todo acceso será anotado en un libro de control de accesos donde se hará constar al menos, la fecha, la hora, el motivo justificado del acceso así como los intervinientes y su cualificación.

El titular podrá acceder a su dirección electrónica al menos, mediante el uso de los navegadores web que cumpla la especificación W3C HTML4.01 o superior u otros medios generalmente aceptados. En el caso de que fuese necesaria la instalación de algún programa de ordenador específico, distinto a los mencionados, para el acceso a la dirección electrónica, éste será suministrado gratuitamente por la FNMT mediante descarga desde su dirección en Internet.

Contenido de la dirección electrónica.

La FNMT pondrá las medidas electrónicas, informáticas y telemáticas que permitan salvaguardar el contenido de la dirección electrónica, así como evitar su eliminación o manipulación por entidades ajenas al servicio.

La FNMT pondrá las medidas de protección generalmente aceptadas para la protección del contenido de la dirección electrónica frente a código dañino, virus, etc. y las mantendrá debidamente actualizadas para evitar, en la medida de lo posible, los daños causados por este tipo de actuaciones.

La FNMT solicitará identificación previa mediante firma electrónica a cualquier entidad que desee depositar información de cualquier tipo en la dirección electrónica. Dicha información permitirá en caso de necesidad, identificar y suspender el acceso a la entidad que haga uso incorrecto de la dirección electrónica.

La FNMT avisará electrónicamente al titular de la dirección electrónica de que se ha introducido información en la misma. Dicho aviso se realizará mediante el envío de correo electrónico, mensajería SMS u otros medios generalmente aceptados, que el titular haya declarado como válidos.

El acceso a los contenidos de la dirección electrónica deberá ser realizado previa firma electrónica cuando el depositario del contenido así lo requiera. En este caso, la FNMT guardará prueba del acceso al contenido con las mismas características explicadas para el acceso a la dirección electrónica.

El contenido estará disponible para su titular, al menos, el tiempo que el depositario de la información haya definido. El titular podrá acceder y descargar la información durante ese tiempo sin límite. Pasado ese plazo la FNMT se reserva el derecho a almacenar dicha información en soportes electrónicos que no estén disponibles en línea.

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.

Precio del servicio.

El servicio de dirección electrónica será inicialmente, gratuito para sus titulares, ya sean estos particulares o empresas. La modificación de las presentes condiciones será comunicada a sus titulares, al menos con 12 meses de antelación a su entrada en vigor.

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.

Servicio de fechado digital.

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

Además, el fechado digital proporciona un valor añadido a la utilización de firma digital ya que ésta por sí 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 Fechado (TSA-Time Stamp Authority) como tercera parte de confianza. La definición del servicio del Fechado Digital está basada en las especificaciones del estándar RFC3161 –«Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)». 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.

Estándares aplicables.

Se sigue la norma IETF-PKIX RFC-3161 y la correspondiente norma ISO 18014-2, en la cual la FNMT-RCM ha participado como elaborador de la misma.

El estándar RFC3161 define entre otros, el formato de la solicitud de un fechado digital 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 fechados digitales generados por la TSA deberían 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 fechados digitales (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 fechado digital que recibe la TSA contengan algún tipo de autenticación del cliente.

En casos especiales, la TSA necesita autenticar la procedencia de las solicitudes, el mencionado estándar recomienda para ello utilizar algún método alternativo, no especificado en RFC3161. El protocolo de fechado digital de la FNMT-RCM hace uso de autenticación basada en firma según Cryptographic Message Syntax (RFC 2630).

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 se 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.

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

La aplicación de Notificación y la aplicación de custodia hacen uso del protocolo basado en sockets utilizando el puerto 318. Los mensajes de servicio tienen la siguiente estructura:

Mensaje	Longitud	Tag	Datos
Petición.	Xxxx bytes.	0x01	Codificación DER de la estructura ASN.1 TimeStampReq encapsulada en una estructura ASN.1 CMSSigned Data (ver RFC 2630).
Respuesta.	Yyyy bytes.	0x02	Codificación DER de la estructura ASN.1 TimeStampResp.

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 extractado en el presente texto.

Fuente de tiempo.

Las fuentes de tiempo utilizadas por la Autoridad de Fechado Digital son receptores GPS que reúnen las siguientes características:

Recibe una referencia temporal con una precisión menor de un (1) microsegundo.

Distribuye la referencia temporal a la Autoridad de Fechado Digital con una precisión de entre uno (1) y diez (10) milisegundos.

La sincronización de la fecha y la hora del servicio se realizará con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992, de 23 de octubre, por el que se declara el Laboratorio del Real Instituto y Observatorio de la Armada como laboratorio depositario del patrón Nacional de Tiempo y laboratorio asociado al Centro Español de Metrología, y según las condiciones técnicas y protocolos que el citado Organismo establezca.

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.

Toolkit de fechado digital.

Librerías y documentación paquetizadas puestas a disposición de los clientes para desarrollar un esquema de fechado digital en conjunción con la Autoridad de Fechado Digital de la FNMT-RCM, así como servicios de implantación a través de partners.

Prácticas del servicio.

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

Servicio de Certificados de Atributos.

Tal como ya ha quedado dicho en el capítulo I del presente anexo, 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.

Se trata del certificado tradicional de clave pública que sirve para identificar a la persona física, es decir: nombre, apellidos, DNI, etc. Estos certificados tienen asociada la pareja de claves pública-privada y están firmados por una autoridad de certificación.

El formato de esos certificados 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 fecha Junio del 97 o superiores (ISO/IEC 9594-8 de 1997). El formato será el correspondiente a la Versión 3 del certificado, especificado en esta norma y serán válidos para el uso con protocolos de comunicación estándares de mercado, tipo SSL, TLS, etc.

Por contra, los certificados de atributos no tienen asociada la pareja de claves pública-privada ni tienen que estar firmados por una autoridad de certificación. Es decir, que el emisor de certificados de atributos no tiene que ser necesariamente un prestador de servicios de certificación

según se entiende en la Ley de Firma Electrónica o en la Directiva de Firma Electrónica.

Esto hace que sean muy útiles para permitir a las distintas entidades emitir sus propios certificados de atributos, para los usos que requieran, apoyándose en certificados de identidad del titular ya expedidos por una Autoridad de Certificación.

En comparación con lo anterior el certificado de atributos no sirve para acreditar una identidad, y ha de asociarse con un certificado básico o de identidad del titular para tal fin.

El formato de esos certificados se basa en el definido por la Unión Internacional de Telecomunicaciones, sector de normalización de las telecomunicaciones, en la Recomendación UIT-T X.509 v4, del año 2000 «El directorio: Infraestructuras de clave pública y certificado de atributos».

Operativa de obtención de los Certificados de Atributos.

El cliente final, por ejemplo un funcionario, desea obtener un certificado de atributos que le acredite como funcionario. Para ello se seguirían los siguientes pasos:

El cliente final se conectaría con el Departamento correspondiente del Ministerio de Medio Ambiente y realizaría una petición firmada con su certificado de identidad (por ejemplo el certificado de usuario de la FNMT-RCM).

El Departamento correspondiente comprobaría la validez de esta petición, es decir:

Comprobación del certificado de identidad mediante CRLs.

y si la persona en cuestión está realmente reconocida como funcionario (consulta de la base de datos del Departamento correspondiente).

Una vez hecha las comprobaciones, el Departamento correspondiente del Ministerio de Medio Ambiente se conectaría a la Autoridad de Certificación de Atributos, en adelante ACA, (estableciendo un canal SSL con el servidor donde está instalada la ACA) y mandaría una petición firmada de emisión del certificado para esta persona. (La FNMT-RCM además de actuar como infraestructura de clave pública proporciona, en régimen de hosting, las distintas autoridades de certificación de atributos (ACA) y se encarga de mantener la publicación y facilitar el acceso a estos certificados).

La ACA contestaría emitiendo este certificado de atributos, publicándolo en un directorio específico y entregándolo al propio funcionario (notificar la disponibilidad para su descarga) y notificando lo ocurrido con este certificado (éxito en la emisión o notificación de la causa de la no emisión).

Todas las operaciones y comunicaciones se establecen vía web mediante la oportuna securización de los distintos procedimientos, según se ha descrito.

Es potestad y responsabilidad de la ACA el desarrollo e implantación de las correspondientes aplicaciones en su servidor que permitan llevar a cabo todos estos procedimientos, tanto la solicitud como posterior descarga de los atributos, de forma totalmente telemática y sin presencia física presencial del funcionario, en el supuesto inicial de que éste posea un certificado de identidad, con anterioridad a la petición de la inclusión de algún atributo en el mismo.

Operativa de uso y revocación de los certificados con atributos:

Si un ciudadano es suscriptor de un certificado con atributos, a él le compete la custodia y buen uso del mismo en todos los ámbitos administrativos de conformidad con la normativa específica. El certificado de atributos irá vinculado al certificado básico o de identidad para poder firmar (el certificado de atributos no contiene datos de creación de firma).

La Autoridad de Certificación de Atributos podrá establecer y publicar unas prácticas de certificación que, en concordancia con su política de certificación, recojan los procedimientos a seguir por sus funcionarios, tanto para la solicitud de la inclusión de atributos en los certificados de identificación como para la revocación de los mismos.

La FNMT-RCM se responsabilizará del alojamiento de la Autoridad Certificadora y de su funcionamiento técnico, y de llevar a cabo las actuaciones técnicas necesarias que permitan la emisión, almacenamiento de incidencias y revocación en tiempo de los certificados según las prácticas que la propia Autoridad Certificadora de Atributos determine, previo consenso con la FNMT-RCM para determinar su viabilidad.

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 de gestión, convenios o contratos

que suscriba la FNMT-RCM con las diferentes administraciones públicas o con personas o entidades privadas.

ANEXO II

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

Se constituirá una oficina central de acreditación, en la siguiente dirección:

C/ Plaza San Juan de la Cruz s/n. 28071 Madrid.

La dirección IP es:

213.422.175.

213.423.173.

ANEXO IV

Precios y plan de implantación

CAPÍTULO I

1. Precio anual de los servicios.

Se establece un precio fijo de cuatrocientos noventa y un mil treinta y cuatro euros al año, (491.034,00 € al año), IVA incluido, cantidad que se incrementará 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 del contrato.

2. Constitución de las oficinas de acreditación.

Podrán implantarse cuantas oficinas de acreditación se estime conveniente por parte del Ministerio de Medio Ambiente que estarán abiertas a los grupos de usuarios que el Ministerio de Medio Ambiente autorice.

Por la FNMT-RCM se facilitará el soporte lógico (software) necesario para que estas oficinas puedan llevar a cabo sus funciones de acreditación.

Por la FNMT-RCM se asumirán los costes de la emisión de una tarjeta por cada persona responsable de llevar a cabo las funciones de acreditación, así como de la formación de las mismas en las instalaciones de la FNMT-RCM. En el caso de que esa formación se preste fuera del municipio de Madrid, se establece el pago de los gastos derivados de la estancia, fijados en 204,38 euros/día por persona, más los derivados del desplazamiento.

3. Soporte Técnico.

Se establece una bolsa de 100 horas de soporte técnico a la implantación, incluidas en el precio fijo establecido, y que serán distintas de las específicamente destinadas a formación contempladas en el punto anterior.

El coste del soporte técnico adicional 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 204,59 euros/día por persona, mas los derivados del desplazamiento y pernocta.

4. Réplica de Directorio.

Se incluye en el precio fijado el servicio de 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 INE, tomando como referencia el del año de la firma de la Encomienda de Gestión.

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

CAPÍTULO II

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

El precio anual de los servicios esenciales establecido en el apartado 1. del cap I del presente Anexo de Precios incluye 15 certificados de servidor o componente y 8 de firma de código.

El precio de los certificados adicionales será de 817,59 euros por cada año de certificado de servidor o componente y de certificado de firma de código siendo emitidos todos ellos por cuatro años.

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

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

2. Tarjetas criptográficas.

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

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

Cantidad	Tarjeta base	Tarjeta 4+4	Tarjeta genérica	Panel de firma
100	10,52	-	11,02	-
300	10,01	-	10,52	-
500	9,16	-	10,34	-
1.000	6,02	10,17	7,60	0,07
2.000	5,64	7,85	6,40	0,04
3.000	5,42	6,90	-	0,03
5.000	4,80	5,63	-	0,03
10.000	4,62	5,04	-	0,03
15.000	4,35	4,62	-	0,03
25.000	4,26	4,43	-	0,03
50.000	3,98	4,08	-	0,03
100.000	3,95	4,01	-	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 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.

Si la tarjeta lleva PIN y Código de Desbloqueo individual, incluyendo carrier genérico de FNMT-RCM y sobre blanco, el precio se incrementará en 0,95 euros por unidad.

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

Transporte e impuestos no incluidos.

No obstante lo anterior la FNMT-RCM suministrará gratuitamente, como aportación voluntaria y siempre que sus disponibilidades se lo permitan, un número suficiente de tarjetas para dotar de las mismas al personal que presta sus servicios en la sede central del Ministerio de Medio Ambiente (plaza de San Juan de la Cruz, s/n, de Madrid); lo que se estima en 500 tarjetas.

4. Fechado Digital.

El precio anual de los servicios esenciales establecido en el apartado 1 del cap 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:

1. 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.

2. 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.

5. Servicio de Infraestructura Técnica de Dirección Electrónica.

El servicio de dirección electrónica será inicialmente, gratuito para sus titulares, ya sean estos particulares o empresas. La modificación de las presentes condiciones será comunicada a sus titulares, al menos con 12 meses de antelación a su entrada en vigor.

El servicio de dirección electrónica permite la existencia de buzones corporativos. Estos buzones corporativos pueden ser accedidos por hasta cinco titulares distintos sin sobrecargo adicional.

6. Servicio de Notificaciones Electrónicas.

Aviso Electrónico.

Si se desean enviar un mensaje SMS al ciudadano, el mismo tendrá un coste adicional de 0,20 euros.

Se facturará por tres conceptos:

Por cuota de alta y mantenimiento en el sistema: Por este concepto el precio es de 10.000 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 10.000 avisos anuales. Su abono es anual.

Por número de avisos. Se contratan paquetes. Estos tendrán una validez máxima de un año, es decir, deben consumirse antes de doce meses desde su adquisición. El importe de cada paquete se facturará de acuerdo a la siguiente tabla:

Tramos en número de avisos por año	Precio por paquete de 10.000 documentos - Euros
Entre 1 y 10.000	1.898
Entre 10.001 y 100.000	1.710
Entre 100.001 y 500.000	1.539
Entre 500.001 y 2.000.000	1.385
Más de 2.000.001	1.249

Por capacidad (volumen) de los mensajes notificados. Este concepto se incluye para no penalizar la capacidad de almacenamiento del sistema. De tal forma que las notificaciones que de forma individual presenten una longitud inferior a 20kB, no contabilizarán como consumo de capacidad. Los mensajes que excedan los 20kB se totalizarán y facturan según la siguiente tabla. Este concepto se facturará anualmente y se totalizarán todos los documentos del cliente que excedan de los 20KB. La custodia estándar del servicio de aviso es por 3 meses, para periodos superiores hay que contratar el servicio de custodia.

Tramos según consumo en GBytes	Precio por paquetes de 1 GByte - Euros
Hasta 1	1.000
Desde 1 hasta 5	750
Desde 5 hasta 50	500
Desde 50 hasta 200	300
Más de 200	100

Nota:

Todos los conceptos son anuales.

Precios para avisos individuales o avisos en buzones corporativos hasta cinco titulares. Para otras condiciones, consultar precios.

Aviso electrónico con custodia.

Si se desean enviar un mensaje SMS al ciudadano, el mismo tendrá un coste adicional de 0,20 euros.

El precio de este servicio se facturará por tres conceptos, de forma análoga al servicio de avisos, pero con otros parámetros:

Por cuota de alta y mantenimiento en el sistema: Por este concepto el precio es de 35.000 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 10.000 custodias anuales. Su abono es anual.

Por número de documentos según paquetes. Los paquetes tendrán una validez máxima de un año, es decir, deben consumirse antes de doce meses desde su adquisición. El importe de cada paquete se facturará anualmente de acuerdo a la siguiente tabla.

Tramos en número notificaciones con custodia y fechado digital por año	Precio por paquete de 10.000 documentos Euros
Entre 1 y 10.000	12.209
Entre 10.001 y 100.000	10.991
Entre 100.001 y 500.000	9.893
Entre 500.001 y 2.000.000	8.905
Más de 2.000.001	8.011

Por capacidad (volumen) de los documentos custodiados. Este concepto se incluye para no penalizar la capacidad de almacenamiento del sistema. De tal forma que los documentos que de forma individual presenten una longitud inferior a 500KB, no contabilizarán como consumo de capacidad que se expone en esta tabla. Los mensajes que excedan los 500KB se totalizarán y facturan según la siguiente tabla. Este concepto se facturará anualmente y se totalizarán todos los documentos del cliente que excedan de los 500KB, incluidos los de años anteriores. La custodia mínima de un documento es por 5 años.

Tramos según consumo en GBytes	Precio (Euros) por paquetes de 1GByte
Hasta 1	1.000
Desde 1 hasta 5	750
Desde 5 hasta 50	500
Desde 50 hasta 200	300
Más de 200	100

Nota: Todos los conceptos son anuales.

Notificación electrónica.

El precio anual de los servicios esenciales establecido en el apartado 1 del cap 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 todas las notificaciones durante el primer año de vigencia de la Encomienda de Gestión, transcurrido el cual sin haberse hecho uso de las mismas, parcialmente o en su totalidad, no será posible su convalidación para los sucesivos periodos anuales.

Las notificaciones se conservan durante 3 meses. Si se desean enviar un mensaje SMS al ciudadano, el mismo tendrá un coste adicional de 0,20 euros.

Por cuota de alta y mantenimiento en el sistema: Por este concepto el precio es de 30.000 Euros. Este precio incluye las librerías necesarias (tanto de fechado digital como de custodia y notificación) para el uso de la aplicación (y el mantenimiento de las mismas, pero no los posibles desarrollos que haya que realizar), 10.000 notificaciones, 10.000 custodias anuales y 10.000 sellados de tiempo. Su abono es anual.

Tramos en número de custodias con fechado digital por año	Precio por paquete de 10.000 documentos (Euros)
Entre 1 y 10.000	5.942
Entre 10.001 y 100.000	5.357
Entre 100.001 y 500.000	4.822
Entre 500.001 y 2.000.000	4.339
Más de 2.000.001	3.907

Por capacidad (volumen) de los mensajes notificados. Este concepto se incluye para no penalizar la capacidad de almacenamiento del sistema. De tal forma que las notificaciones que de forma individual presenten una longitud inferior a 20kB, no contabilizarán como consumo de capacidad. Los mensajes que excedan los 20kB se totalizarán y facturan según la siguiente tabla. Este concepto se facturará anualmente y se totalizarán todos los documentos del cliente que excedan de los 20KB. La custodia estándar del servicio de aviso es por 3 meses, para periodos superiores hay que contratar el servicio de custodia.

Tramos según consumo en GBytes	Precio por paquetes de 1GByte (Euros)
Hasta 1	1.000
Desde 1 hasta 5	750
Desde 5 hasta 50	500
Desde 50 hasta 200	300
Más de 200	100

Notificación electrónica con custodia

El precio anual de los servicios esenciales establecido en el apartado 1 del cap 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 todas las notificaciones con custodia durante el primer año de vigencia de la Encomienda de Gestión, transcurrido el cual sin haberse hecho uso de las mismas, parcialmente o en su totalidad, no será posible su convalidación para los sucesivos periodos anuales.

Las custodias se realizan por cinco años. Si se desean enviar un mensaje SMS al ciudadano, el mismo tendrá un coste adicional de 0,20 euros.

El precio de este servicio se facturará por tres conceptos, de forma análoga al servicio de avisos, pero con otros parámetros:

Por cuota de alta y mantenimiento en el sistema: Por este concepto el precio es de 35.000 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 10.000 transacciones anuales. Su abono es anual.

Por número de documentos según paquetes. Los paquetes tendrán una validez máxima de un año, es decir, deben consumirse antes de doce meses desde su adquisición. El importe de cada paquete se facturará anualmente de acuerdo a la siguiente tabla.

Tramos en número notificaciones con custodia, fechado digital y respuesta por año	Precio por paquete de 10.000 documentos (Euros)
Entre 1 y 10.000	12.209
Entre 10.001 y 100.000	10.991
Entre 100.001 y 500.000	9.893
Entre 500.001 y 2.000.000	8.904
Más de 2.000.001	8.011

Por capacidad (volumen) de los documentos custodiados. Este concepto se incluye para no penalizar la capacidad de almacenamiento del sistema. De tal forma que los documentos que de forma individual presenten una longitud inferior a 500KB, no contabilizarán como consumo de capacidad que se expone en esta tabla. Los mensajes que excedan los 500KB se totalizarán y facturan según la siguiente tabla. Este concepto se facturará anualmente y se totalizarán todos los documentos del cliente que excedan de los 500KB, incluidos los de años anteriores. La custodia mínima de un documento es por 5 años.

Tramos según consumo en GBytes	Precio por paquetes de 1GByte (Euros)
Hasta 1	1.000
Desde 1 hasta 5	750
Desde 5 hasta 50	500
Desde 50 hasta 200	300
Más de 200	100

Nota

Todos los conceptos son anuales.

7. Servicio de Custodia de Documentos Electrónicos.

Las custodias se realizan por cinco años.

El precio de este servicio se facturará por tres conceptos:

Por el precio fijo de este servicio que es de 10.000,00 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) así como la realización de 50.000 custodias, cifra ésta que se contabilizará de forma acumulada, que han de consumirse en el plazo máximo de un año y que de no hacerlo no son acumulables para los años posteriores. Su abono es anual.

Por un coste variable que se establece, en primer lugar, por las custodias realizadas en el plazo de un año cuya cifra supere la cantidad de 50.000, sin mayor límite, contabilizadas de la misma forma que la antes

dicha, a razón de 0,10 €/ custodia siempre que la capacidad (volumen) de los documentos custodiados sea inferior a 500 KB.

Y, en segundo lugar por la capacidad (volumen) de los documentos custodiados. Este concepto se incluye para no penalizar la capacidad de almacenamiento del sistema. De tal forma que los documentos que de forma individual presenten una longitud inferior a 500KB, no contabilizarán como consumo de capacidad que se expone en esta tabla. Los mensajes que excedan los 500KB se totalizarán y facturan según la siguiente tabla. Este concepto se facturará anualmente y se totalizarán todos los documentos del cliente que excedan de los 500KB, incluidos los de años anteriores. La custodia mínima de un documento es por 5 años.

Tramos según consumo en GBytes	Precio (Euros) por paquetes de 1GByte
Hasta 1	1.000
Desde 1 hasta 5	750
Desde 5 hasta 50	500
Desde 50 hasta 200	300
Más de 200	100

Todos los conceptos son anuales.

8. Servicio de Certificados de atributos.

Número de usuarios variable.

Los certificados de atributos serán emitidos por la Autoridad de Certificados de Atributos.

Los certificados de identidad en los que se apoyen los certificados de atributos serán los certificados de usuario de la FNMT-RCM.

(Si los certificados de identidad son otros, se estudiará el uso de los mismos en función de la arquitectura técnica necesaria para modelar el sistema).

La validez temporal de la contratación de este servicio coincidirá con la de la Encomienda de Gestión al que está ligada, coincidiendo sus plazos de renovación con aquél.

1.000 usuarios mínimo y CRLs diarias. Para un número de usuarios mayor habrá que utilizar la fórmula siguiente:

$$\text{Precio (€)} = 234,4 * (\text{número de usuarios})^{1/2} + 7.587,6$$

(se expone, a modo de ejemplo, una valoración para visualizar la evolución de la fórmula):

Número de usuarios	Precio
1 a 1.000	15.000
2.000	18.070
5.000	24.162
10.000	31.028
15.000	36.296
25.000	44.650
50.000	60.000

Al principio de cada anualidad de fecha de contrato se facturará, como cuota de mantenimiento del servicio de los certificados emitidos hasta ese momento, el tramo base de los reflejados en la tabla general anterior, regularizándose sólo el exceso sobre la misma al final de dicho periodo.

Las CRLs se publicarán en un directorio seguro de la FNMT-RCM. Si se desean réplicas de este directorio, llevarán costo adicional. (Consultar Servicio de Réplica de Directorio).

A los efectos de lo expuesto en este apartado, se considerará usuario: la persona titular de un certificado emitido bajo una determinadas condiciones y características (política). Esto quiere decir que si un usuario revoca un certificado y solicita uno nuevo de las mismas condiciones y características del anterior, se está hablando del mismo usuario. Por el contrario, si un usuario dispone de más de un certificado de características diferentes, se estará hablando de usuarios distintos. Decir, finalmente, que cada usuario podrá disponer de un único certificado con iguales condiciones y características (política).

Todos los conceptos son anuales.

Si previamente a la contratación de este servicio se había contratado el uso del certificado de usuario se sumarán ambos conceptos de servicio prestado.

9. 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 sus apartados 1 y 2, habrá que añadirles el IVA legalmente establecido.

Plan de Implantación (Tentativo).

Entrega de documentación y productos.

Aportación de manuales de uso e instalación de los productos.

Aportación del software y documentación técnica, incluyendo ejemplos de aplicación.

Aportación del software de verificación de listas de revocación.

Aportación del software de firma.

Acreditación de encargados de acreditar.

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

Relación del número de puestos por oficina de acreditación.

Selección de los encargados de acreditar.

Relación de encargados de acreditar por puesto, incluyendo su nombre y apellidos, NIF, y dirección postal completa.

Calendario de implantación de las oficinas de acreditación.

Formación de los encargados de acreditar.

Acreditación de encargados de acreditar, entrega de tarjetas, equipo lógico (software), lectores y manuales.

Constitución de las oficinas y comienzo de la acreditación de usuarios.

Implantación de aplicativos.

Aportación de la documentación necesaria para la emisión de los certificados de servidor o componente y las claves a firmar.

Emisión de certificados de firma de código y de servidor o componente necesarios, Definición de los servicios a prestar.

Calendario de puesta en marcha de las aplicaciones.

Soporte técnico a la implantación por la FNMT.

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

Comunicación a los usuarios de los nuevos servicios.

Envío de correo electrónico, comunicando los nuevos servicios disponibles, a los usuarios activos con dirección de correo electrónico.

Redacción conjunta de nota de prensa y envío a los medios.

Publicación de servicios en el apartado de Colaboraciones del web de la FNMT.

MINISTERIO DE CULTURA

14779

ORDEN CUL/2368/2007, de 29 de mayo, por la que se ejercita el derecho de tanteo, sobre una colección de libros y documentos de diversos autores, subastados por la Sala Fernando Durán, en Madrid.

A propuesta de la Dirección General de Bellas Artes y Bienes Culturales, y en aplicación de los artículos 40 y 41 del Real Decreto 111/1986, de 10 de enero de desarrollo parcial de la Ley 16/1985, del Patrimonio Histórico Español, dispongo:

Primero.—Que se ejercite el derecho de tanteo para la Fundación Residencia de Estudiantes, con cargo a sus presupuestos, sobre los bienes muebles que fueron incluidos en el catálogo de la subasta pública celebrada por la Sala Fernando, en Madrid, los días 22, 23 y 24 de mayo de 2007, con los números y referencia detallados en la relación adjunta.

Segundo.—Para el abono a la sala subastadora del precio total de remate de treinta y ocho mil ciento cuarenta y cinco euros (38.145.-€), más los gastos inherentes, así como para la custodia de los bienes subastados, el representante de la entidad de derecho público afectada habrá de acordar directamente con los subastadores las medidas que estime conveniente.

Madrid, 29 de mayo de 2007.—La Ministra de Cultura, P.D. (Orden CUL/2591/2004, de 22 de julio), el Subsecretario de Cultura, Antonio Hidalgo López.