ADENDA AL CONVENIO SUSCRITO EL 26 DE JULIO DE 2002 ENTRE LA JUNTA DE ANDALUCÍA Y LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE – REAL CASA DE LA MONEDA PARA LA PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA.

En Sevilla, 13 de julio de 2005

REUNIDOS

De una parte, la Excma. Sra. Dª. MARÍA JOSÉ LÓPEZ GONZÁLEZ, Consejera de Justicia y Administración Pública de la Junta de Andalucía, en nombre y representación del citado Organismo, en virtud de las competencias atribuidas por el Decreto 12/2004, de 24 de Abril.

Y de otra parte el Ilmo. Sr. D. Sixto Heredia Herrera, Director General de la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (en adelante FNMT-RCM), actuando en representación de esta Entidad Pública Empresarial, en virtud del nombramiento efectuado por el Real Decreto 802/2004, de 23 de abril, y de las competencias que le atribuye el artículo 19 del Estatuto aprobado por Real Decreto 1114/1999, de 25 de junio.

Reconociéndose la capacidad legal necesaria para formalizar la presente Adenda al Convenio citado, ambas partes

EXPONEN

Primero.- Que la Junta de Andalucía y la FNMT-RCM suscribieron, con fecha 26 de julio de 2002, un Convenio para la prestación de servicios de certificación de firma electrónica, y concretamente 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 de la Junta de Andalucía, con el alcance definido en tal convenio y sus documentos anexos.

Segundo.- Que para formalizar adecuadamente la prestación, por parte de la FNMT-RCM, de nuevos servicios no previstos en el vigente Convenio, se tienen que modificar los textos de las cláusulas primera y segunda del mencionado Convenio de títulos "Objeto" y "Ámbito de Aplicación" respectivamente.

Tercero.- Que en la cláusula cuarta, del mencionado Convenio, se indica:

> *"La FNMT-RCM percibirá, por los servicios EIT prestados a la Junta de Andalucía la cantidad de QUINIENTOS UN MIL CIENTO NOVENTA Y NUEVE (501.199) Euros/año (impuestos incluidos).*
>
> *La FNMT-RCM podrá realizar facturaciones parciales contra certificaciones parciales conformadas por el Junta de Andalucía.*
>
> *El pago se efectuará en el plazo de 1 mes contra la prestación de las correspondientes facturas.*
>
> *La demora en el pago se regirá por lo dispuesto en el artículo 45 de la Ley General Presupuestaria..*
>
> *Anualmente se aplicará un incremento en los precios estipulados, correspondiente al Índice de Precios al Consumo (IPC)"*

Cuarto.- Que en la cláusula sexta, del mencionado Convenio, se indica:

> *"PLAZO DE DURACIÓN.-*
>
> *1.- El Convenio tendrá una duración de un año (1 año). No obstante se producirá la prórroga automática del mismo, por periodos iguales, si no mediara denuncia de ninguna de las partes con tres meses de antelación a su vencimiento.*
>
> *2.- Las partes podrán proponer la revisión del Convenio en cualquier momento de su vigencia, a efectos de incluir las modificaciones que resulten pertinentes."*

Quinto.- Siendo necesario ampliar el alcance de la cobertura que en el actual texto del Convenio se contempla, para la prestación de servicios de certificación de firma electrónica, y concretamente 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 de la Junta de Andalucía,

A tal fin, ambas partes, acuerdan modificar el contenido del Convenio citado en lo que concierne al contenido de los expositivos segundo, tercero y cuarto de la presente Adenda, así como en sus Anexos I, II y III, con arreglo a las siguientes

CLÁUSULAS

PRIMERA.- MODIFICACIÓN DE LA CLÁUSULA PRIMERA.

La cláusula primera del Convenio para la prestación de servicios de firma electrónica suscrito entre la Junta de Andalucía y la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, el día 26 de julio de 2002, queda redactada de la siguiente manera:

"PRIMERA.- OBJETO.

1.- ***Constituye el objeto del presente Convenio la prestación 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 de la Junta de Andalucía con las condiciones técnico-administrativas que en las cláusulas siguientes se estipulan.***

2.- ***En particular, la FNMT-RCM prestará los servicios esenciales que al efecto se enumeran en el capítulo I del anexo I de este convenio. También prestará a petición de la Junta de Andalucía cualquiera, o la totalidad, de los servicios avanzados que al efecto se enumeran en el capítulo II del mismo anexo I de este convenio."***

SEGUNDA.- MODIFICACIÓN DE LA CLÁUSULA SEGUNDA.

La cláusula segunda del Convenio para la prestación de servicios de firma electrónica suscrito entre la Junta de Andalucía y la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, el día 26 de julio de 2002, queda redactada de la siguiente manera:

"- ÁMBITO DE APLICACIÓN.-

En virtud del presente Convenio, la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda podrá prestar servicios EIT a las personas físicas que tengan la condición de usuarios de acuerdo con la normativa vigente y las cláusulas de este Convenio, cuando los usuarios se relacionen con la Junta de Andalucía y también con todas sus Diputaciones, con todos sus Municipios, con su Cámara de Cuentas, con El Defensor del Pueblo, con el Parlamento y con todas las Universidades Públicas de la Comunidad Autónoma de Andalucía, en el marco de sus respectivas competencias y siempre que previamente se hubieran adherido las referidas Entidades al Convenio, lo cual deberá formalizarse a través del oportuno Protocolo de Adhesión que se suscriba al efecto entre la Junta de Andalucía y cualquier Entidad interesada de entre las relacionadas, del que se dará traslado a la FNMT-RCM.

A tal efecto, la Junta de Andalucía, 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 ciudadanos con las diferentes Administraciones públicas, los órganos administrativos o en su caso las entidades privadas que hayan suscrito el correspondiente convenio con la FNMT-RCM.

De igual forma los certificados que, al amparo de la normativa vigente y del presente convenio tipo, haya expedido o expida la FNMT-RCM, podrán ser utilizados por los usuarios en sus relaciones con la Junta de Andalucía."

TERCERA.- MODIFICACIÓN DE LA CLÁUSULA CUARTA.

La cláusula cuarta del Convenio para la prestación de servicios de firma electrónica suscrito entre la Junta de Andalucía y la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, el día 26 de julio de 2002, queda redactada de la siguiente manera:

"CUARTA.- Precio y Condiciones de Pago.

> *La FNMT-RCM percibirá, por los servicios EIT prestados a la Junta de Andalucía la cantidad de UN MILLÓN CIENTO NOVENTA Y SIETE MIL CIENTO NOVENTA Y NUEVE €/año (1.197.199,00) Euros/año (impuestos incluidos), repartidos en dos tramos de facturación, el primero desde el 1 de enero hasta el 31 de julio y el segundo desde el 1 de agosto hasta el 31 de diciembre de cada año natural, mientras dure su vigencia, que se incrementarán a partir de la facturación de los dos primeros tramos correspondientes a 2005, aplicando la variación del IPC publicado en los doce meses anteriores de acuerdo con el índice aprobado por el I.N.E,. El detalle de los servicios incluidos en este precio se contiene en el Anexo II de la presente Adenda al Convenio.*

La FNMT-RCM aportará a cada Campaña Publicitaria anual de promoción en el uso del Certificado Electrónico por el ciudadano que la Junta de Andalucía realice en su ámbito de actuación, un líquido del 8% del importe anual, sin impuestos, que ella, a su vez, perciba por los servicios EIT prestados a la Junta de Andalucía en los términos en la presente Adenda recogidos, y siempre que se hubiese dotado la correspondiente partida en su presupuesto anual y que se encuentre vigente el Convenio.

Si hubiera petición expresa de servicios avanzados hecha por la Junta de Andalucía, la cantidad anterior quedaría incrementada por el importe correspondiente que de la aplicación de las tablas del capítulo II del Anexo II de Precios se dedujeran.

La FNMT-RCM podrá realizar facturaciones parciales contra certificaciones parciales conformadas por el Junta de Andalucía.

El pago se efectuará en el plazo de 1 mes contra la prestación de las correspondientes facturas.

La demora en el pago se regirá por lo dispuesto en el artículo 45 de la Ley General Presupuestaria.

Anualmente se aplicará un incremento en los precios estipulados, correspondiente al Índice de Precios al Consumo (IPC)"

CUARTA.- MODIFICACIÓN DE LA CLÁUSULA SEXTA.

La cláusula sexta del Convenio para la prestación de servicios de firma electrónica suscrito entre la Junta de Andalucía y la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, el día 26 de julio de 2002, queda redactada de la siguiente manera:

"PLAZO DE DURACIÓN.-

1.- El Convenio tendrá una duración de un año (1 año). No obstante se producirá la prórroga automática del mismo, por periodos iguales, si no mediara denuncia de ninguna de las partes con tres meses de antelación a su vencimiento.

2.- En el caso de que durante la vigencia del Convenio o de cualquiera de sus prórrogas automáticas se produjera que la FNMT-RCM llegase a firmar uno nuevo, del mismo objeto que el presente, en el que quedara reflejado que su ámbito de aplicación fuera a dar cobertura, además de a la Junta de Andalucía, a otros Organismos y Administraciones Públicas, manteniendo las mismas o mejores condiciones que aquellas con las que se encontrase en ese momento definido el

Convenio, se procederá, a propuesta de la Junta de Andalucia, a la cancelación del Convenio previa adhesión expresa de la Junta de Andalucía al nuevo.

3.- Las partes podrán proponer la revisión del Convenio en cualquier momento de su vigencia, a efectos de incluir las modificaciones que resulten pertinentes."

QUINTA.- MODIFICACIÓN DEL ANEXO I.

Con el fin de adecuar lo contenido en la cláusula anterior e incluir los nuevos servicios que la FNMT-RCM está en condiciones de prestar: certificado de persona jurídica (en desarrollo normativo), certificado de atributos, publicación en directorio externo y validación de certificados vía OCSP, se modifica el Anexo I del Convenio de referencia, insertando su actual texto contenido bajo la denominación de capítulo I y añadiendo uno nuevo, el capítulo II, que se detalla al final de la presenta adenda.

SEXTA.- MODIFICACIÓN DEL ANEXO II.

Con el fin de adecuar lo contenido en la cláusula anterior e incluir los precios de los nuevos servicios que la FNMT-RCM está en condiciones de prestar, así como para adecuar el nuevo contenido de la cláusula cuarta del Convenio, más arriba referida, al del parágrafo 1 del Anexo II, se modifica éste, incluyendo un capitulado en su contenido, que se inserta al final de la presente adenda.

SÉPTIMA.- MODIFICACIÓN DEL ANEXO III.

Con el fin de adecuar el contenido del Anexo III del Convenio a los actuales formularios de solicitud de emisión, revocación, suspensión y cancelación de suspensión de certificados que en la actualidad están vigentes, se modifica el referido Anexo III por la inclusión en el mismo de los referidos formularios.

OCTAVA.- Quedan subsistentes y sin alteración alguna, el resto de condiciones que integran el Convenio suscrito entre la Junta de Andalucía y la FNMT-RCM, con fecha 26 de julio de 2002, del que esta Adenda constituye parte integrante a todos los efectos.

NOVENA.- La presente Adenda entrará en vigor el día de su firma.

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

EL DIRECTOR GENERAL DE LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE – REAL CASA DE LA MONEDA	LA CONSEJERA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA DE LA JUNTA DE ANDALUCÍA
Fdo.: Sixto Heredia Herrera.	Fdo.: María José López González

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

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

- registro de usuarios
- emisión, revocación y archivo de certificados de clave pública
- publicación de certificados y del Registro de Certificados
- registro de eventos significativos

GENERACIÓN Y GESTIÓN DE CLAVES

Generación y gestión de las claves

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

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

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

La FNMT-RCM garantizará que el usuario, Titular del certificado, puede tener el control exclusivo de las claves privadas correspondientes a las claves públicas que se

consignan en el certificado, mediante la obtención de las pruebas de posesión oportunas, a través de la adjudicación del número de identificación único.

Archivo de las claves públicas

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

Exclusividad de las claves

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

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

Renovación de claves

La FNMT-RCM identifica una relación uno a uno entre la clave pública de un usuario y su certificado de clave pública, no previéndose utilizar distintos certificados para una misma clave. Es por esto que las claves se renovarán con los certificados cuando dicha renovación esté contemplada en la normativa específica aplicable.

REGISTRO DE USUARIOS

Registro de usuarios

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

Este registro podrá ser realizado por la propia FNMT-RCM o cualquier otra Administración pública y, en su caso, por las demás personas, entidades o corporaciones habilitadas a tal efecto por las normas que resulten de aplicación. En todo caso el registro se llevará a cabo según lo dispuesto por la FNMT-RCM, al objeto de que este registro se realice de acuerdo con lo establecido por la normativa específica aplicable y

homogéneo en todos los casos. De igual manera será la FNMT-RCM, quien defina y aporte los medios necesarios para la realización de este registro.

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

a) Aportación de la aplicación informática de registro

b) Aportación de la documentación relativa a la instalación y manejo de la aplicación, así como toda aquella referente a los procedimientos y normas sobre el registro.

c) Registro y formación de los encargados del registro, lo que supone la emisión de un certificado emitido por la FNMT-RCM para cada encargado del registro, que permita garantizar la seguridad de las comunicaciones con la FNMT-RCM, incluyendo la firma electrónica de las solicitudes de registro.

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

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

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

En caso de que solicite un certificado de persona jurídica, será de aplicación el procedimiento de verificación de la identidad del solicitante y de comprobación de los datos de constitución de la persona jurídica y de la suficiencia, extensión y vigencia de las facultades de representación del solicitante que se establece en el artículo 13 de la Ley 59/2003, de 19 de diciembre. El detalle del procedimiento figura en la Declaración de Prácticas de Certificación: http://www.cert.fnmt.es/convenio/dpc.pdf.

Necesidad de presentarse en persona

El procedimiento de registro requiere presencia física del interesado para formalizar el procedimiento de registro en la oficina de acreditación. No obstante, serán válidas y se dará el curso correspondiente a las solicitudes de emisión de certificados electrónicos cumplimentadas según el modelo trascrito en el anexo III de la presente adenda al convenio siempre que la firma del interesado haya sido legitimada notarialmente en los términos señalados en el referido modelo.

Necesidad de confirmar la identidad de los componentes por la FNMT-RCM

Si se trata de solicitudes relativas a certificados electrónicos a descargar en un servidor u otro componente, la FNMT-RCM requerirá la aportación de la documentación necesaria que le acredite como responsable de dicho componente y, en su caso, la propiedad del nombre del dominio o dirección IP. (Certificado de componente no es un certificado reconocido ni se recoge en la legislación española)

Incorporación de la dirección de correo electrónico del titular al certificado

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

Esta incorporación se realizará a los efectos de que el certificado pueda soportar el protocolo S/MIME en el caso de que la aplicación utilizada por el usuario así lo requiera.

Cuando la dirección del correo electrónico del titular del certificado conste en una de las extensiones del propio certificado, ni la FNMT–RCM, como firmante y responsable del mismo, ni la Junta de Andalucía como encargado del registro de usuarios responden de que esta dirección esté vinculada con el titular del certificado.

Obtención del "Certificado Básico" o "Título de usuario"

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

EMISIÓN, REVOCACIÓN Y ARCHIVO DE CERTIFICADOS DE CLAVE PÚBLICA

Emisión de los certificados

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

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

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

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

La FNMT-RCM garantiza para un certificado emitido:

a) Que el usuario dispone de la clave privada correspondiente a la clave publica del certificado, en el momento de su emisión.

b) Que la información incluida en el certificado se basa en la información proporcionada por el usuario.

c) Que no omite hechos conocidos que puedan afectar a la fiabilidad del certificado

Aceptación de certificados

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

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

✓ La Junta de Andalucía garantizará que, al solicitar un certificado electrónico, su titular acepta que:

a) La clave privada con la que se genera la firma electrónica corresponde a la clave pública del certificado.

b) Únicamente el titular del certificado tiene acceso a su clave privada.

c) Toda la información entregada durante el registro por parte del titular es exacta.

d) El certificado será usado exclusivamente para fines legales y autorizados y de acuerdo con lo establecido por la FNMT-RCM.

e) El usuario final del certificado no es un Prestador de Servicios de Certificación y no utilizará su clave privada asociada a la clave pública que aparece en el certificado para firmar otros certificados (u otros formatos de certificados de clave pública), o listados de certificados, como un Prestador de Servicios de Certificación o de otra manera.

✓ La Junta de Andalucía garantizará que, al solicitar un certificado electrónico, su titular asume las siguientes obligaciones sobre su clave privada:

a) A conservar su control.

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

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

Revocación y suspensión de certificados electrónicos

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

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

b) Resolución judicial o administrativa que lo ordene.

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

d) Finalización del plazo de vigencia del certificado.

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

f) Utilización indebida por un tercero.

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

h) Cualquier otra prevista en la normativa vigente.

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

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

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

La extinción de la condición de usuario público se regirá por lo dispuesto en el presente convenio o lo que se determine, en su caso, por la normativa vigente o por resolución judicial o administrativa.

Comunicación y publicación en el Registro de Certificados de circunstancias determinantes de la suspensión y extinción de la vigencia de un certificado ya expedido.

La FNMT-RCM suministrará a la Junta de Andalucía 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.
La Junta de Andalucía y la FNMT-RCM responderán de los daños y perjuicios causados por cualquier dilación que les sea imputable en la comunicación y publicación en el Registro de Certificados, respectivamente, de las circunstancias de que tengan conocimiento y que sean determinantes de la suspensión, revocación o extinción de un certificado expedido.

PUBLICACION DE CERTIFICADOS DE CLAVE PÚBLICA Y REGISTRO DE CERTIFICADOS

-Publicación de certificados de clave pública

La FNMT-RCM publicará los certificados emitidos en un directorio seguro.

Cuando el certificado sea revocado, temporal o definitivamente, este será publicado en el Registro de certificados que incluirá una lista de certificados revocados, comprensiva de los certificados expedidos por la FNMT-RCM cuya vigencia se ha extinguido o suspendido al menos hasta un año después de su fecha de caducidad.

Esta publicación puede ser:

a) Publicación directa por parte de la FNMT-RCM.- Esta operación la realiza la FNMT-RCM a través de la publicación en un directorio propio en que ofrece acceso a:

- Listas de certificados revocados

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

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

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

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

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

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

Frecuencia de la publicación en directorios externos

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

Control de acceso

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

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

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

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

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

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

REGISTRO DE EVENTOS SIGNIFICATIVOS

Tipos de eventos registrados

La FNMT-RCM registrará todos aquellos eventos relacionados con sus servicios que puedan ser relevantes con el fin de verificar que todos los procedimientos internos

necesarios para el desarrollo de la actividad se desarrollan de acuerdo a la normativa legal aplicable y a lo establecido en el Plan de Seguridad Interna, y permitan detectar las causas de una anomalía detectada.

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

Frecuencia y periodo de archivo de un registro de un evento

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

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

Archivo de un registro de eventos

La FNMT-RCM realizará una grabación segura y constante de todos los eventos relevantes desde el punto de vista de la seguridad y auditoría (operaciones realizadas) que vaya realizando, con el fin de reducir los riesgos de vulneración, mitigar cualquier daño que se produjera por una violación de la seguridad y detectar posibles ataques.

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

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

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

Datos relevantes que serán registrados

Serán registrados los siguientes eventos relevantes:

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

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

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

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

e) Eventos relevantes de la generación de claves.

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

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

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

Protección de un registro de actividad

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

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

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

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

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

CAPITULO II

1. 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 dentro de un determinado esquema de firmas. Para ello se seguirían los siguientes pasos:

- El cliente final se conectaría con el Departamento correspondiente de la Junta de Andalucía 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 de la Junta de Andalucía 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).

Toda 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 ligado 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.

2. Certificados wildcard

El certificado electrónico wildcard permite a las organizaciones asegurar todos los sub-dominios asociados a un dominio determinado, sin necesidad de adquirir y gestionar múltiples certificados electrónicos.

3. Validación de certificados vía OCSP

OCSP Responder

El servidor de OCSP (OCSP responder) comprueba la firma de la petición OCSP efectuada por un cliente OCSP registrado en el sistema (base de datos de clientes de los cuales se admiten peticiones) y verifica los certificados incluidos en la misma (el usuario no es el cliente que firma). En caso de que la firma sea inválida (certificado revocado o caducado, por ejemplo), la petición se rechaza y se retorna al cliente una respuesta negativa. En la respuesta de OCSP se informará del estado en el que se encuentran los certificados en ese momento.

Para ilustrar la explicación:

- Tenemos una empresa cliente, por ejemplo una gran superficie, que tiene un servidor en la que hay instalada un plataforma de compra de artículos.
- Un ciudadano, un cliente, se conecta con el servidor y decide comprar un artículo.
- Se le pide al ciudadano que se autentique y firme la petición de compra (con su certificado).
- Antes de admitir esta petición de compra, el servidor de la gran superficie hace una petición OCSP a la FNMT-RCM.

- El servidor de la FNMT-RCM (OCSP responder) responde si este certificado del ciudadano es válido o no (emite un comprobante de esta validación y lo firma en nombre de la FNMT-RCM para que quede constancia).
- Sin embargo, antes de esto, el servidor OCSP de la FNMT-RCM consultará si el servidor de la gran superficie se ha identificado correctamente y esta identificación (certificado de servidor) está dada de alta como cliente en la base de datos de clientes OCSP autorizados a transaccionar. Si no es así, no se atiende la petición.
- En caso de que se admita la petición, se comprobará por parte del servidor de la FNMT-RCM el estado del certificado del ciudadano y se le devolverá a la empresa cliente en la respuesta de OCSP.

OCSP cliente

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

OCSP toolkit

Librerías y documentación que permiten al cliente instalar el servicio de OCSP en conjunción con el OCSP responder de la FNMT-RCM y un OCSP cliente, así como servicios de implantación a través de partners.

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