

### III. OTRAS DISPOSICIONES

## CONSEJO DE SEGURIDAD NUCLEAR

**13890** *Resolución de 6 de noviembre de 2017, del Consejo de Seguridad Nuclear, por la que se publica el Convenio de colaboración con la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, para la extensión de los servicios públicos electrónicos.*

El Director General de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM) y el Presidente del Consejo de Seguridad Nuclear han suscrito, con fecha 1 de enero de 2017, un Convenio de colaboración interadministrativa para la extensión de los servicios públicos electrónicos.

Para general conocimiento, y en cumplimiento de lo establecido en el artículo 48.8 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, dispongo la publicación en el «Boletín Oficial del Estado», del referido Convenio, como anejo a la presente resolución.

Madrid, 6 de noviembre de 2017.–Presidente del Consejo de Seguridad Nuclear, Fernando Marti Scharfhausen.

#### ANEJO

#### **Convenio de colaboración interadministrativa entre la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda y el Consejo de Seguridad Nuclear para la extensión de los servicios públicos electrónicos**

En Madrid, a 1 de enero de 2017.

#### REUNIDOS

De una parte, don Fernando Marti Scharfhausen, como Presidente, en nombre y representación del Consejo de Seguridad Nuclear (en adelante CSN) en virtud de las competencias atribuidas por el Real Decreto 1732/2012 de 28 de diciembre (BOE número 313, del 29).

Y de otra, don Jaime Sánchez Revenga, como Director General, cargo para el que fue nombrado por el Real Decreto 286/2012, de 27 de enero (BOE número 24, del 28), en nombre y representación de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM), según resulta del artículo 19 de su Estatuto, siendo esta entidad organismo público, entidad pública empresarial, teniendo su domicilio institucional en Madrid, calle Jorge Juan, número 106, y código de identificación Q28/26004J.

Ambas partes, reconociéndose respectivamente capacidad legal y competencia suficientes para formalizar el presente Convenio,

#### EXPONEN

Primero.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que para el funcionamiento de las Administraciones Públicas la utilización de los medios electrónicos ha de ser lo habitual (firma y sedes electrónicas, el intercambio electrónico de datos en entornos cerrados de comunicación y la actuación administrativa automatizada mediante sello electrónico).

Por su parte, 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.

La disposición adicional cuarta de la Ley 59/2003, antes citada, constata la especialidad en la regulación que afecta a la actividad de la FNMT-RCM, al señalar 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, y la normativa de desarrollo prevista en el Real Decreto 1317/2001, de 30 de noviembre, facultan a la FNMT-RCM para que, mediante Convenio de colaboración, extienda la utilización de la Plataforma Pública de Certificación mediante técnicas y medios electrónicos, informáticos y telemáticos (EIT), a las Administraciones, organismos y entidades públicas en el actual marco de impulso de la Administración electrónica, tal y como se desprende de las modificaciones introducidas en el referido artículo 81 por las Leyes 55/1999, 14/2000, 44/2002, 53/2002 y 59/2003.

Tercero.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, reconoció el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos y los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa en las relaciones entre las Administraciones Públicas, partiendo de un principio general de cooperación entre administraciones para el impulso de la administración electrónica. También se regulan las relaciones de los ciudadanos con las administraciones con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas derogó, con efectos 2 de octubre de 2016, la Ley 11/2007, de 22 de junio. Esta Ley consolida el derecho de los ciudadanos a relacionarse, preferentemente por medios electrónicos, con las administraciones públicas admitiendo diversos sistemas electrónicos para identificación y firma por parte de los interesados, siendo, no obstante, obligatoria la utilización de medios electrónicos para trámites administrativos a determinados colectivos (personas jurídicas, entidades sin personalidad jurídica, profesionales colegiados, etc.), según las normas de desarrollo.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, antes mencionada, recoge, con las adaptaciones necesarias, las normas hasta ahora contenidas en la Ley 11/2007, de 22 de junio, en lo relativo al funcionamiento electrónico del sector público, y algunas de las previstas en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la anterior. La Ley establece que la utilización de los medios electrónicos ha de ser lo habitual, como la firma y sedes electrónicas, el intercambio electrónico de datos en entornos cerrados de comunicación y la actuación administrativa automatizada. Se establece asimismo la obligación de que las Administraciones Públicas se relacionen entre sí por medios electrónicos, previsión que se desarrolla posteriormente en el título referente a la cooperación interadministrativa mediante una regulación específica de las relaciones electrónicas entre las Administraciones. Para ello, también se contempla como nuevo principio de actuación la interoperabilidad de los medios electrónicos y sistemas y la prestación conjunta de servicios a los ciudadanos.

El capítulo V del título Preliminar de la Ley 40/2015, de 1 de octubre, regula, específicamente, el funcionamiento electrónico del sector público, integrado por la Administración General del Estado, las Administraciones de las Comunidades Autónomas, las Entidades que integran la Administración Local y el Sector Público Institucional.

Cuarto.

La FNMT-RCM ha desarrollado, desde 1999, diversas infraestructuras de clave pública (PKI), que cubren las necesidades de la Ley 39/2015, de 1 de octubre, y Ley 40/2015, de 1 de octubre, soluciones que son potencialmente extensibles a otras Administraciones Públicas.

Estas PKI se han puesto en marcha obedeciendo a los siguientes criterios:

- Aprovechamiento de la experiencia acumulada en el proyecto de Certificación Española CERES, que constituye el núcleo de la infraestructura de clave pública.
- Reducción de riesgos en la consolidación de la «Administración sin papeles».
- Economía de medios, derivada de la experiencia existente con CERES y transferencia de tecnologías entre Administraciones Públicas.
- Reutilización de tecnologías, equipamientos, tarjetas y aplicaciones actualmente en uso.

Quinto.

Por otra parte, el Real Decreto 589/2005, de 20 de mayo, por el que se reestructuran los órganos colegiados responsables de la Administración electrónica, estableció, en su Disposición adicional cuarta, que la prestación de los servicios de certificación y firma electrónica realizados por la FNMT-RCM en el ámbito público, se desarrollarán de acuerdo con las normas que le son de aplicación y tendrá la consideración de proyecto de interés prioritario. Este Real Decreto fue derogado por el Real Decreto 806/2014, de 19 de septiembre, sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus Organismos Públicos, que mantiene, en su artículo 11, este tipo de proyectos cuando tengan como objetivo la colaboración y cooperación con las comunidades autónomas y los entes que integran la Administración local y la Unión Europea en materia de Administración digital.

Sexto.

El régimen de colaboración administrativa entre la FNMT-RCM y el CSN en cuanto al ejercicio de las respectivas competencias se instrumenta a través del presente Convenio, de acuerdo con lo previsto en los artículos 47 y siguientes y la Disposición adicional séptima, de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que dispone que la Administración General y los Organismos públicos, vinculados o dependientes de la misma, podrán celebrar convenios de colaboración (en este caso interadministrativos) con los órganos correspondientes para la utilización de medios, servicios y recursos en el ejercicio de competencias propias o delegadas.

De acuerdo con lo expuesto, ambas partes formalizan el presente Convenio de Colaboración Interadministrativa, de conformidad con las siguientes

## CLÁUSULAS

Primera. *Objeto.*

Constituye la finalidad de este Convenio de Colaboración, la creación del marco de actuación institucional entre las dos partes firmantes, que permita el impulso de servicios públicos electrónicos y el cumplimiento de los derechos de acceso electrónico de los ciudadanos a los servicios públicos reconocidos en la Ley 39/2015 y 40/2015, ambas de 1 de octubre, a través de la extensión al ámbito de competencias del CSN de la Plataforma Pública de Certificación y de servicios electrónicos, informáticos y telemáticos desarrollada por la FNMT-RCM para su uso por las diferentes Administraciones.

En particular, la actividad de la FNMT-RCM comprenderá:

1. La extensión de la Plataforma Pública de Certificación mediante la implementación de las actividades que al efecto se enumeran en los capítulos I y III, del anexo I, de este

Convenio, tanto para identificación de las Administraciones Públicas, como de los ciudadanos (según las leyes citadas).

1.2.1 Expedición y gestión del ciclo de vida de certificados de usuario para personas físicas que se encuentren colegiadas o presten sus servicios en el ICGSB, a través de la AC USUARIOS.

1.2.2 Expedición y gestión del ciclo de vida de 15 certificados de componente, recogidos en el capítulo II del anexo I.

Segunda. *Ámbito de aplicación.*

1. El ámbito de aplicación del presente Convenio es el CSN, sus órganos y unidades administrativas.

2. No forman parte del presente Convenio, los organismos y entidades de derecho público o privado, integrantes del Sector Público Institucional, dependientes de la Administración contratante.

Tercera. *Actividad de las partes.*

De acuerdo con el régimen de competencias y funciones propias de cada parte, corresponde a la FNMT-RCM, de acuerdo con lo dispuesto en el objeto de este Convenio y en la normativa referida en el mismo, la puesta a disposición del CSN de la Plataforma Pública de Certificación desarrollada para la Administración Electrónica, para ofrecer seguridad en la utilización de instrumentos de identificación electrónica por parte de los ciudadanos. Estas Plataformas, junto con otras funcionalidades adicionales como el Sellado de Tiempo, permiten, a la FNMT-RCM, la realización de las actividades de carácter material y técnico en el ámbito de la securización de las comunicaciones, de la certificación y firma electrónica, con efectos en el ámbito público y para todos los ciudadanos del territorio nacional que opten por el acceso electrónico a través de esta Entidad, cumpliendo, por tanto, con su mandato de extensión de la Administración Electrónica.

De otra parte, corresponde al CSN la realización de las actuaciones administrativas y el desarrollo de sus competencias dirigidas a la implementación de las Plataformas en sus procedimientos, extendiéndose a la identificación y registro de sus empleados, así como, en su caso, la acreditación y valoración de la identidad y capacidad, de los ciudadanos, que ejerzan los derechos de acceso electrónico a los Servicios Públicos del CSN y el resto de actividades recogidas en este Convenio.

Para la adecuada consecución del objeto de este Convenio, las partes han de desplegar una serie de actuaciones de colaboración, que son:

1. La FNMT-RCM, realizará las siguientes actuaciones:

1.1 De carácter material, administrativo y técnico:

- Aportar la infraestructura técnica y organizativa adecuada para procurar la extensión e implementación de las Plataformas, con las funcionalidades previstas para el desarrollo de las relaciones administrativas de los ciudadanos, a través de sistemas EIT y de conformidad con lo contenido en el objeto, los Anexos y el estado de la técnica.

- Aportar los derechos de propiedad industrial e intelectual necesarios para tal implementación, garantizando su uso pacífico. La FNMT-RCM, excluye cualesquiera licencias o sublicencias, a terceras partes o al CSN, para aplicaciones y sistemas del CSN o de terceros, distintas de las aportadas para ser utilizadas, en calidad de usuarios, directamente por la FNMT-RCM, en virtud de este Convenio.

- Asistencia técnica, de conformidad con lo establecido en los Anexos, con objeto de facilitar al CSN la información necesaria para el buen funcionamiento de los sistemas.

- Actualización tecnológica de los sistemas, de acuerdo con el estado de la técnica y los Esquemas Nacionales de Interoperabilidad y Seguridad, sin perjuicio de la aprobación

de los requisitos técnicos correspondientes por la Comisión de Estrategia TIC o, en su caso, por el órgano competente.

- Aportar la tecnología necesaria para que las obligaciones del CSN puedan ser realizadas; en particular las aplicaciones necesarias para la constitución de las Oficinas de Registro y Acreditación y la tramitación de las solicitudes de emisión de certificados electrónicos.

- Emisión de informes, a petición del CSN y de los Juzgados, Tribunales y, en su caso, órganos administrativos y/o supervisores competentes, acreditativos de la actividad realizada por la FNMT-RCM en virtud del presente Convenio.

- Tener disponible para consulta del CSN 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:

<https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion>.

Esta DPC, podrá ser consultada por todos los interesados y podrá ser modificada por la FNMT-RCM, por razones legales o de procedimiento. Las modificaciones en la DPC serán comunicadas a los usuarios a través de avisos en la dirección Web de la FNMT. En relación con la DPC, y sus anexos, es necesario tener en cuenta la Declaración de Prácticas de Certificación General y las Políticas y Prácticas de Certificación Particulares para cada tipo de certificado o ámbito de los mismos.

En todo caso, los medios técnicos y tecnología empleados por la FNMT-RCM permitirán demostrar la fiabilidad de la actividad de certificación electrónica, la constatación de la fecha y hora de expedición, suspensión o revocación de un certificado, la fiabilidad de los sistemas y productos (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, a través de las Oficinas de Registro y Acreditación autorizadas y, en su caso, —exclusivamente frente a la parte o entidad a través de la cual se ha identificado y registrado al titular del certificado— los atributos pertinentes, así como, en general, los que resulten de aplicación de conformidad con la normativa comunitaria o nacional correspondiente.

1.2 De desarrollo de las facultades establecidas en su normativa específica, realizando su actividad en los términos y con los efectos previstos en el Real Decreto 1317/2001, de 30 de noviembre, en especial:

- Funciones de comprobación, coordinación y control de las Oficinas de Registro y Acreditación, sin perjuicio de su dependencia, orgánica y funcional, de la Administración u organismo público a que pertenezcan.

- Resolución de los recursos y reclamaciones de competencia de la FNMT-RCM derivadas de la actividad convenida.

- Comunicación Dirección General de Tecnologías de la Información y las Comunicaciones a los efectos de coordinación e interoperabilidad correspondientes para el desarrollo de la Administración electrónica.

2. El CSN realizará las siguientes actuaciones:

2.1 De carácter administrativo y de desarrollo de sus competencias:

- Emitir, cuando proceda, el recibo de presentación firmado electrónicamente, donde se haga constancia expresa de la fecha y hora de recepción de las comunicaciones recibidas, de conformidad con lo dispuesto en la normativa aplicable.

- Conservar las notificaciones, comunicaciones o documentación emitida y recibida en las transacciones y actos durante el tiempo pertinente.

- Cifrar las comunicaciones emitidas y recibidas.

- Realizar las actividades de autoridad de registro consistentes en la identificación previa a la obtención del certificado electrónico y, en su caso, de comprobación y suficiencia de los atributos correspondientes, cargo y competencia de los firmantes/custodios, a través de la Oficina de Registro acreditada ante la FNMT-RCM.

- Reconocer el carácter universal de los certificados de firma electrónica que expide la FNMT-RCM y que, por tanto, servirán para las relaciones jurídicas que mantengan los usuarios con las diferentes Administraciones públicas y, en su caso, en el ámbito privado que admitan la utilización de estos certificados, en sus registros, procedimientos y trámites. De esta forma, los certificados que haya expedido o expida la FNMT-RCM, para otros órganos, organismos y administraciones en el ámbito público de actuación, podrán ser utilizados por los usuarios en sus relaciones con el CSN cuando así lo admita el ordenamiento jurídico.

- Resolver los recursos y reclamaciones de su competencia.

Régimen de las Oficinas de Registro y Acreditación.

– General.

El número y ubicación de las Oficinas de Registro y Acreditación donde se llevarán a cabo las actividades de identificación, recepción y tramitación de solicitudes de expedición de certificados electrónicos será informado a la FNMT-RCM, así como cualquier modificación o alteración de dicha relación o de la ubicación de las Oficinas.

Las aplicaciones informáticas necesarias para llevar a cabo las actividades de acreditación e identificación serán facilitadas por la FNMT-RCM. Tales aplicaciones serán tecnológicamente compatibles en función de los avances tecnológicos y el estado de la técnica.

Las solicitudes de emisión y revocación y/o suspensión, en su caso, de certificados se ajustarán a los modelos aprobados por la FNMT-RCM y a los procedimientos recogidos en la Declaración de Prácticas de Certificación de la Entidad accesible como en la dirección:

<https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion>.

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

El CSN dispondrá de Oficina u Oficinas de Registro y Acreditación que deberán contar con los medios informáticos precisos para conectarse telemáticamente con la FNMT-RCM. En ellas, la acreditación e identificación de los solicitantes de los certificados exigirá la comprobación de su identidad y de su voluntad de que sea expedido un certificado electrónico y, en su caso, de las facultades de representación, competencia e idoneidad para la obtención del certificado correspondiente, verificándose de conformidad y con pleno respeto a lo dispuesto en la normativa aplicable.

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

– Para los servicios de la Ley 40/2015.

Las Oficinas de Registro y Acreditación del CSN para el ámbito de la Ley 40/2015, dependerán orgánica y funcionalmente de esta Administración (sin perjuicio de las funciones de comprobación, coordinación y control de la FNMT-RCM) y determinarán la identidad y competencia del propio CSN y la de los diferentes usuarios (firmantes/custodios) designados por la Administración suscriptora de los certificados, de conformidad

con la DPC General y las Políticas y Prácticas de Certificación Particulares de Administración Pública, disponibles para consulta en la web:

<https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion>.

A tal efecto, el CSN dispondrá de la/las Oficinas de Registro y Acreditación que considere necesarias para la acreditación de este tipo de certificados y deberán contar con los medios informáticos precisos para conectarse telemáticamente con la FNMT-RCM y realizar las solicitudes de emisión de los certificados. En estas Oficinas de Registro, donde se acreditarán e identificarán a los titulares y custodios de los certificados, se exigirá la comprobación de su identidad, del cargo y de las facultades de representación, competencia e idoneidad para la obtención del certificado correspondiente y de la voluntad del titular del certificado, verificándose de conformidad y con pleno respeto a lo dispuesto en la normativa aplicable.

#### Cuarta. *Financiación.*

Las partes de este Convenio asumirán cada una los costes por la actividad desplegada en el mismo de acuerdo con sus competencias.

No obstante, el CSN asume la obligación de financiar las actuaciones desarrolladas por la FNMT-RCM, desarrolladas específicamente para el CSN en el marco competencial de actuación de esta administración, de conformidad con lo que se relaciona a continuación:

1. Reembolso de gastos por colaboración administrativa en materia de certificación Electrónica sobre la base del artículo 81 (Ciudadanos/Empresas).

La FNMT-RCM, como compensación por las actividades desarrolladas, percibirá por su actividad de extensión de la Administración Electrónica en el CSN (según el capítulo I, del anexo I, y calculada de acuerdo con el artículo 30 del Estatuto de la FNMT-RCM), la cantidad de cinco mil euros al año (5.000,00 euros/año), impuestos no incluidos.

Tanto durante el primer año, como en el de las eventuales prórrogas, si hubiera petición expresa, por parte del CSN, de extensión de otras funcionalidades de entre las recogidas en el capítulo II, del anexo I distintas a las establecidas en el objeto de este Convenio, podrá formalizarse un pedido adicional y la cantidad anterior quedaría incrementada por el importe correspondiente que se dedujera de la aplicación de las tablas de los capítulos I y II, del anexo II, de Precios y Plan de Implantación, del presente Convenio en función de las actividades prestadas.

2. Reembolso de gastos por colaboración administrativa sobre la base de la Ley 40/2015 (Empleado/Sede/Sello). En caso de ser solicitada la activación de estos servicios de forma expresa por parte del CSN, la FNMT-RCM, como compensación por las actividades desarrolladas, percibirá por su actividad de extensión de la Administración Electrónica en el CSN dentro del ámbito de la Ley 40/2015 recogida en el capítulo III del anexo I, la cantidad de cinco mil euros al año (5.000,00 euros/año), impuestos no incluidos.

Si hubiera petición expresa, por parte del CSN, de extensión de otras funcionalidades de entre las recogidas en el capítulo III, del anexo I distintas a las establecidas en el objeto de este Convenio, podrá formalizarse un pedido adicional y la cantidad anterior quedaría incrementada por el importe correspondiente que se dedujera de la aplicación de las tablas del capítulo III del anexo II, de Precios y Plan de Implantación, del presente Convenio en función de las actividades prestadas.

3. Reembolso total. La cantidad total anual de compensación, a la FNMT-RCM, por aplicación del Convenio asciende a 5.000,00 euros/año, impuestos no incluidos. Siendo el IVA de aplicación un 21% de dicho importe (1.050,00 euros), la compensación total anual es de 6.050,00 euros, IVA incluido.

En caso de ser solicitada la activación de los servicios sobre la base de la Ley 40/2015 de forma expresa de forma expresa por parte del CSN, la cantidad total de compensación, a la FNMT-RCM, por aplicación del Convenio en un año asciende a doce mil cien euros al año (12.100,00 euros/año), impuestos incluidos.

Esta cantidad se obtiene de la suma de las cantidades establecidas en los apartados 1 y 2 anteriores, sin perjuicio de su incremento por petición de funcionalidades adicionales. Para sucesivos años, se aplicará el mismo criterio en función de las compensaciones a percibir, servicios solicitados y prórrogas del Convenio.

4. Facturación. La FNMT-RCM, podrá realizar facturaciones semestrales contra certificaciones o autorizaciones parciales conformadas por el CSN mediante el prorrateo de la cantidad anual a abonar pudiendo, además, liquidar en tales facturas mensuales aquellos servicios adicionales solicitados. El abono de las facturas se realizará mediante transferencia bancaria a la cuenta de la FNMT-RCM: Código cuenta: 0182 2370 49 0208501334, IBAN: ES28 0182 2370 4902 0850 1334, código BIC: BBVAESMM), en un plazo no superior a treinta días de la fecha de factura.

Las facturas de la FNMT-RCM se emitirán a nombre de:

Denominación: Consejo de Seguridad Nuclear. Registro General.

Domicilio: Pedro Justo Dorado Dellmans, 11.

Población: 28040 Madrid.

Provincia: Madrid.

NIF: Q2801036A.

Departamento o persona de contacto/Teléfono: .....

Referencia: .....

6. Servicios de validación. De conformidad con el artículo 24.4 del «Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE», la puesta a disposición de la información sobre el estado de validez de los certificados reconocidos o cualificados, que emita la FNMT-RCM, no tendrán coste para las Administraciones Públicas.

#### Quinta. *Plazo de duración.*

El presente Convenio entrará en vigor el día de su firma, y su duración se extenderá hasta el 31 de diciembre de 2017, teniendo en cuenta lo establecido en la cláusula duodécima.

La duración del Convenio podrá prorrogarse, por años naturales, hasta un máximo de dos prórrogas, si así lo acordaran las partes antes de su vencimiento.

El régimen de colaboración administrativa prevista en este Convenio más allá de su duración inicial y, en su caso, las dos posibles prórrogas solo podrá realizarse por nuevo Convenio.

#### Sexta. *Revisión.*

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

#### Séptima. *Comisión.*

A instancia de cualquiera de las partes, podrá constituirse una Comisión Mixta con funciones de vigilancia y control, así como de resolución de cuestiones derivadas de los problemas de interpretación y cumplimiento del presente Convenio.

#### Octava. *Responsabilidad.*

La FNMT-RCM y el CSN a los efectos previstos en el objeto de este Convenio, responderán cada una en el ámbito de sus respectivas funciones y competencias, en relación con 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 del presente Convenio.

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

*Novena. Resolución y extinción del Convenio.*

El Convenio podrá resolverse a instancia de la parte perjudicada, cuando existieran incumplimientos graves de las respectivas obligaciones atribuidas en este instrumento.

La FNMT-RCM podrá instar la resolución del Convenio por el incumplimiento grave de las obligaciones correspondientes al CSN, en especial, por el incumplimiento de las obligaciones de reembolso de gastos previstas.

Por su parte, el CSN podrá instar la resolución cuando la FNMT-RCM realizara su actividad de carácter material y técnico con manifiesta falta de calidad.

Causas de extinción. Serán causas de extinción:

- El cumplimiento del plazo previsto en Convenio y sus prórrogas.
- El mutuo acuerdo de las partes.

*Décima. Protección de datos.*

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

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

Comunicación de datos. La comunicación de datos de carácter personal que el CSN realice a la FNMT-RCM sobre los datos de los empleados públicos de aquella para la emisión de certificados de firma electrónica en el ámbito de la Ley 40/2015 (y, en su caso, en el de la Ley 66/1997, artículo 81), no requerirá consentimiento del interesado al estar, tal cesión o comunicación, amparada por el artículo 11.2.c) de la Ley Orgánica 15/1999, ya que tal comunicación resulta ineludible para que la FNMT-RCM expida los certificados de firma electrónica a los empleados del CSN.

Acceso a los datos por cuenta de terceros (Encargado del Tratamiento). No tendrá carácter de comunicación de datos el acceso que el CSN en calidad de Oficina de Registro y Acreditación de la FNMT-RCM, realice sobre los datos de carácter personal que la FNMT-RCM mantiene, como responsable del fichero, sobre sus usuarios, personas físicas, con la finalidad de solicitar los servicios EIT en el ámbito del art. 81 de la Ley 66/1997, descritos en el presente Convenio. Tales datos son los que figuran en el fichero regulado, en el número 5 del anexo de la citada Orden EHA/2357/2008.

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

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

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

*Undécima. Derecho aplicable y resolución de conflictos.*

Sin perjuicio de la facultad de las partes de constituir la Comisión Mixta establecida en la cláusula octava, la colaboración administrativa prevista en este Convenio y Anexos en cuanto al contenido y características de los mismos se realizará con sujeción a la regulación contenida en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas; la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público; 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 el resto de disposiciones que sean de aplicación.

El presente Convenio tiene naturaleza administrativa y se regirá por lo expresamente pactado por las partes en este instrumento, por las normas citadas en el mismo y, en su defecto, por las normas de derecho administrativo que resulten de aplicación. Las partes se comprometen a resolver de mutuo acuerdo las incidencias que pudieran surgir en su interpretación y cumplimiento. Las cuestiones litigiosas que se suscitaren entre las partes durante el desarrollo y ejecución del mismo, se someterán, en caso de que sea de aplicación su intervención, al Servicio Jurídico del Estado y, en caso contrario, a la jurisdicción contencioso-administrativa, conforme a lo dispuesto en la Ley reguladora de la misma.

*Duodécima. Aprobación, inicio de la actividad información y publicación.*

El presente Convenio surtirá efectos desde el momento de su firma previa su entrada en vigor previa aprobación o siempre que sea ratificado, según proceda, por el Consejo de Administración de la FNMT-RCM. En caso de ratificación, la FNMT-RCM, comunicará al CSN tal hecho para su constancia y efectos.

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

Y, en prueba de conformidad, ambas partes suscriben el presente Convenio de Colaboración Interadministrativa y todos sus Anexos, en el lugar y fecha indicados en el encabezamiento.—El Director General de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, Jaime Sánchez Revenga.—El Presidente del Consejo de Seguridad Nuclear, Fernando Marti Scharfhausen.

## ÍNDICE DE ANEXOS

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

- Capítulo I. Servicios EIT (artículo 81, Ley 66/1997).
- Capítulo II. Servicios avanzados.
- Capítulo III. Servicios APE (Ley 40/2015).

Anexo II. Precios y Plan de Implantación.

- Capítulo I. Servicios EIT (art. 81, Ley 66/1997).
- Capítulo II. Servicios avanzados.
- Capítulo III. Servicios AP (Ley 40/2015).

## ANEXO I

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

#### CAPÍTULO I

#### Servicios Eit

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

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

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

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

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

#### *Generación y gestión de claves*

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

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

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

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

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

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

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

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

### *Registro de usuarios*

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

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

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

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

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

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

En caso de que solicite un certificado de persona jurídica, será de aplicación el procedimiento de verificación de la identidad del solicitante y de comprobación de los datos de constitución de la persona jurídica y de la suficiencia, extensión y vigencia de las facultades de representación del solicitante que se establece en el artículo 13 de la Ley 59/2003, de 19 de diciembre. El detalle del procedimiento figura en la Declaración de Prácticas de Certificación: <https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion>.

Necesidad de presentarse en persona. El procedimiento de registro requiere presencia física del interesado para formalizar el procedimiento de registro en la oficina de

acreditación. No obstante, serán válidas y se dará el curso correspondiente a las solicitudes de emisión de certificados electrónicos cumplimentadas según el modelo aprobado por la FNMT-RCM para este fin siempre que la firma del interesado haya sido legitimada notarialmente en los términos señalados en el referido modelo.

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

Incorporación de la dirección de correo electrónico del titular al certificado. En su caso, la incorporación de la dirección de correo electrónico del titular al certificado se realizará a los efectos de que el certificado pueda soportar el protocolo S/MIME en el caso de que la aplicación utilizada por el usuario así lo requiera.

Cuando la dirección del correo electrónico del titular del certificado conste en una de las extensiones del propio certificado, ni la FNMT-CM, como firmante y responsable del mismo, ni el CSN 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, solo 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 pública 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.

- El CSN garantizará que, al solicitar un certificado electrónico, su titular acepta que:
- a) La clave privada con la que se genera la firma electrónica corresponde a la clave pública del certificado.
  - b) Únicamente el titular del certificado tiene acceso a su clave privada.
  - c) Toda la información entregada durante el registro por parte del titular es exacta.
  - d) El certificado será usado exclusivamente para fines legales y autorizados y de acuerdo con lo establecido por la FNMT-RCM.
  - e) El usuario final del certificado no es un Prestador de Servicios de Certificación y no utilizará su clave privada asociada a la clave pública que aparece en el certificado para firmar otros certificados (u otros formatos de certificados de clave pública), o listados de certificados, como un Prestador de Servicios de Certificación o de otra manera.
- El CSN 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 al CSN los mecanismos de la transmisión segura para el establecimiento de un servicio continuo e ininterrumpido de comunicación entre ambas a fin de que, por medios telemáticos o a través de un centro de atención telefónica a usuarios, se ponga de inmediato en conocimiento de la FNMT-RCM cualquier circunstancia de que tenga conocimiento y que sea determinante para la suspensión, revocación o extinción de la vigencia de los certificados ya expedidos, a fin de que se pueda dar publicidad de este hecho, de manera inmediata, en el directorio actualizado de certificados a que se refiere el artículo 18 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

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

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

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

#### *Publicación de certificados de clave pública y registro de certificados*

Publicación de certificados de clave pública. La FNMT-RCM publicará los certificados emitidos en un directorio seguro.

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

Esta publicación puede ser:

a) Publicación directa por parte de la FNMT-RCM.—Esta operación la realiza la FNMT-RCM a través de la publicación en un directorio propio. La actualización en el directorio seguro de las listas de revocación se realizará de forma continuada.

La consulta de este directorio se realizará en línea, por acceso directo del usuario. Este servicio permite la disponibilidad continua y la integridad de la información almacenada en el directorio. Las listas de revocación serán firmadas con la clave privada de firma de la FNMT-RCM.

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

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

Control de acceso. En la publicación directa por parte de la FNMT-RCM, el acceso al directorio se realizará con autenticación previa. Este acceso estará restringido a solo lectura y búsqueda, pudiendo utilizar como clave de búsqueda cualquier información contenida en una entrada de un usuario.

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

*Registro de eventos significativos*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

## CAPÍTULO II

### Servicios avanzados

Certificados para servidor o componente y firma de código. La FNMT-RCM emite certificados de componente genérico, de servidor y de firma de código, por lo que se hereda la confianza que representa la FNMT-RCM como Autoridad de Certificación instalada en los navegadores de Microsoft.

- Certificado SSL/TLS estándar: es aquel que permite establecer comunicaciones seguras con sus clientes utilizando el protocolo SSL/TLS. Este tipo de certificados garantiza la identidad del dominio donde se encuentra su servicio Web

- Certificado wildcard: Identifica todos los sub-dominios asociados a un dominio determinado, sin necesidad de adquirir y gestionar múltiples certificados electrónicos. Por ejemplo, el certificado wildcard emitido a «\*.ejemplo.es» garantiza la identidad de dominios como compras.ejemplo.es, ventas.ejemplo.es o altas.ejemplo.es.

- Certificado SAN: El certificado de tipo SAN, también conocido como certificado multidominio, UC o Unified Communications Certificates, le permite securizar con un solo certificado hasta doce dominios diferentes.

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

- Certificado de sello de entidad es aquel que se utiliza habitualmente para establecer conexiones seguras entre componentes informáticos genéricos. Su flexible configuración permite dotarle de diferentes usos:

- Autenticación de componentes informáticos de una Entidad en su acceso a servicios informáticos, o a otras infraestructuras tecnológicas, con acceso restringido o identificación de cliente.

- Intercambio de mensajes o datos cifrados con garantías de confidencialidad, autenticación e integridad.

## CAPITULO III

### Servicios administración pública (Ley 40/2015)

Servicio de Validación del Certificado de la AC Administración Pública. Para comprobar la validez del certificado de la Autoridad de Certificación de la Administración Pública, se ha dispuesto dos mecanismos para la descarga de la CRL asociada a dicho certificado. Ambos, se encuentran disponibles en el propio certificado de la AC, como CRLDistributionPoints y son, por este orden:

– LDAP.

Localización del servicio ldap para la descarga de la CRL de la AC RAIZ de la FNMT-RCM:

ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC RAIZ FNMT-RCM,O=FNMT-RCM,C=E S?authorityRevocationList?base?objectclass=cRLDistributionPoint.

Este servicio ldap se prestará en su versión 3, en modo binario, estando disponible en el puerto estándar para el servicio ldap (389), y sin requerir ningún tipo de autenticación.

La prestación del servicio será de carácter universal, gratuito, y sin control de acceso, teniendo únicamente la restricción de poder descargarse una única crl en cada conexión realizada que en este caso solo existe una CRL, la ARL.

El acceso a este servicio estará disponible a través de Internet así como a través de la Red SARA.

La CRL emitida para esta infraestructura tendrá un periodo de validez de 3 meses y se publicará 10 días antes de su caducidad y, en cualquier caso, siempre que se revoque algún certificado emitido por la AC RAIZ de la FNMT-RCM.

La FNMT-RCM se reserva el derecho a bloquear el acceso a aquellas direcciones IP para las que se observe un uso indebido o abusivo de este servicio.

– HTTP.

Localización del servicio http para la descarga de la CRL de la AC RAIZ de la FNMT-RCM:

[Http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl](http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl).

La CRL emitida para esta infraestructura tendrá un periodo de validez de 3 meses y se publicará 10 días antes de su caducidad y, en cualquier caso, siempre que se revoque algún certificado emitido por la AC RAIZ de la FNMT-RCM.

La prestación del servicio será de carácter universal, gratuito, y sin control de acceso, teniendo únicamente la restricción de poder descargarse una única crl en cada conexión realizada.

El acceso a este servicio estará disponible a través e Internet así como a través de la Red SARA.

La FNMT-RCM se reserva el derecho a bloquear el acceso a aquellas direcciones IP para las que se observe un uso indebido o abusivo de este servicio.

Servicio de Validación de Certificados de Entidad Final para Administración Pública. El servicio de Validación de Certificados para la infraestructura Administración Pública, se prestará mediante los siguientes servicios:

- Servicio de descarga de CRLs de AC Administración Pública mediante protocolo LDAP.
- Servicio de descarga de CRLs de AC Administración Pública mediante protocolo http.

La disponibilidad de múltiples servicios para la validación de certificados, proporciona compatibilidad total con las distintas necesidades de las aplicaciones en las que deberán integrarse los certificados de Entidad Final emitidos por la infraestructura de la Administración Pública.

Servicio de descarga de CRLs mediante protocolo LDAP. Este servicio será de carácter universal, anónimo, gratuito y si ningún tipo de autenticación, de tal forma que cualquier cliente podrá descargarse la CRL para poder validar un certificado de Entidad Final emitido por la AC Administración Pública.

Este servicio se prestará desde la siguiente URL en el puerto estándar ldap 389:

<ldap://ldapape.cert.fnmt.es/CN=CRLnnn,OU=AC APE, O=FNMT-RCM, C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint>.

Este punto de distribución de CRLs, irá insertado en todos los certificados de Entidad Final emitidos por la AC de la Administración Pública, siendo en cada caso CRLnnn el número de CRL que le corresponde a dicho certificado.

El acceso a este servicio estará disponible a través de Internet así como a través de la Red SARA.

La FNMT-RCM se reserva el derecho a bloquear el acceso a aquellas direcciones IP para las que se observe un uso indebido o abusivo de este servicio.

Servicio de descarga de CRLs mediante protocolo HTTP. Este servicio será de carácter universal, anónimo, gratuito y si ningún tipo de autenticación, de tal forma que cualquier cliente podrá descargarse la CRL para poder validar un certificado de Entidad Final emitido por la AC Administración Pública.

Este servicio se prestará desde la siguiente URL en el puerto estándar http 80:

[Http://www.cert.fnmt.es/crlsape/CRLnnn.crl](http://www.cert.fnmt.es/crlsape/CRLnnn.crl).

Este punto de distribución de CRLs, irá insertado en todos los certificados de Entidad Final emitidos por la AC de la Administración Pública, siendo en cada caso CRLnnn el número de CRL que le corresponde a dicho certificado al igual que el anteriormente descrito.

El acceso a este servicio estará disponible a través de Internet así como a través de la Red SARA.

La FNMT-RCM se reserva el derecho a bloquear el acceso a aquellas direcciones IP para las que se observe un uso indebido o abusivo de este servicio.

Servicio de Sellado de Tiempo para Administración Pública. El servicio de Sellado de Tiempo, se prestará a través de la URL:

[Https://apuseg.cert.fnmt.es/TimeStampAPE/TimeStampServer](https://apuseg.cert.fnmt.es/TimeStampAPE/TimeStampServer).

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

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

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

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

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

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

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

La FNMT-RCM se reserva el derecho a bloquear el acceso a aquellas direcciones Ip para las que se observe un uso indebido o abusivo de este servicio.

### *Certificado de firma electrónica del personal al servicio de las Administraciones Públicas*

FNMT-RCM no regula el uso de este certificado, dado que se establece en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y demás legislación aplicable, limitándose a crear una infraestructura técnica a disposición de la Administración, Organismo o Entidad pública titular correspondiente. Asimismo, todas aquellas circunstancias y requisitos referentes a los usuarios, por la propia naturaleza de los certificados de empleado público, serán controlados, exclusivamente, por la Administración, informando a la FNMT-RCM de su alteración o modificación; todo ello, a través de las Oficinas de Registro habilitadas por las Administraciones, Organismos y Entidades públicas.

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

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

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

La identidad del Firmante y custodio de las Claves (personal al servicio de las Administraciones Públicas que realiza firmas electrónicas utilizando el Certificado en nombre de la Administración actuante), número de identificación personal, cargo, puesto de trabajo y/o condición de autorizado y, al Suscriptor del Certificado, que es el órgano, organismo o entidad de la Administración Pública, bien sea ésta General, autonómica, local o institucional, donde ejerce sus competencias, presta sus servicios, o desarrolla su actividad.

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

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

4. Marco legislativo. El uso del certificado de empleado público se realizará en el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y de conformidad con las competencias de la Administración, Organismo o Entidad pública actuante y de las facultades conferidas a su personal (independientemente de su condición: funcionarial, laboral, estatutaria, etc.) en virtud de su nombramiento, designación, contrato o instrumento jurídico que regule su relación con tales Administraciones.

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

### *Sello electrónico de las Administraciones Públicas*

FNMT-RCM no regula el uso de este certificado, dado que se establece en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y demás legislación aplicable, limitándose a crear una infraestructura técnica a disposición de los usuarios y custodios de la Administración, Organismo o Entidad pública titular del certificado, propietario o responsable de la unidad administrativa y del componente informático correspondiente. Asimismo, todas aquellas circunstancias y requisitos referentes a los usuarios y custodios, por la propia naturaleza de los certificados de Sello electrónico de las AA.PP., serán controlados, exclusivamente, por la Administración, informando a la FNMT-RCM de su alteración o modificación; todo ello, a través de las Oficinas de Registro habilitadas por las Administraciones, Organismos y Entidades públicas.

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

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

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

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

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

3) Marco legislativo. El uso del certificado de Sello electrónico de las AA.PP. se realizará en el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector

Público, y de conformidad con las competencias de la unidad perteneciente a la Administración, Organismo o Entidad pública titular de la misma y de la infraestructura que alberga el certificado de Sello electrónico de las AA.PP.

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

#### *Sedes electrónicas de las Administraciones Electrónicas*

FNMT-RCM no regula el uso de este certificado, dado que se establece en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y demás legislación aplicable, limitándose a crear una infraestructura técnica a disposición de los usuarios y custodios de la Administración, Organismo o Entidad pública titular de la Sede electrónica correspondiente. Asimismo, todas aquellas circunstancias y requisitos referentes a los usuarios y custodios, por la propia naturaleza de los certificados para la identificación de Sedes electrónicas, serán controlados, exclusivamente, por la Administración, informando a la FNMT-RCM de su alteración o modificación; todo ello, a través de las Oficinas de Registro habilitadas por las Administraciones, Organismos y Entidades públicas.

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

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

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

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

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

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

## **ANEXO II**

### **Precios y plan de implantación**

#### **CAPÍTULO I**

#### **Servicios EIT**

1. Precio anual de los servicios. Se establece un precio fijo para los servicios de 5.000,00 euros al año, impuestos no incluidos.

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

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

3. Réplica de Directorio para los servicios EIT. Se establece un precio de 20.539,66 euros/año por la réplica diaria de las listas de certificados revocados desde la FNMT-RCM a las instalaciones del conviniente por redes públicas. Este precio incluye la licencia de uso del directorio X.500 InJoin Directory Server de Critical Path en las propias instalaciones del cliente.

Este servicio no incluye la instalación ni el mantenimiento, que serán por cuenta del conviniente.

El directorio y su contenido no podrá ser cedido a terceros bajo ningún concepto, y deberá ser protegido contra todo acceso por entidades ajenas al conviniente, incluyendo el acceso de consulta.

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

## CAPÍTULO II

### Servicios avanzados

1. Certificados para servidor o componente y firma de código. El precio anual establecido en el apartado 1 del capítulo I del presente anexo de Precios incluye un número máximo de 15 certificados de componente.

El precio de los certificados adicionales será el estipulado en el apartado correspondiente de la página web de Ceres:

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

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

## CAPÍTULO III

### Servicios administración pública (Ley 40/2015)

1. Certificados para los servicios del ámbito de la Ley 40/2015. En caso de ser solicitada la activación de forma expresa por parte del CSN, el precio anual para los servicios del ámbito de la Ley 40/2015 asciende a 5.000,00€ Euros/año impuestos no incluidos, incluye la emisión de 1 certificado de sede electrónica y 3 certificados de sello electrónico para actuaciones automatizadas, así como los todos certificados de empleado público que el conviniente requiera.

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

2. Servicio de autoridad de Sellado de Tiempo para Administración Pública. El precio anual de los servicios del ámbito de la Ley 40/2015 establecido en el apartado 1 del capítulo III del presente anexo II de Precios incluye el servicio de Sellado de Tiempo para Administración Pública junto con un certificado de firma electrónica necesario para la suscripción de las peticiones de sellados. La FNMT-RCM no aceptará certificados de firma electrónica de Prestadores de Servicios de Certificación no reconocidos por la propia FNMT-RCM.

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

*Plan de Implantación (Tentativo)*

Entrega de documentación y productos.

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

Acreditación de encargados de acreditar.

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

Implantación de aplicativos.

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

Comunicación a los usuarios de los nuevos servicios.

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