

# Boletín Oficial

## DE LA PROVINCIA DE TOLEDO



Depósito Legal: TO - 1 - 1958

Franqueo Concertado: Núm. 45/2

**ADVERTENCIA OFICIAL**

Las Leyes entrarán en vigor a los veinte días de su completa publicación en el «Boletín Oficial del Estado», si en ellas no se dispone otra cosa (artículo 2 del Código Civil).

De acuerdo con lo previsto en el segundo párrafo del apartado 1 del artículo 6 de la Ley 5 de 2002, de 4 de abril, reguladora de los Boletines Oficiales de la Provincia, las órdenes de inserción de los anuncios, edictos, circulares y demás disposiciones que hayan de insertarse en el «Boletín Oficial» de la provincia de Toledo, se remitirán al «Ilmo. Sr. Presidente de la Diputación Provincial de Toledo. Registro de Edictos y Anuncios «Boletín Oficial» de la provincia de Toledo, en el supuesto de Administraciones Públicas o Administración de Justicia, por el órgano competente de la Administración anunciante, o en otro supuesto, por la persona que en cada caso compete.

El orden de inserción correspondiente respetará los plazos previstos en el artículo 7.3 de la citada Ley 5 de 2002, de 4 de abril.

**ANUNCIOS**

**Por cada línea o fracción de 18 centímetros: 1,56 euros.**

El importe de las tarifas a aplicar a los anuncios insertados con carácter **urgente** será, en cada caso, el doble de las establecidas anteriormente.

**ADMINISTRACIÓN**

Plaza de la Merced, 4. Teléfono 925 25 93 00.-Diputación Provincial

Se publica todos los días (excepto los sábados, domingos y días festivos)

**PAGOS POR ADELANTADO**

### Diputación Provincial de Toledo

#### ORGANISMO AUTÓNOMO PROVINCIAL DE GESTIÓN TRIBUTARIA DE TOLEDO

##### ADENDA DE MODIFICACIÓN A LA ENCOMIENDA POR LA QUE EL ORGANISMO AUTÓNOMO PROVINCIAL DE GESTIÓN TRIBUTARIA DE TOLEDO ENCOMIENDA A LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE – REAL CASA DE LA MONEDA, LA EXTENSIÓN DE LOS SERVICIOS PÚBLICOS ELECTRÓNICOS

En Madrid, en la fecha de firma

**REUNIDOS**

De una parte, Don Santiago García Aranda, Presidente del Organismo Autónomo Provincial de Gestión Tributario de Toledo, nombrado por Decreto número 804, de fecha 11 de julio de 2019 (BOP de Toledo número 132, de 16 de julio de 2019), en nombre y representación de este Organismo Autónomo, en virtud de las competencias atribuidas en el artículo 12 de los Estatutos del Organismo Autónomo Provincial de Gestión Tributaria, (BOP de Toledo BOP número 235, de fecha 11 /10/1996) con domicilio institucional en C/ Real nº 4 de Toledo y CIF P9500003J.

Y de otra parte, doña María Isabel Valldecabres Ortiz, Directora General de la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda, nombrada por Real Decreto 726/2021, de 3 de agosto (BOE núm. 185, de 4 de agosto), en nombre y representación de esta Entidad, según el artículo 19.2 del Real Decreto 1114/1999, de 25 de junio, por el que sea aprueba el Estatuto de la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (BOE nº 161, de 7 de julio) con domicilio institucional en Madrid, calle Jorge Juan, 106 y NIF Q2826004J.

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

**EXPONEN**

**PRIMERO.-** Que el ORGANISMO AUTÓNOMO PROVINCIAL DE GESTIÓN TRIBUTARIO DE TOLEDO y la FNMT-RCM suscribieron, con fecha 23 de febrero de 2021, una Encomienda de gestión, cuyo objeto consiste en la prestación de servicios de certificación de firma electrónica y otros servicios relativos a la administración electrónica y de la sociedad de la información, de conformidad con las condiciones que son detalladas en la encomienda.

**SEGUNDO.-** La realización de estas actividades está regulada por el Reglamento (UE) 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.

En el ámbito del derecho interno sobre esta materia, se ha aprobado la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. La función de esta Ley es complementar al Reglamento europeo en aquellos aspectos concretos que no han sido armonizados y cuyo desarrollo su prevé en los ordenamientos de los diferentes Estados miembros, cuyas disposiciones han de ser interpretadas de acuerdo con él.

En relación con la actividad y efectos de los sistemas de identificación y demás servicios, la Disposición adicional segunda de esta Ley 6/2020, de 11 de noviembre, establece que todos los sistemas de identificación, firma y sello electrónico previstos en la Ley 39/2015, de 1 de octubre, y en la Ley 40/2015, de 1 de octubre, tendrán plenos efectos jurídicos.



**TERCERO.**-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 encomienda de gestión de colaboración, extienda la utilización de la Plataforma Pública de Certificación mediante técnicas y medios electrónicos, informáticos y telemáticos (EIT). Este mismo artículo 81, en su apartado cinco, señala que la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, procurará la máxima extensión de la prestación de los servicios señalados para facilitar a los ciudadanos, las relaciones a través de técnicas y medios EIT con la Administración General del Estado y, en su caso, con las restantes Administraciones.

El apartado nueve de este artículo, cita que, en relación con las actividades de identificación y registro, la FNMT-RCM, podrá celebrar convenios con personas, entidades y corporaciones que ejerzan funciones públicas, en los que se establezcan las condiciones en las que éstas puedan participar en tales actividades.

**CUARTO.**-El Real Decreto 1317/2001, de 30 de noviembre, por el que se desarrolla el artículo 81, antes citado, regula el régimen de prestación de servicios de seguridad por la FNMT-RCM en la emisión y recepción de comunicaciones y escritos a través de medios y técnicas electrónicas, informáticas y telemáticas. Su artículo 6 faculta a la FNMT-RCM para convenir con las entidades incluidas en su ámbito de aplicación, entre las que se encuentra el ORGANISMO AUTÓNOMO PROVINCIAL DE GESTIÓN TRIBUTARIO DE TOLEDO, los términos que deben regir la prestación de sus servicios en relación con las comunicaciones empleando técnicas y medios electrónicos, informáticos y telemáticos.

**QUINTO.**-La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda es una entidad pública empresarial dependiente del Ministerio de Hacienda, a través de la Subsecretaría de este departamento, que ejerce la dirección estratégica y el control de eficacia de la entidad.

El artículo 2 del Estatuto de la FNMT-RCM, aprobado mediante el Real Decreto 1114/1999, de 25 de junio, reconoce como fines de la Entidad la prestación, en el ámbito de las Administraciones Públicas o sus Organismos Públicos, vinculados o dependientes, de servicios de seguridad, técnicos y administrativos, en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT) así como la expedición, fabricación y suministro de títulos o certificados de usuarios, de acuerdo con lo que establezcan las disposiciones legales correspondientes. El apartado 1. h) de este artículo permite a la Entidad realizar actividades o prestación de servicios relacionados con los ramos propios de sus fines para personas o entidades públicas o privadas, tanto nacionales como extranjeras.

**SEXTO.**- Que de acuerdo a lo recogido en su cláusula SEXTA de la encomienda suscrita, las partes podrán proponer en cualquier momento de su vigencia, a efectos de incluir, de mutuo acuerdo, las modificaciones que resulten pertinentes.

**SEPTIMO.**- Estando ambas partes interesadas en procurar la máxima extensión de la prestación de estos servicios para facilitar a los ciudadanos las relaciones administrativas y cumplir con los requerimientos que las normas establecen para las Corporaciones de Derecho Público a través de las técnicas y medios electrónicos, informáticos y telemáticos (EIT), y de conformidad con lo previsto en los apartados cinco y nueve del artículo 81 de la Ley 66/1997, de 30 de diciembre, se procede a la formalización de la presente adenda con arreglo a las siguientes

## CLÁUSULAS

### PRIMERA.- MODIFICACIÓN CLÁUSULA PRIMERA OBJETO

La cláusula PRIMERA "Objeto" quedará redactada de la siguiente manera:

Constituye la finalidad de esta Encomienda la creación del marco de actuación institucional entre las dos partes firmantes, que permita el impulso de servicios públicos electrónicos del Organismo Autónomo Provincial de Gestión Tributario de Toledo, a través de la extensión al ámbito de competencias del Organismo Autónomo Provincial de Gestión Tributario de Toledo 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:

La extensión de la Plataforma Pública de Certificación mediante la implementación de las actividades que al efecto se enumeran en los Capítulos I, II y III, del Anexo I, de esta encomienda, para identificación de la ciudadanía y de las Administraciones Públicas.

1.1. Expedición y gestión del ciclo de vida de certificados recogidos en la Ley 40/2015, de 1 de octubre y mantenimiento de las Plataformas seguras de gestión de certificados: Certificados de Personal, Certificados de Sede Electrónica (autenticación de sitio Web) y Certificados de Sello Electrónico de Administración Pública:

- certificados de empleado/a público/a ilimitados
- 5 certificados de sello electrónico para la Administración Pública
- 1 certificado de sede electrónica para la Administración Pública
- 1.2.- Servicio sellado de tiempo
- 1.3.- Certificados de componente:
  - 1 certificado de componente (SSL estándar)
  - 1 certificado de componente (wildcard)



También podrá integrar a petición del Organismo Autónomo Provincial de Gestión Tributario de Toledo cualquiera, o la totalidad, de las funcionalidades y actividades que se enumeran en los Capítulos I y II, del mismo Anexo I, de esta Encomienda.

2. Reconocimiento y validación de certificados a través de la Plataforma de Validación Multi-AC de la FNMT-RCM, de acuerdo con lo previsto en la disposición adicional quinta del Real Decreto 1671/2009, por el que se desarrolló parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

#### **SEGUNDA.- MODIFICACIÓN DEL REEMBOLSO DE GASTOS DE LA CLÁUSULA CUARTA**

La Cláusula Cuarta de título "Financiación" en su punto 1 quedará redactada de la siguiente forma:

1- REEMBOLSO DE GASTOS POR LA REALIZACIÓN DE ACTIVIDADES EN MATERIA DE CERTIFICACIÓN ELECTRÓNICA.

La FNMT-RCM como compensación por las actividades, de carácter material o técnico, realizadas según los Capítulos I, II y III del Anexo I, al Organismo Autónomo Provincial de Gestión Tributaria de Toledo percibirá, anualmente, la cantidad total de dos mil novecientos cincuenta euros al año (2.950,00 €) IVA excluido.

Siendo el IVA de aplicación un 21% de dicho importe (619.50 euros), la compensación total anual es de 3.569,50 Euros, IVA incluido.

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

Si hubiera petición expresa, por parte del Organismo Autónomo Provincial de Gestión Tributario de Toledo, de extensión de otras funcionalidades de entre las recogidas en los Capítulos I, II y III, del Anexo II, la cantidad anterior quedaría incrementada por el importe correspondiente que se dedujera de la aplicación de las tablas contenidas en dicho Anexo II, de Precios y Plan de Implantación, del presente Encomienda.

#### **TERCERA.- MODIFICACIÓN DE ANEXOS**

Se adjunta la modificación de los correspondientes anexos de la Encomienda suscrita entre el ORGANISMO AUTÓNOMO PROVINCIAL DE GESTIÓN TRIBUTARIO DE TOLEDO y la FNMT-RCM.

#### **CUARTA.-**

Quedan subsistentes y sin alteración alguna, el resto de condiciones que integran la Encomienda suscrita entre el ORGANISMO AUTÓNOMO PROVINCIAL DE GESTIÓN TRIBUTARIO DE TOLEDO y la FNMT-RCM.

#### **QUINTA.- ENTRADA EN VIGOR Y DURACIÓN.**

La presente adenda entrará en vigor el día de su firma y tendrá la misma vigencia del Encomienda de la que trae causa.

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

### **ANEXO I**

#### **CAPITULO I - SERVICIOS EIT**

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

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

El certificado será 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 apartado 4 del Artículo 7 de la Ley 6/2020, de 11 de noviembre. 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-RCM, como firmante y responsable del mismo, ni el Organismo Autónomo Provincial de Gestión Tributario de Toledo 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 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 Organismo Autónomo Provincial de Gestión Tributario de Toledo 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 Organismo Autónomo Provincial de Gestión Tributario de Toledo garantizará que, al solicitar un certificado electrónico, su titular asume las siguientes obligaciones en el uso de clave privada:

a) A conservar su control.

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

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

#### **Revocación y suspensión de certificados electrónicos**

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

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



- b) Resolución judicial o administrativa que lo ordene.
- c) Fallecimiento o extinción de la personalidad del usuario o incapacidad sobrevenida.
- d) Finalización del plazo de vigencia del certificado.
- e) Pérdida o inutilización por daños en el soporte del certificado.
- f) Utilización indebida por un tercero.
- g) Inexactitudes graves en los datos aportados por el usuario para la obtención del certificado.
- h) Cualquier otra prevista en la normativa vigente.

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

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

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

La extinción de la condición de usuario público se regirá por lo dispuesto en la presente Orden de encargo 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 el Organismo Autónomo Provincial de Gestión Tributario de Toledo 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 apartado 4 del artículo 9 de la Ley 6/2020, de 11 de noviembre, de Servicios electrónicos de confianza,

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 Organismo Autónomo Provincial de Gestión Tributario de Toledo 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. 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 sólo 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 sólo acceso de lectura, estando restringido a las personas autorizadas por la FNMT-RCM.

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

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

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

## **CAPITULO II - SERVICIOS AVANZADOS**

### **Certificados de componente**

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 principales.

-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 subdominios 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 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.

#### **Servicio de Sellado de Tiempo**

-La FNMT-RCM, es un Prestador de Servicios de Confianza, entre los que se incluye el Sellado de Tiempo o creación de sellos cualificados de tiempo electrónicos, conforme al Reglamento eIDAS, cuyo objeto es dar fe de la existencia de un conjunto de datos en un instante determinado en la línea de tiempo. Para ello utiliza como fuente de información temporal vinculada al Tiempo Universal Coordinado (UTC) la proporcionada por la Sección de Hora del Real Instituto y Observatorio de la Armada (ROA) en San Fernando, mediante el acuerdo alcanzado entre dicha Entidad y la FNMT-RCM para la sincronización continua de sus sistemas. El ROA tiene como misión el mantenimiento de la unidad básica de tiempo, declarado a efectos legales como Patrón Nacional de dicha unidad, así como el mantenimiento y difusión oficial de la escala “Tiempo Universal Coordinado” (UTC -ROA), considerada a todos los efectos como la base de la hora legal en todo el territorio español (Real Decreto 1308/1992, de 23 octubre 1992).

- El Sistema de Sincronismo con el Real Observatorio de la Armada (SS-ROA) instalado en el Centro de Proceso de Datos (CPD) de la FNMT-RCM tiene como objetivo proporcionar una fuente de referencia temporal trazable a la escala de tiempo UTC (ROA), para la prestación del Servicio de Sellado de Tiempo de la FNMT-RCM.

- Dicho sistema produce una serie de ficheros que contienen los datos de los seguimientos efectuados en un día y son utilizados por el ROA para elaborar los informes de diferencia de fase del patrón con la escala UTC (ROA).

-La precisión declarada para la sincronización de la TSU con UTC es de 100 milisegundos, cumpliendo así sobradamente con los requisitos del estándar europeo [ETSI EN 319 421]. Por tanto, el Servicio de Sellado de Tiempo de la FNMT-RCM no expedirá ningún Sello de tiempo electrónico durante el periodo de tiempo en el que existiera un desfase mayor de 100 milisegundos entre los relojes de la TSU y la fuente de tiempo UTC del ROA.

-La FNMT-RCM suministrará a los Departamentos, organismos y entidades del sector público destinatarios de los servicios del presente encargo que así lo soliciten el acceso a este servicio de Sellado de Tiempo.

-Tanto las peticiones de Sellado de Tiempo como las respuestas se gestionarán conforme a lo descrito en la recomendación RFC 3161.

-Las respuestas de la Autoridad de Sellado de Tiempo, del tipo “application/timestamp-reply”, irán firmadas con un certificado con un tamaño de claves RSA de 3072 bits y algoritmo de firma SHA-256 y podrá validarse mediante cualquiera de los métodos de validación de los certificados que la FNMT-RCM pone a disposición de los usuarios y terceras partes que confían en los certificados y que se describe en el apartado anterior.

### **CAPITULO III - SERVICIOS ADMINISTRACIÓN PÚBLICA (LEY 40/2015)**

#### **Servicio de Validación del Certificado de la AC Sector Público**

Para comprobar la validez del certificado de la Autoridad de Certificación de Sector Público, 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=ACRAIZFNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint

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

La prestación del servicio será de carácter universal 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>

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 Sector Público mediante protocolo LDAP.

-Servicio de descarga de CRLs de AC Sector Público 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/Sector Público.

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

<ldap://ldapape.cert.fnmt.es/CN=CRLnnn,OU=ACAPE/SP,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/Sector Público, 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 Sector Público.

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/crlssp/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.

#### **CERTIFICADO DE FIRMA ELECTRONICA DEL PERSONAL AL SERVICIO DE LAS ADMINISTRACIONES PÚBLICAS Y CERTIFICADO DE FIRMA ELECTRÓNICA DEL PERSONAL AL SERVICIO DE LAS ADMINISTRACIONES PÚBLICAS CON SEUDÓNIMO**

Este certificado se emite por la FNMT-RCM por cuenta de la Administración Pública correspondiente a la que la FNMT-RCM presta los servicios técnicos, administrativos y de seguridad necesarios como Prestador Cualificado de Servicios de Confianza.

El certificado para personal al servicio de la Administración Pública es desarrollado por la FNMT-RCM mediante una infraestructura PKI específica y ad hoc, basada en actuaciones de identificación y registro realizadas por la red de Oficinas de Registro designadas por el órgano, organismo o entidad Suscriptora del certificado. Los "Procedimientos de Emisión" podrán establecer, en el ámbito de actuación de las Administraciones Públicas, Oficinas de Registro comunes para este ámbito de actuación con efectos uniformes para cualesquiera Administraciones, organismos y/o entidades públicas.

Son expedidos por la FNMT-RCM como Prestador Cualificado de Servicios de Confianza cumpliendo con los criterios establecidos en la Ley 6/2020, de 11 de noviembre, citada y en la normativa técnica EESSI, concretamente de conformidad con el estándar europeo ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y "ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons". Estos certificados electrónicos son emitidos exclusivamente al personal al servicio de la Administración, y por tanto no se emiten al público general.



Los certificados de firma electrónica del personal al servicio de la Administración Pública son cualificados conforme al Reglamento (UE) No 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. Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza (TSL, por sus siglas en inglés) de España, a través del enlace <https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl..>

El tamaño de las claves RSA relativas al certificado raíz de la Autoridad de certificación que emite los certificados electrónicos es actualmente de 4.096 bits.

El tamaño de las claves RSA relativas a los certificados electrónicos cualificados para identificar a los empleados públicos es actualmente de 2.048 bits.

El algoritmo de cifrado de todos los certificados emitidos es de SHA-265.

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.

Las Administraciones sólo podrán requerir Certificados con seudónimo de firma electrónica del personal al servicio de la Administración Pública y de la Administración de Justicia para su uso en aquellas actuaciones que, realizadas por medios electrónicos, afecten a información clasificada, a la seguridad pública, a la defensa nacional o a otras actuaciones en las que esté legalmente justificado el anonimato para su realización.

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

#### **Servicio de firma electrónica centralizada para empleados públicos (firma en la nube)**

La AC Sector Público expide certificados de firma electrónica centralizada para funcionarios, personal laboral, estatutario a su servicio y personal autorizado, al servicio de la Administración Pública, órgano, organismo público o entidad de derecho público.

Estos Certificados son válidos como sistemas de firma electrónica de conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y de conformidad con la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

El certificado de firma electrónica centralizada para empleados públicos es un certificado cualificado para la creación de firmas electrónicas avanzadas generadas en un dispositivo de creación de firma remoto, en un entorno seguro y confiable. Esto es, la generación de las Claves pública y privada no se realiza directamente en el navegador de Internet del Firmante o en otro dispositivo en su poder, sino que se generan y se almacenan en un entorno seguro perteneciente a la FNMT-RCM. Para proveer este servicio, se ha integrado en la infraestructura de la FNMT-RCM, el módulo TrustedX eIDAS de Safelayer.

El Certificado de firma electrónica centralizada para empleado público, confirma de forma conjunta, la identidad del personal al servicio de las Administraciones Públicas, y al suscriptor del certificado, que es el órgano, organismo o entidad de la Administración Pública, donde dicho personal ejerce sus competencias, presta sus servicios, o desarrolla su actividad.

Asimismo, la firma electrónica se realiza de forma centralizada, garantizándose en todo momento el control exclusivo del proceso de firma por parte del Personal al servicio de la Administración al que se le ha expedido el Certificado. El acceso a las claves privadas del firmante se llevará a cabo garantizando siempre un Nivel de Aseguramiento ALTO (usuario+password + 2º factor de autenticación OTP).

Las funcionalidades y propósitos del Certificado de firma electrónica centralizada para empleado público permiten garantizar la autenticidad, integridad y confidencialidad de las comunicaciones. La expedición y firma del Certificado se realizará por la "AC Sector Público" subordinada de la "AC Raíz" de la FNMT-RCM.

Los Certificados de firma electrónica centralizada para empleado público expedidos por la FNMT-RCM tendrán validez durante un periodo máximo de tres (3) años contados a partir del momento de la expedición del Certificado, siempre y cuando no se extinga su vigencia. Transcurrido este periodo y si el Certificado sigue activo, caducará, siendo necesaria la expedición de uno nuevo en caso de que se desee seguir utilizando los servicios del Proveedor de Servicios de Confianza.

La longitud de la clave utilizada en la "AC Sector Público" es de 2048 bits y en la "AC Raíz" es de 4096 bits.

La validación del estado de vigencia de este tipo de certificados se puede comprobar a través del servicio de información y consulta del estado de los Certificados que provee la FNMT – RCM mediante el protocolo OCSP, disponible en la ubicación especificada en el propio certificado.

#### **SELLO ELECTRÓNICO CUALIFICADO DE LAS ADMINISTRACIONES PÚBLICAS**

Certificado cualificado de Sello electrónico para Administración Pública, órgano, organismo público o entidad de derecho público, como sistema de identificación y para la actuación administrativa automatizada y para la actuación judicial automatizada, que permite autenticar documentos expedidos por dicha Administración o cualquier activo digital.



Se expiden de conformidad con el estándar europeo ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates", y ETSI EN 319 412- 3 "Certificate profile for certificates issued to legal persons".

Los certificados de sello electrónico son cualificados conforme al Reglamento (UE) No 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. Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza (TSL, por sus siglas en inglés) de España, a través del enlace <https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl>.

La duración de los mismos se establece en 1 año y la longitud de clave RSA en 2.048 bits. Cuentan con servicio validación mediante OCSP, de libre acceso por parte de cualquier interesado, operativo las 24 horas del día, todos los días del año, y cuya URL, accesible desde internet, se refleja en los propios certificados.

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.

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

#### **CERTIFICADOS CUALIFICADOS DE AUTENTICACIÓN DE SITIOS WEB PARA SEDE ELELCTRÓNICA DE LAS ADMINISTRACIONES ELECTRONICAS**

Certificados para la identificación de sedes electrónicas de la administración pública, organismos y entidades públicas vinculadas o dependientes emitidos por la FNMT – RCM bajo la denominación de certificados administración.

Se expiden de conformidad con el estándar europeo ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates", y ETSI EN 319 412- 4 "Certificate profile for web site certificates".

Estos certificados se expiden como cualificados conforme al Reglamento (UE) N° 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, de conformidad con los estándares europeos ETSI EN 319 411-1 "Policy and Security Requirements for Trust Services Providers issuing certificates- General Requirements".

Emitidos en conformidad con los "Requisitos base para la emisión y gestión de certificados de confianza", requisitos establecidos por la entidad CA/Browser fórum.

La duración de los mismos se establece en 1 año y la longitud de clave RSA en 2.048 bits. Cuentan con servicio validación mediante OCSP, de libre acceso por parte de cualquier interesado, operativo las 24 horas del día, todos los días del año, y cuya URL, accesible desde internet, se refleja en los propios certificados.

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.

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

### **ANEXO II**

#### **CAPITULO I - SERVICIOS EIT**

##### **1. Precio anual de los servicios.**

Se establece un precio fijo para los servicios EIT de 308,70 Euros al año, impuestos no incluidos. Incluye una oficina con tres registradores.

Se establece un precio fijo de 81,90 euros al año por registrador adicional.

##### **2. Soporte Técnico**

El coste del soporte técnico especializado 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 conuiniente, 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. Condiciones**

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



## CAPITULO II - SERVICIOS AVANZADOS

### 1. Certificados de componente

En el precio indicado en la cláusula CUARTA incluye:

- 1 certificado de componente (SSL estándar)
- 1 certificado de componente (wildcard)

El precio de los certificados de componentes 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. Servicio de Sellado de Tiempo

El servicio de sellado de tiempo tiene una cuota anual fija de 500 € para un consumo real que no sobrepase los 10.000 sellados al año, estimados como razonables por ambas partes. La superación de dicha estimación de forma consolidada habilitará la revisión de esa tarifa plana y su adaptación a los precios de mercado aplicados por lo FNMT-RCM.

### 3. Condiciones

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

## CAPITULO III - SERVICIOS ADMINISTRACIÓN PÚBLICA (LEY 40/2015)

### 4. Certificados para los servicios del ámbito de la Ley 40/2015

El precio anual para los servicios del ámbito de la Ley 40/2015 asciende a 1.500,00 Euros/año impuestos no incluidos, incluye la emisión de todos los certificados de empleado público (software, seudónimo y firma centralizada), un certificado de sede electrónica y un certificado de sello electrónico para la administración pública.

Se incluyen en el precio indicado en la Cláusula cuarta cuatro certificados de sello electrónico adicionales para la administración pública.

#### 2. Condiciones

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

En Madrid, a 31 de mayo de 2023.-La Directora de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, María Isabel Valldecabres Ortiz.-El Director del Organismo Autónomo Provincial de Gestión Tributaria de Toledo, Santiago García Aranda.

Nº. I.-3173