TÉRMINOS Y CONDICIONES DE USO PARA LOS CERTIFICADOS DE COMPONENTE ELECTRÓNICO DE LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA (FNMT-RCM).

El *Solicitante* manifiesta que, una vez descargue e instale el *Certificado de Componente* utilizará el *Certificado* de conformidad con las condiciones adjuntas y atendiendo al contenido de Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica **y en las** Políticas y Prácticas Particulares de los certificados de componente de la FNMT-RCM**,** (https://www.sede.fnmt.gob.es/dpcs/accomponentes) **declarando expresamente que las acepta en toda su extensión y que su capacidad no se encuentra limitada para contratar con esta Entidad.**

Estas condiciones son un extracto de las *Políticas y Prácticas Particulares de los certificados de componente de la FNMT-RCM,* con las normas básicas para la expedición de estos *Certificados*. Se pone a disposición del *Solicitante* la siguiente información básica y que, por razones de espacio, el deber de información quedará satisfecho con la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* (DGPC) y con las *Políticas y Prácticas Particulares de los certificados de componente de la FNMT-RCM*, puestas a disposición en formato digital en el anterior enlace.

Tipo de certificado y límites de uso

La Autoridad de Certificación "AC Componentes" expide los siguientes tipos de certificados electrónicos, con su ámbito de uso específico:

• Certificado de autenticación de sitio web estándar: Permite establecer comunicaciones seguras utilizando el protocolo SSL/TSL. Este tipo de Certificado garantiza la identidad del dominio donde se encuentre una web. Este certificado tendrá una validez durante un periodo máximo de un (1) año contado a partir del momento de su expedición, siempre y cuando no se extinga su vigencia.

• Certificado de autenticación de sitio web multidominio (SAN/UCC): Garantiza la seguridad de un conjunto de dominios independientes entre sí. Este certificado tendrá una validez durante un periodo máximo de un (1) año contado a partir del momento de su expedición, siempre y cuando no se extinga su vigencia.

• Certificado de autenticación de sitio web wildcard: El certificado wildcard identifica todos los sub-dominios asociados a un dominio determinado, sin necesidad de adquirir y gestionar múltiples certificados electrónicos. Este certificado tendrá una validez durante un periodo máximo de un (1) años contado a partir del momento de su expedición, siempre y cuando no se extinga su vigencia.

• Certificado de sello de entidad: Se utiliza para la automatización de procesos de firma y autenticación entre componentes informáticos. Además, se permite al usuario elegir el uso extendido de claves del Certificado (autenticación de cliente, protección de correo electrónico). Este certificado tendrá una validez durante un periodo máximo de tres (3) años contados a partir del momento de su expedición, siempre y cuando no se extinga su vigencia.

Transcurrido el periodo de validez de los certificados y si el certificado sigue activo, caducará, siendo necesaria la expedición de uno nuevo en el caso de que se desee seguir utilizando los servicios del Proveedor de Servicios de Confianza. Los certificados de componente no podrán ser utilizados cuando expire su periodo de validez, cuando sea solicitada su revocación o se cumpla alguna de las otras causas de extinción de su vigencia, establecidas en la Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica y en las Políticas y Prácticas Particulares de los Certificados de Componente de la FNMT-RCM

Estos certificados electrónicos son expedidos en cumplimiento con los requisitos del 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, y por la que se deroga la directiva 1999/93/CE. La longitud de la clave utilizada en la "AC Componentes" 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.

Obligaciones de la Entidad Suscriptora y del solicitante del certificado

- No usar el *Certificado* fuera de los límites especificados en la presente *Política y Prácticas de Certificación* particulares.
- No usar el *Certificado* en caso de que el *Prestador de Servicios de Confianza* haya cesado su actividad como Entidad emisora de *Certificados* que expidió el certificado en cuestión, especialmente en los casos en los que los *Datos de Creación de Firma* del prestador puedan estar comprometidos, y así se haya comunicado.
- Aportar información veraz en la solicitud de los *Certificados* y mantenerla actualizada, suscribiendo los contratos por persona con capacidad suficiente.
- No solicitar para el *Sujeto* del certificado signos distintivos, denominaciones o derechos de propiedad industrial o intelectual de las que no sea titular, licenciatario o cuente con autorización demostrable para su uso.
- Actuar con diligencia respecto de la custodia y conservación de los *Datos de creación de Firma* o cualquier otra información sensible como *Claves*, códigos de activación del *Certificado*, palabras de acceso, números de identificación personal, etc., así como de los soportes de los *Certificados,* lo que comprende en todo caso, la no revelación de ninguno de los datos mencionados.
- Conocer y cumplir las condiciones de utilización de los *Certificados* previstas en las condiciones de uso y en la *Declaración de Prácticas de Certificación* y en particular, las limitaciones de uso de los *Certificados*
- Conocer y cumplir las modificaciones que se produzcan en la *Declaración de Prácticas de Certificación*.
- Solicitar la revocación del correspondiente *Certificado*, según el procedimiento descrito en el presente documento, notificando diligentemente a la FNMT-RCM, las circunstancias para la revocación o sospecha de pérdida de la *Confidencialidad*, la divulgación, modificación o uso no autorizado de los *Datos de Creación de Firma*,
- Revisar la información contenida en el *Certificado*, y notificar a la FNMT-RCM cualquier error o inexactitud.
- Verificar con carácter previo a confiar en los *Certificados,* la *Firma electrónica reconocida* del *Prestador de Servicios de Confianza* emisor del *Certificado.*
- Notificar diligentemente a la FNMT-RCM cualquier modificación de los datos aportados en la solicitud del *Certificado*, solicitando, cuando consecuentemente fuere pertinente, la revocación del mismo.
- Devolver o destruir el *Certificado* cuando así lo exija la FNMT-RCM, y no usarlo con propósito de firmar o identificarse electrónicamente cuando el *Certificado* caduque, o sea revocado.

Obligaciones de verificación del estado de los certificados de las terceras partes

Cualquier tercera parte que confía de manera razonable en un certificado, tendrá qué:

- Asegurar que la confianza en los certificados emitidos bajo la política de certificación está restringida a los usos apropiados (véase el documento Política y Prácticas de Certificación Particulares).
- Verificar la validez del certificado, asegurándose de que no ha caducado.
- Asegurarse de que el certificado no ha sido suspendido o revocado, accediendo a la información sobre el estado actual de revocación, disponible en la ubicación especificada en el propio certificado.
- Determinar que dicho certificado ofrece garantías suficientes para el uso previsto.

Limitaciones de responsabilidad

La FNMT-RCM únicamente responderá por deficiencias en los procedimientos propios de su actividad como Prestador de Servicios de Confianza, y conforme a lo dispuesto en las correspondientes Políticas y Prácticas de Certificación. En ningún caso será responsable de las acciones o de las pérdidas en las que incurran, solicitantes, firmantes, suscriptores, entidades usuarias o, en su caso, terceros involucrados, que no se deban a errores imputables a la FNMT-RCM en los correspondientes procedimientos de expedición y/o de gestión de los certificados.

La FNMT-RCM no responderá en los supuestos de caso fortuito, fuerza mayor, atentado terrorista, huelga salvaje, así como en los supuestos que se trate de acciones constitutivas de delito o falta que afecten a sus infraestructuras prestadoras, salvo que hubiera mediado culpa grave de la entidad.

La FNMT-RCM no responderá ante personas cuyo comportamiento en la utilización de los certificados haya sido negligente, debiendo considerarse a estos efectos y en todo caso como negligencia la falta de observancia de lo dispuesto en la Declaración de Prácticas de Certificación y, en especial, lo dispuesto en los apartados referidos a las obligaciones y a la responsabilidad de las partes.

En todo caso y con la condición de cláusula penal, la cuantía que la FNMT – RCM debiera satisfacer, en concepto de daños y perjuicios, por imperativo judicial a terceros perjudicados o miembros de la Comunidad Electrónica en cualquier ámbito de actuación público o privado, en defecto de regulación específica en los contratos o convenios, se limita a un máximo de SEIS MIL EUROS (6.000€).

En caso de terminación de la actividad del Prestador de Servicios de Confianza, la FNMT – RCM se regirá por lo dispuesto en la normativa vigente sobre firma electrónica. En todo caso, informará debidamente y con antelación suficiente a los titulares de los certificados, así como a los usuarios de los servicios afectados y transferirá, con el consentimiento expreso de los titulares, aquellos certificados que sigan siendo válidos en la fecha efectiva de cese de actividad a otro Prestador de Servicios de Confianza que los asuma. De no ser posible esta transferencia la vigencia de los certificados quedará extinguida.

La FNMT – RCM registra y mantiene archivados aquellos eventos significativos necesarios para verificar la actividad de esta Autoridad de Certificación durante un periodo nunca inferior a 15 años, conforme a la legislación aplicable

Política de devolución

En un contexto de buenas prácticas empresariales la FNMT - RCM ha adoptado una política de devolución del certificado emitido que permite la solicitud de reembolso dentro del periodo de desistimiento establecido, aceptando que este hecho llevará consigo la revocación automática del certificado.

Ley aplicable, quejas y resolución de disputas

La provisión de servicios de confianza de la FNMT – RCM se regirá por lo dispuesto por las Leyes del Reino de España.

Con carácter general, los miembros de la Comunidad Electrónica y los Usuarios de los servicios de confianza de la FNMT-RCM aceptan que todo litigio, discrepancia, cuestión o reclamación resultante de la ejecución o interpretación de las Políticas y/o Declaraciones de Prácticas de Servicios de Confianza y de Certificación electrónica o relacionada con ellas, directa o indirectamente, se resolverá de conformidad con lo establecido en los correspondientes contratos, condiciones generales y/o encomiendas o convenios, en los términos previstos en el Estatuto de la entidad, aprobado por RD 51/2023, de 31 de enero (BOE nº 27 de 1 de febrero de 2023). En caso de que los contratos, condiciones generales y/o encomiendas o convenios, no especificasen sistemas de resolución de conflictos, todas las partes se someten a la jurisdicción exclusiva de los tribunales del Estado español en la ciudad de Madrid. Asimismo, podrán pactarse, previa aprobación de los órganos competentes de la FNMT-RCM, procedimientos de mediación o arbitraje, de acuerdo con lo establecido en la legislación aplicable.

Licencias y repositorio, marcas confiables y auditoría

La FNMT-RCM cuenta con una larga trayectoria histórica en la realización de sus actividades industriales, así como el respaldo del Estado, como Entidad Pública Empresarial adscrita al Ministerio de Hacienda y Función Pública. Desde la entrada en vigor del artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social y sus modificaciones, ha contribuido a impulsar la extensión de los servicios a los que ha sido facultada y ha obtenido el reconocimiento del entorno privado en el sector de la certificación electrónica y las redes telemáticas abiertas, alcanzando un destacado puesto en la prestación de los servicios de certificación.

La FNMT – RCM, como Prestador de Servicios de Confianza, mantiene varias acreditaciones y certificaciones de su infraestructura de clave pública, de las cuales aplican especialmente a estos tipos de certificados las siguientes:

- Certificados de sello de entidad, SSL estándar, SSL multidominio, y wildcard : Emitidos en conformidad con el estándar europeo ETSI EN 319 411-1 “Policy and Security Requirements for Trust Services Providers issuing certificates- General Requirements”
- Certificados de Sello de Entidad: Expedición y administración de certificados electrónicos cualificados de conformidad con los estándares europeos ETSI EN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates”, ETSI EN 319 412-3 “Certificate profile for certificates issued to legal persons”.
- Certificados de autenticación de sitio web estándar con políticas de Organization Validation (OV): Expedición y administración de certificados electrónicos cualificados de conformidad con los estándares europeos 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”.

Esta auditoría se lleva a cabo con la periodicidad requerida y por un Organismo de Evaluación de la Conformidad acreditado para tal fin.

Los certificados cualificados de autenticación de sitio web estándar con políticas de Organization Validation (OV) y los certificados de Sello de Entidad, 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://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx

Información de contacto del Prestador de Servicios de Confianza

Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda
C/ Jorge Juan, 106
28009 Madrid
https://www.sede.fnmt.gob.es/
Contacto: ceres@fnmt.es

La FNMT-RCM pone a disposición de los Suscriptores, terceros que confían, proveedores de software y terceras partes una vía de comunicación a través de la sede electrónica de la FNMT-RCM (https://www.sede.fnmt.gob.es/) con instrucciones claras, para permitirles reportar cualquier asunto relacionado con este tipo de Certificados, en cuanto a un supuesto compromiso de Clave Privada, uso indebido de los Certificados u otros tipos de fraude, compromiso, mal uso o conducta inapropiada

PROTECCIÓN DE DATOS.

Información básica sobre los datos de carácter personal recogida. Esta información se realiza en dos capas sobre la base de la regulación europea (arts. 13 y 14 del REGLAMENTO (UE) 2016/679 - Reglamento General de Protección de Datos) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

RESPONSABLE	*FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA, E.P.E., M.P. (FNMT-RCM)*
FINALIDAD	*Gestión de la prestación de servicios de confianza y demás servicios de la administración electrónica y sociedad de la información, relacionados y previstos en los fines de la Entidad y en la normativa vigente.* *Gestionar la prestación de los anteriores servicios en todas las fases de su desarrollo y ejecución.* *Gestión de calidad, consultas y sondeos de opinión relacionados con los servicios de confianza..*
LEGITIMACIÓN	*Ejecución de un contrato para la prestación de un servicio del que los interesados son parte* *Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.*
COMUNICACIONES DE DATOS	*Administraciones públicas, organismos y entidades vinculadas o dependientes, en el ámbito del artículo 81 de la ley 66/1997, de 30 de diciembre y el resto de supuestos contemplados en normas europeas y nacionales con rango de Ley. Se producirán comunicaciones de datos al incluir el número de serie del certificado en la lista de certificados revocados. Además, el uso del certificado posibilita que los terceros puedan acceder a datos que nos ha proporcionado (nombre, apellidos y DNI).* *Comunicaciones a las Fuerzas y Cuerpos de Seguridad del Estado y órganos judiciales. No se realizan transferencias internacionales fuera de la UE.*
DERECHOS	*Puede acceder, rectificar, suprimir los datos y ejercitar el resto de derechos, según se informa en https://www.fnmt.es/politica-privacidad*
PROCEDENCIA	*Consentimiento inequívoco del interesado. De empresas y organizaciones donde prestan servicios los interesados.*
MEDIDAS DE SEGURIDAD	*Esquema Nacional de Seguridad. Más información en enlace inferior.*

CATEGORÍA DE DATOS	*Datos identificativos: NIF/DNI, nombre y apellidos, dirección, teléfono, edad, correo electrónico, cargo, denominación o razón social.* *Datos de características personales: clave pública de autenticidad, clave privada para firma en la nube, número de serie del certificado, código de solicitud del certificado,* *Datos de circunstancias sociales: atributos relativos a la capacidad y poder de representación. Datos de información comercial: dirección electrónica (URL).*

Puede consultar información adicional y detallada sobre este tratamiento en:

https://www.fnmt.es/politica-privacidad (TRATAMIENTO Nº 13)

Los interesados autorizan a la FNMT-RCM a incluir el número de serie del certificado en la lista de certificados revocados (comunicación de datos) para que sea visualizado por cualquier usuario, aunque no disponga de un certificado electrónico, tanto en el ámbito público como privado. Además, le informamos y usted consiente, que el uso del certificado a efectos de identificación o si realiza una firma electrónica, posibilita que los terceros puedan acceder a los datos que nos ha proporcionado incluidos en el certificado. Información sobre Registros públicos de Certificate Transparency (CT).