Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DECLARACIÓN INFORMATIVA DE LA PKI DE LA FNMT – RCM

Certificados de la "AC Servidores Seguros Tipo 2"

Ref. PDS_ES_ServidoresSegurosTipo2_v1.1

21/04/2023
FNMT – RCM

Contenido

Información de contacto del Prestador de Servicios de Confianza 2
Tipo de certificado, procedimientos de validación y uso 2
Límites de uso 2
Obligaciones de las partes 3
Obligaciones de verificación del estado de los certificados de las terceras partes 3
Limitaciones de responsabilidad 3
Acuerdos aplicables y Declaración de Prácticas y Políticas de Certificación 4
Política de privacidad 4
Política de devolución 6
Ley aplicable, quejas y resolución de disputas 6
Licencias y repositorio, marcas confiables y auditoría 6

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.

Tipo de certificado, procedimientos de validación y uso

La Autoridad de Certificación "AC Servidores Seguros Tipo 2" expide los siguientes tipos de certificados electrónicos, con su ámbito de uso específico:

- **Certificado de autenticación de sitio web SSL OV**: Permite establecer comunicaciones seguras utilizando el protocolo SSL/TSL. Este tipo de Certificado garantiza la identidad del dominio donde se encuentre una web.
- **Certificado de autenticación de sitio web multidominio SAN OV**: Garantiza la seguridad de un conjunto de dominios independientes entre sí.
- **Certificado de autenticación de sitio web wildcard OV**: Garantiza la seguridad de un conjunto de subdominios ilimitado, a partir del tercer nivel, con un único Certificado de autenticación de sitio web

Estos certificados electrónicos son expedidos en conformidad 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.

Límites de uso

Si cualquier parte usuaria confía en un Certificado de autenticación de sitio web sin realizar la comprobación del estado del Certificado, no se obtendrá cobertura de la Declaración de Prácticas de Certificación aplicable a este tipo de certificados y se carecerá de legitimidad alguna para reclamar o emprender acciones judiciales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un Certificado de autenticación de sitio web.

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.

Obligaciones de las partes

En la Política y Prácticas de Certificación Particulares quedan definidas las obligaciones de todas las partes que actúan en relación con el uso de estos certificados.

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 de los certificados de autenticación de sitios web).
- 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, suscriptores, representantes, entidades usuarias o, en su caso, terceros involucrados, que no se deban a errores imputables a la FNMT-RCM en los mencionados 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 Certificación, 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 Certificación que los asuma. De no ser posible esta transferencia la vigencia de los certificados quedará extinguida.

Acuerdos aplicables y Declaración de Prácticas y Políticas de Certificación

El documento Política y Prácticas de Certificación Particulares de los certificados de autenticación de sitios web de la "AC RAIZ FNMT-RCM Servidores Seguros", publicado en la dirección http://www.ceres.fnmt.es/dpcs/, recoge la información pública de las condiciones y características de los servicios de certificación y servicios de expedición de certificados electrónicos por parte de la FNMT-RCM como Prestador de Servicios de Confianza, recogiendo las obligaciones y procedimientos que se compromete a cumplir en relación con la expedición de estos tipos de certificados.

Las actividades que la FNMT – RCM pueda subcontratar para llevar a cabo su actividad como Prestador de Servicios de Confianza se desarrollan según lo establecido en su Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica (DGPC) y en los contratos y acuerdos formalizados con las entidades que realizan tales actividades. En estos casos, el acceso a la información propiedad de la FNMT – RCM por parte de terceros sigue el protocolo definido en la Política de Seguridad de esta entidad, en cuanto a la identificación de riesgos, establecimiento de controles de seguridad para proteger el acceso a la información y la formalización de los correspondientes acuerdos de confidencialidad y, si procede, el contrato para el tratamiento de datos de carácter personal en cumplimiento de la normativa vigente.

Política de privacidad

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.

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 las 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.

En el siguiente enlace, podrá encontrar información sobre Registros públicos de *Certificate Transparency (CT).*

Política de devolución

La FNMT – RCM cuenta con una política de devolución que permite la solicitud de reembolso dentro del período de desistimiento establecido, aceptando que este hecho llevará consigo la revocación automática del certificado. El procedimiento se publicará en la sede electrónica de la FNMT – RCM.

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 del 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 autenticación de sitios web OV: Expedición y administración de certificados electrónicos cualificados de conformidad con los estándares europeos ETSI EN 319 411-1 “Policy and Security Requirements for Trust Services Providers issuing certificates- General Requirements”.

Esta auditoría se lleva a cabo anualmente por una entidad externa acreditada para tal fin.

Estos certificados emitidos por “AC Servidores Seguros Tipo 2” se expiden 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.