

TÉRMINOS Y CONDICIONES PARA LA IDENTIFICACIÓN REMOTA POR VÍDEO PARA LA EMISIÓN DE LOS CERTIFICADOS CUALIFICADOS DE FIRMA ELECTRÓNICA DE LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA (FNMT-RCM)

El *Solicitante* y futuro *Firmante* manifiesta que acepta la realización del proceso de verificación e identificación remota por video para la emisión de certificados cualificados de la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM) y utilizará el *Servicio de Identificación Remota por Video* de conformidad con las condiciones adjuntas, la [Política y Prácticas de Certificación Particulares de los Certificados solicitados](#) y la [Declaración General de Prácticas de Certificación](#) de la FNMT-RCM y con arreglo a la “Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados” y normas concordantes, aceptando también la política de devolución y la política de privacidad y de información sobre protección de datos de la FNMT-RCM, consintiendo la grabación íntegra de su imagen y voz y la obtención de otras evidencias durante el proceso de registro, así como el tratamiento y conservación de categorías especiales de datos personales (datos biométricos) y la no aplicación de derecho de desistimiento una vez el servicio haya sido completamente ejecutado, de acuerdo con lo dispuesto en el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

La aceptación de estos términos y condiciones por el *Solicitante* se realiza sobre todo su contenido, no pudiendo limitar su aplicación y declarando responsablemente que su capacidad no se encuentra limitada para contratar con esta Entidad.

Condiciones de Uso

Estos términos y condiciones se establecen con el fin de proporcionar información clara y comprensible a los *Solicitantes*, *Firmantes* y usuarios sobre el proceso de identificación remota por vídeo, de las recomendaciones de seguridad aplicables y de la información sobre privacidad, según se establece en las normas de aplicación. El *Solicitante*, mediante la aceptación de las presentes condiciones, otorga consentimiento expreso para la grabación íntegra del vídeo y para el tratamiento y conservación de categorías especiales de datos personales. Al pulsar la opción de Aceptar, para realizar el proceso de verificación de identidad remota por video para la obtención de un certificado de firma electrónica cualificado, está aceptando también la política de privacidad, de información sobre protección de datos y las presentes condiciones de uso. La no aceptación de estas condiciones supone que no podrá tener acceso al servicio de video identificación.

La FNMT-RCM, como Prestador de Servicios de Confianza, le informa de que existen otras alternativas para la identificación que no requieren el tratamiento y la conservación de su imagen y sus datos biométricos, bien mediante la presencia física ante una Oficina de Registro, con personal cualificado para ello, con la que la FNMT-RCM tenga suscrito un acuerdo o a la que sea de aplicación de una norma o una resolución administrativa; o bien mediante la utilización de un Certificado de firma electrónica que confirme la identidad del solicitante.

Acceso al Servicio

1) La modalidad de identificación remota por vídeo que se va a realizar es no asistida (asíncrona), sin interacción en línea entre un operador y el *Solicitante* y revisión posterior de un operador designado por la FNMT-RCM. Para iniciar el proceso de verificación de identidad por video identificación de la FNMT-RCM, el usuario deberá haber realizado previamente la solicitud del Certificado y obtenido el correspondiente código de solicitud. Además, se deben de aceptar previamente la política de privacidad, protección de datos y las presentes condiciones de uso, así como la política de cookies del sitio web.

2) Una vez seleccionada la opción de video identificación, el sistema le guiará por diferentes pasos y actuaciones que el *Solicitante* ha de realizar para poder obtener las evidencias que establezcan la acreditación de la identidad con un grado adecuado de seguridad, según los estándares aprobados. La verificación de identidad se basará en un reconocimiento facial mediante procedimientos biométricos, la grabación de voz y prueba de vida mediante vídeo y la aportación de documento de identidad válido.

Si tiene alguna duda, puede consultar las instrucciones del [proceso de video identificación](#).

3) Una vez realizado el proceso de obtención de evidencias, la FNMT-RCM, directamente o por medio de operadores cualificados contratados por ella, revisará el proceso de identificación grabado y comprobará las evidencias generadas por el sistema para aceptar o rechazar su validez. Se verificará la autenticidad, vigencia e integridad física y lógica del documento de identificación utilizado y la correspondencia del titular del documento con el *Solicitante*. Se tomarán medidas para reducir al mínimo el riesgo de que la identidad del solicitante no coincida con la identidad reclamada, teniendo en cuenta el riesgo de documentos perdidos, robados, suspendidos, revocados o expirados.

El proceso de identificación se interrumpirá o no se considerará válido cuando concurra alguna de las siguientes circunstancias:

- Existan indicios de falsedad, manipulación o falta de validez del documento de identificación.
- Existan indicios de falta de correspondencia entre el titular del documento y el solicitante.
- La calidad de la imagen o el sonido impidan o dificulten verificar la autenticidad e integridad del documento de identificación y la correspondencia entre el titular del documento y el solicitante.
- Las condiciones, seguridad o la calidad de la comunicación impidan o dificulten completar el proceso con la fiabilidad adecuada.
- Existan indicios de uso de archivos pregrabados.
- Existan indicios de que para la transmisión de vídeo no se ha utilizado un único dispositivo.

- g) Existan indicios de que la transmisión de vídeo no se ha realizado en tiempo real o de que el proceso no se ha realizado en unidad de acto.
- h) Existan indicios de que el solicitante está siendo coaccionado o intimidado.
- i) Cualquier otra en la que exista una duda razonable sobre la seguridad del proceso de identificación que se está realizando.

En caso de que la FNMT-RCM, a través de los sistemas técnicos implementados, interrumpa o no considere válido el proceso de identificación, se indicará la causa dejando constancia fehaciente en el sistema.

El operador de registro que revise las evidencias obtenidas en el proceso de registro, basará su decisión de aprobación o denegación de la solicitud de emisión del certificado en la revisión de todas las pruebas recabadas en el proceso de identificación, incluyendo, al menos, el vídeo, la comprobación de caracteres aleatorios enviados al solicitante, la existencia de elementos de seguridad del documento de identidad extraídos del mismo durante el proceso de identificación y la comparación biométrica realizada.

Se tomarán las medidas adecuadas para detectar una posible manipulación de la imagen de vídeo, del documento de identidad o del solicitante, garantizándose su prueba de vida. Para ello, se implantarán al menos:

- a) Medidas procedimentales que hagan patente dicha manipulación con la introducción de un código único, aleatorio e impredecible y de un solo uso generado al efecto y remitido al solicitante. El código constará de un mínimo de seis caracteres o sistema con entropía equivalente. El prestador comprobará que el dispositivo móvil al que se remite el código se encuentra en posesión del usuario durante el proceso de identificación.
- b) En el caso de la identificación remota por vídeo no asistida, el sistema requerirá al solicitante la realización activa de interacciones y actuaciones físicas, que incluirá acciones tanto comunes como aleatorias y diferenciadas.

4) La FNMT-RCM, como Prestador de Servicios de Confianza le informa que la grabación y obtención de pruebas, se realiza bajo las siguientes condiciones:

- a) El vídeo realizado se grabará íntegramente y sin interrupciones.
- b) Se constatará de manera fehaciente la fecha y hora de la grabación mediante el uso de un sello cualificado de tiempo.
- c) Se conservará una copia de la grabación del vídeo durante un periodo mínimo de tiempo de quince años desde la extinción de la vigencia del certificado obtenido por este medio.
- d) Se conservarán, por un periodo mínimo de tiempo de quince años, fotos o capturas de pantalla del solicitante y del documento de identidad utilizado, en las que serán claramente reconocibles tanto la persona como el anverso y el reverso del documento de identidad.
- e) Se conservará, por un periodo mínimo de tiempo de quince años, el resultado automático de la verificación realizada por la aplicación, así como la evaluación y observaciones realizadas por el operador junto a su decisión de aprobación o rechazo de la identificación.
- f) Se conservarán todas las pruebas de los procesos de identificación incompletos que no hayan llegado a término por sospecha de intento de fraude durante un plazo de 5 años desde la ejecución del proceso de identificación, especificándose la causa por la que no llegaron a completarse.
- g) Se garantizará la integridad y autenticidad de la grabación, así como de las otras pruebas obtenidas durante el proceso de identificación remota, mediante la utilización de servicios de confianza cualificados, así como su confidencialidad. La conservación se realizará mediante el bloqueo de los datos, conforme a lo previsto en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- h) La grabación y las imágenes obtenidas durante el proceso de identificación reunirán las condiciones de calidad y nitidez suficientes para garantizar su uso en investigaciones o análisis posteriores.
- i) Las imágenes obtenidas durante el proceso de identificación podrán ser tratadas con el objeto de realizar mejoras técnicas en la plataforma de vídeo identificación y establecer referencias sobre las que realizar mediciones.

5) Durante el proceso de registro, cuando el solicitante presenta el Documento Nacional de Identidad (DNI), se comprueban los datos de identidad del mismo, utilizando el número del documento, a través de la plataforma de intermediación del Servicio de Verificación y Consulta de Datos de la Secretaría de Estado de Digitalización e Inteligencia Artificial. En caso de problemas técnicos vinculados a la plataforma de comprobación y ajenos al prestador, se realizarán al menos tres intentos de consulta y se conservarán las respuestas recibidas.

La acreditación se realizará respetando en todo momento la normativa vigente de protección de datos personales, debiendo aceptar la política de privacidad y protección de datos de forma previa a su tratamiento. Los datos personales recabados durante la verificación de identidad serán almacenados por la FNMT-RCM durante los plazos de tiempo establecidos por la normativa específica de aplicación.

Obligaciones del Solicitante

La persona física *Solicitante* de video identificación, debe:

- Proporcionar información veraz, precisa y completa para realizar el registro.
- Proporcionar documentos de identidad válidos, vigentes y de su uso exclusivo.
- Conocer y cumplir las presente condiciones de utilización, la [Política y Prácticas de Certificación Particulares de los Certificados solicitados](#) y la [Declaración General de Prácticas de Certificación](#) de la FNMT-RCM.
- Mantener indemne a la FNMT-RCM, de cualquier reclamación o reivindicación en relación con el uso fraudulento de documentos de identidad o con la aportación de datos falsos, tergiversados o incompletos en el proceso de identificación remota por video. Cualquier intento o sospecha de suplantación o actuación fraudulenta por parte del *Solicitante* en el proceso de video identificación, será puesta en conocimiento de los Cuerpos y Fuerzas de Seguridad del Estado competentes y/o de la Fiscalía.

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

Los miembros de la Comunidad Electrónica, la entidades usuarias y los terceros que confían en los *Certificados*, expedidos mediante video identificación certificada, y en las firmas electrónicas generadas con los mismos, deberán conocer la Política y Prácticas de Certificación Particulares de Certificados —siendo documentos aprobados y publicados en la sede electrónica de la FNMT-RCM, accesibles desde el propio Certificado— y cumplir las siguientes obligaciones, exonerando al Prestador de Servicios de Confianza (FNMT-RCM) de cualquier responsabilidad en caso de que alguna no sea cumplida:

- Verificar, con carácter previo a confiar en los *Certificados*, la firma electrónica o el sello electrónico avanzados del Prestador de Servicios de Confianza que expidió el *Certificado*.
- Verificar que el *Certificado* continúa vigente.
- Verificar el estado de los *Certificados* en la cadena de certificación, mediante consulta al “Servicio de información y consulta sobre el estado de validez de los certificados” de la FNMT-RCM, incluida en el propio *Certificado* o Sistema.
- Comprobar las limitaciones de uso aplicables al *Certificado* que se verifica.
- Notificar a la FNMT-RCM, o a cualquier Oficina de Registro, cualquier anomalía o información relativa al *Certificado* y que pueda ser considerada como causa de revocación del mismo, aportando todos los elementos probatorios de los que disponga.

Limitaciones de responsabilidad

La FNMT-RCM únicamente responde de la correcta expedición y gestión de los Certificados, basándose en la video identificación del *Solicitante* y futuro *Firmante*, así como de incorporar esos datos a un *Certificado*. Esta identificación personal se realiza mediante un proceso de video identificación (*On Boarding*), utilizando sistemas de identificación a distancia y su posterior verificación. Para la aplicación de garantías, obligaciones y responsabilidades, es necesario que el hecho se haya producido en el ámbito de la Comunidad Electrónica (agentes implicados en las actividades conducentes a la expedición y uso de los certificados).

La FNMT-RCM solo responderá por deficiencias en los procedimientos propios de su actividad como Prestador de Servicios de Confianza, y conforme a lo dispuesto en la Política y Prácticas de Certificación Particulares de Certificados o en la Ley. En ningún otro caso será responsable de las acciones o de las pérdidas en las que incurran los titulares, *Firmantes*, Entidades usuarias, oficinas de registro o terceros involucrados, que no se deban a errores imputables a la FNMT-RCM en los procedimientos de expedición y/o de gestión de los Certificados.

FNMT-RCM no responderá en caso de fuerza mayor, caso fortuito, 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. En todo caso, en los correspondientes contratos y/o convenios FNMT-RCM podrá establecer cláusulas de limitación de responsabilidad. En todo caso, la cuantía que en concepto de daños y perjuicios debiera satisfacer por imperativo judicial la FNMT-RCM a terceros perjudicados, y/o miembros de la Comunidad electrónica vinculada en operaciones que afecten a la expedición y uso del Certificado, en defecto de regulación específica en los contratos o convenios, se limitan a un máximo de SEIS MIL EUROS (6.000€) euros.

La FNMT-RCM no responderá ante *Solicitantes* que incumplan las presente condiciones y ante personas cuyo comportamiento en la utilización de los Certificados haya sido descuidado o negligente, debiendo considerarse, a estos efectos y en todo caso, como negligencia la falta de observancia de lo dispuesto en la Política y Prácticas de Certificación Particulares de Certificados y, en especial, lo dispuesto en los apartados referidos a las obligaciones y responsabilidades de las partes.

La FNMT-RCM no responderá por ningún software que no haya proporcionado directamente. No obstante, la FNMT-RCM pondrá las medidas de protección adecuadas para la protección de sus sistemas y aplicaciones frente a software malicioso (Malware) y otros sistemas dañinos o de ataque a sus infraestructuras y las mantendrá actualizadas para colaborar con los usuarios en evitar los daños que este tipo de software puede causar.

La FNMT-RCM no garantiza los sistemas de video identificación, aunque estén certificados, ni los algoritmos criptográficos, y no responderá de los daños causados por ataques exitosos externos a los sistemas y/o algoritmos criptográficos usados, si guardó la diligencia debida de acuerdo al estado actual de la técnica, normalización y certificación y procedió conforme a lo dispuesto en la Política y Prácticas de Certificación Particulares de Certificados y en la Ley.

Política de Devolución

La política de devolución adoptada por la FNMT-RCM para la comercialización del proceso de verificación e identificación remota por vídeo para la emisión de certificados cualificados, establece que, debido a la naturaleza del servicio de video-identificación para la emisión de los certificados cualificados, una vez que la acreditación de la identidad sea aprobada por nuestros agentes cualificados, el servicio habrá sido ejecutado íntegramente, no siendo aplicable para el *Solicitante* el derecho de desistimiento, conforme a lo dispuesto en el artículo 103.a) del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

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, implicados en la expedición y uso de los *Certificados* 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 la Política y Prácticas de Certificación Particulares de Certificados o relacionada con ellas, directa o indirectamente, se resolverá de conformidad con lo establecido en los correspondientes contratos, condiciones generales o particulares y/o encomiendas o convenios, en los términos previstos en el Estatuto de la entidad, aprobado por Real Decreto 51/2023, de 31 de enero (BOE núm. 27, de 1 de febrero de 2023).

En caso de que los contratos, condiciones generales o particulares y/o encomiendas o convenios, no especificasen sistemas de resolución de conflictos, todas las partes se someten a la jurisdicción exclusiva de los juzgados y 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 su correspondiente normativa de desarrollo, la FNMT-RCM ha contribuido a impulsar la extensión de los servicios para los que ha sido facultada y ha obtenido el reconocimiento del sector público y privado en el entorno de la certificación electrónica y las redes telemáticas abiertas, alcanzando un destacado puesto en la prestación de los servicios de confianza.

Los procedimientos y métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados por parte de la FNMT-RCM, como Prestador de Servicios de Confianza, han sido certificados en el marco del 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 y por la que se deroga la Directiva 1999/93/CE, así como en el de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y en el de la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados

Puede comprobarse la habilitación de la FNMT-RCM para la video identificación en la expedición de certificados cualificados, a través del enlace: <https://sedeaplicaciones.minetur.gob.es/Prestadores/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

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: Procedimientos de identificación y verificación de identidad mediante procedimientos online (en remoto) para la obtención de productos o la prestación de servicios que lo requieran.

LEGITIMACIÓN: Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte. Consentimiento otorgado por el propio interesado. Art. 6.1.a) y Art. 9.2.a) RGPD (para el tratamiento de datos biométricos). Cumplimiento de una obligación legal aplicable al responsable del tratamiento. Art. 6.1.c) RGPD: Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

COMUNICACIONES DE DATOS: Administraciones públicas, organismos y entidades vinculadas o dependientes. 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/en/politica-privacidad>

PROCEDENCIA: consentimiento inequívoco del interesado.

MEDIDAS DE SEGURIDAD: Esquema Nacional de Seguridad. Más información en enlace inferior.

CATEGORÍA DE DATOS: Datos identificativos: DNI o Pasaporte (contenido completo), nombre y apellidos, dirección, teléfono, edad, correo electrónico, fotografía y video de los interesados (prueba de vida). Datos de características personales: clave pública de autenticidad, clave privada para firma en la nube, datos biométricos (reconocimiento facial, voz).

Puede consultar información adicional y detallada sobre este tratamiento en: <https://www.fnmt.es/en/politica-privacidad> (TRATAMIENTO N° 21)

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.