POLÍTICA DE IDENTIFICACIÓN Y FIRMA ELECTRÓNICA

INSTITUT RAMON LLULL

Versión 3.0

Índice

0. Histórico de versiones 2
1. Introducción 2
2. Consideraciones generales 2
2.1. Objeto del documento 4
2.2. Ámbito de aplicación 4
3. La política de identificación y firma electrónica 5
3.1. Alcance de la política 5
3.2. Agentes involucrados 5
4. Mecanismos de identificación y firma electrónica 5
4.1. Tipología de mecanismos admitidos 5
4.2. Mecanismos de identificación y firma electrónica de la ciudadanía y las entidades 7
4.3. Mecanismos de identificación y firma electrónica del Institut Ramon Llull 7
4.4. Criterios de verificación 8
5. Normativa relacionada 9
Anexo I 10
Anexo II 11

0. Histórico de versiones

Nombre del documento	Data	Descripción
Política de identificación y firma electrónica del Institut Ramon Llull	18/03/2016	Versión 1.0
Política de identificación y firma electrónica del Institut Ramon Llull	01/03/2017	Versión 2.0
Política de identificación y firma electrónica del Institut Ramon Llull	23/05/2025	Versión 3.0

1. Introducción

La presente Política de Identificación y Firma Electrónica del Institut Ramon Llull establece el marco normativo, técnico y operativo para garantizar la seguridad jurídica y técnica de las interacciones electrónicas con la ciudadanía, empresas y otras administraciones. Está fundamentada en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y a los servicios de confianza para las transacciones electrónicas en el mercado interior, en adelante Reglamento eIDAS, la Ley 6/2020 y otras normativas estatales y autonómicas. Esta política define los mecanismos de identificación y firma admitidos, los perfiles de los agentes involucrados y los criterios de verificación aplicables a partir del año 2026. El objetivo es facilitar un modelo interoperable, seguro y adaptado al ámbito internacional en el que opera la entidad.

2. Consideraciones generales

El Reglamento eIDAS, normativa vigente que respalda la Ley española 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza, define los siguientes conceptos (art. 3):

- Firma electrónica: los datos en formato electrónico anexos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza la persona firmante para firmar.

- Firma electrónica avanzada: la firma electrónica que cumple los siguientes requisitos (comentados en el art. 26):
    - Estar vinculada al firmante de manera única.
    - Permitir la identificación del firmante.
    - Haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede usar, con un alto nivel de confianza, bajo su control exclusivo.

  - Estar vinculada con los datos firmados de forma que se pueda detectar cualquier modificación de estos

- Firma electrónica cualificada: una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado de firma electrónica.

- Certificado de firma electrónica: una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de dicha persona.

- Certificado cualificado de firma electrónica: un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los siguientes requisitos (enumerados en el Anexo I):
  - Una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de firma electrónica.
  - Un conjunto de datos que represente inequívocamente al prestador cualificado de servicios de confianza que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho prestador está establecido, y:
    - Para personas jurídicas: el nombre y el número de registro según conste en los registros oficiales, cuando proceda.
    - Para personas físicas: el nombre de la persona.
  - El nombre del firmante o un seudónimo.
  - Datos de validación de la firma electrónica que correspondan a los datos de creación de firma electrónica.
  - Datos relativos al inicio y final del período de validez del certificado.
  - El código de identidad del certificado, que debe ser único para el prestador cualificado de servicios de confianza.
  - La firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza emisor.
  - El lugar en el que está disponible, gratuitamente, el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado.
  - La localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado.
  - Indicación en una forma apta para el procesamiento automático cuando los datos de creación de firma electrónica relacionados con los datos de validación de firma electrónica se encuentren en un dispositivo cualificado de creación de firma electrónica.

Cuando se firman datos, el firmante indica la aceptación de unas condiciones generales y unas condiciones particulares aplicables a esa firma electrónica mediante la inclusión de un campo firmado, dentro de la firma, que especifica una política explícita o implícita.

Si el campo correspondiente a la normativa de firma electrónica está ausente y no se identifica ninguna normativa como aplicable, se podrá asumir que la firma ha sido generada o verificada sin ninguna restricción normativa y, por tanto, que no se le ha asignado ningún significado legal contractual concreto. Se trataría de una firma que no especifica de forma expresa ninguna semántica o significado concreto y, por tanto, deberá derivarse el significado de la firma a partir del contexto.

El propósito de una política de firma es reforzar la confianza en las transacciones electrónicas a través de una serie de condiciones para un contexto dado, el cual puede ser una transacción determinada, un requisito jurídico o un rol que asume la parte firmante, entre otros.

2.1. Objeto del documento

La política de identificación y firma electrónica del Institut Ramon Llull tiene como objetivo establecer el conjunto de criterios comunes en relación con la autenticación y la firma electrónica, que afecta a las relaciones de la entidad con la ciudadanía, empresas y el resto de administraciones públicas, según lo previsto en el Capítulo II de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En general, una política de firma electrónica es un documento legal que contiene una serie de normas relativas al tema, organizadas en torno a los conceptos de generación y validación de firma, en un contexto particular (contractual, jurídico, legal, etc.), definiendo las reglas y obligaciones de todos los agentes involucrados en el proceso. El objetivo de este proceso es determinar la validez de la firma para una transacción en particular, especificando la información que debería incluir el firmante en el proceso de generación de la firma y la información que debería comprobar el verificador en el proceso de validación de esta.

El consorcio del Institut Ramon Llull sigue las directrices de la política de firma electrónica de la Administración General del Estado. Así, tal como se indica en el artículo 18 del ENI (RD 4/2010), la institución cumple con las condiciones establecidas en las normas técnicas de interoperabilidad aplicables.

El mantenimiento, actualización y difusión de la Política de identificación y firma electrónica corresponderá a la Gerencia del Institut Ramon Llull.

2.2. Ámbito de aplicación

Esta política se aplica a las relaciones entre el Institut Ramon Llull y la ciudadanía, empresas y otras administraciones públicas que realicen trámites a través de la sede electrónica. Su entrada en vigor será el 1 de enero de 2026.

3. La política de identificación y firma electrónica

3.1. Alcance de la política

Este documento detalla las condiciones generales para la validación y la relación de los formatos de objetos binarios y archivos de referencia que deberán ser admitidos en los trámites con terceros mediante la sede electrónica del Institut Ramon Llull.

3.2. Agentes involucrados

Los agentes involucrados en el proceso de creación y validación de firma electrónica son:

- Firmante: persona que dispone de un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.
- Verificador: entidad, persona física o jurídica, que valida o verifica una firma electrónica mediante la comparación con las condiciones exigidas por una Política de Firma concreta. Puede ser una entidad de validación de confianza o una tercera parte interesada en conocer la validez de una firma electrónica.
- Prestador de servicios de firma electrónica: la persona física o jurídica que expide certificados electrónicos o presta otros servicios relacionados con la firma electrónica.
- Emisor de la Política de Firma Electrónica: entidad encargada de generar o gestionar el documento de Política de Firma, mediante el cual quedarán vinculados el firmante y el verificador en los procesos de generación y validación de la firma electrónica.

4. Mecanismos de identificación y firma electrónica

4.1. Tipología de mecanismos admitidos

La Sede electrónica del Institut Ramon Llull admite los siguientes mecanismos de identificación y firma electrónica:

a. **Certificado digital**: medio de identificación para personas físicas y jurídicas, que determina tanto la identidad del usuario como su tipo de acreditación. El tipo de perfil de acreditación identifica el grado de representación de la persona que se identifica y actúa frente a terceros o en nombre propio. Esta última información será definida por los datos que incorpore el certificado digital utilizado por la ciudadanía.

Los certificados digitales válidos para realizar trámites con el Institut Ramon Llull son los indicados por la Comisión Europea en la *Trusted Services List*[1] de prestadores de servicios de certificación. Si una persona física o jurídica dispone de un certificado emitido por alguno de estos, podrá realizar los trámites que desee con cualquier administración pública de los países incluidos en la UE, de acuerdo con lo establecido en el Reglamento eIDAS.

b. **idCAT Mòbil**: mecanismo de identificación y firma electrónica para personas físicas basado en el envío de contraseñas de un solo uso al móvil. Es necesario registrar previamente los datos de contacto en el fichero de la Sede electrónica de la Administración de la Generalitat. Este servicio lo proporciona el Consorci d'Administració Oberta de Catalunya. También está disponible el alta de idCAT mediante videoidentificación para ciudadanía residente fuera de Cataluña, y puede ser utilizado por personas físicas tanto dentro como fuera de Europa.

c. **Cl@ve**: sistema de acceso electrónico de la ciudadanía a los servicios públicos. Su objetivo principal es permitir la identificación ante la Administración mediante claves (usuario y contraseña), sin necesidad de recordar más de una para diversos servicios. Cl@ve sirve tanto para la identificación, la autenticación como para la firma electrónica. Existen dos tipos de claves de acceso: Cl@ve PIN (para accesos esporádicos con una validez muy corta) y Cl@ve permanente (para accesos habituales y con una validez más larga).

d. Mecanismo no criptográfico de **acreditación** (usuario y contraseña): el Institut Ramon Llull se encarga de generar los datos y enviarlos de forma segura tras haber verificado la documentación que acredite la identidad de la persona física o jurídica solicitante. Por este motivo, si es la primera vez que se presenta una solicitud al Institut Ramon Llull y aún no se dispone de usuario y contraseña, no se podrá realizar el trámite a través de la sede electrónica. En la sede electrónica se encuentra la solicitud de acreditación, que se facilita en un plazo máximo de 72 horas. El usuario y la contraseña tienen una validez de cinco años a partir de la fecha de presentación de la documentación que acredita la identidad de la persona interesada, salvo que haya habido algún cambio.

   Este sistema cuenta con doble factor de autenticación (2FA), que consiste en un segundo factor temporal de un solo uso, enviado a la persona interesada mediante un canal seguro (correo electrónico verificado) para poder finalizar el trámite. Esta acción es conforme a lo establecido en el Real Decreto 311/2022 (Esquema Nacional de Seguridad) y la Orden VPD/93/2022, y contribuye a garantizar el nivel de seguridad medio exigible para la tramitación electrónica con la Administración pública.

Dada la previsión de supresión de los mecanismos de identificación no criptográficos (usuario y contraseña) a partir de enero de 2026, la solicitud de acreditación será eliminada de la página web del IRL. Este sistema se contemplará como excepcional y temporal en aquellos casos en los

[1] El enlace se encuentra en el Anexo II.

que sea urgente la tramitación y no haya sido posible por ninguno de los otros medios contemplados anteriormente. En todo caso, la validez de las credenciales ya no será de cinco años, sino que será de uso temporal para realizar el trámite en cuestión.

4.2. Mecanismos de identificación y firma electrónica de la ciudadanía y las entidades

RESIDENCIA	**MECANISMOS DE IDENTIFICACIÓN Y FIRMA**	**PERFIL DEL SOLICITANTE**
Cataluña/ España	Certificado digital	Personas físicas y personas jurídicas
	idCAT Mòbil	Personas físicas y personas jurídicas (representante legal)
	Cl@ve	Personas físicas y personas jurídicas (representante legal)
Resto de países (dentro y fuera de la UE)	Certificado digital europeo[2]	Personas físicas y personas jurídicas
	idCAT Mòbil	Personas físicas y personas jurídicas (representante legal)

Tal como se indica en la tabla, las personas jurídicas podrán realizar trámites con el Institut Ramon Llull mediante la identificación de una persona física como representante legal de la entidad o empresa en cuestión.

4.3. Mecanismos de identificación y firma electrónica del Institut Ramon Llull

El personal del Institut Ramon Llull utiliza el certificado reconocido o cualificado que el Consorci AOC emite a los empleados del sector público de Cataluña en un dispositivo seguro de creación de firma, la T-CAT o T-CAT P, así como otros sistemas no criptográficos, como los usuarios y contraseñas de las plataformas EACAT y GICAR.

El Institut Ramon Llull utiliza el código seguro de verificación (CSV), aceptado como mecanismo de firma electrónica por los entes de la Administración de la Generalitat de Catalunya, y los

[2] Certificado digital europeo: certificado emitido por una entidad certificadora cualificada y admitida por la Unión Europea.

certificados reconocidos o cualificados de sello electrónico que el Consorci AOC emite a los entes del sector público de Cataluña.

Las firmas electrónicas avanzadas incorporan sellos de tiempo generados por el servicio de sello de tiempo del Consorci AOC.

4.4. Criterios de verificación

Los atributos que podrá utilizar el verificador para comprobar que se cumplen los requisitos de la política de firma según la cual se ha generado la firma, independientemente del formato utilizado, son los siguientes:

- *Signing Time*: se utilizará únicamente en la verificación de las firmas electrónicas como indicación para comprobar el estado de los certificados en la fecha señalada, dado que únicamente se pueden asegurar las referencias temporales mediante un sello de tiempo. Si se ha realizado el sellado de tiempo, el sello más antiguo dentro de la estructura de la firma se utilizará para determinar la fecha de la firma.

- *Signing Certificate*: se utilizará para comprobar y verificar el estado del certificado (y, si procede, la cadena de certificación) en la fecha de generación de la firma, en el caso de que el certificado no haya caducado y se pueda acceder a los datos de verificación, o bien en el caso de que el prestador ofrezca un servicio de validación histórica del estado del certificado (AOC).

- *Signature Policy*: se deberá comprobar que la política de firma que se ha utilizado para la generación de la firma se corresponde con la que debe utilizarse para un trámite o servicio concreto.

5. Normativa relacionada[3]

- Política de Firma Electrónica y de Certificados de la Administración Pública Española (2012).
- Reglamento (UE) núm. 910/2014, de 23 de julio, del Parlamento Europeo y del Consejo relativo a la identificación electrónica y a los servicios de confianza para las transacciones electrónicas en el mercado interior.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Ley 26/2010, de 3 de agosto, de régimen jurídico y de procedimiento de las administraciones públicas de Cataluña.
- Ley 29/2010, de 3 de agosto, del uso de los medios electrónicos en el Sector Público de Cataluña.
- Ley 10/2011, de 29 de diciembre, de simplificación y mejora de la regulación normativa.
- Resolución de 29 de noviembre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se publica el Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados de la Administración General del Estado y se anuncia su publicación en la sede correspondiente.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- ORDEN VPD/93/2022, de 28 de abril, por la que se aprueba el Catálogo de sistemas de identificación y firma electrónica.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- ORDEN PRE/158/2022, de 30 de junio, por la que se aprueba la Guía de uso de los sistemas de identificación y firma electrónica en el ámbito de la Administración de la Generalitat.

(Este documento es la traducción al español de la versión actualizada de la *Política de identificación y firma electrónica* aprobada y firmada el 23 de mayo de 2025 por el Consejo de Dirección del Instituto Ramon Llull. Para ver el documento original, ir a la versión en catalán.)

[3] Los enlaces con los textos normativos originales están en el Anexo I.

Anexo I

Enlaces de páginas web y textos disponibles en línea referenciados:

- Lista de prestadoras de certificados de confianza (UE): Trusted Services List
- Política de Firma Electrónica y de Certificados de la Administración Pública Española (2012).
- Reglamento (UE) núm. 910/2014, de 23 de julio, del Parlamento Europeo y del Consejo relativo a la identificación electrónica y a los servicios de confianza para las transacciones electrónicas en el mercado interior.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Ley 26/2010, de 3 de agosto, de régimen jurídico y de procedimiento de las administraciones públicas de Cataluña.
- Ley 29/2010, de 3 de agosto, del uso de los medios electrónicos en el Sector Público de Cataluña.
- Ley 10/2011, de 29 de diciembre, de simplificación y mejora de la regulación normativa.
- Resolución de 29 de noviembre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se publica el Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados de la Administración General del Estado y se anuncia su publicación en la sede correspondiente.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- ORDEN VPD/93/2022, de 28 de abril, por la que se aprueba el Catálogo de sistemas de identificación y firma electrónica.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- ORDEN PRE/158/2022, de 30 de junio, por la que se aprueba la Guía de uso de los sistemas de identificación y firma electrónica en el ámbito de la Administración de la Generalitat.

Anexo II

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica[4].

Artículo 18. Interoperabilidad en la política de firma electrónica y de certificados.

1. La Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para el reconocimiento mutuo de las firmas electrónicas basadas en certificados de documentos administrativos en las Administraciones Públicas.

Todos los organismos y entidades de derecho público de la Administración General del Estado aplicarán la política de firma electrónica y de certificados a que se refiere el párrafo anterior. La no aplicación de dicha política deberá ser justificada por el órgano u organismo competente y autorizada por la Secretaría General de Administración Digital.

2. Las restantes Administraciones Públicas podrán acogerse a la política de firma electrónica y de certificados a que hace referencia el apartado anterior.

3. Sin perjuicio de lo expuesto en el apartado anterior, las Administraciones Públicas podrán aprobar otras políticas de firma electrónica dentro de sus respectivos ámbitos competenciales.

Las políticas de firma electrónica que aprueben las Administraciones Públicas partirán de la norma técnica establecida a tal efecto en la disposición adicional primera, de los estándares técnicos existentes, y deberán ser interoperables con la política marco de firma electrónica mencionada en el apartado 1, en particular, con sus ficheros de implementación. La Administración Pública proponente de una política de firma electrónica particular garantizará su interoperabilidad con la citada política marco de firma electrónica y con sus correspondientes ficheros de implementación según las condiciones establecidas en la norma técnica de interoperabilidad recogida a tal efecto en la disposición adicional primera.

4. Al objeto de garantizar la interoperabilidad de las firmas electrónicas emitidas conforme a las políticas establecidas, las políticas de firma electrónica que las Administraciones Públicas aprueben deberán ser comunicadas, junto con sus correspondientes ficheros de implementación, a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital.

5. Las Administraciones Públicas receptoras de documentos electrónicos firmados, siempre que hayan admitido con anterioridad la política de firma del emisor, permitirán la validación de las firmas electrónicas según la política de firma indicada en la firma del documento electrónico.

6. Los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de manera que tanto la identificación como la firma electrónica generada a partir de estos perfiles

[4] Disponible en línea a: https://www.boe.es/eli/es/rd/2010/01/08/4/con [08/04/2025].

comunes puedan ser reconocidos por las aplicaciones de las distintas Administraciones Públicas sin ningún tipo de restricción técnica, semántica u organizativa.

7. Los procedimientos en los que se utilicen certificados de firma electrónica deberán atenerse a la política de firma electrónica y de certificados aplicable en su ámbito, particularmente en la aplicación de los datos obligatorios y opcionales, las reglas de creación y validación de firma electrónica, los algoritmos a utilizar y longitudes de clave mínimas aplicables.