ELECTRONIC IDENTIFICATION AND SIGNATURE POLICY

INSTITUT RAMON LLULL

Version 3.0

institut ramon llull

Contents

0. Version history

Document name	Date	Description
Institut Ramon Llull Electronic identification and signature policy	18/03/2016	Version 1.0
Institut Ramon Llull Electronic identification and signature policy	01/03/2017	Version 2.0
Institut Ramon Llull Electronic identification and signature policy	23/05/2025	Version 3.0

1. Introduction

This Institut Ramon Llull Electronic identification and signature policy establishes the legal, technical and operational framework for ensuring the legal and technical security of electronic interactions with individuals, companies and other administrations. Based on Regulation (EU) 910/2014 of the European Parliament and of the Council, on electronic identification and trust services for electronic transactions in the internal market, hereinafter the eIDAS Regulation, Law 6/2020 and other Spanish and Catalan regulations. This policy establishes the accepted identification and signature mechanisms, profiles of stakeholders involved and the verification criteria that apply from 2026. The purpose is to allow for an interoperable model that is secure and adapts to the international arena the organisation moves in.

2. General considerations

The current eIDAS Regulation incorporated into the Spanish legal framework in Law 6/2020, regulating certain aspects of electronic trust services, establishes the following definitions (Art. 3):

- Electronic signature: data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

- Advanced electronic signature: an electronic signature which meets the requirements set out in Article 26:
    - Is uniquely linked to the signatory;
    - Is capable of identifying the signatory
    - Is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
    - Is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

- Qualified electronic signature: an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

- Certificate for electronic signature: an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person.

- Qualified certificate for electronic signature: a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I:
    - An indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature
    - A set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and:
        - For a legal person: the name and, where applicable, registration number as stated in the official records
        - For a natural person: the person's name
    - At least the name of the signatory, or a pseudonym
    - Electronic signature validation data that corresponds to the electronic signature creation data
    - Details of the beginning and end of the certificate's period of validity
    - The certificate identity code, which must be unique for the qualified trust service provider
    - The advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider
    - The location where the certificate supporting the advanced electronic signature or advanced electronic seal
    - The location of the services that can be used to enquire about the validity status of the qualified certificate
    - Where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.

When data is signed, the signatory accepts general conditions and specific conditions that apply to that electronic signature in a signed field within the signature that specifies an explicit or implicit policy.

If the field corresponding to the electronic signature regulation is missing and no applicable regulation is identified, the signature will be assumed to have been created or verified without any regulatory restrictions and, therefore, it hasn't been assigned any specific contractual legal significance. This would be a signature that doesn't expressly specify any specific significance or semantics and, therefore, the significance of the signature must be derived from its context.

The purpose of the signature policy is to reinforce trust in electronic transactions through a series of conditions for a given context, which could be a specific transaction, a legal requirement or a role taken on by the signatory, among others.

2.1. Purpose of the document

The purpose of the Institut Ramon Llull Electronic identification and signature policy is to establish all the common criteria related to electronic signature and authentication that affect relations between the organisation and individuals, companies and other public administrations, as per Chapter II of Law 39/2015 of 1 October, on Common Administrative Procedure of Public Administrations.

In general, an electronic signature policy is a legal document containing a series of rules on the topic, organised under concepts of creating and validating signatures, in a specific context (contractual, legal, etc.), defining the rules and obligations of all the stakeholders involved in the process. The purpose of this process is to determine the validity of the signature for a specific transaction, specifying the information that must be included by the signatory in generating the signature and the information the validator must check in validating it.

The Consortium of the Institut Ramon Llull follows the directives of the General State Administration's electronic signature policy. As laid out in ENI Article 18 (RD 4/2010), the institution complies with the conditions established in the technical regulations of interoperability that apply.

Maintaining, updating and sharing the Electronic identification and signature policy is the purview of Institut Ramon Llull management.

2.2. Scope of application

This policy applies to relations between Institut Ramon Llull and individuals, companies and other public administrations that carry out procedures through its Virtual Office. It will go into effect on 1 January 2026.

3. Electronic identification and signature policy

3.1. Scope of the policy

This document lays out the general validation conditions and a list of binary objects and reference files to be admitted in processes with third parties via the Institut Ramon Llull Virtual Office.

3.2. Stakeholders involved

The stakeholders involved in the process of creating and validating the electronic signature are:

- Signatory: person who has an electronic signature creation device and acts on their own behalf or on behalf of a natural or legal person they represent.
- Validator: body. Physical or legal person that validates or verifies an electronic signature by comparing it against the conditions required by a specific Signature policy. It may be a trust service or third party interested in verifying the validity of an electronic signature.
- Electronic signature services provider: the physical or legal person that issues electronic certificates or provides other services related to electronic signatures.
- Electronic signature policy issuer: the entity in charge of generating or managing the Signature policy document, which binds the signatory and the validator in the processes of generating and validating the electronic signature.

4. Electronic identification and signature mechanisms

4.1. Types of mechanisms allowed

The Institut Ramon Llull Virtual Office allows the electronic identification and signature mechanisms described below:

a. **Digital certificate**: means for identifying physical and legal persons that determines both the identity of the user and their type of accreditation. The type of accreditation profile identifies the level of representation of the person identified and acting on behalf of third parties or on their own behalf. The latter is established by data in digital certificates used by individuals.
   Institut Ramon Llull accepts digital certificates on the European Commission Trusted Services List[1]. If a physical or legal person has a certificate issued by any of these services, they may carry out any procedures with any public administration in EU Member States, as per ReIDAS.

b. **IdCAT Mòbil**: electronic identification and signature mechanism for physical persons based on sending single-use passwords to mobile phones. Users must register their contact details in advance on the Government of Catalonia virtual office. This service is provided by the Open Administration Consortium of Catalonia. Users can also register with IdCAT via a video-identification if they live outside of Catalonia. This method is available to physical persons in Europe or beyond.

[1] The link is in Annex I.

c. **Cl@ve**: electronic system for individuals to access public services. The main purpose is to identify the user with the Administration using keys (username and password) without having to remember different ones for each service. Cl@ve is used to identify, authenticate and provide electronic signatures. There are two options: Cl@ve pin (single use only valid for a short time) and Cl@ve permanent (regular use, valid for a longer period).

d. Non-cryptographic **accreditation** mechanism (username and password): Institut Ramon Llull generates the data and sends them securely after having verified the documents accrediting the identity of the physical or legal person in question. Therefore, first-time applicants that don't have a username and password can't carry out procedures via the Virtual Office. On the Virtual Office, there is a section to request accreditation, which will be provided within 72 hours. The username and password are valid for five years from the submission date of the documents accrediting the identity of the person in question, unless there have been any changes.

   This system features two-factor authentication (2FA), which includes a second temporary, single-use factor that is sent to the person in question via a secure channel (verified email) so they can carry out the procedure. This is in line with the provisions of Royal Decree 311/2022 (National Security Framework) and Order VPD/93/2022, and helps ensure the level of security required for electronic processing with the Public administration.

As non-cryptographic accreditation mechanisms (username and password) are expected to be eliminated from January 2026, the request section will be removed from the IRL website. This system will be used exceptionally and on a temporary basis only in cases when the procedure is urgent and couldn't be completed by any other means. However, the credentials will only be valid for the procedure in question, not for five years.

4.2. Electronic identification and signature mechanisms for individuals and organisations

RESIDENCE	**IDENTIFICATION AND SIGNATURE MECHANISMS**	**APPLICANT PROFILE**
Catalonia/ Spain	Digital certificate	Physical and legal persons
	idCAT Mòbil	Physical and legal persons (legal representative)
	Cl@ve	Physical and legal persons (legal representative)

Other countries (EU and non-EU)	European digital certificate[2]	Physical and legal persons
	idCAT Mòbil	Physical and legal persons (legal representative)

4.3. Electronic identification and signature mechanisms of Institut Ramon Llull

Institut Ramon Llull staff use the recognised or qualified certificate issued by AOC Consortium to employees in the public sector in Catalonia on a secure signature creation device, T-CAT or T-CAT P, as well as other non-cryptographic systems such as usernames and passwords on the EACAT and GICAR platforms.

Institut Ramon Llull uses the secure verification code (CSV), accepted as an electronic signature mechanism for bodies in the Administration of the Government of Catalonia, and the recognised or qualified certificate issued by AOC Consortium to bodies in the public sector in Catalonia.

Advanced electronic signatures incorporate time stamps generated by the AOC Consortium time-stamp service.

4.4. Verification criteria

The attributes that the validator may use to check that the signature complies with the requirements of the signature policy according to which it was generated, regardless of the format used, are as follows:

- Signing time: only used to verify electronic signature as an indication to check the status of certificates on the given date, as time references can only be assured via a time stamp. If there is a time stamp, the oldest stamp in the signature structure will be used to determine the signature date.
- Signing certificate: will be used to check and verify the status of the certificate (and, if necessary, the certification chain) on the date the signature was generated, if the certificate is not expired and the validation data can be accessed, or if the provider offers a historical verification service for the certificate status (AOC).
- Signature policy: it must check that the signature policy used to generate the signature corresponds to the one required for a specific service or procedure.

[2] European digital certificate: certificate issued by a qualified certification service approved by the European Union.

5. Related laws and regulations[3]

- Electronic Signature and Certificate Policy of the Spanish Public Administration (2012)
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- Royal Decree 4/2010, of 8 January, regulating the National Interoperability Framework in the field of Electronic Administration
- Law 26/2010, of 3 August, on the legal regime and procedure of the public administrations of Catalonia
- Law 29/2010, of 3 August, on the use of electronic means in the Public Sector of Catalonia
- Law 10/2011, of 29 December, on the simplification and improvement of regulatory legislation
- Resolution of 29 November 2012, of the Secretary of State for Public Administrations, publishing the Agreement approving the Electronic Signature and Certificate Policy of the General State Administration and announcing its publication on the corresponding website
- Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations
- Law 40/2015, of 1 October, on the Legal Regime of the Public Sector
- Law 6/2020, of 11 November, regulating certain aspects of electronic trust services
- Royal Decree 203/2021, of 30 March, approving the Regulation on the operation and functioning of the public sector through electronic means
- Order VPD/93/2022, of 28 April, approving the Catalogue of electronic identification and signature systems
- Royal Decree 311/2022, of 3 May, regulating the National Security Framework
- Order PRE/158/2022, of 30 June, approving the Guide on the use of electronic identification and signature systems within the Administration of the Government of Catalonia

Barcelona, 23 of May 2025

(This document is the English translation of the updated version of the Electronic Identification and Signature Policy approved and signed on 23 May 2025 by the Board of Directors of the Institut Ramon Llull. To view the original document, please refer to the Catalan version.)

[3] For more information, see the links in Annex I.

Annex I

Links of the related webs, laws and regulations:

- European Commission Trusted Services List (digital certificates)
- Electronic Signature and Certificate Policy of the Spanish Public Administration (2012) (es)
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- Royal Decree 4/2010, of 8 January, regulating the National Interoperability Framework in the field of Electronic Administration (es)
- Law 26/2010, of 3 August, on the legal regime and procedure of the public administrations of Catalonia (ca)
- Law 29/2010, of 3 August, on the use of electronic means in the Public Sector of Catalonia (ca)
- Law 10/2011, of 29 December, on the simplification and improvement of regulatory legislation (ca)
- Resolution of 29 November 2012, of the Secretary of State for Public Administrations, publishing the Agreement approving the Electronic Signature and Certificate Policy of the General State Administration and announcing its publication on the corresponding website (es)
- Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations (es)
- Law 40/2015, of 1 October, on the Legal Regime of the Public Sector (es)
- Law 6/2020, of 11 November, regulating certain aspects of electronic trust services (es)
- Royal Decree 203/2021, of 30 March, approving the Regulation on the operation and functioning of the public sector through electronic means (es)
- Order VPD/93/2022, of 28 April, approving the Catalogue of electronic identification and signature systems (ca)
- Royal Decree 311/2022, of 3 May, regulating the National Security Framework (es)
- Order PRE/158/2022, of 30 June, approving the Guide on the use of electronic identification and signature systems within the Administration of the Government of Catalonia (ca)

Annex 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] Available online at the following link: 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.