institut ramon llull
Llengua i cultura catalanes

POLÍTICA D'IDENTIFICACIÓ I SIGNATURA ELECTRÒNICA

INSTITUT RAMON LLULL

Versió 3.0

institut ramon llull
Llengua i cultura catalanes

Índex

institut ramon llull
Llengua i cultura catalanes

0. Històric de versions

Nom del document	Data	Descripció
Política d'identificació i signatura electrònica Institut Ramon Llull	18/03/2016	Versió 1.0
Política d'identificació i signatura electrònica Institut Ramon Llull	01/03/2017	Versió 2.0
Política d'identificació i signatura electrònica Institut Ramon Llull	23/05/2025	Versió 3.0

1. Introducció

La present Política d'Identificació i Signatura Electrònica de l'Institut Ramon Llull estableix el marc normatiu, tècnic i operatiu per garantir la seguretat jurídica i tècnica de les interaccions electròniques amb la ciutadania, empreses i altres administracions. Fonamentada en el Reglament (UE) 910/2014 del Parlament Europeu i del Consell, relatiu a la identificació electrònica i als serveis de confiança per a les transaccions electròniques al mercat interior, d'ara endavant Reglament eIDAS, la Llei 6/2020 i altres normatives estatals i autonòmiques. Aquesta política defineix els mecanismes d'identificació i signatura admesos, els perfils dels agents involucrats i els criteris de verificació aplicables a partir de l'any 2026. L'objectiu és facilitar un model interoperable, segur i adaptat a l'àmbit internacional en què opera l'entitat.

2. Consideracions generals

El Reglament eIDAS, normativa vigent que empara la llei espanyola 6/2020, reguladora de determinats aspectes dels serveis electrònics de confiança, defineix els següents conceptes (art. 3):

- Signatura electrònica: les dades en format electrònic annexes a altres dades electròniques o associades de manera lògica amb elles que utilitza la persona firmant per firmar.

- Signatura electrònica avançada: la firma electrònica que compleix els següents requisits (comentats a l'art. 26):
    - Estar vinculada al firmant de manera única

- Permetre la identificació del firmant
- Haver estat creada utilitzant dades de creació de la firma electrònica que el firmant pot usar, amb un alt nivell de confiança, sota el seu control exclusiu
- Estar vinculada amb les dades firmades per així poder detectar qualsevol modificació d'aquestes.

- Signatura electrònica qualificada: una firma electrònica avançada que es crea mitjançant un dispositiu qualificat de creació de signatures electròniques i que es basa en un certificat de signatura electrònica.

- Certificat de signatura electrònica: una declaració electrònica que vincula les dades de validació d'una firma amb una persona física i confirma, almenys, el nom o el pseudònim d'aquesta persona.

- Certificat qualificat de signatura electrònica: un certificat de signatura electrònica que ha sigut expedit per un prestador qualificat de serveis de confiança i que compleix els següents requisits (enumerats a l'Annex I):
  - Una indicació, almenys, en un format adequat per al processament automàtic, del fet que el certificat ha estat expedit com a certificat qualificat de signatura electrònica
  - Un conjunt de dades que representi inequívocament al prestador qualificat de serveis de confiança que expedeix els certificats qualificats, inclòs com a mínim l'Estat membre en el qual aquest prestador està establert, i:
    - Per persones jurídiques: el nom i el número de registre segons consti en els registres oficials, quan procedeixi
    - Per persones físiques: el nom de la persona
  - El nom del firmant o un pseudònim
  - Dades de validació de la signatura electrònica que corresponguin a les dades de creació de signatura electrònica
  - Dades relatives a l'inici i final del període de validació del certificat
  - El codi d'identitat del certificat, que ha de ser únic pel prestador qualificat de serveis de confiança
  - La signatura electrònica avançada o el segell electrònic avançat del prestador de serveis de confiança expedidor
  - El lloc en el qual està disponible, gratuïtament, el certificat que recolza la signatura electrònica avançada o el segell electrònic avançat
  - La localització dels serveis que poden utilitzar-se per consultar l'estat de validesa del certificat qualificat
  - Indicació en una forma apta pel processament automàtic quan les dades de creació de signatura electrònica relacionades amb les dades de validació de signatura electrònica es trobin en un dispositiu qualificat de creació de firma electrònica.

Quan es signen dades, el signant indica l'acceptació d'unes condicions generals i unes condiciones particulars aplicables a aquella signatura electrònica mitjançant la inclusió d'un camp signat, dins de la signatura, que especifica una política explícita o implícita.

Si el camp corresponent a la normativa de signatura electrònica està absent i no s'identifica cap normativa com aplicable, es podrà assumir que la signatura ha estat generada o verificada sense cap restricció normativa i, per tant, que no se li ha assignat cap significat concret legal contractual. Es tractaria d'una signatura que no especifica de forma expressa cap semàntica o significació concreta i, per tant, s'haurà de derivar el significat de la signatura a partir del context.

La finalitat d'un política de signatura és reforçar la confiança en les transaccions electròniques a través d'un sèrie de condicions per a un context donat, el qual pot ésser una transacció determinada, un requisit jurídic o un rol que assumeix la part signant, entre d'altres.

2.1. Objecte del document

La política d'identificació i signatura electrònica de l'Institut Ramon Llull té per objectiu establir el conjunt de criteris comuns en relació amb l'autenticació i la signatura electrònica, que afecta les relacions de l'entitat amb la ciutadania, empreses i la resta d'administracions públiques, segons allò previst en el Capítol II de la Llei 39/2015 d'1 d'octubre, del procediment administratiu comú de les administracions públiques.

En general, una política de signatura electrònica és un document legal que conté una sèrie de normes relatives al tema, organitzades al voltant dels conceptes de generació i validació de signatura, en un context particular (contractual, jurídic, legal, etc.), definint les regles i obligacions de tots els agents involucrats en el procés. L'objectiu d'aquest procés és determinar la validesa de la signatura per a una transacció en particular, especificant la informació que hauria d'incloure el signant en el procés de generació de la signatura i la informació que hauria de comprovar el verificador en el procés de validació de la mateixa.

El consorci de l'Institut Ramon Llull segueix les directrius de la política de signatura electrònica de l'Administració General de l'Estat. Així, tal com s'indica a l'article 18 de l'ENI (RD 4/2010), la institució compleix amb les condicions establertes a les normes tècniques d'interoperabilitat aplicables.

El manteniment, actualització i difusió de la Política d'identificació i signatura electrònica correspondrà a la Gerència de l'Institut Ramon Llull.

2.2. Àmbit d'aplicació

Aquesta política és d'aplicació a les relacions entre l'Institut Ramon Llull i la ciutadania, empreses i altres administracions públiques; que realitzen tràmits a través de la seu electrònica. La seva entrada en vigor serà l'1 de gener de 2026.

3. La política d'identificació i signatura electrònica

3.1. Abast de la política

Aquest document detalla les condicions generals per a la validació i la relació dels formats d'objectes binaris i fitxers de referència que hauran de ser admesos en els tràmits amb tercers mitjançant la seu electrònica de l'Institut Ramon Llull.

3.2. Agents involucrats

Els agents involucrats en el procés de creació i validació de signatura electrònica són:

- Signant: persona que disposa d'un dispositiu de creació de signatura i que actua en nom propi o en nom d'una persona física o jurídica a la qual representa.
- Verificador: entitat. Persona física o jurídica, que valida o verifica una signatura electrònica mitjançant el contrast amb les condicions exigides per una Política de Signatura concreta. Pot ser una entitat de validació de confiança o una tercera part que estigui interessada en conèixer la validesa d'una signatura electrònica.
- Prestador de serveis de signatura electrònica: la persona física o jurídica que expedeix certificats electrònics o presta altres serveis en relació amb la signatura electrònica.
- Emissor de la Política de Signatura Electrònica: entitat que s'encarrega de generar o gestionar el document de Política de Signatura, mitjançant el qual quedaran vinculats el signant i el verificador en els processos de generació i validació de la signatura electrònica.

4. Mecanismes d'identificació i signatura electrònica

4.1. Tipologia de mecanismes admesos

La Seu electrònica de l'Institut Ramon Llull admet els mecanismes d'identificació i signatura electrònica que es descriuen a continuació:

a. **Certificat digital**: mitjà d'identificació per a persones físiques i jurídiques, que determina tant la identitat de l'usuari com el seu tipus d'acreditació. El tipus de perfil d'acreditació identifica el grau de representació de la persona que s'identifica i actua envers tercers o ella mateixa. Aquesta darrera informació serà definida per les dades que incorpora el certificat digital que faci servir la ciutadania.
Els certificats digitals vàlids per a fer tràmits amb l'Institut Ramon Llull són els indicats per la Comissió Europea a la *Trusted Services List*[1] de prestadores de serveis de certificació. Si una persona física o jurídica disposa d'un certificat emès per alguna d'aquestes, podrà dur a terme els tràmits que desitgi amb qualsevol administració pública dels països inclosos a la UE, d'acord amb el que estableix el ReIDAS.

b. **IdCAT Mòbil**: mecanisme d'identificació i signatura electrònica per a persones físiques basat en l'enviament de paraules de pas d'un sol ús al mòbil. Cal registrar prèviament les dades de contacte al fitxer de la Seu electrònica de l'Administració de la Generalitat. Aquest servei el proporciona el Consorci d'Administració Oberta de Catalunya. També està disponible l'alta d'idCAT mitjançant la videoidentificació per a ciutadania resident fora de Catalunya, aquest sistema pot ser emprat per persones físiques de dins i fora d'Europa.

c. **Cl@ve:** sistema d'accés electrònic de la ciutadania als serveis públics. L'objectiu principal és poder-se identificar a l'Administració mitjançant claus (usuari i contrasenya), sense haver de recordar-ne més d'una per a diversos serveis. Cl@ve serveix tant per la identificació, l'autenticació i la signatura electrònica. Hi ha dos tipus de claus d'accés: la Cl@ve pin (per accessos esporàdics amb una validesa molt curta) i la Cl@ve permanent (per accessos habituals i amb una validesa més llarga).

d. Mecanisme no criptogràfic d'**acreditació** (usuari i contrasenya): L'Institut Ramon Llull s'encarrega de generar les dades i fer-les arribar d'una manera segura després d'haver verificat la documentació que acrediti la identitat de la persona física o jurídica sol·licitant. Per aquest motiu, si és la primera vegada que presenten una sol·licitud a l'Institut Ramon Llull i encara no disposen d'usuari i contrasenya, no podran realitzar el tràmit a través de la seu electrònica. A la seu electrònica hi ha la petició d'acreditació, que es facilita en un termini màxim de 72 hores. L'usuari i la contrasenya tenen una validesa de cinc anys a comptar a partir de la data de presentació

[1] L'enllaç es troba a l'Annex II.

de la documentació que acredita la identitat de la persona interessada, llevat que hi hagi hagut algun canvi.

Aquest sistema compta amb el doble factor d'autenticació (2FA), el qual consisteix en un segon factor temporal d'un sol ús, que es fa arribar a la persona interessada mitjançant un canal segur (correu electrònic verificat) per tal de poder finalitzar el tràmit. Aquesta acció és conforme al que estableixen el Reial decret 311/2022 (Esquema Nacional de Seguretat) i l'Ordre VPD/93/2022, i contribueix a garantir el nivell de seguretat mitjà exigible per a la tramitació electrònica amb l'Administració pública.

Atesa la previsió de supressió dels mecanismes d'identificació no criptogràfics (usuari i contrasenya) a partir del gener de 2026, la petició d'acreditació serà eliminada de la pàgina web de l'IRL. Aquest sistema es contemplarà com a excepcional i temporal en aquells casos en els quals sigui urgent la tramitació i no hagi estat possible per cap dels altres mitjans contemplats anteriorment. Amb tot, la validesa de les credencials ja no serà de cinc anys, sinó que serà d'ús temporal per a dur a terme el tràmit en qüestió.

4.2. Mecanismes d'identificació i signatura electrònica de la ciutadania i les entitats

RESIDÈNCIA	MECANISMES D'IDENTIFICACIÓ I SIGNATURA	PERFIL DEL SOL·LICITANT
Catalunya/ Espanya	Certificat digital	Persones físiques i persones jurídiques
	idCAT Mòbil	Persones físiques i persones jurídiques (representant legal)
	Cl@ve	Persones físiques i persones jurídiques (representant legal)
Resta de països (dins i fora de la UE)	Certificat digital europeu[2]	Persones físiques i persones jurídiques
	idCAT Mòbil	Persones físiques i persones jurídiques (representant legal)

[2] Certificat digital europeu: certificat emès per una entitat certificadora qualificada i admesa per la Unió europea.

Tal com s'indica a la taula, les persones jurídiques podran fer tràmits amb l'Institut Ramon Llull mitjançant la identificació d'una persona física com a representant legal de l'entitat o empresa en qüestió.

4.3. Mecanismes d'identificació i signatura electrònica de l'Institut Ramon Llull

El personal de l'Institut Ramon Llull utilitza el certificat reconegut o qualificat que el Consorci AOC emet als empleats del sector públic de Catalunya en dispositiu segur de creació de signatura, la T-CAT o T-CAT P, així com altres sistemes no criptogràfics, com ara els usuaris i contrasenyes de les plataformes EACAT i GICAR.

L'Institut Ramon Llull utilitza el codi segur de verificació (CSV), acceptat com a mecanisme de signatura electrònica dels ens de l'Administració de la Generalitat de Catalunya, i els certificats reconeguts o qualificats de segell electrònic que el Consorci AOC emet als ens del sector públic de Catalunya.

Les signatures electròniques avançades incorporen segells de temps generats pel servei segell de temps del Consorci AOC.

4.4. Criteris de verificació

Els atributs que podrà utilitzar el verificador per comprovar que es compleixen els requisits de la política de signatura segons la qual s'ha generat la signatura, independentment del format utilitzat, són les següents:

- *Signing Time*: només s'utilitzarà en la verificació de les signatures electròniques com a indicació per comprovar l'estat dels certificats en la data assenyalada, donat que únicament es poden assegurar les referències temporals mitjançant un segell de temps. Si s'ha realitzat el segellat de temps, el segell més antic dins l'estructura de la firma s'utilitzarà per determinar la data de la signatura.
- *Signing Certificate*: s'utilitzarà per comprovar i verificar l'estat del certificat (i, si s'escau, la cadena de certificació) en data de la generació de la signatura, en el cas que el certificat no hagi caducat i es pugui accedir a les dades de verificació o bé en el cas que el prestador ofereixi un servei de validació històric de l'estat del certificat (AOC).
- *Signature Policy*: s'haurà de comprovar que la política de signatura que s'ha utilitzat per a la generació de la signatura es correspon amb la que s'ha d'utilitzar per a un tràmit o servei concret.

5. Normativa relacionada[3]

- Política de Firma Electrònica y de Certificados de la Administración Pública Española (2012).
- Reglament (UE) núm. 910/2014, de 23 de juliol, del Parlament Europeu i del Consell relatiu a la identificació electrònica i als serveis de confiança per a les transaccions electròniques en el mercat interior.
- Reial Decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica.
- Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya.
- Llei 29/2010, de 3 d'agost, de l'ús dels mitjans electrònics al Sector Públic de Catalunya.
- Llei 10/2011, del 29 de desembre, de simplificació i millorament de la regulació normativa.
- Resolució de 29 de novembre de 2012, de la Secretaria d'Estat d'Administracions Públiques, per la qual es publica l'Acord d'aprovació de la Política de Signatura Electrònica i de Certificats de l'Administració General de l'Estat i s'anuncia la seva publicació a la seu corresponent.
- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.
- Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.
- Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveix electrònics de confiança.
- Reial Decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics.
- ORDRE VPD/93/2022, de 28 d'abril, per la qual s'aprova el Catàleg de sistemes d'identificació i signatura electrònica.
- Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.
- ORDRE PRE/158/2022, de 30 de juny, per la qual s'aprova la Guia d'ús dels sistemes d'identificació i signatura electrònica en l'àmbit de l'Administració de la Generalitat.

Barcelona, 23 de maig de 2025

[3] Els enllaços amb els textos normatius originals es troben a l'Annex I.

institut ramon llull
Llengua i cultura catalanes

Annex I

Enllaços de pàgines web i textos disponibles en línia referenciats:

- Llista de prestadores de certificats de confiança (UE): Trusted Services List
- Política de Firma Electrònica y de Certificados de la Administración Pública Española (2012)
- Reglament (UE) núm. 910/2014, de 23 de juliol, del Parlament Europeu i del Consell relatiu a la identificació electrònica i als serveis de confiança per a les transaccions electròniques en el mercat interior.
- Reial Decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica.
- Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya.
- Llei 29/2010, de 3 d'agost, de l'ús dels mitjans electrònics al Sector Públic de Catalunya.
- Llei 10/2011, del 29 de desembre, de simplificació i millorament de la regulació normativa.
- Resolució de 29 de novembre de 2012, de la Secretaria d'Estat d'Administracions Públiques, per la qual es publica l'Acord d'aprovació de la Política de Signatura Electrònica i de Certificats de l'Administració General de l'Estat i s'anuncia la seva publicació a la seu corresponent.
- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.
- Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.
- Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveix electrònics de confiança.
- Reial Decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics.
- ORDRE VPD/93/2022, de 28 d'abril, per la qual s'aprova el Catàleg de sistemes d'identificació i signatura electrònica.
- Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.
- ORDRE PRE/158/2022, de 30 de juny, per la qual s'aprova la Guia d'ús dels sistemes d'identificació i signatura electrònica en l'àmbit de l'Administració de la Generalitat.

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.

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

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 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.