institut ramon llull barcelona 08008/diagonal 373/ tel. (+34) 93467 80 00 /fax (+34) 93467 80 06 /irl@llull.cat www.llull.cat

INSTITUT RAMON LLULL

ELECTRONIC IDENTIFICATION AND SIGNATURE POLICY

Version 2.0

INDEX

1 GENERAL CONSIDERATIONS

Electronic Signature Act 59/2003, of 19 December, defines electronic signature making a distinction between the following concepts:

- Electronic signature: data in electronic form, attached to or associated with other data, which may be used as a means of identifying the signatory.
- Advanced electronic signature: electronic signature capable of identifying the signatory and detecting any subsequent change in the signed data, uniquely linked to the signatory and to the data and which has been created through means that the signatory can keep under his/her sole control.
- Qualified electronic signature: advanced signature based on a qualified certificate and generated through a secure signature creation device.

In order for an electronic signature to be considered an advanced electronic signature in the terms of Act 59/2003, the following requisites are implied:

- Identification: enabling the signatory's identity to be guaranteed uniquely.
- Integrity: guaranteeing that the content of a data message has remained complete and unaltered, independently of any changes undergone by the medium containing it as a result of the communication, filing or submission process.
- Non-repudiation: assurance that messages in an electronic communication cannot be denied.

When data are signed, the signatory indicates acceptance of general conditions and particular conditions applicable to that electronic signature through the inclusion of a signed field, within the signature, that specifies an express or implied policy.

If the field corresponding to the electronic signature regulation is absent and no legislation is identified as being applicable, it may be assumed that the signature has been generated or verified with no regulatory restriction and, therefore, no specific contractual legal meaning has been assigned to it. This would be a signature that does not expressly specify any specific semantics or meaning and, therefore, the meaning of the signature would have to be derived from the context.

The purpose of a signature policy is to reinforce trust in electronic transactions through a number of conditions for a given context, which may be a certain transaction, a legal requirement or a role undertaken by the signatory, among others.

1.1 Object of the document

The purpose of the Institut Ramon Llull electronic signature policy is to establish common criteria in relation to authentication and electronic signature affecting the Institute's relations with citizens, in accordance with the provisions of article 24.1 of Royal Decree 1671/2009, of 6 November, partially developing Act 11/2007, of 22 June, on citizens' access to public services.

In general, an electronic signature policy is a legal document containing a set of rules concerning electronic signature, organized around concepts of signature generation and validation, in a particular context (contractual, legal, etc.), defining the rules and obligations of all the parties involved in the process. The purpose of this process is to determine the validity of the signature for a particular transaction, specifying the information that the signatory must include in the signature generation process and the information that the verifier must check in the signature validation process.

1.2 Scope of application

This policy is applicable to relations between citizens and the Institut Ramon Llull in the actions they carry out through the electronic site.

2 ELECTRONIC SIGNATURE POLICY

2.1 Scope of the signature policy

This document proposes an electronic signature policy that details the general conditions for validation and a list of formats of binary objects and reference files that are to be admitted in operations with third parties through the electronic site of the Institut Ramon Llull.

2.2 Policy identification particulars

Document name	Electronic identification and signature policy
Version	2.0
Date of issue	1.03.2017
Scope	This policy is applicable to relations between citizens and the Institut Ramon Llull in the actions they carry out through the electronic site.

2.3 Parties involved

The parties involved in the electronic signature creation and validation process are:

- Signatory: person with a signature creation device acting on his/her own behalf or on behalf of a natural or legal person he/she is representing.
- Verifier: entity. Natural or legal person that validates or verifies an electronic signature by checking against the conditions required by a specific Signature Policy. This may be a trust validation entity or a third party interested in knowing the validity of an electronic signature.
- Electronic signature service provider: the natural or legal person that issues electronic certificates or provides other services in relation to the electronic signature.
- Electronic Signature Policy Issuer: entity that undertakes to generate or manage the Signature Policy document through which the signatory and the verifier are bound in the electronic signature generation and validation processes.

2.4 Management of the signature policy

The maintenance, updating and electronic publication of this document shall correspond to Management of the Institut Ramon Llull.

When updating the document, the place where the validator may find previous versions in order to verify an electronic signature made prior to the current policy will be identified.

3 ELECTRONIC IDENTIFICATION AND SIGNATURE MECHANISMS

3.1 Type of mechanisms accepted

The Institut Ramon Llull electronic site accepts the electronic identification and signature mechanisms described below:

a. Digital certificates issued by all certifying entities classified by the Open Administration Consortium of Catalonia (*Consorci d'Administració Oberta de Catalunya*) as valid for identifying citizens and companies in their dealings with Catalan public administrations.

   The digital certificate is therefore a means of identification that determine both the user's identity and his/her type of accreditation. The type of accreditation profile determines the level of representation of the person identified and acting on behalf of third parties and/or him/herself. This information will be determined by the data incorporated in the digital certificate used by citizens.

b. The IdCat_Mobile citizen-oriented identification and electronic signature mechanism based on sending single-use passwords to a mobile. Contact details must first be recorded in the file at the Electronic Office of the Government of Catalonia. This service is provided by the Catalan Open Administration Consortium. It is a mechanism accepted only for middle-level administrative processes.

c. The ID mechanism, a non-cryptographic system involving username and password, which the Institut Ramon Llull will undertake to generate and transmit securely to interested persons after verifying the documentation attesting to their identity. This mechanism grants access solely to the case file to which it is associated.

d. Non-cryptographic username and password mechanism for non-resident foreign citizens. The Institut Ramon Llull undertakes to generate and transmit it securely to non-resident foreign citizens after verifying the documentation attesting to their identity. Accordingly, non-resident foreign citizens who are submitting an application to the Institut Ramon Llull for the first time and therefore do not have a username and password will be unable to submit the application using the electronic site.

   The username and password are valid for five years as of the date of presenting the documentation attesting to the interested person's identity, unless there has been a change.

   Unlike the ID mechanism, the username and password mechanism grants access to all the applicant's case files.

The incorporation of new electronic identification and signature mechanisms as they become available on the market for users of the subjective scope will take place in accordance with the provisions of section 2.4 of this document.

3.2 Electronic identification and signature mechanisms according to type of act

The electronic identification and signature mechanisms vary according to the significance of the act being carried out. The aim of the electronic signature policy is to indicate the contemplated uses for a given sphere and with a given scope, specifying the conditions required for each of the corresponding uses in accordance with ruling legislation.

Section 8.3 of Order GRI/233/2015, of 20 July, approving the Protocol for electronic identification and signature, establishes that a low security level will be required in electronic identification and signature systems for all the electronic transactions or electronics services of an administrative procedure, except for the following: submitting applications,, presenting declarations of responsibility, filing appeals, withdrawing from actions or waiving rights. Accordingly, for **procedural acts** carried out by citizens

through the electronic site of the Institut Ramon Llull, low-level mechanisms are accepted (for instance, the **ID mechanism).**

On the other hand, to **submit applications, present supporting documentation, present declarations of responsibility, file appeals, withdraw from actions or waive rights,** the use of identification and/or signature mechanisms of a higher security level is required, specifically **digital certificates** and **IdCat Mobile** (middle-level). In the case of foreigners who are not residents in Spain, both the **username and password mechanism** will be accepted.

3.3 Electronic identification and signature mechanisms in relation to the signatory

3.3.1 Spanish citizens and foreign citizens who are residents in Spain

a. Submitting applications

To submit an application through the electronic office of the Institut Ramon Llull you must have the pertinent **digital certificate**, as described in section 3.1.a) or **IdCat_Mobile** as described in section 3.1 b).

In the case of legal persons, **digital certificates** for natural persons or **IdCat Mobile** are accepted as long as the certificate identifies the legal representative of the legal person.

As established in section 3.1.a), in the virtual office digital certificates issued by all certifying entities classified by the Catalan Certifying Agency as valid to identify natural persons and legal persons in dealings with Catalan public administrations where validation of the certificate is carried out through their identification and signature services platform (VÀLID) may be used.

It should be borne in mind that depending on the service or act in question, the list of accepted certificates may be restricted under the provisions of particular aspects of its security policy and/or regulations.

b. Presentation of documents for ongoing case files

In the case of declarations of responsibility, withdrawals, waivers, supporting documentation or appeals, Spanish citizens and residents in Spain who wish to present such documents electronically must have the corresponding **digital certificate** or **IDCAT Mobile**. On the other hand, presentation of all other documents through the electronic site in the context of an ongoing case file may be carried out either using the corresponding electronic certificate or using the **ID mechanism** described in section 3.1.c).

c. Presentation of supporting documentation

In order to present supporting documentation using electronic media, the beneficiary must have a digital certificate. To assure that they match the originals, all supporting documents must be signed with a **digital certificate** or **IdCat Mobile**, following the steps described in the **Guide for presenting supporting documents electronically**.

3.3.2 Foreign citizens who are not residents in Spain

a. Submitting applications

To identify non-resident foreign citizens, the identification system with **username and password** on the electronic site is used (section 3.1.c).

The Institut Ramon Llull undertakes to send the username and password in a secure manner to interested persons after verifying the documentation attesting to their identity. Accordingly, non-resident foreign citizens who are submitting an application to the Institut Ramon Llull for the first time and therefore do not have a username and password will be unable to submit the application using the electronic site.

b. Presentation of documents for ongoing case files

In the case of declarations of responsibility, withdrawals, waivers, supporting documentation or appeals, foreign citizens who are not resident in Spain who wish to present such documents electronically must user the username and password identification system. On the other hand, presentation of all other documents through the electronic site in the context of an ongoing case file may be carried out also using the **ID mechanism**

c. Presentation of supporting documentation

In order to present supporting documentation using electronic media, it is necessary to use **username and password** system and follow the steps described in the **Guide for presenting supporting documents electronically**.

3.4 Institut Ramon Llull electronic identification and signature mechanisms

Institut Ramon Llull personnel use the qualified certificate which the AOC Consortium issues to public sector employees in Catalonia in a secure signature creation device, the T-CAT, as well as other non-cryptographic systems, such as the usernames and passwords of the EACAT and GICAR platforms.

The Institut Ramon Llull uses the secure verification code (SVC), accepted as an electronic signature mechanism of bodies of the Administration of the Catalan Government, and the qualified electronic seal certificates that the AOC Consortium issues to Catalan public sector bodies.

Advanced electronic signatures incorporate time stamps generated by the time stamp services of the AOC Consortium.

3.5 Verification criteria

The attributes that the verifier may use to check that the signature policy requisites according to which the signature has been generated are met, independently of the format used, are as follows:

- *Signing Time*: used only in the verification of electronic signatures as an indication to check the status of certificate on the date indicated, as time references can only be assured through a time stamp. If time is stamped, the oldest stamp in the signature structure will be used to determine the date of signature.

- *Signing Certificate*: used to check and verify the certificate status (and, as the case may be, the certification path) on the date the signature is generated, if the certificate has not expired and the verification data can be accessed or if the provider offers a historic validation service of the certificate status.

- *Signature Policy*: it will be checked that the signature policy used to generate the signature is the correct policy to be used for a specific action or service.

4 REFERENCES

- Regulation (EU) number 910/2014 of the European Parliament and of the Council, of 23 July, on electronic identification and trust services for electronic transactions in the internal market.
- Act 11/2007, of 22 June, on electronic access by citizens to public services.
- Royal Decree 1671/2009, of 6 November, partially developing Act 11/2007, de 22 June, on citizens' electronic access to public services.
- Royal Decree 3/2010, of 8 January, regulating the National Security Scheme in the area of Electronic Administration.
- Royal Decree 4/2010, of 8 January, regulating the National Interoperability Scheme in the area of Electronic Administration.
- Decree 56/2009, of 7 April, for the promotion and development of electronic media in the Administration.
- Act 26/2010, of 3 August, on the legal regime and procedure of public administrations of Catalonia.
- Act 29/2010, of 3 August, on the use of electronic media in the Public Sector in Catalonia.
- Act 10/2011, of 29 December, on the simplification and improvement of regulation.
- Order GRI/233/2015, of 20 July, approving el Protocol for electronic identification and signature.
- Public sector legal system act, Law 40/2015 of 1st October 2015
- Public Administrations and Common Administrative Procedure Act, Law 39/2015 of 1 October

Barcelona, 1 March 2017

Josep Marcé i Calderer

Manager

5 APPENDIX: ELECTRONIC PRESENTATION OF DOCUMENTS

Electronic identification and signature mechanisms admissible for each act or document.

SPANISH CITIZENS and FOREIGN CITIZENS WHO ARE RESIDENTS IN SPAIN		
	Document signature	**Document submission**
Application	**Digital Certificate/ idCat Mobile**	**Digital Certificate/ idCat Mobile**
Declarations of responsibility	**Digital Certificate/ idCat Mobile**	**Digital Certificate/ idCat Mobile/ID**
Withdrawal	**Digital Certificate/ idCat Mobile**	**Digital Certificate/ idCat Mobile/ID**
Waiver	**Digital Certificate/ idCat Mobile**	**Digital Certificate/ idCat Mobile/ID**
Appeal	**Digital Certificate/ idCat Mobile**	**Digital Certificate/ idCat Mobile/ID**
Supporting documentation form	**Digital Certificate/ idCat Mobile**	**Digital Certificate/ idCat Mobile/ID**
Invoices and proof of payment	**Digital Certificate/ idCat Mobile**	**Digital Certificate/ idCat Mobile/ID**
Other documents	**Not required**	**Digital Certificate/ idCat Mobile/ID**

FOREIGN CITIZENS WHO ARE NOT RESIDENTS IN SPAIN	
	Document signature Document submission
Application	**User/password**
Declarations of responsibility	**User/password**
Withdrawal	**User/password**
Waiver	**User/password**
Appeal	**User/password**
Supporting documentation form	**User/password**
Invoices and proof of payment	**User/password**
Other documents	**User/password**