

Certification services provided by ESCB-PKI's Certification Authority Application form for ESCB/SSM users

Certificate applicant's data¹

Personal data

First name²

Middle name (if any)²

Surname²

[National identity number³]

[Birth date³]

[Birth place³]

Central Bank / National Competent Authority related data
--

CB / NCA²

ESCB User ID²

E-mail address²

Employee number³

Technical data

Certificate level

Token serial number

By signing this document and upon receipt of the ESCB-PKI certificate, you (hereinafter “you” or “certificate applicant”) agree to the following terms and conditions, and acknowledge the ESCB-PKI certification practice statement (“CPS”) and the certificate policies (“CP”) for the ESCB/SSM users’ certificates, as well as any modifications of those documents. The ESCB-PKI will not contact you to communicate any change to these documents, but they are available at <https://pki.escb.eu>.

Inon

The validation of the identity has been carried out based on the employee identification card or an official identification document according to the legislation applicable to the central bank or national competent authority acting as registration authority

.....
Name and signature of the certificate applicant

.....
Name and signature of the person who validates the certificate applicant’s identity

¹ In line with Section 9.4.3 of the CPS, each CP shall establish the personal data to be included in the personal certificates. Acceptance by the applicants of the certificates issued in their name constitutes their consent to publish the certificates in the repositories described in section 2.2 of the CPS and CP. Access to the repositories is granted on a need-to-know basis.

² Information to be included in the certificate.

³ Either the number of a national recognized identity document, according to the legislation applicable to the central bank or national competent authority acting as registration authority, or the date and place of birth, or, in the alternative, if the certificate applicant has already been identified by the central bank or national competent authority acting as registration authority through a face-to-face identification process and a proof of identity, the number of the employee identification card or the employee number if this is printed on the employee identification card

Terms and Conditions

These Terms and Conditions constitute the terms and conditions between you and your central bank or national competent authority, in representation of the Eurosystem central banks and the European Central Bank (as the owners of the ESCB-PKI), for the provision of the ESCB-PKI services as described in the CPS and the corresponding CP. The terms used in these ESCB-PKI Terms and Conditions will have the meaning given to them in the CPS and the CP unless stated otherwise. These Terms and Conditions shall, therefore, be binding upon both you (the certificate applicant) and your central bank or national competent authority. Your central bank or national competent authority shall endeavour to ensure that their users comply with their obligations.

1. Obligations

The certificate applicant/you shall:

- 1.1 Provide accurate, full and truthful information when filling the application form.
- 1.2 Inform its central bank (hereinafter “CB”) or national competent authority (hereinafter “NCA”) of any modification of personal data collected in this form.
- 1.3 Limit the certificate’s use to the boundaries set out in his/her contractual relationship with the CB/NCA.
- 1.4 Take the necessary security measures within its control in order to avoid any loss, modification or unauthorised use of the cryptographic card.
- 1.5 Be responsible for the secure custody of the PIN and PUK secret numbers for activation and unlocking the cryptographic card.
- 1.6 Request the revocation of the certificate in case the data specified in the certificate changes, or when you have knowledge that the private key might be under risk due to, among other causes, loss, theft, or knowledge by third parties of the PIN and/or PUK.
- 1.7 Not monitor, manipulate or carry out any reverse engineering (i.e. try to discover the technical principles through analysis of its structure, function or operation) on the technical implementation (hardware and software) of the certification services.
- 1.8 Not transfer or delegate to third parties the obligations pertaining to the certificate assigned to them (e.g. not transfer the cryptographic card or the PIN and PUK).

2. Personal data protection

In compliance with the [General Data Protection Regulation](#) and the [Regulation \(EU\) 2018/1725](#), please be informed that the personal data recorded in this form shall be processed by the members of the [European System of Central Banks](#) (ESCB), as joint controllers, and, in particular, by the Banco de España, as service provider, for the purpose of providing the data subject with a digital certificate on the basis of the performance of a task carried out in the public interest -article 6.1(b) of the General Data Protection Regulation and article 5.1(a) of the Regulation (EU) 2018/1725- pursuant to the following decisions of the European Central Bank (ECB):

- [Decision of the ECB of 11 January 2013 laying down the framework for a public key infrastructure for the ESCB \(ECB/2013/1\), as amended by Decision of the ECB of 11 December 2015 \(ECB/2015/46\);](#) and
- [Decision of the ECB of 11 December 2015 on the access and use of SSM electronic applications, systems, platforms and services by the ECB and the national competent authorities of the SSM \(ECB/2015/47\).](#)

Besides the data subject, personal data might be disclosed to the following recipients:

- Designated employees of the ESCB members and SSM competent authorities with assigned ESCB-PKI roles (e.g. registration officers, Banco de España’s employees acting as service providers...).
- Data processors acting on behalf of the joint controllers (e.g. support and maintenance services); and
- Public administrations, judicial bodies and competent supervisory authorities in compliance with legal obligations.

Likewise, certain details recorded on issued certificates (i.e. full name, ID number, corporate email or public key) might be accessible by IAM account ESCB users through IAM IDM and White Pages.

Personal data shall be retained for 15 years in compliance with the applicable legal regulations. Once the retention period expires, or in the event a data subject exercises a right of erasure or objection, the personal data shall remain stored solely for the purposes of addressing potential liabilities deriving from the processing during the statute of limitations, after which the data shall be deleted.

Data subjects may exercise their rights of access, rectification, objection, erasure and other rights referred to in the General Data Protection Regulation and the Regulation (EU) 2018/1725, properly evidencing their identity:

- In person or by ordinary post addressed to the Banco de España’s DPO at Calle Alcalá 48, 28014, Madrid, or
- By electronic means through the procedure referred to in BDE’s [Privacy Policy](#).

Should the data subjects consider their rights have not been observed, they may contact [Banco de España’s DPO](#) or file a claim with the competent [Data Protection Authorities](#).

3. Limitation of liability

The Eurosystem central banks and the European Central Bank do not assume any liability whatsoever for the content of documents signed using its certificates, nor for any other use of its certificates, such as message or communication encipherment processes.