Certification services provided by ESCB-PKI's Certification Authority
Certificate reactivation form

Certificate Subscriber's Data

Personal Data		
First name		
Middle name		
Surname		
Central Bank Related Data		
Organisation		
ESCB User ID		
E-mail address		
Technical Data		
Certificate level	☐ STANDARD	☐ ADVANCED

By signing this document and upon receipt of the ESCB-PKI certificate, You (hereinafter "You" or "Certificate Subscriber") request to reactivate your suspended certificate as described in the Certification Practice Statement ("CPS") and the corresponding Certificate Policy ("CP"). The CSP and the CP can be accessed at http://pki.escb.eu.

In .....on .....

Name and signature of the Certificate Subscriber	Name and signature of the person who validates the Certificate Subscriber's identity

Terms and Conditions

These Terms and Conditions constitute the terms and conditions between You and the ESCB-PKI's Certification Authority for the provision of the ESCB-PKI Services as described in the CPS and the corresponding CP (the "ESCB-PKI Terms and Conditions"). Any used terms in these ESCB-PKI Terms and Conditions will have the same meaning given in the CPS and the CP unless stated otherwise. These Terms and Conditions shall, therefore, be binding upon both You (the Certificate Subscriber) and the ESCB-PKI's Certification Authority (CA).

1. Obligations

The Certificate Subscriber shall:

1.1 Provide accurate, full and truthful information when filling the application form.

1.2. Inform the ESCB-PKI of any data modification.

1.3. Limit the certificate's use to the boundaries set out in his/her contractual relationship with the CB and in the CPS and corresponding CP.

1.4. Take the all necessary security measures in order to avoid any loss, disclosure, modification or unauthorised use of the cryptographic card issued.

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 certificate's revocation in case of data application form's variation or inaccuracy, or when 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 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.

1.9. Fulfil any other obligation derived from the applicable legislation, the CPS or the CP.

2. Personal Data Protection

Personal data contained in the secure Certificate's Directory and provided in the application form are deem to be personal data pursuant to the Spanish Personal Data Protection Act (*Ley Orgánica de Protección de Datos de Carácter Personal, LOPD*) and related regulation.

Certificate Subscribers are, therefore, informed and agree that the personal data provided in his/her application form will be recorded and process by the Banco de España as the ESCB-PKI Service Provider, for the sole purpose of providing the PKI services and the generation of the certificates. Certificate Subscribers might access, rectify and cancel his/her personal data by contacting Banco de España at the following address or through the CB Registration Officer below:

Name	Information Systems Department Banco de España's ESCB-PKI Policy Administration Authority
E-mail address	escb-pki@pki.escb.eu
Address	C/Alcala, 48. 28014 - Madrid (Spain)

3. Limitation of liability

Banco de España, as ESCB-PKI Service Provider, does not accept 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.