What if …

Your token is lost / stolen

Suspend your certificates
https://ra-pki.escb.eu/epkuser/hold
Obtain a new token
Request certificates (Reason: Lost certificate)

Your token is damaged

Obtain a new token
Request certificates (Reason: Replaced token)

Your certificates are about to expire

Request certificates (Reason: Certificate expiration)

You have forgotten your PIN & PUK

Obtain a new token
Request certificates (Reason: Replaced token)

Other issues

Contact with your Local Service Desk.

To learn more

Have a look at:

The ESCB-PKI subscriber's guide (end-user procedures)
The ESCB-PKI RA subscriber's manual (end-user RA tool)
The FAQ section in the ESC-PKI Website
http://pki.escb.eu

Terms & Conditions

Certificate Subscriber's obligations

1 Provide accurate, full and truthful information regarding the data requested by those entrusted with their verification in order to carry out the registration process.

2 To inform the corresponding RA of any modification to said data.

3 To understand and accept the terms and conditions of use of the certificates and, specifically, those contained in this CPS and the applicable CPs, as well as any modifications thereto.

4 To restrict and condition the use of the certificates to that permitted under the corresponding CP and this CPS.

5 To take reasonable precautions for the safekeeping of their cryptographic card, preventing its loss, modification or unauthorised use.

6 The process to obtain the certificates requires the personal selection of a control PIN for the cryptographic card and activation of the private keys and a PUK for unlocking. The subscriber is responsible for keeping the PIN and PUK numbers secret.

7 To immediately request the RA the revocation or suspension of a certificate upon detecting any inaccuracy in the information contained therein or upon becoming aware of or suspecting any compromise of the private key corresponding to the public key contained in the certificate due, among other causes, to: loss, theft, potential compromise, knowledge by third parties of the PIN and/or PUK.

8 Not monitor, manipulate or carry out any reverse engineering on the technical implementation (hardware and software) of the certification services.

9 Not to transfer or delegate to third parties their obligations pertaining to a certificate assigned to them.

10 Any other obligation under this CPS or the CP.

ESCB-PKI

QUICK REFERENCE

http://pki.escb.eu

ECB-PUBLIC

BANCO DE ESPAÑA
Eurosistema

2012/02

What is a digital certificate?

"A digital certificate is an electronic document which uses a digital signature to bind a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual". (Wikipedia)

It can provide...

Authentication	Access to systems and/or applications on a secure way;
Confidentiality	Keep the privacy of information;
Integrity	Exchange information with third parties being sure it has not been modified; and
Non repudiation	Ensure that the sender cannot deny what he sent.

You can request two different kinds of certificates:

Standard	The keys and certificates will be stored in a file protected by a PIN
Advanced	The keys and certificates will be generated and stored in your personal secure token (protected by your PIN)

Documentation needed

The following documentation will be needed to request a personal certificate:

A valid document to verify your identity (i.e. national id. card)

A valid document to verify your relation with the Central Bank (i.e. employee id. card)

Requesting a certificate

1. Preparation

Prepare a copy of the documentation needed to verify your identity and your relation with the Central Bank

Obtain your secure token and set your personal PIN **(*)**

2. Request

Request your ESCB-PKI certificates

Select the reason: new certificate; certificate expiration; lost certificate; replaced token/unrecoverable certificate

3. Validation/Acceptance

Validate the information included in the terms & conditions document

Sign the document

4. Download

Option 1: face-to-face download

Insert your secure token **(*)**

Type your PIN

Option 2: remote download

Access to the ESCB-PKI web application
https://ra-pki.escb.eu/epkuser/delivery

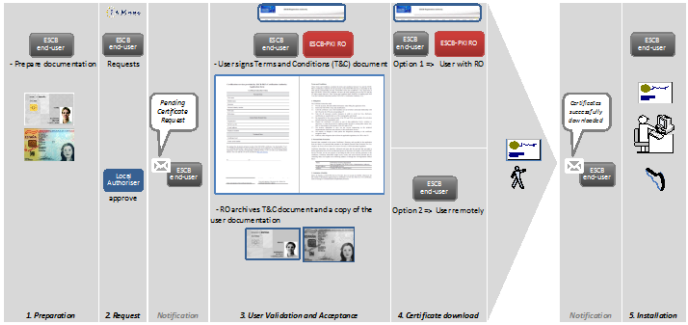
Insert your secure token **(*)**

Type your PIN

5. Verify your certificate (advisable)

Access to the ESCB-PKI web service to verify the requested certificates
http://pki.escb.eu/epkweb/en/support.html

(*) Only applicable for advanced certificates requests



Advanced certificate request

How to …

Set your suspension code

Choose your suspension code

Access to the ESCB-PKI web service
https://ra-pki.escb.eu/epkuser/certmgt

Select the option ***suspension code***

Manage your certificates

Access to the ESCB-PKI web service
https://ra-pki.escb.eu/epkuser/certmgt

Change the PIN of your token

Download and install the token driver in your PC
http://pki.escb.eu/epkweb/en/support.html

Select the option ***Token → Change PIN***