BANCO DE ESPAÑA
Eurosistema

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI PROJECT

REGISTRATION OFFICER’S GUIDE

VERSION 3.1

ECB-Restricted
31-December-2023

TABLE OF CONTENTS

TABLE OF ILLUSTRATIONS

Project name:	ESCB-PKI
Author:	ESCB-PKI Project team
File name:	ESCB-PKI - Registration Officer's Procedures v.3.1.docx
Version:	3.1
Date of issue:	31.12.2023
Status:	Final
Approved by:	
Distribution:	

RELEASE NOTES

In order to follow the current status of this document, the following matrix is provided. The numbers mentioned in the column "Release number" refer to the current version of the document.

Release number	**Status**	**Date of issue**	**Revisions**
0.1	Draft	07.10.2011	Initial version
0.2	Draft	15.10.2011	Several additions
0.10	Draft	14.11.2011	BdE Revision
0.13	Draft	28.11.2011	BdE Revision
1.0	Draft	24.01.2012	Version for SRM-WG revision
1.1	Final	13.03.2012	Final version
1.2	Final	29.10.2012	Adaptation to the Legal Framework
1.3	Final	15.04.2014	Introduction of new certificate types
2.0	Final	11.09.2018	BdE Revision
3.0	Final	20.12.2022	Terms and Conditions acceptance procedure update
3.1	Final	31.12.2023	Updated http links to ESCB-PKI website to https

GLOSSARY AND ACRONYMS

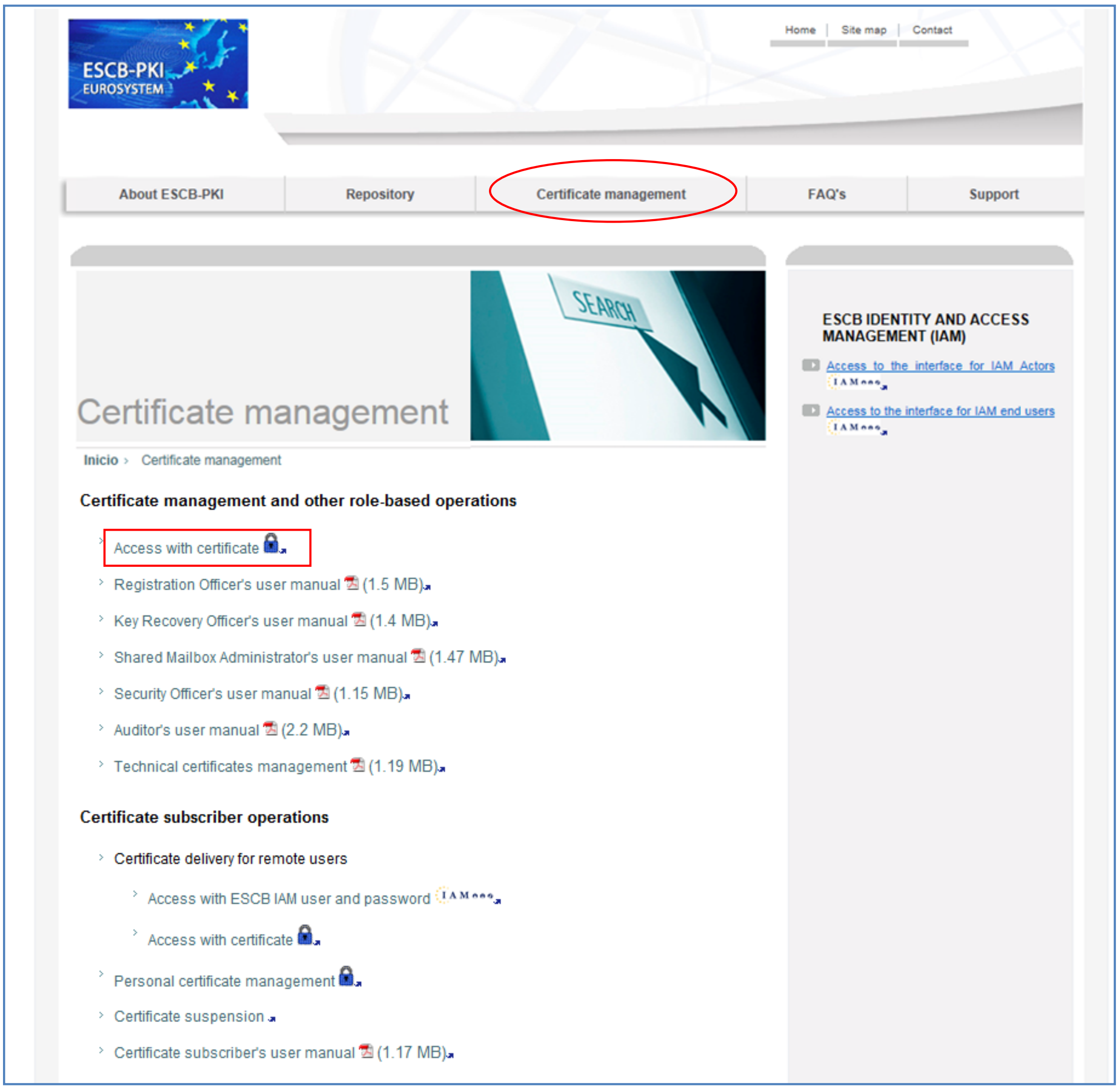
Acronym	Definition
ESCB-PKI	European System of Central Banks - Public Key Infrastructure
FAQ	Frequently Asked Questions
IAM	Identity and Access Management
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SSCD	Secure Signature Creation Device

1. INTRODUCTION

The present document aims at providing information on how to manage ESCB-PKI certificates from the Registration Officer 's point of view.

1.1. CERTIFICATE MANAGEMENT

In the ESCB-PKI Website click on the ***Certificate management*** tab. This page contains the list of the ESCB-PKI services available. Click the ***Access with certificate*** link available in the ***Certificate management and other role-based operations*** section. You will be asked for a certificate to authenticate with, and any CAF compliant advanced authentication certificate mapped to your account will be valid to authenticate (not only ESCB-PKI certificates).



Certificate management and other role-based operations

- Access with certificate
- Registration Officer's user manual (1.5 MB)
- Key Recovery Officer's user manual (1.4 MB)
- Shared Mailbox Administrator's user manual (1.47 MB)
- Security Officer's user manual (1.15 MB)
- Auditor's user manual (2.2 MB)
- Technical certificates management (1.19 MB)

Certificate subscriber operations

- Certificate delivery for remote users
  - Access with ESCB IAM user and password
  - Access with certificate
- Personal certificate management
- Certificate suspension
- Certificate subscriber's user manual (1.17 MB)

ESCB IDENTITY AND ACCESS MANAGEMENT (IAM)

- Access to the interface for IAM Actors
- Access to the interface for IAM end users

Figure 1 - ESCB-PKI Website: Certificate management

2. PERSONAL CERTIFICATES PROVIDED BY THE ESCB-PKI

The following certificates will be available for ESCB users:

Software-based

1) Standard certificates: used for authentication, signing and encryption.

2) Mobile device certificates: used within mobile devices for authentication and signature.

3) Secure e-mail gateway: to be installed in a secure e-mail gateway to sign and encrypt on behalf of the end user.

Token-based

1) Advanced certificates: used for authentication, signing and encryption.

2) Administrator certificates: used for users that have got a second account that they use for administrator tasks. They are mainly valid for authentication although they can also be used for signature.

3) Provisional certificates: used temporarily when a user with token-based certificates (either advanced or administrator) has forgotten his smartcard or token. They have limited lifetime.

The difference between standard and advanced certificates relies on where the digital certificate is kept: while for token-based certificates the private keys are stored inside a physical token (i.e. smart card, USB token, etc.), for software-based certificates the private keys are stored in a software container such as a file or a keystore.

This simple difference has further implications regarding the level of trust that can be achieved. The usage of token-based certificates provides a higher level of trust.

2.1. SOFTWARE-BASED CERTIFICATES

According to the *ESCB Identity and Access Management Policy* software-based certificates can be used to authenticate against applications with a criticality assessment up to Medium.

ESCB-PKI provides the following types of software-based certificates:

- Standard certificates: general purpose software-based certificate valid for authentication, signature and encryption
- Mobile device certificates: typically used in a mobile device for authentication and signature. This certificate can be complemented with a copy of the encryption private key that is part of an advanced certificate package and that has been recovered in software format.
- Secure e-mail gateway certificates: certificate valid for encryption and signature to be installed in a secure e-mail gateway to implement secure e-mail.

2.2. TOKEN-BASED CERTIFICATES

According to the *ESCB Identity and Access Management Policy*, token-based certificates can be used to authenticate against applications which have a criticality assessment Medium, High or Very High.

ESCB-PKI provides the following types of token-based certificates:

- Advanced certificates: this is a package of three different certificates: i) authentication, ii) signature and iii) encryption. Depending on what your Central Bank has decided, there could be two different types of advanced certificate packages:
  - Advanced certificate package with encryption key recovery.
    - The authentication and signature private keys are generated inside the cryptographic token, so that there is not any other copy. Therefore, these certificates are considered "advanced"
    - The encryption private key is generated by the Certification Authority and stored i) in the token and ii) in the Key Archive. In the future you will be able to recover a copy of the encryption private key from the Key Archive in software or token-based formats when i) your smartcard card has been replaced and you need to decrypt old information or ii) you need a software-based copy of your encryption private key to be stored in a mobile device. Since the private key can be recovered in software-based format, this certificate is considered "standard"
  - Advanced certificate package without encryption key recovery.
    - The authentication, signature and encryption private keys are generated inside the cryptographic token, so that there is not any other copy. Therefore, the three certificates are considered "advanced". You have to take into account and, if your smartcard is replaced, you will not be able to decrypt old information that was encrypted for you.
- Administrator certificates: this is a single certificate mainly valid for authentication, although you can also use it for signature. This certificate is used in case that you have got an account that is linked to the authentication certificate included in the advanced certificate package, and a second account used for administrator tasks and that is linked to this certificate. The private key is generated inside the token.
- Provisional certificates: this is a certificate with a limited lifetime that is stored in a provisional token in case that you have forgotten your smartcard or token with advanced or administrator certificates. The certificate is valid for authentication and signature. The certificate will expire at the end of the date of the issuance. Optionally, your Registration Officer can request a longer certificate with the maximum lifetime defined by your Central Bank's Security Officer.

3. ESCB-PKI REGISTRATION OFFICER PROCESSES

3.1. REQUEST CERTIFICATES. FACE-TO-FACE REQUESTS

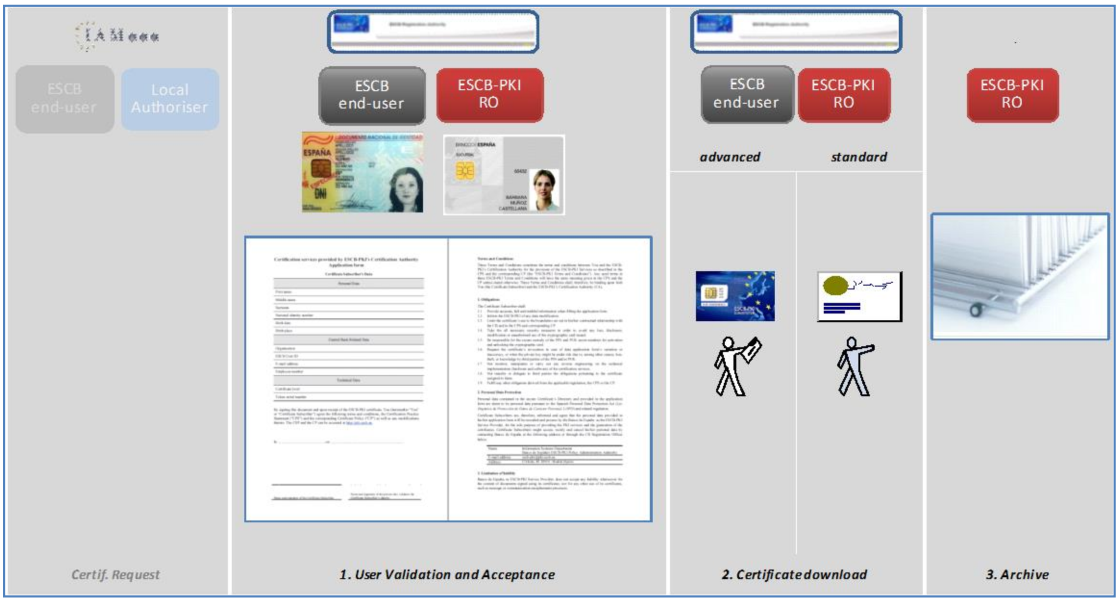


Figure 2 - Face-to-face requests

The process, which will be described in greater detail in the following sections, can be summarized as follows:

1) In case the request is a token-based certificate, the user did not fill the serial number to the request, and a new token is expected to be needed because the reason for the renewal is not certificate expiration or superseded, you will receive a notification to assign the user a token and fill the request with that token serial number.

2) The user will come to you with all the documentation needed. You must validate user's identity and the documentation provided. According to the Certificate Policy the documentation presented by the user must be

    a. If the user requesting the certificate has already been identified by the Central Bank through a face-to-face identification process and a proof of identity, the employee identification card is accepted as sufficient to identify the certificate applicant.
    This could be the normal situation for Central Bank employees.

    b. If the user requesting the certificate has not already been identified by the Central Bank using a formal process, the user must present a legal document accepted by the legislation applicable to the Central Bank acting as Registration Authority to dully identify an individual.
    This would be the normal situation for non ESCB users (belonging to external organizations).

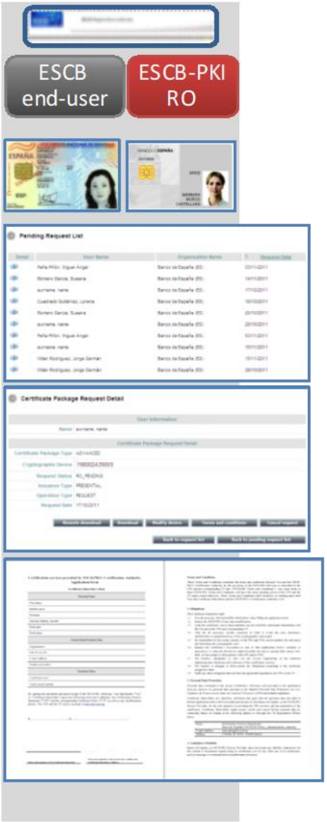
3) The user must accept and sign the Terms and Conditions (T&C) document online.

4) You can start the certificate download process.

5) According to the ESCB-PKI CPS an evidence of the signed Terms and Conditions document will be kept for 15 years.

3.1.1. STEP 1: VERIFY USER'S IDENTITY

The user will come to you holding the documentation needed to obtain the requested certificates:



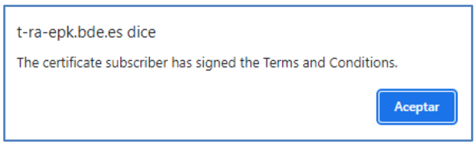
1) In the ESCB-PKI Website select the "**Certificate management**" option. You have to authenticate using your certificate.

2) In the ***Pending Request*** link select the request associated with the user clicking on the 👁 button. The details of the request will be shown.

3) Validate the correctness of the information included (validate it against the user documentation).

4) Check whether the Terms and Conditions have already been signed or not by using the "*Terms and Conditions*" button.

   If the user has signed this document, you will see the following pop-up when clicking on the button:

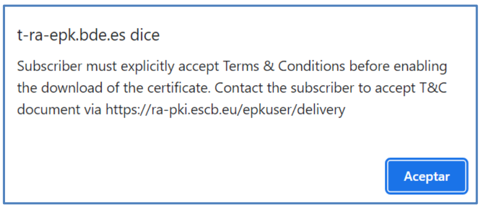


t-ra-epk.bde.es dice

The certificate subscriber has signed the Terms and Conditions.

Figure 3 - Terms and Conditions already accepted pop up

Whereas if the signature of the Terms and Conditions document is still pending the pop-up would look like the following:



t-ra-epk.bde.es dice

Subscriber must explicitly accept Terms & Conditions before enabling the download of the certificate. Contact the subscriber to accept T&C document via https://ra-pki.escb.eu/epkuser/delivery

Figure 4 - Terms and Conditions not accepted yet pop up

6) According to the ESCB-PKI CPS an evidence of the signed Terms and Conditions document will be kept for 15 years.

3.1.2. STEP 2: TOKEN-BASED CERTIFICATE DOWNLOAD

1) Ask the user to insert their personal secure token in the reader and click on the ***Download*** button.

2) The system will present the list of certificates that will be generated. Click on the ***Accept*** button

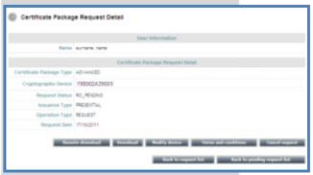
3) The system will request the PIN of the token. Ask the user to introduce it

   - The key-pairs will be generated into the secure token. The process will take some time because, in the case of the advanced certificate package, three key-pairs will be generated (authentication, encryption and signing)
   - The 3 certificates will be generated and stored in the secure token

4) According to the ESCB-PKI CPS these documents must be kept for 15 years.

ESCB end-user

ESCB-PKI RO



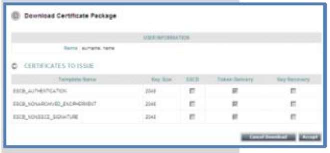
Certificate Package Request Detail

User Information

Name: surname, name

Certificate Package Request Detail

Certificate Package Type	ADVANCED
Cryptographic Device	1880002A39005
Request Status	RO_PENDING
Issuance Type	PRESENTIAL
Operation Type	REQUEST
Request Date	17/10/2011



Download Certificate Package

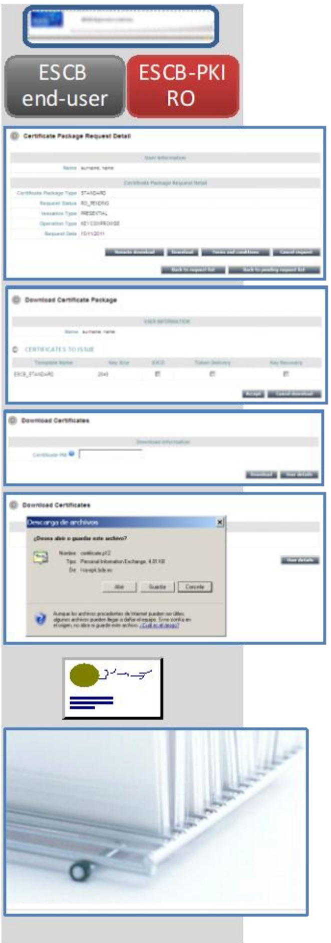
USER INFORMATION

Name: surname, name

CERTIFICATES TO ISSUE

Template Name	Key Size	ESCB	Token Delivery	Key Recovery
ESCB_AUTHENTICATION	2048	☐	☑	☐
ESCB_NONARCHIVED_ENCIPHERMENT	2048	☐	☑	☐
ESCB_NONSSCD_SIGNATURE	2048	☐	☑	☐

3.1.3. STEP 2: SOFTWARE-BASED CERTIFICATE DOWNLOAD



1) Click on the ***Download*** button.

2) The details of the certificate are shown. Click on the ***Accept*** button.

3) The system will request a PIN to protect both the certificate and keys generated.

   - Ask the user to type in their PIN and click on the ***Download*** button.

4) A File Download dialog box will pop up asking "***Do you want to open or save this file***?"

   - Click **Save** to download the keys into a file protected by the PIN.

   ⚠ **DO NOT SELECT THE OPEN OPTION!!**[1]

The certificate will be downloaded to the local system, protected by the PIN; this will ensure that only the user and no one else can access to the private key.

5) According to the ESCB-PKI CPS these documents must be kept for 15 years.

NOTE: Recommend the user to keep this file as a backup copy of their certificate. This will permit them to recover the certificate in the future in case it gets damaged.

[1] When you open a .p12 file Windows will automatically start the installation of the certificate in your PC

3.2. REQUEST CERTIFICATES. REMOTE REQUESTS

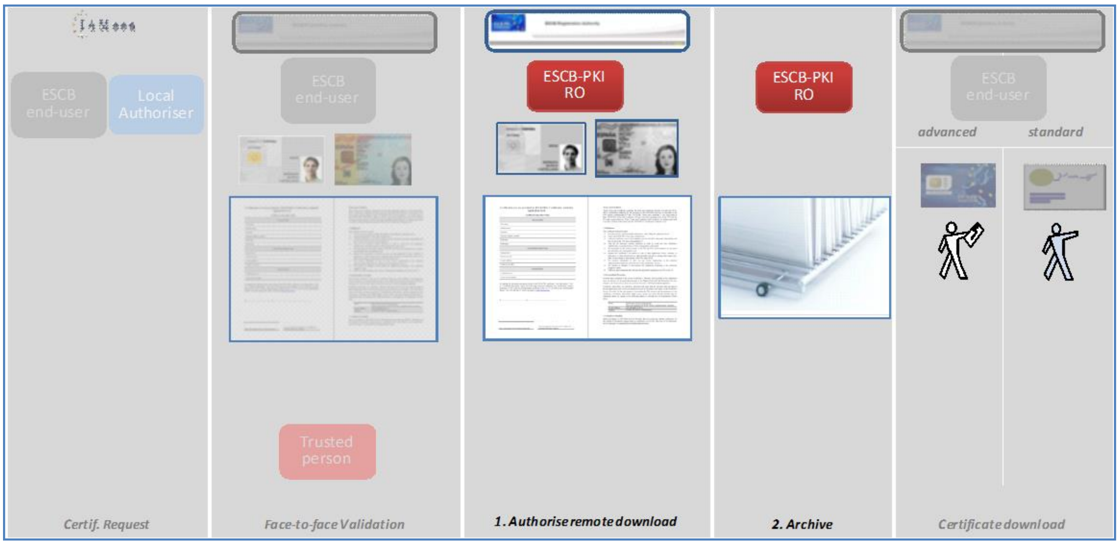


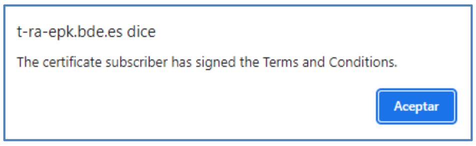
Figure 5 - Remote requests

The process, which will be described in greater detail in the following sections, can be summarized as follows:

1) In case the request is a token-based certificate, the user did not fill the serial number to the request, and a new token is expected to be needed because the reason for the renewal is not certificate expiration or superseded, you will receive a notification to assign the user a token and fill the request with that token serial number.

2) Check whether the Terms and Conditions have already been signed or not by using the "*Terms and Conditions*" button.

   If the user has signed this document, you will see the following pop-up when clicking on the button:

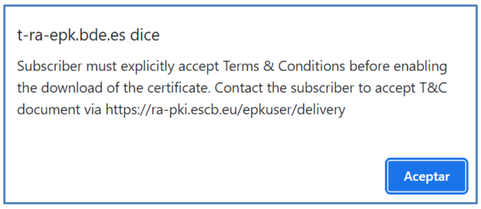


t-ra-epk.bde.es dice

The certificate subscriber has signed the Terms and Conditions.

Figure 6 - Terms and Conditions already accepted pop up

   Whereas if the signature of the Terms and Conditions document is still pending the pop up would look like the following:



t-ra-epk.bde.es dice

Subscriber must explicitly accept Terms & Conditions before enabling the download of the certificate. Contact the subscriber to accept T&C document via https://ra-pki.escb.eu/epkuser/delivery

Figure 7 - Terms and Conditions not accepted yet pop up

3) The user will accept and sign Terms and Conditions (T&C) document online and send, when required, a copy of the documentation used to identify them.

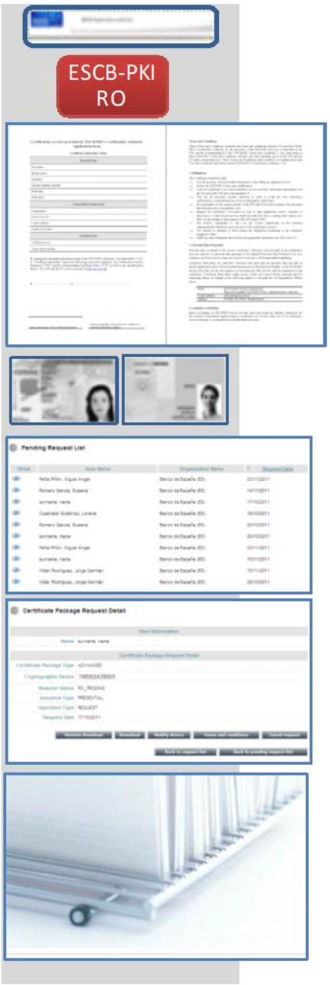
   – If the user requesting the certificate has already been identified by the Central Bank through a face-to-face identification process and a proof of identity, the employee identification card is accepted as sufficient to identify the certificate applicant and there is no need to send a copy of this document. This could be the normal situation for Central Bank employees.

   – If the user requesting the certificate has not already been identified by the Central Bank using a formal process, the user must present a legal document accepted by the legislation applicable to the Central Bank acting as Registration Authority to dully identify an individual and a copy of the document must be sent to the RO.
     This would be the normal situation for non ESCB users (belonging to external organizations).

4) You must validate the documentation provided. If everything is correct you can authorize the remote download.

5) According to the ESCB-PKI CPS these documents must be kept for 15 years.

3.2.1. STEP 1: VERIFY USER'S IDENTITY AND AUTHORISE REMOTE DOWNLOAD



The Terms and Conditions document must be accepted and signed online by the user and the personal documentation has to be validated by a trusted person (i.e. the user's local manager or the user's IAM local authoriser).

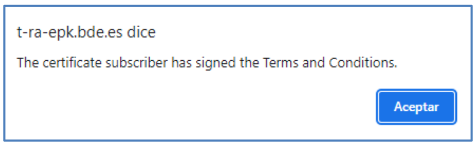
To validate the information received and authorise the remote download:

1) In the ESCB-PKI Website select the "**Certificate management**" option. You have to authenticate using your certificate.

2) In the ***Pending Request*** link select the request associated to the user clicking on the button. The details of the request will be shown.

3) Check whether the Terms and Conditions have already been signed or not by using the "*Terms and Conditions*" button.

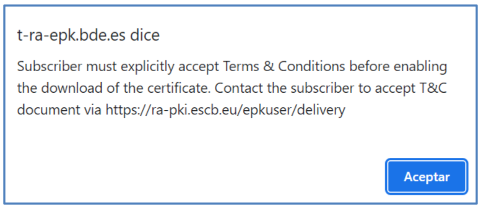
   If the user has signed this document, you will see the following pop-up when clicking on the button:


t-ra-epk.bde.es dice

The certificate subscriber has signed the Terms and Conditions.

Figure 8 - Terms and Conditions already accepted pop up

   Whereas if the signature of the Terms and Conditions document is still pending the pop-up would look like the following:


t-ra-epk.bde.es dice

Subscriber must explicitly accept Terms & Conditions before enabling the download of the certificate. Contact the subscriber to accept T&C document via https://ra-pki.escb.eu/epkuser/delivery

Figure 9 - Terms and Conditions not accepted yet pop up

4) If everything is correct authorise the remote download clicking on the ***Remote download*** button.

5) According to the ESCB-PKI CPS these documents must be kept for 15 years.

3.3. REQUEST PROVISIONAL CERTIFICATES

Users may forget their token sometimes. You may request provisional certificates for them using directly the ESCB-PKI.

To request a provisional certificate:

1) In the ESCB-PKI Website select the "**Certificate management**” option. You will have to authenticate using your certificate.

2) Using the ***Search user*** link search the user. The column in the righter side of the search results allows to directly creating a provisional certificates request for the user.

3.4. REACTIVATE SUSPENDED CERTIFICATES

Users may ask you to reactivate their suspended certificates in case they suspended them for any reason and after that they discover that no compromise has taken place.

To reactivate a certificate:

3) In the ESCB-PKI Website select the "**Certificate management**” option. You will have to authenticate using your certificate.

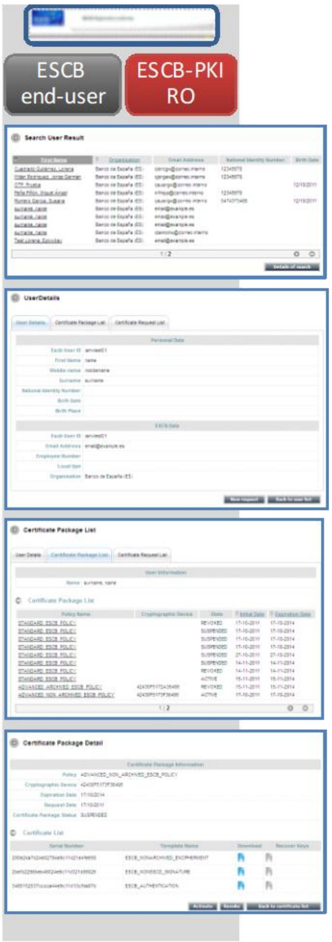
4) Using the ***Search user*** link search the user. Select the user.

5) Click on the Certificate package list tab.

6) Select the certificates the user wants to get reactivated.

7) Click on the ***Reactivate*** button.

IMPORTANT: Suspended certificates will be revoked after 60 days of their suspension.



3.5. REVOKE CERTIFICATES

Users may ask you to revoke their certificates if they discover that their private keys have been compromised.

In order to revoke a certificate the process is similar to the previous one:

1) In the ESCB-PKI Website select the "**Certificate management**" option. You will have to authenticate using your certificate.

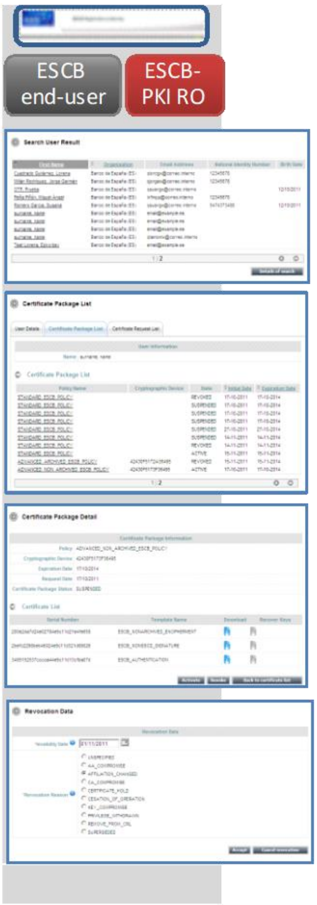
2) Using the ***Search user*** link search the user. Select the user.

3) Click on the Certificate package list tab.

4) Select the certificates the user wants to revoke.

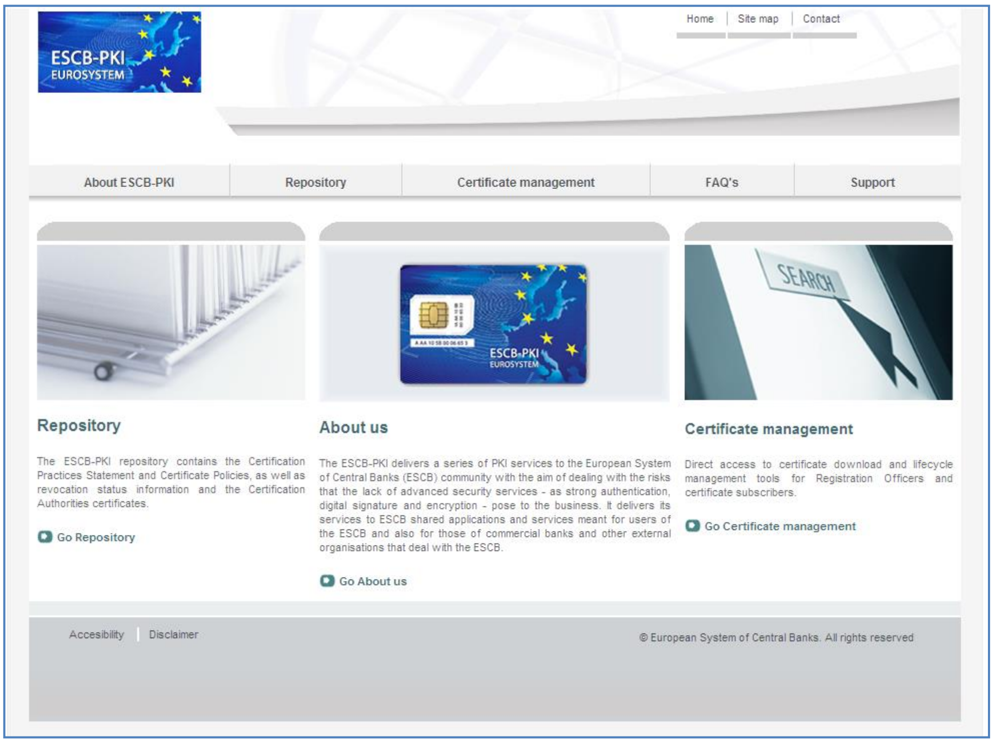
5) Click on the ***Revoke*** button.

6) Type the date for the revocation request, select the reason to revoke the certificates and click on the ***Accept*** button.



4. MORE INFORMATION ABOUT ESCB-PKI

For further information see the ESCB-PKI Website, https://pki.escb.eu (you may want to bookmark this site for future references).The Frequently Asked Questions (FAQ) section will be your best source of support information.



Repository

The ESCB-PKI repository contains the Certification Practices Statement and Certificate Policies, as well as revocation status information and the Certification Authorities certificates.

About us

The ESCB-PKI delivers a series of PKI services to the European System of Central Banks (ESCB) community with the aim of dealing with the risks that the lack of advanced security services - as strong authentication, digital signature and encryption - pose to the business. It delivers its services to ESCB shared applications and services meant for users of the ESCB and also for those of commercial banks and other external organisations that deal with the ESCB.

Certificate management

Direct access to certificate download and lifecycle management tools for Registration Officers and certificate subscribers.

© European System of Central Banks. All rights reserved

Figure 10 - ESCB-PKI Website

In the ESCB-PKI Website you will find the following information:

- ***About ESCB-PKI*** Generic information with regards to the ESCB-PKI services.
- ***Repository*** ESCB-PKI public information: Certificate Practice Statement (CPS) document, Certificate Policy (CP) documents, Certificate Authority certificates, CRLs, etc.
- ***Certificate management*** ESCB-PKI Registration Authority tool.
- ***FAQ*** Frequently asked questions.
- ***Support*** Software needed to manage ESCB-PKI tokens and utilities to test ESCB-PKI certificates.

Note: The last version of this document can be found in the ESCB-PKI Website, along with other ESCB-PKI guides and manuals.