

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI PROJECT



ESCB-PKI REGISTRATION AUTHORITY APPLICATION

KEY RECOVERY OFFICER'S MANUAL

VERSION 3.1

TABLE OF CONTENTS

GLOSSARY AND ACRONYMS 6

1. Introduction 7

 1.1. The Key Recovery Process 7

 1.2. The ESCB-PKI Website 8

2. The ESCB-PKI Registration Authority application 9

 2.1. System requirements 9

 2.2. Layout 9

 2.3. Access 11

3. ESCB-PKI RA: Key Recovery processes 12

 3.1. Initiate a key recovery request 13

 3.2. Approve a token key recovery request 15

 3.3. Approve a software key recovery request 16

 3.4. Cancel a key recovery request 17

 3.5. Process a pending token key recovery request 18

4. ESCB-PKI RA: Other available options 20

 4.1. Search users 20

 4.1.1. User details 21

 4.1.2. Certificate package list 21

 4.1.3. Certificate request list 22

 4.2. Pending request list option 24

5. More information about ESCB-PKI 25

TABLE OF ILLUSTRATIONS

Figure 1 - The Key Recovery Process 7

Figure 2 - ESCB-PKI Website 8

Figure 3 - Production frame..... 9

Figure 4 - Acceptance frame..... 10

Figure 5 - Certificate Management..... 10

Figure 6 - ESCB-PKI Website - Registration Authority Application 11

Figure 7 - Certificate management 12

Figure 8 - Organisation user list 13

Figure 9 - Certificate list..... 13

Figure 10 - Certificate details..... 13

Figure 11 - Initiate a key recovery process 14

Figure 12 - Key recovery request generated 14

Figure 13 - Mail to participate in the key recovery process 15

Figure 14 - Mail to participate in the key recovery process 16

Figure 15 - Key recovery request list 17

Figure 16 - Key Recovery request detail (requestor KRO) 17

Figure 17 - Key Recovery request detail (other KROs)..... 18

Figure 18 - Process a Key Recovery request 18

Figure 19 - Complete the Key Recovery request 18

Figure 20 - Starting recovery process 19

Figure 21 - Download keys and certificate 19

Figure 22 - Encryption key recovered 19

Figure 23 - Certificates management. Search user option 20

Figure 24 - Organisation user list..... 20

Figure 25 - User details 20

Figure 26 - User details 21

Figure 27 - Certificate list..... 21

Figure 28 - Certificate details..... 22

Figure 29 - Certificate requests list..... 22

Figure 30 - Certificate Request details..... 23

Figure 31 - Pending requests list 24

Figure 32 - Request detail..... 24

Figure 33 - ESCB-PKI Website 25

Project name:	ESCB-PKI
Author:	ESCB-PKI Project team
File name:	ESCB-PKI - RA Application Key Recovery Officer's Manual v.3.1.docx
Version:	3.1
Date of issue:	07-11-2024
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
1.0	final	10.10.2012	Initial version
1.1	Final	15.04.2014	Update of the ESCB-PKI website
2.0	Final	11.09.2018	Added the software recovery
3.0	Final	15.11.2021	Compatibility with other browsers
3.1	Final	07.11.2024	Update <i>http</i> links to <i>https</i>

GLOSSARY AND ACRONYMS

Acronym	Definition
CA	Certificate Authority
CB	ESCB Central Bank (ECB or NCB)
CP	Certification Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
ECB	European Central Bank
ESCB	European System of Central Banks, including the ECB and the NCBs of all States member of the European Union (regardless of whether they use the Euro or not).
ESCB-PKI	European System of Central Banks - Public Key Infrastructure
IAM	Identity and Access Management
NCB	National Central Bank
PKI	Public Key Infrastructure
KRO	Key Recovery Officer
RA	Registration Authority

1. INTRODUCTION

This document aims at providing Key Recovery Officers (KRO) information on how to use the ESCB-PKI Registration Authority application to recover encryption keys.

1.1. THE KEY RECOVERY PROCESS

Key Recovery Officers (KROs) participate during the recovery of encryption key pairs from the Key Archive **when the owner of the key pair is not present**. This process is only available at those Central Banks that request the use of the Key Recovery service. Four-eye principle will always be required to recover any key pair and, therefore, there shall be at least two KROs at each CB as to carry away the process of Key recovery without the participation of the subscriber.

Recovery of encryption certificates requested by someone else than the certificate subscriber will involve the participation of, at least, **K** different KROs of the total **M** KROs available at the subscriber's Central Bank. The precise values for **K** and **M** will be determined by the Central Bank.

- K** is the minimum number of KROs that MUST participate in a key recovery process
- M** is the total number of KROs nominated at the Central bank

The KROs shall assume one or more of the following interim roles for every key recovery operation:

- The **Requestor KRO** will request the key recovery of an encryption key pair
- The **Approver KROs** endorse the recovery request placed by the Requestor KRO
- The **Operator KRO** recovers the key pair and stores it in a cryptographic token

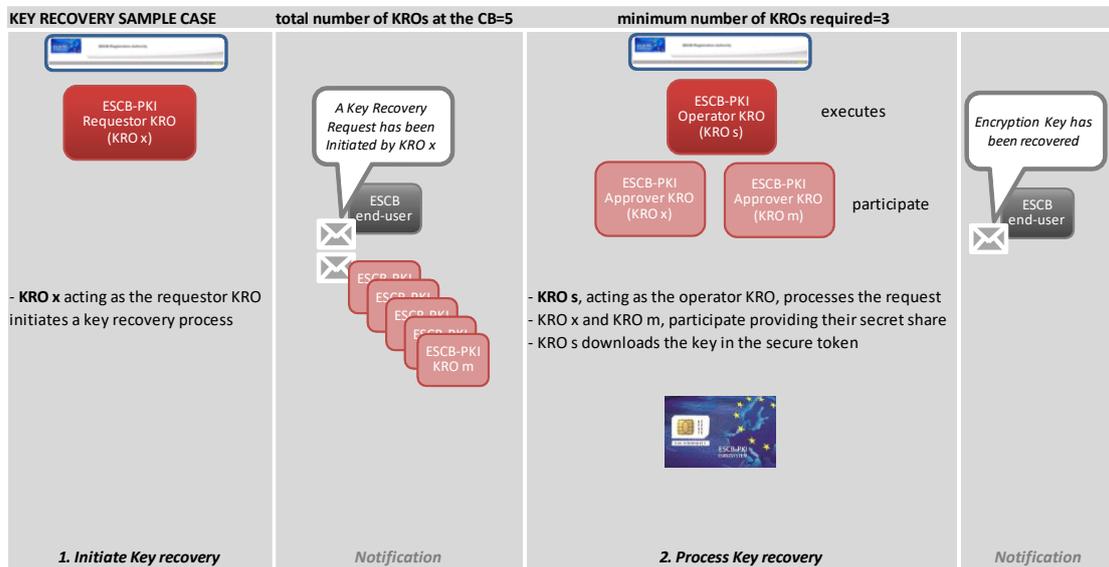


Figure 1 - The Key Recovery Process

In the example shown in the figure above, the procedure will be the following:

- One of the KROs, acting as a **Requestor KRO**, requests the key recovery of an encryption key pair that belongs to a particular subscriber from that Central Bank;
- All the KROs (5) from the CB receive an e-mail with one of the 5 pieces of a shared secret. It is required the participation of at least 3 KROs to get access to the encryption certificate. These 3 KROs will act as **Approver KROs**;

- One of the KROs, acting as the **Operator KRO** (cannot be the same that the Requestor KRO), introduces her piece of the shared secret and the shared secret of other 2 **Approver KROs**;
- The **Operator KRO** recovers the key pair and stores it in a cryptographic token.

1.2. THE ESCB-PKI WEBSITE

From this Website you can have access to the ESCB-PKI services and you can also find additional information connected to certificate management, token management and Public Key Infrastructures.

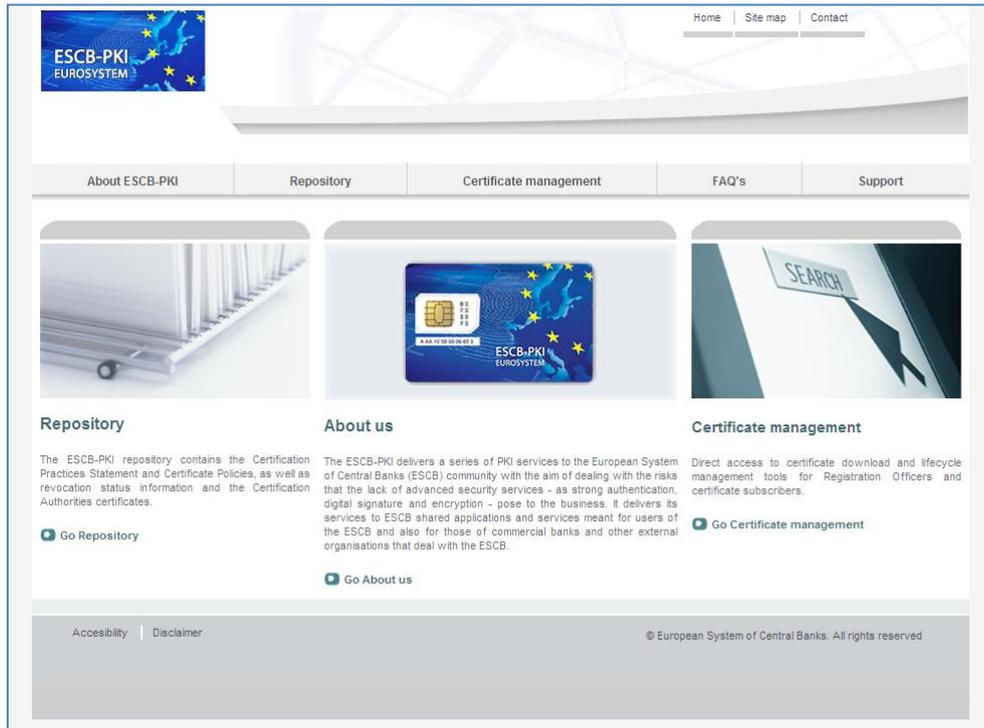


Figure 2 - ESCB-PKI Website

To access to the ESCB-PKI services, open your web browser and type the following URL address, <https://pki.escb.eu/>. 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 (CA) certificates, Certificate Revocation Lists (CRLs), etc.
- **Certificate management** ESCB-PKI Registration Authority application links and related guidelines
- **FAQ** Frequently Asked Questions
- **Support** Software needed to manage ESCB-PKI tokens and utilities to test ESCB-PKI certificates

2. THE ESCB-PKI REGISTRATION AUTHORITY APPLICATION

2.1. SYSTEM REQUIREMENTS

The following software is required to use the ESCB Registration Authority application:

- ESCB-PKI Smartcard drivers
- Native application required to manage certificates in a smart card.
- One of the following web extensions of your choice, according to your browser preferences:
 - Mozilla Firefox ESCB-PKI Certificate Enrollment extension.
 - Chrome and Edge ESCB-PKI Certificate Enrollment extension.

Instructions on the installation of the aforementioned software are available in the ESCB-PKI User guide - Browser configuration, which may be downloaded from the ESCB-PKI portal support area:

<https://pki.escb.eu/epkweb/en/support.html>

The following browsers have been thoroughly tested and are therefore recommended:

- Internet Explorer 11
- Google Chrome 94
- Mozilla Firefox 92
- Microsoft Edge 95

Note. - “JavaScript” and “Cookies” must be enabled in the web browser for the application to work properly.

2.2. LAYOUT

Please be aware that two different ESCB-PKI services environments are reachable by ESCB-PKI customers: acceptance and production. Each environment has a different frame colour so the customer can easily tell the difference and use the one that better suits their intended usage; furthermore, the acceptance environment includes an acceptance label in the upper right position indicating that the acceptance environment is the one being accessed.

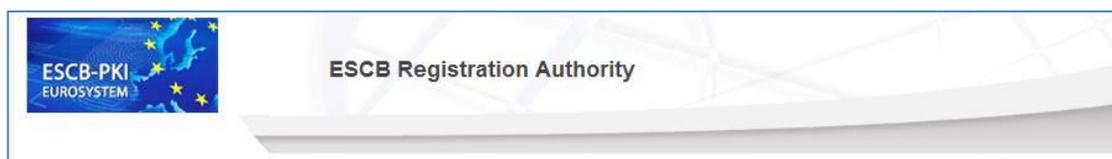


Figure 3 - Production frame



Figure 4 - Acceptance frame

After logging into RA application the following features will always be available to the user:

- A menu will be shown on the left frame to facilitate quick access to all available options
- A **Logout** option in the upper-right corner to end the user session

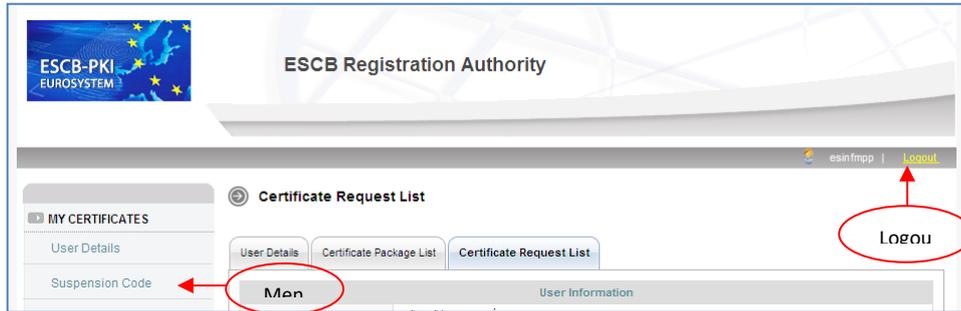


Figure 5 - Certificate Management

2.3. ACCESS

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

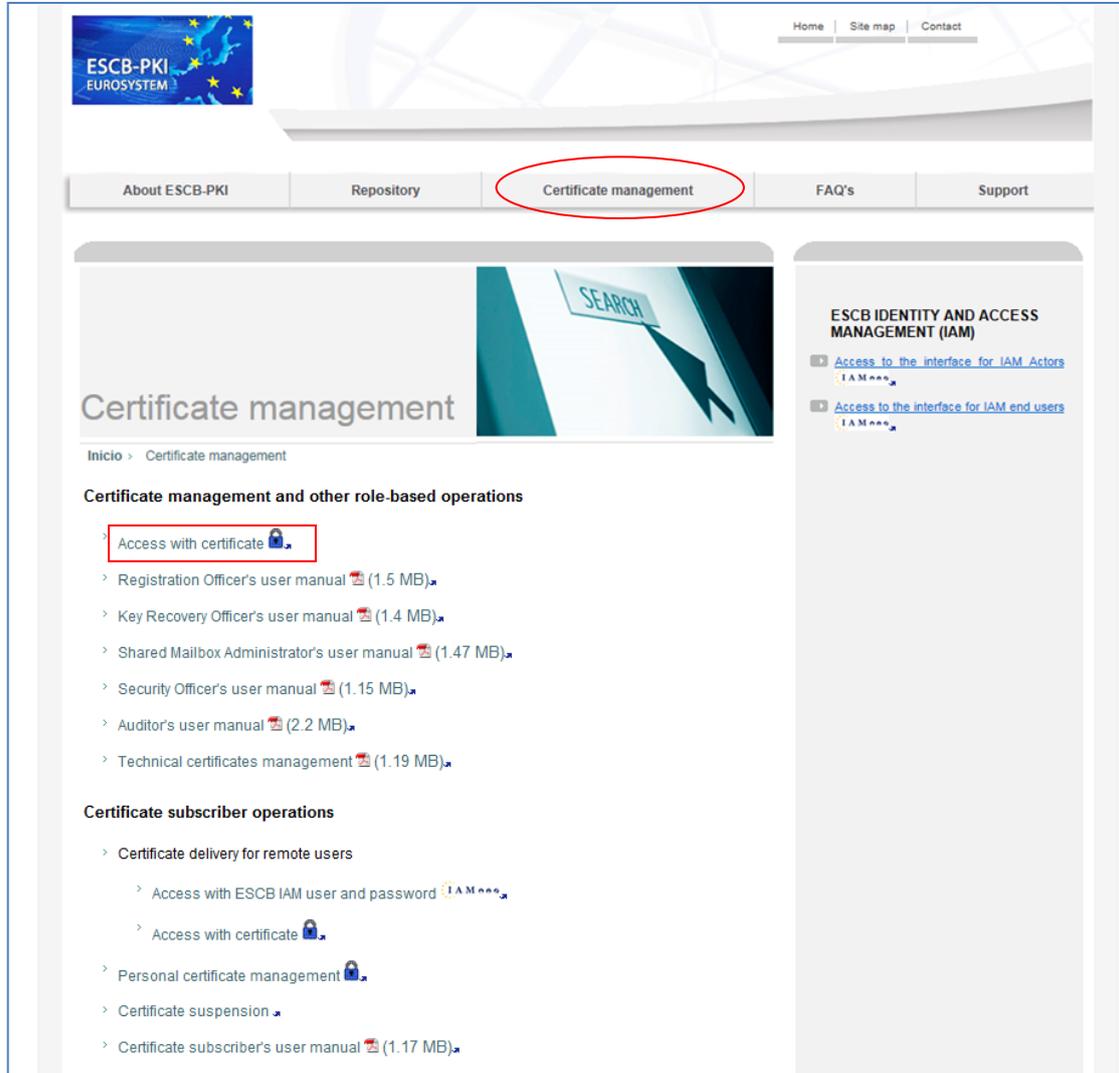


Figure 6 - ESCB-PKI Website - Registration Authority Application

Next sections of this document provide step by step instructions and background information on how to use the Registration Authority application to recover encryption keys.

3. ESCB-PKI RA: KEY RECOVERY PROCESSES

Enter to the ESB-PKI Website and click on the **Certificate Management** link. You must use an advanced CAF-compliant certificate (i.e. your ESCB-PKI certificate) to authenticate.

If you have been granted the role of Key Recovery Officer (KRO) you may:

- Key recovery process
 - Initiate a key recovery process (create a key recovery request)
 - Cancel the request
 - Recover the keys and certificates
- Other options available to KROs are:
 - Review the list of users pertaining to your organisation which have applied for ESCB-PKI certificates. For every user in the list you may perform the following operations.
 - Check the registered personal data
 - Check her/his requests
 - Check her/his certificates
 - Check pending certificate requests for your Central Bank

Note: If you have been granted additional application roles in the ESCB-KI application, additional options may also be available.

Certificate management menu



Figure 7 - Certificate management

Three options will be available in the left frame menu:

- **Search users** To select users from your Central Bank
- **Pending Request** To show all pending certificate requests from your Central Bank
- **Pending Key Recovery Request** To show all pending key recovery requests from your Central Bank

Next sections of this document will further develop these three options.

3.1. INITIATE A KEY RECOVERY REQUEST

1. From the **Search users** option you can find the user whose certificates you want to recover (see 4.1)

Detail	First Name	Organisation	Email Address	ESCB UID	National Identity Number
	APELLIDOS TRES, Usuariotres	Banco de España(ES)	usuario.tres@bde.es	t-esinfppr3	
	APELLIDO APELLIDO, Otro	Banco de España(ES)	otro.apellico@bde.es	t-esinfppr4	
	APELLIDOS REPES, Menganita	Banco de España(ES)	e-mai@empresas-externas.bde.es	t-esqlrcgx	
	ESPAÑOL DOS, Fulanito Dos	Banco de España(ES)	fulanito.dos@bde.es	t-esinfppr2	
	ESPAÑOL ONE, Fulanito	Banco de España(ES)	fulanito.uno@bde.es	t-esinfppr1	
	Integración lam, Pruebas	Banco de España(ES)	qlrcgx@correo.interno	t-espruebas	12345678

Figure 8 - Organisation user list

2. From this list you can select any specific user in order to recover her/his certificates. Clicking on the eye icon () the user details will be displayed.
3. Select the **Certificate Package** tab. This tab shows all ESCB-PKI certificates currently associated with the user and the status of these certificates.

Certificate Request List

User Details | **Certificate Package List** | Certificate Request List

User Information

Name: APELLIDOS TRES, Usuariotres

Certificate Request List

Detail	Certificate Package Type	Request Status	Request Date	IssuanceType	Operation Type
	STANDARD	USER PENDING	15-02-2012 10:49:34	REMOTE	KEYCOMPROMISE
	ADVANCED	COMPLETED	15-02-2012 10:48:54	REMOTE	KEYCOMPROMISE
	ADVANCED	CANCELLED	13-02-2012 16:57:19	PRESENTIAL	KEYCOMPROMISE

Figure 9 - Certificate list

4. Select the certificate package you want to recover. The certificate details will be presented

Certificate Package Detail

Certificate Package Detail | Certificate Package History

Certificate Package Information

Policy: ADVANCED_ARCHIVED_ESCB_POLICY

Cryptographic Device: 602130142089C643

Expiration Date: 05/07/2015

Request Date: 05/07/2012

Certificate Package Status: REVOKED

Certificate List

Serial Number	Template Name	Download	Recover Keys
f31f93c8425b8574f5bb7d1442a5d2	ESCB AUTHENTICATION		Recover keys
3ba719f1ae9609e4f5bb7c6a146a80	ESCB ARCHIVED ENCIPHERMENT		
5281de7537d113654f5bb7d5ea8ec3e	ESCB NONSSCD SIGNATURE		

Back to certificate list

Figure 10 - Certificate details

- Clicking on the  button in the certificate detail screen a key recovery process will be initiated and the following information will be presented:

 **Key recovery request**

 **Begin key recovery process**

Certificate details	
User name	APELLIDOS TRES, Usuariotres
Certificate serial number	317fb56d2a93629951c183e7f3406a98
CA number	63c2015488244a08c23496676a1c07bc2bf43e78
Issue date	19/06/2013
Expiration date	19/06/2016
Certificate template	ESCB ARCHIVED ENCIPHERMENT

Comments for the request	
Comments	<input type="text" value="The user left the organisation and some CB information is encrypted"/>

Type Download	
*Type Download	<input checked="" type="radio"/> TOKEN <input type="radio"/> SOFTWARE

Figure 11 - Initiate a key recovery process

You must indicate in the comments field the reason for this key recovery process and how will the certificate download be managed, onto a token or using a PKCS#12 file, and press the **Accept** button.



Figure 12 - Key recovery request generated

A key recovery request will be generated and, at the same time, every nominated KRO in your organization will receive an e-mail inviting her/him to participate in this key recovery process.

Remember that, for this specific request, you are playing the role of the “requestor KRO” and therefore you will NOT be allowed to finalize the key recovery process.

Another KRO from your organization must enter to the system and process your request.

3.2. APPROVE A TOKEN KEY RECOVERY REQUEST

Every nominated KRO at the Central Bank receives an e-mail with her secret share and her secret number to participate in the key recovery process.

Dear ESCB-PKI Key Recovery Officer,
The Key Recovery Officer t-esinfmpp has initiated a request to recover a copy of the encryption key of the user t-esinfpr4.
Please find below the information that you will need to participate in the key recovery process:
Secret number: 3
Secret share: 128243225465948307428086365520903784718
You can access the ESCB-PKI web interface in the following link:
<https://a-ra-pki.escb.eu/epkmain/>
You will need to authenticate with you ESCB-accepted certificate.
Best regards,
The ESCB-PKI support team

Figure 13 - Mail to participate in the key recovery process

If you agree with the request and you want to participate in the process you may either process the request or communicate your shared secret to the KRO that will process it .

3.3. APPROVE A SOFTWARE KEY RECOVERY REQUEST

Every nominated KRO at the Central Bank receives an e-mail informing a request has been created.

Dear Key Recovery Officer,

The Key Recovery Officer t-esinfflc has initiated a request to recover a copy of the encryption key of the user t-esinfflc (PKCS#12 file format).

The certificate recovery request has to be approved by at least another Key Recovery Officer. To do so, access the ESCB-PKI Registration Authority and press the button "process" for the desired PKCS#12 file, using the following link:

<https://a-ra-pki.escb.eu/epkmain/>

After the request has been approved by all the required Key Recovery Officers, those who have participated in the recovery process will be provided with a part of the PKCS#12 file password.

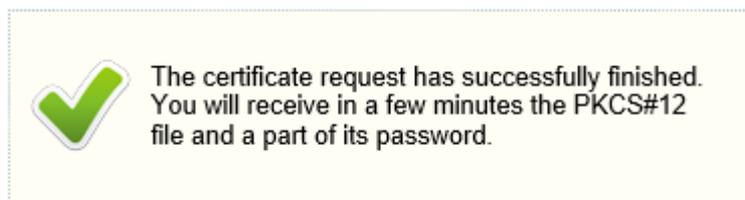
Figure 14 - Mail to participate in the key recovery process

K Key Recovery Officers will have to approve the request, by accessing the Registration Authority and pressing the Process button:

 Request detail

Request data	
User name	APELLIDOS TRES, Usuariotres
Requestor KRO	Millán Rodríguez, Jorge
Request date	22/08/2018
Comments	The user left the organisation and some CB information is encrypted
Certificate data	
Serial number	317fb56d2a93629951c183e7f3406a98
Subject	CN=[ENC-K] Usuariotres APELLIDOS TRES Pseudonym=t-esinffpr3,OU=Banco de España(ES),O=EUROPEAN SYSTEM OF CENTRAL BANKS,C=ES
Issue date	19/06/2013
Expiration date	19/06/2016
Template name	ESCB ARCHIVED ENCIPHERMENT
Type Download	SOFTWARE

The last required approval will be enough for the process to be completed. The PKCS#12 file will be sent by email to the last Key Recovery Officer who participated in the process. All the other participants will receive a section of the password needed to be able to use this PKCS#12 file:



3.4. CANCEL A KEY RECOVERY REQUEST

1. From the **Pending Key recovery request list** option you can access to all pending key recovery requests for your Central Bank.

Detail	Request date	Comments	User name
	04/10/2012	The user left the organisation and some CB information is encrypted	APELLIDOS CUATRO, Usuariocuatro

Figure 15 - Key recovery request list

2. Clicking on the button further details of the request will be displayed. You may cancel the request clicking on the **Cancel** button.

Request data	
User name	APELLIDOS CUATRO, Usuariocuatro
Requestor KRO	VIDAL GONZALEZ, Esther
Request date	04/10/2012
Comments	The user left the organisation and some CB information is encrypted
Certificate data	
Serial number	3ba719f1ae9609e4f5bb7c6a146a80
Subject	CN=[ENC:K] Usuariocuatro APELLIDOS CUATRO.SERIALNUMBER=0000000T.Pseudonym=1-esinfppr4.OU=Banco de España(ES),O=EUROPEAN SYSTEM OF CENTRAL BANKS,C=ES
Issue date	05/07/2012
Expiration date	05/07/2015
Template name	ESCB ARCHIVED ENCIPHERMENT

Figure 16 - Key Recovery request detail (requestor KRO)

3.5. PROCESS A PENDING TOKEN KEY RECOVERY REQUEST

- From the **Pending Key recovery** request list option you can access to all pending key recovery requests for your Central Bank. If you are NOT the KRO who requested the key recovery you will be allowed to process it.

Request detail

Request data	
User name	APELLIDOS CUATRO, Usuariocuatro
Requestor KRO	PENA PINON, Miguel
Request date	04/10/2012
Comments	Need to recover keys in a new card

Certificate data	
Serial number	b8280cd348bbc74#5bbecad326d70
Subject	CN=[ENC K] Usuariocuatro APELLIDOS CUATRO, SERIALNUMBER=00000000T, Pseudonym=t-esinfpr4, OU=Banco de España (ES), O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=ES
Issue date	05/07/2012
Expiration date	05/07/2015
Template name	ESCB ARCHIVED ENCIPHERMENT

Buttons: Process, Cancel, Back to pending key recovery requests

Figure 17 - Key Recovery request detail (other KROs)

- The next figure shows the information displayed when the KRO clicks on the **Process** button

Key recovery processing

Certificate data	
Serial number	b8280cd348bbc74#5bbecad326d70
Subject	CN=[ENC K] Usuariocuatro APELLIDOS CUATRO, SERIALNUMBER=00000000T, Pseudonym=t-esinfpr4, OU=Banco de España (ES), O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=ES
Validity date	05/07/2012
Expiration date	05/07/2015
Template name	ESCB ARCHIVED ENCIPHERMENT
* Token serial number	<input type="text"/>

KRO secrets	
* Secret share	<input type="text"/>
* Secret number	<input type="text"/>
* Secret share	<input type="text"/>
* Secret number	<input type="text"/>

Buttons: Accept

Figure 18 - Process a Key Recovery request

- To initiate the process you must complete the information marked with a *
 - Token serial number** Type the SN of the smart-card where the keys and certificate will be downloaded
 - Secret share** Type the “secret share” received by one of the nominated KROs
 - Secret number** Type the “secret number” associated to the “secret share”

The number of secret shares to be included will be equal to the minimum number of KRO (at least two) required by your organization to recover an encryption key.

Key recovery processing

Certificate data	
Serial number	b8280cd348bbc74#5bbecad326d70
Subject	CN=[ENC K] Usuariocuatro APELLIDOS CUATRO, SERIALNUMBER=00000000T, Pseudonym=t-esinfpr4, OU=Banco de España (ES), O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=ES
Validity date	05/07/2012
Expiration date	05/07/2015
Template name	ESCB ARCHIVED ENCIPHERMENT
* Token serial number	999999999999C999

KRO secrets	
* Secret share	120512782894146323321952944003087051026
* Secret number	1
* Secret share	121379389535193084061084928566111114894
* Secret number	3

Buttons: Accept

Figure 19 - Complete the Key Recovery request

- Click on the **Accept** button. The key recovery process will be launched

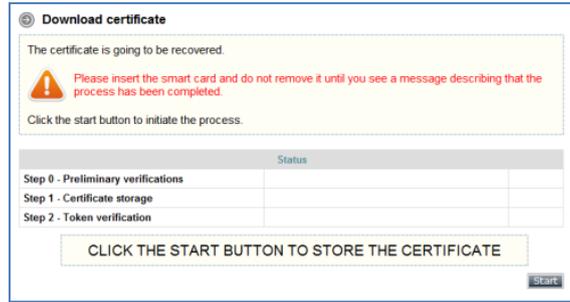


Figure 20 - Starting recovery process

- Click on the **Start** button. The system will prompt you to enter the PIN of the token.

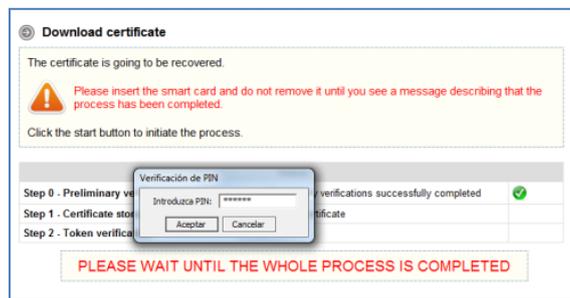


Figure 21 - Download keys and certificate

You will be informed when the keys and the certificate are recovered

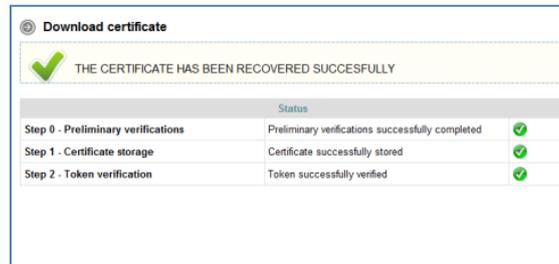


Figure 22 - Encryption key recovered

4. ESCB-PKI RA: OTHER AVAILABLE OPTIONS

4.1. SEARCH USERS

- From the **Search users** option you can find the list of users pertaining to your organisation which have applied for ESCB-PKI certificates. Several filtering criteria can be applied to narrow the search.

Figure 23 - Certificates management. Search user option

- Press the **Search user** button

Detail	First Name	Organisation	Email Address	ESCB UID	National Identity Number
(eye icon)	APELLIDOS TRES, Usuariotres	Banco de España(ES)	usuario.tres@bde.es	t-esinfppr3	
(eye icon)	APELLIDO APELLIDO, Otro	Banco de España(ES)	otro.apellido@bde.es	t-esinfppr4	
(eye icon)	APELLIDOS REPES, Menganita	Banco de España(ES)	e-mal@empresas-externas.bde.es	t-esqlorcpx	
(eye icon)	ESPAÑOL DOS, Fulanito Dos	Banco de España(ES)	fulanito.dos@bde.es	t-esinfppr2	
(eye icon)	ESPAÑOL ONE, Fulanito	Banco de España(ES)	fulanito.uno@bde.es	t-esinfppr1	
(eye icon)	Integración lam, Pruebas	Banco de España(ES)	qlorcpx@correo.interno	t-espruebas	12345678

Figure 24 - Organisation user list

- From this list you can select any specific user in order to recover her/his certificates. Clicking on the eye icon (👁) the user details will be displayed.

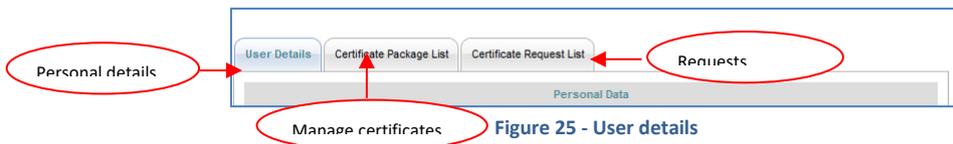


Figure 25 - User details

The following operations may be executed:

- Check personal details (User Details Tab)
- Check certificates (Certificate Package List Tab)
- Check requests (Certificate Request List Tab)

4.1.1. USER DETAILS

Clicking on this tab it displays the user attributes (first name, surname, user-id, etc.) and the information of the organisation he belongs to.

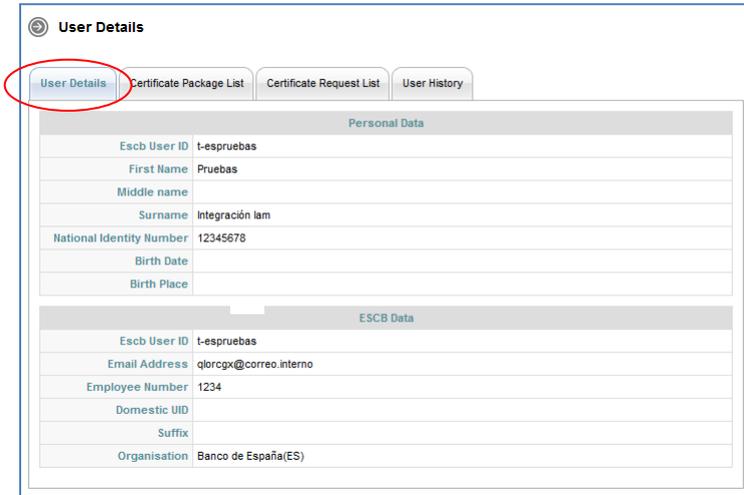


Figure 26 - User details

4.1.2. CERTIFICATE PACKAGE LIST

This tab shows all ESCB-PKI certificates currently associated with the user and the status of these certificates. Possible statuses are:

- **Active** Certificates are valid
- **Revoked** Certificates cannot be used any more
- **Suspended** Certificates have been temporarily invalidated
- **Damaged** Certificates have been replaced due to damage (e.g. broken token)
- **Renewed** Certificates have been replaced due to expiration

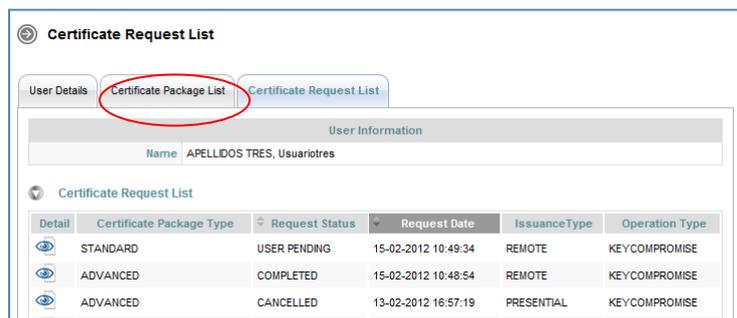


Figure 27 - Certificate list

Certificates are grouped into “packages”. A certificate package is a collection of certificates defined by a Certificate Policy; for instance, the “**advanced_archived**” certificate package will contain the following certificates: advanced authentication, advanced signature and advanced encryption (with key recovery) certificates.

Clicking on a certificate package you can have access to the certificate details:

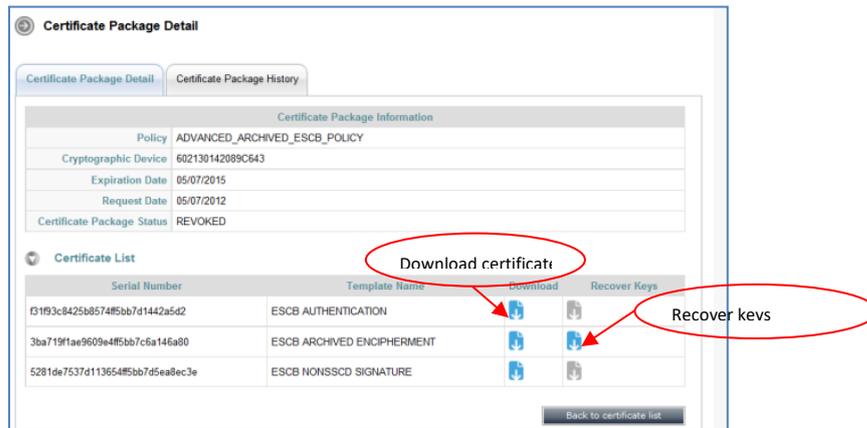


Figure 28 - Certificate details

And request the following operations:

- **Certificate download** Clicking on the button a copy of the certificate (**only public information**) will be downloaded to be locally stored in a file (a .cer file containing the certificate). It is important to notice that the private key will not be provided.
- **Key recovery** Clicking on the button a key recovery process will be initiated (see 3.1).

4.1.3. CERTIFICATE REQUEST LIST

This tab displays all certificate requests that currently belong to the user together with the status of these certificates:

- **Completed** The request has been processed and the certificates have been generated
- **Cancelled** The request has been cancelled
- **Expired** The request has expired
- **RO-Pending** The RO shall still process the request
- **User-Pending** The user can generate and download the certificates. The RO has already handled the request and has allowed a remote download

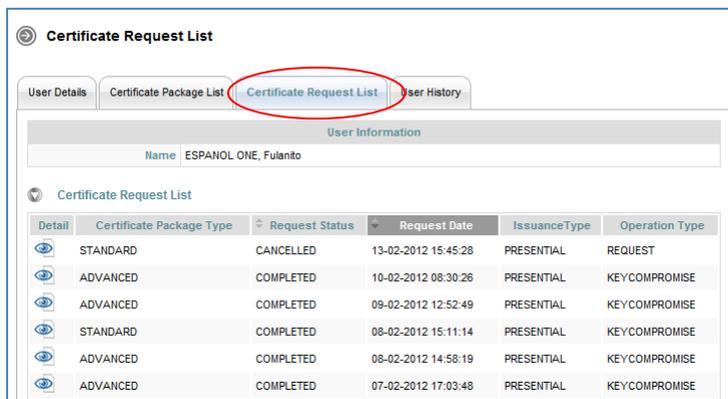


Figure 29 - Certificate requests list

Clicking on the  button the details of the certificate request are displayed

Certificate Package Request Detail

Request detail | Request history

User Information	
Name	APELLIDOS TRES, Usuariotres

Requestor details	
Requestor name	apellido apellido_nombre
Requestor mail	e-mail @correo.interno

Certificate Package Request Detail	
Certificate Package Type	STANDARD
Request Status	RO PENDING
Issuance Type	PRESENTIAL
Operation Type	KEYCOMPROMISE
Request Date	13/02/2012

Figure 30 - Certificate Request details

4.2. PENDING REQUEST LIST OPTION

From the **Pending request list** option you can access to all pending certificate requests for your Central Bank.

Detail	User Name	Organisation Name	Request Date
	ESPAÑOL ONE, Fulanto	Banco de España(ES)	20-01-2012 13:33:33
	ESPAÑOL DOS, Fulanto Dos	Banco de España(ES)	20-01-2012 13:23:02

Figure 31 - Pending requests list

Clicking on the button further details of the request will be displayed

Certificate Package Request Detail

Request detail | Request history

User Information

Name: APELLIDOS TRES, Usuariotres

Requestor details

Requestor name: apellido apellido, nombre
Requestor mail: e-mail @correo interno

Certificate Package Request Detail

Certificate Package Type: STANDARD
Request Status: RO PENDING
Issuance Type: PRESENTIAL
Operation Type: KEYCOMPROMISE
Request Date: 13/02/2012

Figure 32 - Request detail

The status of the request can be:

- **RO-Pending** The RO shall process the request
- **User-Pending** The user can generate and download the certificates. The RO has already handled the request and has allowed a remote download

5. 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.

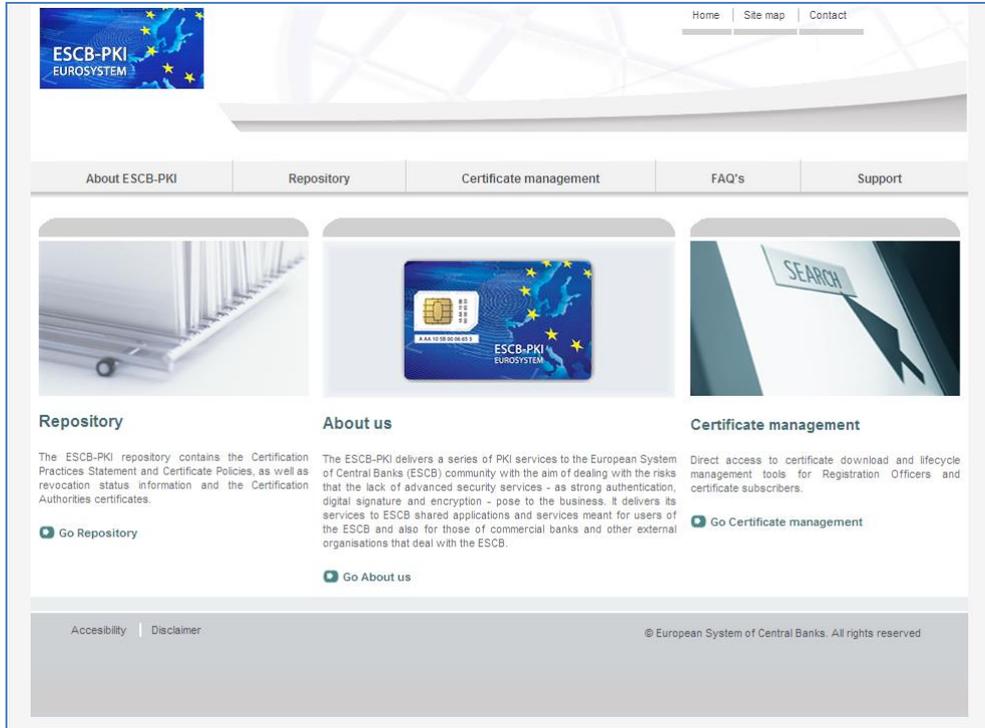


Figure 33 - ESCB-PKI Website

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.