

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI PROJECT



ESCB-PKI REGISTRATION AUTHORITY APPLICATION

AUDITOR'S MANUAL

VERSION 3.1

TABLE OF CONTENTS

GLOSSARY AND ACRONYMS 6

1. Introduction..... 7

 1.1. The ESCB-PKI Website 7

2. The ESCB-PKI Registration Authority application 8

 2.1. System requirements 8

 2.2. Layout..... 8

 2.3. Access..... 10

3. ESCB-PKI RA: auditor tasks 11

 3.1. Search users 12

 3.1.1. User details..... 14

 3.1.2. Certificate package list 15

 3.1.3. Certificate request list 17

 3.1.4. User history 19

 3.2. Search shared mailboxes 20

 3.2.1. Shared mailbox details 22

 3.2.2. Certificate package list 23

 3.2.3. Certificate request list 24

 3.2.4. Shared mailbox history..... 26

 3.3. Search devices..... 27

 3.3.1. Device details 28

 3.3.2. Device certificate requests 29

 3.3.3. Device certificates 30

 3.3.4. Device profiles 31

 3.3.4.1. Profile details..... 31

 3.3.4.2. Profile certificate requests 31

 3.3.4.3. Profile certificates 32

 3.4. Certificates 34

 3.5. Certificate requests..... 36

 3.6. Events..... 38

4. More information about ESCB-PKI 40

TABLE OF ILLUSTRATIONS

Figure 1 - ESCB-PKI Website 7

Figure 2 - Production frame..... 8

Figure 3 - Acceptance frame..... 9

Figure 4 - Certificate management..... 9

Figure 5 - ESCB-PKI Website - Registration Authority Application 10

Figure 6 - Auditor menu 11

Figure 7 - Certificates management. Search user option 12

Figure 8 - Organisation user list..... 12

Figure 9 - User details..... 14

Figure 10 - Certificate list..... 15

Figure 11 - Certificate details..... 15

Figure 12 - Certificate activity..... 16

Figure 13 - Certificate requests list..... 17

Figure 14 - Certificate request details 17

Figure 15 - Request activity 18

Figure 16 - User activity 19

Figure 17 - Search shared mailbox 20

Figure 18 - Shared mailbox list 20

Figure 19 - Shared mailbox details 20

Figure 20 - Shared mailbox details 22

Figure 21 - Shared mailbox certificate package list 23

Figure 22 - Shared mailbox certificate requests list 24

Figure 23 - Shared mailbox certificate request details 24

Figure 24 - Shared mailbox activity 26

Figure 25 - Search device 27

Figure 26 - List of devices 27

Figure 27 - Device detail 27

Figure 28 - Device detail tab 28

Figure 29 - Device request list 29

Figure 30 - Device certificate list 30

Figure 31 - Device profile details 31

Figure 32 - Device certificate requests 31

Figure 33 - Device certificate request detail..... 32

Figure 34 - Device certificates 33

Figure 35 - Device certificate detail 33

Figure 36 - Search certificates 34

Figure 37 - Certificates list 34

Figure 38 - Search certificate requests 36

Figure 39 - Certificate requests list..... 36

Figure 40 - Search events 38

Figure 41 - Event list 38

Figure 42 - Event details 39

Figure 43 - ESCB-PKI Website 40

Project name:	ESCB-PKI
Author:	ESCB-PKI Project team
File name:	ESCB-PKI - RA Application Auditor'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	15.04.2014	First version
2.0	Final	11.09.2018	BdE Revision
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
RA	Registration Authority
RO	Registration Officer
RO4EO	Registration Officer for External Organisations
RO4TC	Registration Officer for Technical Components
SMA	Shared Mailbox Administrator
TCS	Technical Certificate Subscriber

1. INTRODUCTION

This document aims at providing information on how to use the ESCB-PKI Registration Authority application developed as part of the ESCB-PKI project which delivers a series of PKI services to ESCB and non-ESCB members.

1.1. 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.

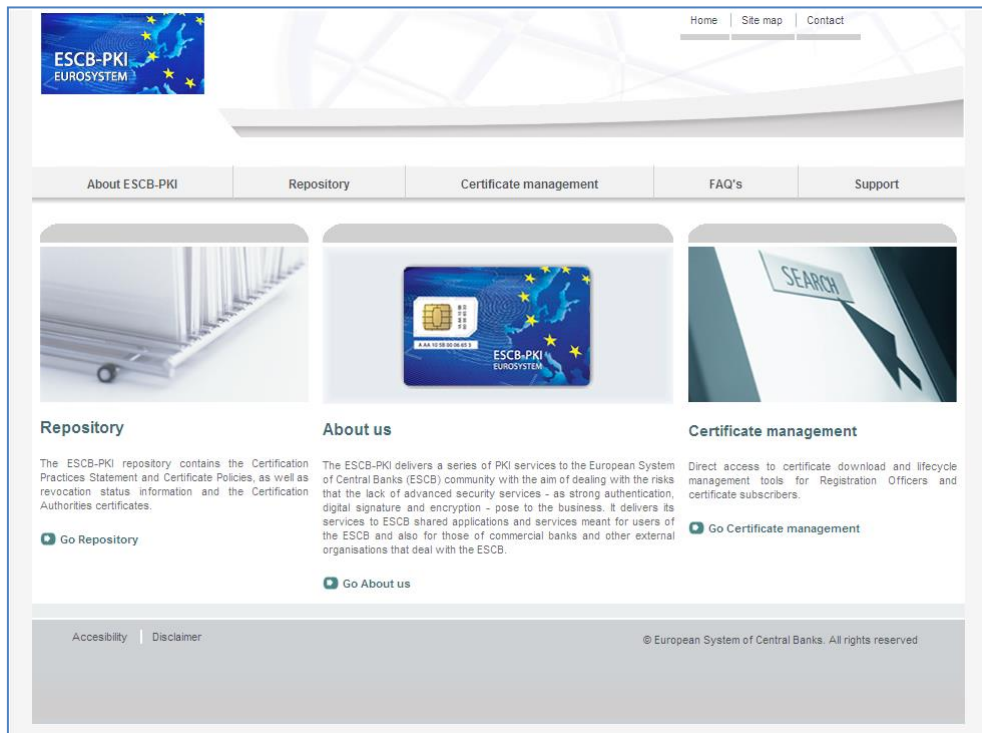


Figure 1 - ESCB-PKI Website

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.

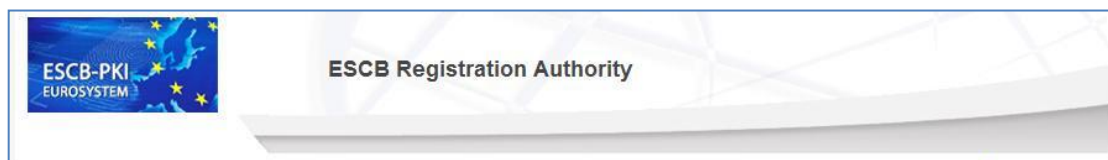


Figure 2 - Production frame



Figure 3 - 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

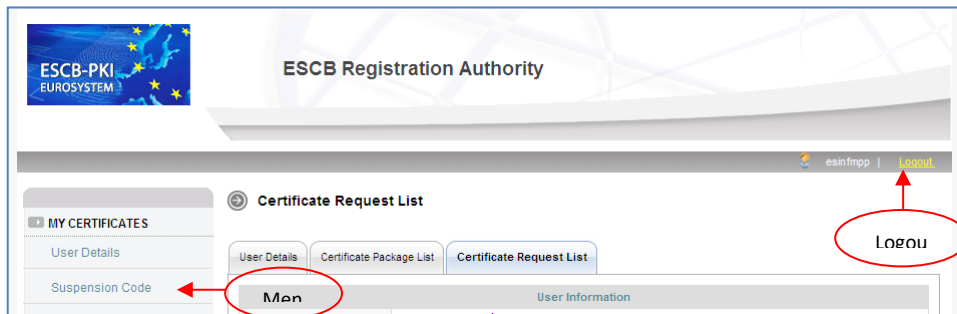


Figure 4 - Certificate management

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

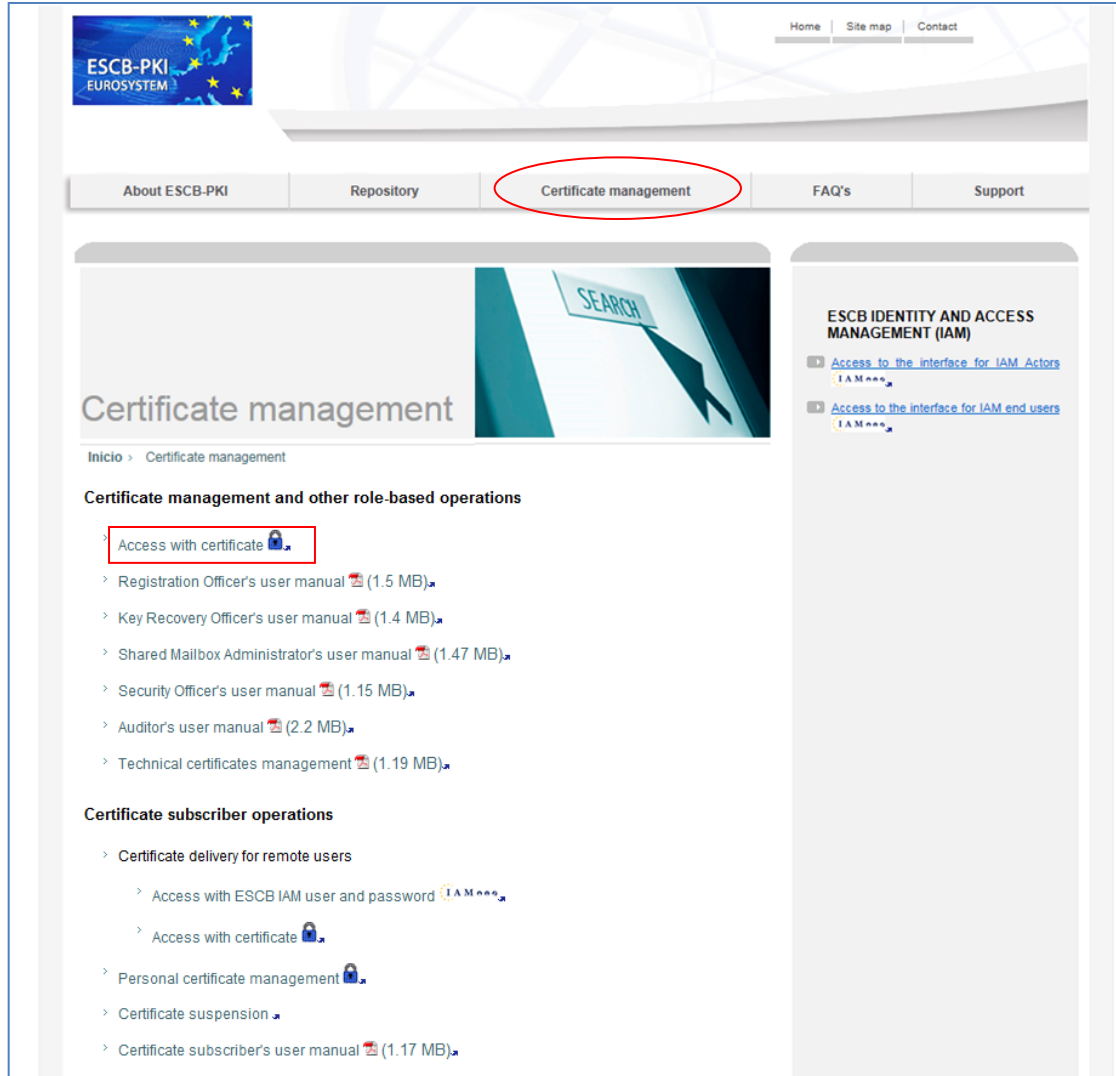


Figure 5 - ESCB-PKI Website - Registration Authority Application

Next sections of this document provide step by step instructions and background information on how to use the Registration Authority application as an auditor.

3. ESCB-PKI RA: AUDITOR TASKS

Enter to the ESB-PKI Website and click the **Access with certificate** link available in the **Certificate management and other role-based operations** section. You must use an advanced CAF-compliant certificate (i.e. your ESCB-PKI certificate) to authenticate.

From this option you may:

- Review the list of users, shared mailboxes and devices (i.e. technical components) pertaining to your organisation which have applied for ESCB-PKI certificates. For every user, shared mailbox or device you may perform the following operations.
 - Check the information about the user, shared mailbox or device
 - Check the certificate requests
 - Check the certificates
- Review and obtain reports of the certificates and certificate requests that have been managed in your organisation.
- Review and obtain reports of the security events generated in the ESCB-PKI system for your organisation.

Auditor menu

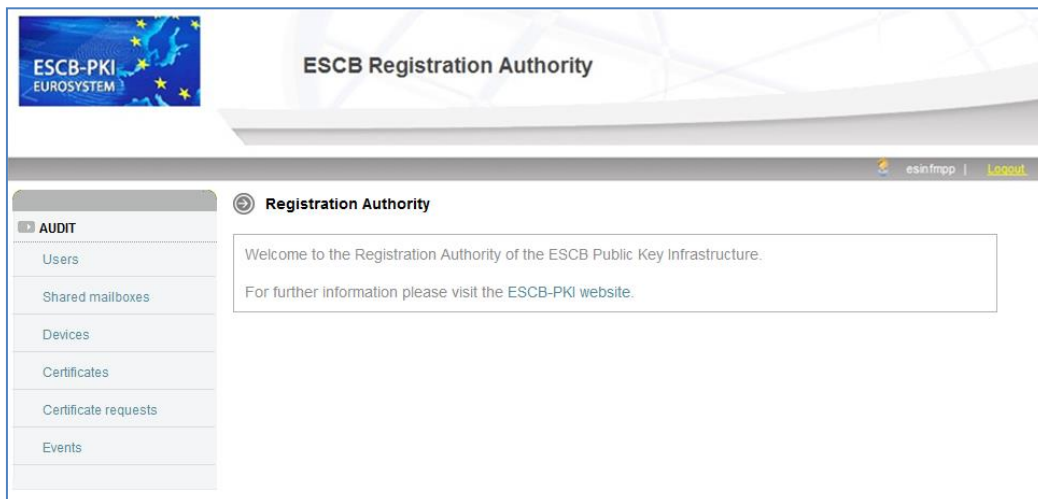


Figure 6 - Auditor menu

The following options will be available in the left frame menu:

- **Users** To select users from your Central Bank
- **Shared mailboxes** To select shared mailboxes from your Central Bank
- **Devices** To select devices from your Central Bank
- **Certificates** To show the certificates from your Central Bank
- **Certificate Requests** To show the certificate requests from your Central Bank
- **Events** To show the security events generated in the ESCB-PKI system for your Central Bank

Next sections of this chapter will further develop these menu options.

3.1. 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 7 - Certificates management. Search user option

Press the **Search user** button

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-mal@empresas-externas.bde.es	t-esqlorcgx	
	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)	qlorcgx@correo.interno	t-espruebas	12345678
	LASTFIVE, Namecinco	Banco de España(ES)	user5@empresas-externas.bde.es	t-esinfppr5	
	JJJJ LOPEZ, Menganito	Banco de España(ES)	menganito@bde.es	t-esmengano	
	ESPAÑOL ESPAÑOL, Juan	Banco de España(ES)	juan.espanol@bde.es	t-esespanol	
	ESPAÑOLA ESPAÑOLA, JUANA	Banco de España(ES)	juana.espnola@bde.es	t-esjuanita	
	REPETIDO OTRO, NOMBRE	Banco de España(ES)	nombre.otro@bde.es	t-esotrousu	
	APELLIDO DOS, Roberto	Banco de España(ES)	roberto.dos@bde.es	t-esroberto	1111111111
	ESPAÑOL ESPAÑOLA, Zutano	Banco de España(ES)	zutano@empresas-externas.bde.es	t-eszutano	
	ESPAÑOLA APELLIDO, Pepa	Banco de España(ES)	pepa@bde.es	t-espepita	123456789012

Figure 8 - Organisation user list

From this list you can select any specific user in order to manage her/his certificates or her/his requests. Clicking the eye icon () the user details will be displayed

Figure 9 - User details

The following operations may be executed:

- Review personal details (User Details Tab)
- Review certificates (Certificate Package List Tab)
- Review certificate requests (Certificate Request List Tab)
- Check the activity associated with the user (User History Tab)

3.1.1. USER DETAILS

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

The screenshot shows a web application interface with a 'User Details' tab highlighted. The interface includes a header with the title 'User Details' and a navigation bar with four tabs: 'User Details', 'Certificate Package List', 'Certificate Request List', and 'User History'. Below the tabs, there are two main sections: 'Personal Data' and 'ESCB Data'. The 'Personal Data' section contains fields for Escb User ID, First Name, Middle name, Surname, National Identity Number, Birth Date, and Birth Place. The 'ESCB Data' section contains fields for Escb User ID, Email Address, Employee Number, Domestic UID, Suffix, and Organisation.

Personal Data	
Escb User ID	t-espruebas
First Name	Pruebas
Middle name	
Surname	Integración lam
National Identity Number	12345678
Birth Date	
Birth Place	

ESCB Data	
Escb User ID	t-espruebas
Email Address	qlorcpx@correo.interno
Employee Number	1234
Domestic UID	
Suffix	
Organisation	Banco de España(ES)

Figure 9 - User details

3.1.2. 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

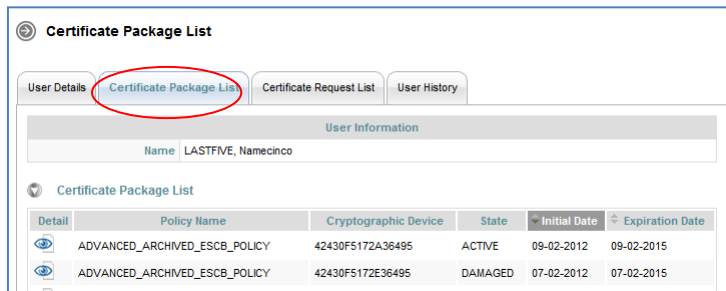


Figure 10 - Certificate list

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

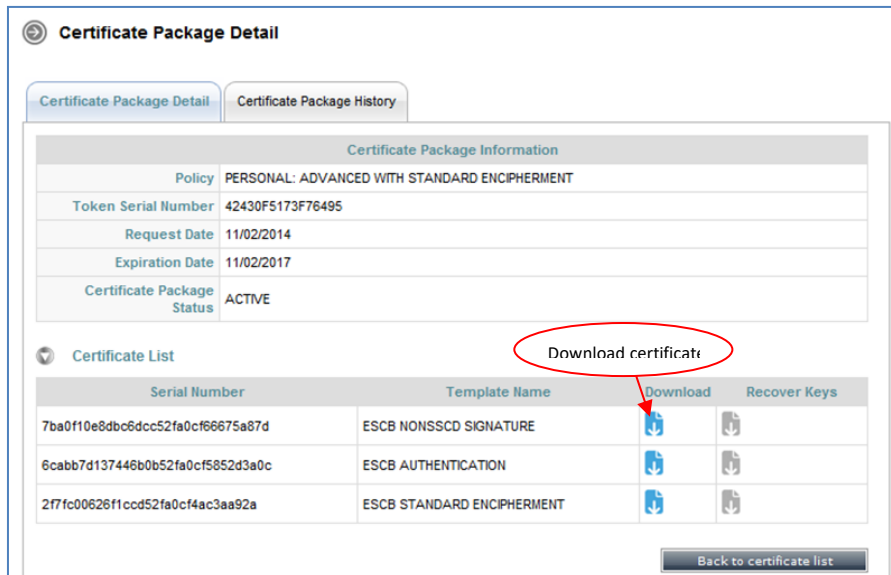

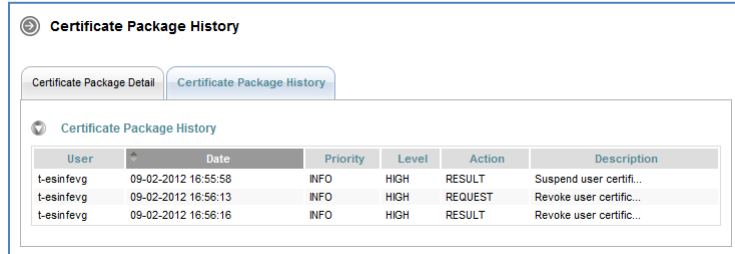


Figure 11 - Certificate details

You have access to the following operations:

- **Certificate download** Clicking 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.
- **Certificate Package History** This tab shows the activity associated with this certificate package.



User	Date	Priority	Level	Action	Description
t-esinfvg	09-02-2012 16:55:58	INFO	HIGH	RESULT	Suspend user certifi...
t-esinfvg	09-02-2012 16:56:13	INFO	HIGH	REQUEST	Revoke user certifi...
t-esinfvg	09-02-2012 16:56:16	INFO	HIGH	RESULT	Revoke user certifi...

Figure 12 - Certificate activity

3.1.3. 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

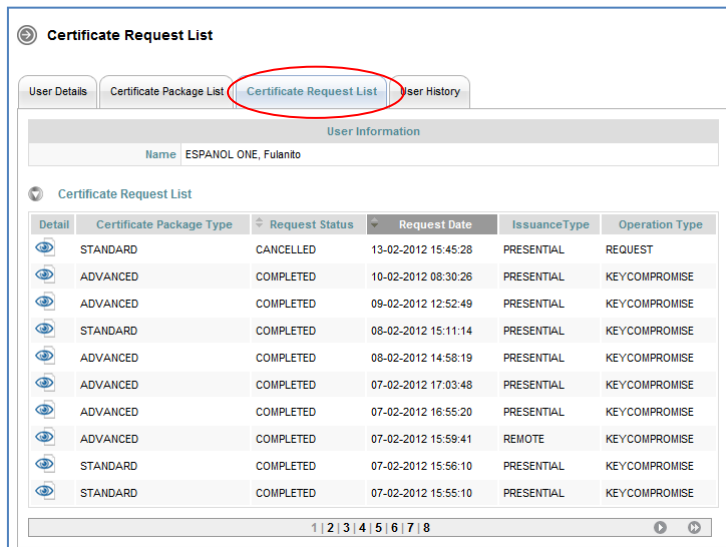


Figure 13 - Certificate requests list

Clicking the button the details of the certificate request are displayed

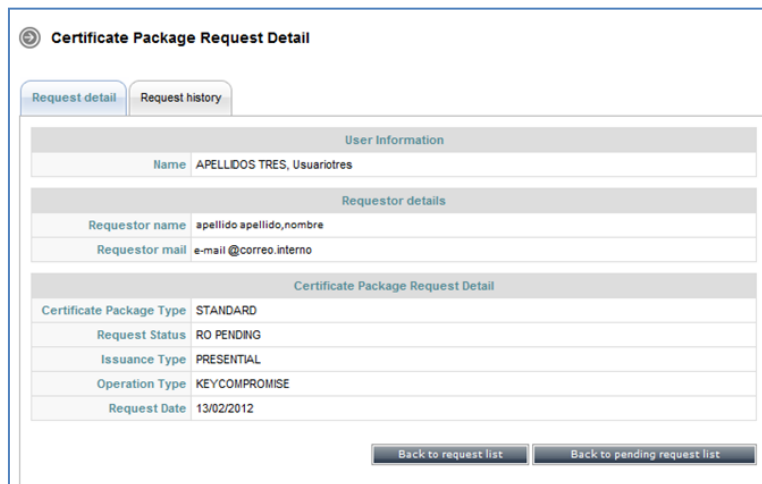


Figure 14 - Certificate request details

You may select the following operations (the available options will be dependent on the status of the request):

- **Request history** This tab shows the activity associated to this certificate package.

The screenshot shows a web interface titled "Certificate Package Request History". It has two tabs: "Request detail" and "Request history", with the latter being selected. Below the tabs is a table with the following data:

User	Date	Priority	Level	Action	Description
t-esinfmpp	01-02-2012 10:00:51	INFO	MEDIUM	REQUEST	Enable remote downlo...
t-esinfmpp	01-02-2012 10:00:46	INFO	MEDIUM	RESULT	Load information of ...
t-esinfmpp	01-02-2012 10:00:46	INFO	MEDIUM	REQUEST	Load information of ...
iam	01-02-2012 10:00:16	INFO	MEDIUM	RESULT	User certificate pac...

Figure 15 - Request activity

3.1.4. USER HISTORY

Displays all the activity related to the user.

The screenshot shows a web interface titled 'User History'. At the top, there are four tabs: 'User Details', 'Certificate Package List', 'Certificate Request List', and 'User History'. The 'User History' tab is selected. Below the tabs is a table with the following data:

User	Date	Priority	Level	Action	Description
t-esinfmpp	03-02-2012 15:50:57	INFO	MEDIUM	RESULT	Register certificate...
t-esinfmpp	01-02-2012 10:00:51	INFO	MEDIUM	RESULT	Enable remote downlo...
t-esinfmpp	01-02-2012 10:00:51	INFO	MEDIUM	REQUEST	Enable remote downlo...
t-esinfmpp	01-02-2012 10:00:46	INFO	MEDIUM	RESULT	Load information of ...
t-esinfmpp	01-02-2012 10:00:46	INFO	MEDIUM	REQUEST	Load information of ...
iam	01-02-2012 10:00:16	INFO	MEDIUM	RESULT	User certificate pac...
t-esinfmpp	01-02-2012 08:16:21	INFO	HIGH	RESULT	Issue ADVANCED certi...
t-esinfmpp	01-02-2012 08:16:13	INFO	HIGH	REQUEST	Issue ADVANCED certi...
t-esinfmpp	01-02-2012 08:14:12	INFO	MEDIUM	RESULT	Begin ADVANCED certi...
t-esinfmpp	01-02-2012 08:14:12	INFO	MEDIUM	REQUEST	Begin ADVANCED certi...
t-esinfmpp	01-02-2012 08:14:09	INFO	MEDIUM	RESULT	Load information of ...
t-esinfmpp	01-02-2012 08:14:08	INFO	MEDIUM	REQUEST	Load information of ...
t-esinfmpp	01-02-2012 08:14:02	INFO	MEDIUM	RESULT	Register certificate...
t-esinfmpp	01-02-2012 08:13:13	INFO	MEDIUM	RESULT	Cancel certificate p...
t-esinfmpp	01-02-2012 08:13:13	INFO	MEDIUM	REQUEST	Cancel certificate p...

At the bottom of the table, there is a pagination control showing '1 | 2 | 3'.

Figure 16 - User activity

3.2. SEARCH SHARED MAILBOXES

From the **Search Shared Mailboxes** option you can find the list of shared mailboxes that one Shared Mailbox Administrator (SMA) from your Central Bank has created in the ESCB-PKI system. Several filtering criteria can be applied to narrow the search.

Figure 17 - Search shared mailbox

Press the **Search shared mailbox** button

Detail	Display Name	Email Address	Name of custodian	Email of custodian
	BDE_PRUEBA_SMB	pkibde@bde.es	PENA PINON, Miguel	miguelangel.pena@bde.es
	PRUEBA_SMB2	escb-pki@bde.es	PENA PINON, Miguel	miguelangel.pena@bde.es
	SEE PROJECT USER 120	ESCBPKI-revoked-certificate@bde.es	CALERO LAGUIA, Sebastian	sebastian.calero@bde.es

Figure 18 - Shared mailbox list

From this list you can select any specific shared mailbox in order to manage its certificates or certificate requests. Clicking the eye icon () the shared mailbox details will be displayed

Figure 19 - Shared mailbox details

The following operations may be executed:

- Review shared mailbox details (Shared Mailbox Detail Tab)
- Review certificates (Certificate Package List Tab)
- Review requests (Certificate Request List Tab)
- Check the activity associated with the shared mailbox (Shared Mailbox History Tab)

3.2.1. SHARED MAILBOX DETAILS

Clicking this tab it displays the shared mailbox attributes (display name, e-mail address, etc.) and the information about its custodian (first name, surname, user-id, etc.)

Shared Mailbox Details

Shared Mailbox Detail | Certificate Package List | Certificate Request List | Shared Mailbox History

Shared Mailbox	
Unique Identifier	t-esbdepruebasmb
Display Name	BDE_PRUEBA_SMB
Description	PRUEBA SHARED MAILBOX
Email Address	pkibde@bde.es

Custodian of the Shared Mailbox	
Escb User ID	t-esinfmpp
Name	Miguel
Middle Name	
Surnames	PENA PINON
Email Address	miguelangel.pena@bde.es
National Identity Number	
Employee Number	
Birth Date	29/12/1974
Birth Place	MADRID

Back to shared mailbox list

Figure 20 - Shared mailbox details

3.2.2. CERTIFICATE PACKAGE LIST

This tab shows all ESCB-PKI certificates currently associated with the shared mailbox 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
- **Renewed** Certificates have been replaced due to expiration

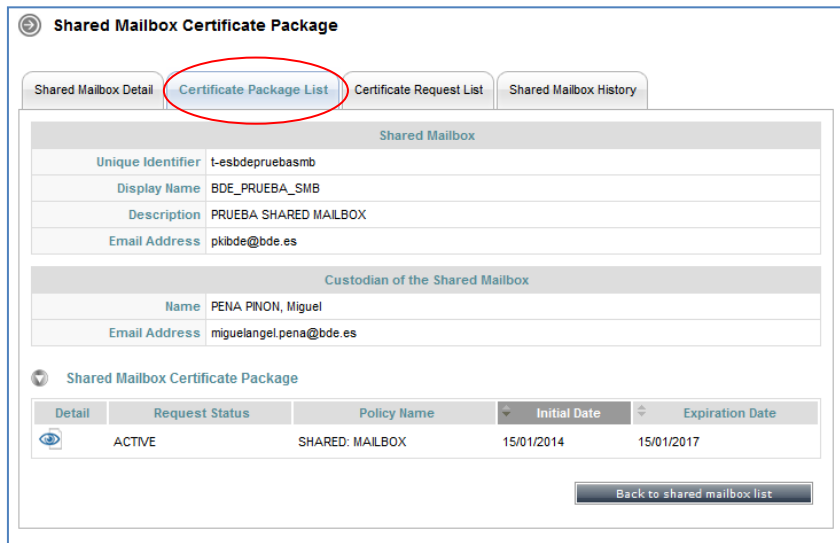



Figure 21 - Shared mailbox certificate package list

Certificates are grouped into “packages”. A certificate package is a collection of certificates defined by a Certificate Policy.

Clicking a certificate package shows the certificate details and allows the following operations:

- **Certificate download** Clicking 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.
- **Certificate Package History** This tab shows the activity associated with this certificate.

3.2.3. CERTIFICATE REQUEST LIST

This tab displays all certificate requests that currently belong to the shared mailbox 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 certificate can be downloaded by the person that created the certificate request. The RO has already approved the request

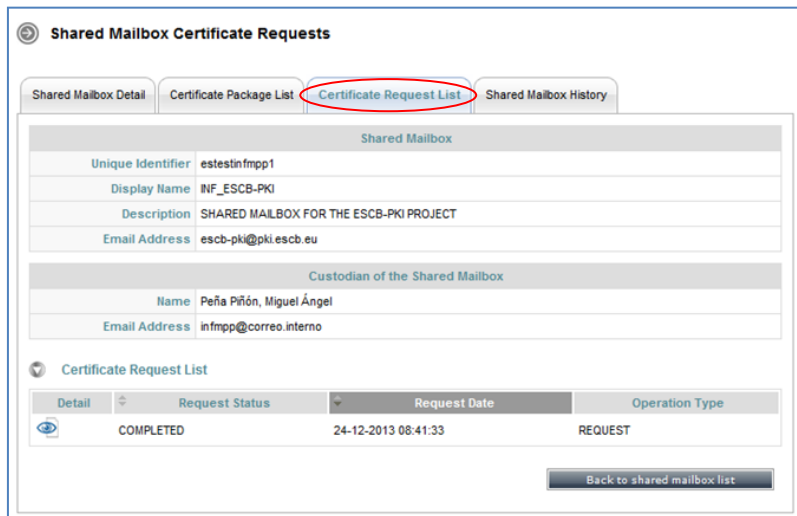


Figure 22 - Shared mailbox certificate requests list

You can click the button to access the certificate request details:

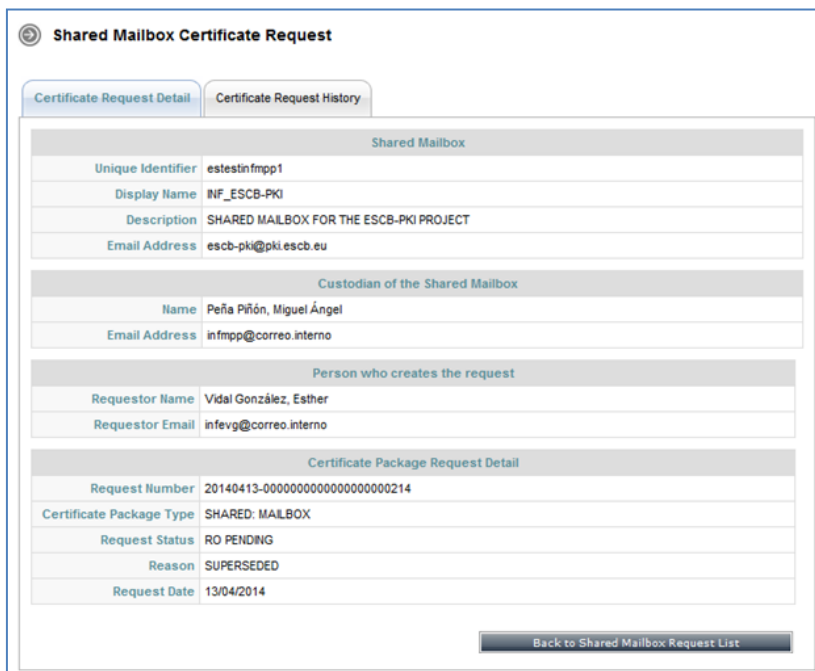


Figure 23 - Shared mailbox certificate request details

You may select the following operations:

- ***Back to shared mailbox request list*** To go back to the shared mailbox certificate requests list
- ***Certificate request history*** This tab shows the activity associated to this certificate request.

3.2.4. SHARED MAILBOX HISTORY

Displays all the activity related to the shared mailbox.

The screenshot shows a web interface titled "Shared Mailbox History". It features four tabs: "Shared Mailbox Detail", "Certificate Package List", "Certificate Request List", and "Shared Mailbox History" (which is selected). Below the tabs is a "History List" section containing a table with the following data:

Who	When	What	Result
t-esinfmpp	15-01-2014 08:22:58	Download issued certificate.	INFO
t-esinfmpp	15-01-2014 08:22:58	Download issued certificate.	INFO
t-esinfmpp	15-01-2014 08:22:56	Issue certificate package.	INFO
t-esinfmpp	15-01-2014 08:22:56	Issue certificate package.	INFO
t-esinfmpp	15-01-2014 08:22:05	Generation of the terms and conditions document.	INFO
t-esinfvfg	14-01-2014 19:33:55	Approve shared mailbox certificate request.	INFO
t-esinfmpp	14-01-2014 17:10:43	Generation of the terms and conditions document.	INFO
t-esinfmpp	14-01-2014 17:10:39	Register new shared mailbox certificate request.	INFO
t-esinfmpp	14-01-2014 17:10:12	Register new shared mailbox.	INFO

At the bottom right of the table area, there are two buttons: "Export XLS" and "Back to shared mailbox list".

Figure 24 - Shared mailbox activity

3.3. SEARCH DEVICES

From the **Search devices** option you can search devices that have been registered in your Central Bank.

Figure 25 - Search device

It is possible to use any device or contact person attribute to search. Once clicked the “Search device” button, the list of devices that follow the search criteria is shown:

Detail	Name	Description	Contact name	Contact mail	Contact phone
	deviceTest2	description	SurnameContact, Namecontact	contactmail@mail.com	(+64) 123 45 45
	deviceValid	description	contactSurnames, contactName	qraqpbx@correo.interno	123456789

Figure 26 - List of devices

Clicking the eye icon () the device details will be displayed. From this menu you can review the device details, profiles and certificates:

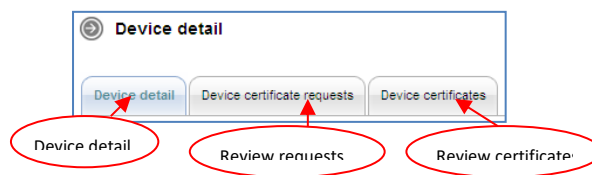


Figure 27 - Device detail

3.3.1. DEVICE DETAILS

This tab allows performing the following operations:

- Review the device and contact person information
- Review the profiles registered for the device

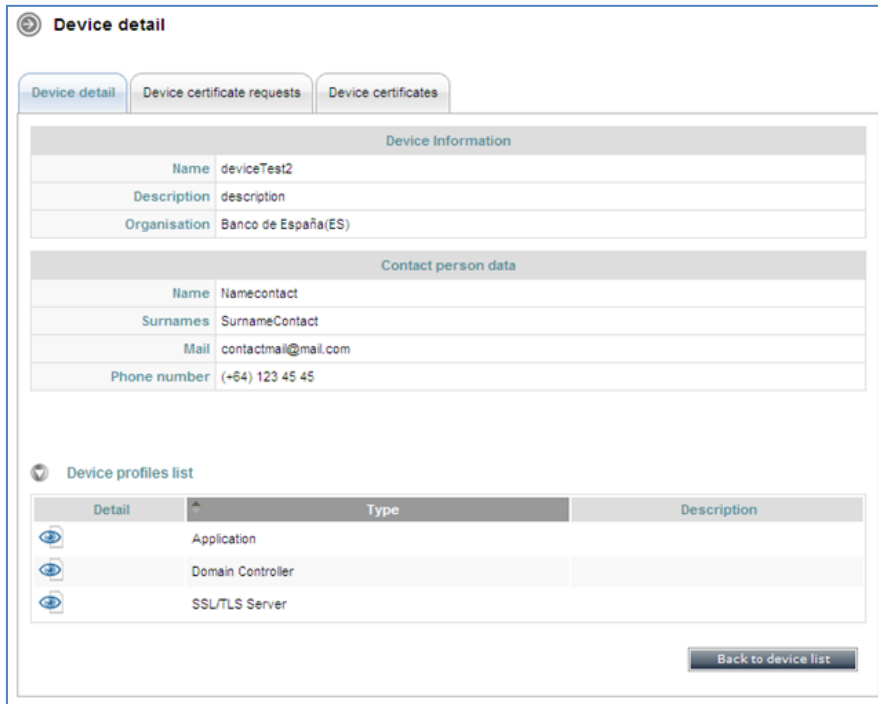


Figure 28 - Device detail tab

The eye icon () under the “device profile list” allows displaying the profile details (see section 3.3.4)

3.3.2. DEVICE CERTIFICATE REQUESTS

This tab allows watching the details of the certificate requests of all the profiles associated to the device.

The screenshot shows a web interface titled "Device request list". It has three tabs: "Device detail", "Device certificate requests" (which is active), and "Device certificates".

Under the active tab, there are two sections:

- Device Information:** A table with fields: Name (deviceTestExternal), Description (description), and Organisation (Police ES).
- Contact person data:** A table with fields: Name (contactName), Surnames (contactSurname), Mail (qaguspx@correo.interno), and Phone number (+34)123456789.

Below these sections is a "Request list" section containing a table with the following data:

Detail	Request type	Request status	Operation type	Request date	Device profile
	Generate .p12 file	CANCELLED	REQUEST	24/05/2012	Application
	Generate .p12 file	CANCELLED	REQUEST	24/05/2012	Application
	Generate .p12 file	COMPLETED	REQUEST	24/05/2012	Application
	Process a .csr or .p10 file	CANCELLED	REQUEST	26/04/2012	Application
	Generate .p12 file	COMPLETED	REQUEST	26/04/2012	Application

At the bottom right of the interface is a button labeled "Back to device list".

Figure 29 - Device request list

The eye icon () under the "request list" takes to the "device certificate request detail" screen (see section 3.3.4.2)

3.3.3. DEVICE CERTIFICATES

This tab allows watching the details of the certificates of all the profiles associated to the device.

The screenshot shows a web interface titled "Device certificate list". It has three tabs: "Device detail", "Device certificate requests", and "Device certificates". The "Device certificates" tab is active. Below the tabs, there are two sections: "Device Information" and "Contact person data".

Device Information:

- Name: DeviceInterno
- Description: Device interno pruebas
- Organisation: Banco de España(ES)

Contact person data:

- Name: Águeda
- Surnames: Soto
- Mail: qaguspx@correo.interno
- Phone number: 91 338 63 07

Below these sections is a "Certificate list" section with a table. The table has columns: "Detail", "Serial number", "Issuance date", "Expiration Date", "Status", and "Policy". There are 10 rows of data, each with an eye icon in the "Detail" column.

Detail	Serial number	Issuance date	Expiration Date	Status	Policy
	273685876d876f334fe2cf3ad9fe77a3	21/06/2012	21/06/2014	REVOKED	SSLSERVER_STANDAR
	4eaecef17684e1a14fe2c2e651ca0e5b	21/06/2012	21/06/2014	REVOKED	SSLSERVER_STANDAR
	5515ca0454c0e2c74fe2c26950ee26e7	21/06/2012	21/06/2014	REVOKED	SSLSERVER_STANDAR
	49467505effc32d64fe2bd6ae2a0f6d6	21/06/2012	21/06/2014	REVOKED	SSLSERVER_STANDAR
	2c89a5fc0672971c4fe2bc78ed22886a	21/06/2012	21/06/2014	DAMAGED	SSLSERVER_STANDAR
	5336b833c3c40274fe2bbf4f3b1d37f1	21/06/2012	21/06/2014	REVOKED	SSLSERVER_STANDAR
	58689e93ad6cdb674fe08f336874acc9	19/06/2012	19/06/2014	REVOKED	SSLSERVER_STANDAR
	668f2c59539163574fc62d4e5b4ccc80	30/05/2012	30/05/2014	REVOKED	SSLSERVER_STANDAR
	781e276041697414faa409e7593d247	09/05/2012	09/05/2014	REVOKED	SSLSERVER_STANDAR
	22ad273cdd96a1034f96b06a854fe48f	24/04/2012	24/04/2014	REVOKED	SSLSERVER_STANDAR

At the bottom of the table, there is a pagination bar showing "1 | 2" and a "Back to device list" button.

Figure 30 - Device certificate list

The eye icon () under the "certificate list" takes to the "device certificate detail" screen (see section 3.3.4.3)

3.3.4. DEVICE PROFILES

The “device details” screen (see section 3.3.1) allows reviewing profiles for the device.

3.3.4.1. Profile details

The profile details tab shows the profile information:

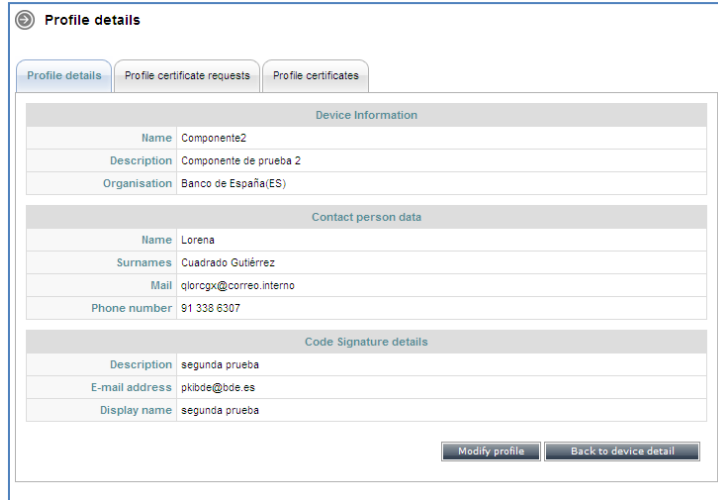


Figure 31 - Device profile details

3.3.4.2. Profile certificate requests

The “profile certificate requests” tab allows displaying the certificate requests associated to the device profile.

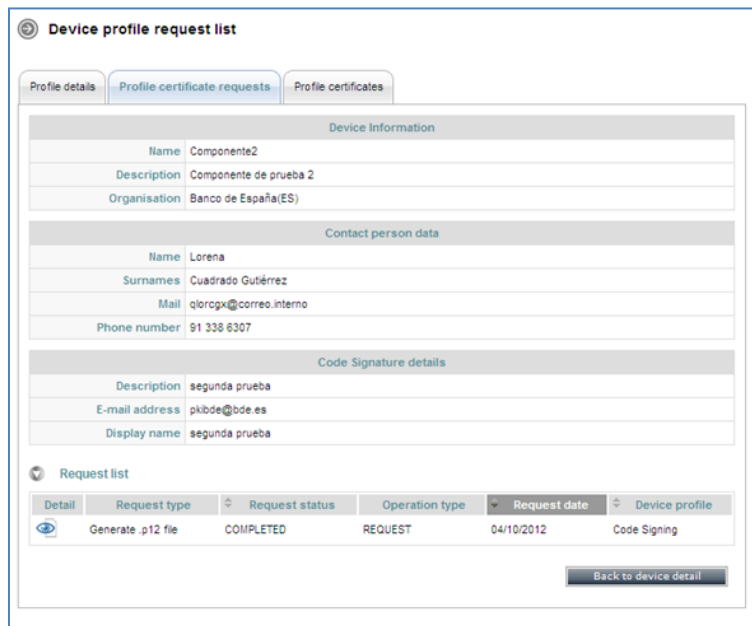


Figure 32 - Device certificate requests

The eye icon () under the “request list” takes to the “request detail” screen

Request detail

Device Information	
Name	SAMPLE_DEVICE
Description	THIS IS A SAMPLE DEVICE
Organisation	Banco de España(ES)

Contact person data	
Name	JOHN
Surnames	SMITH
Mail	john.smith@bde.es
Phone number	+34 1233344

Code Signature details	
Description	THIS IS A CERTIFICATE USED TO SIGN ACTIVEXS AND APPLETS
E-mail address	support@application.escb.eu
Display name	DOWNLOADABLE COMPONENT

Device request detail	
Request type	Generate .p12 file
Request status	RO PENDING
Operation type	REQUEST
Request date	11/03/2013
Profile	Code Signing
Requestor id	infmpp
Requestor name	Miguel Ángel
Requestor surname	Peña, Piñón
Requestor mail	infmpp@correo.interno

[Back to request list](#)

Figure 33 - Device certificate request detail

The possible certificate request states are the following:

- RO PENDING: the request has been created and has to be approved (or cancelled) by a RO4TC
- USER PENDING: the request has been approved by a RO4TC and has to be processed by a TCS
- CANCEL: the request has been canceled by a RO4TC
- FINISH: the request has been completed
- EXPIRED: the request has expired before completion

3.3.4.3. Profile certificates

The “profile certificates” tab allows displaying the certificates associated to the device.

Device profile certificate list

Profile details | Profile certificate requests | Profile certificates

Device Information	
Name	SAMPLE_DEVICE
Description	THIS IS A SAMPLE DEVICE
Organisation	Banco de España(ES)

Contact person data	
Name	JOHN
Surnames	SMITH
Mail	john.smith@bde.es
Phone number	+34 1233344

SSL Server details	
Description	THIS IS A SSL SERVER
E-mail address	service@bde.es
Common name	service.bde.es
DNS name	service.bde.es;help.bde.es;other.bde.es
IP address	

Certificate list

Detail	Serial number	Issuance date	Expiration Date	Status	Policy
	ae9a9fb0c86fd85139f190b7c655ef	08/03/2013	08/03/2016	ACTIVE	SSLSERVER_STANDARD
	6a93ae10a73587d5139f101021dfeca	08/03/2013	08/03/2016	REVOKED	SSLSERVER_STANDARD
	2ee5a7a404cd04e75139f02dc933d237	08/03/2013	08/03/2016	DAMAGED	SSLSERVER_STANDARD

Back to device detail

Figure 34 - Device certificates

The eye icon () under the “certificate list” takes to the “certificate detail” screen:

Certificate Detail

Device Information	
Name	SAMPLE_DEVICE
Description	THIS IS A SAMPLE DEVICE
Organisation	Banco de España(ES)

Contact person data	
Name	JOHN
Surnames	SMITH
Mail	john.smith@bde.es
Phone number	+34 1233344

SSL Server details	
Description	THIS IS A SSL SERVER
E-mail address	service@bde.es
Common name	service.bde.es
DNS name	service.bde.es;help.bde.es;other.bde.es
IP address	

Certificate Information	
Serial number	ae9a9fb0c86fd85139f190b7c655ef
Issuance date	08/03/2013
Expiration date	08/03/2016
Status	ACTIVE
Policy	SSLSERVER_STANDARD

Download | Back to certificate list

Figure 35 - Device certificate detail

The **Download** button allows downloading a copy of the certificate (.cer file)

3.4. CERTIFICATES

From the **Certificates** option you can access to the information about the certificates issued for your Central Bank.


Figure 36 - Search certificates

Clicking the Search button shows the certificates that meet the search criteria

Detail	Subscriber	Policy Name	State	Initial Date	Expiration Date
	APLICACION_PRUEBAS	TECHNICAL: DOMAIN CONTROLLER PKCS12	Active	24-03-2014 14:51:44	24-03-2017 14:51:44
	t-esinfpr5	PERSONAL: MOBILE DEVICE	Active	12-03-2014 17:15:56	12-03-2017 17:15:56
	PRUEBAS_EPK	TECHNICAL: APPLICATION PKCS12	Active	12-03-2014 17:11:38	12-03-2017 17:11:38
	t-esinfpr4	PERSONAL: ADVANCED PROVISIONAL	Expired	26-02-2014 17:32:38	27-02-2014 23:58:59
	ESCB-PKI_LDAP	TECHNICAL: SSL SERVER PKCS12	Active	19-02-2014 09:03:23	19-02-2017 09:03:23
	ESCB-PKI_LDAP	TECHNICAL: SSL SERVER PKCS12	Active	19-02-2014 09:00:44	19-02-2017 09:00:44
	ESCB-PKI_LDAP	TECHNICAL: SSL SERVER PKCS12	Active	19-02-2014 08:57:24	19-02-2017 08:57:24
	SEE PROJECT USER 120	SHARED: MAILBOX	Revoked	11-02-2014 16:28:58	11-02-2017 16:28:58
	t-esinfpr5	PERSONAL: SECURE EMAIL GATEWAY	Active	10-02-2014 18:40:54	10-02-2017 18:40:54
	t-esinfpr5	PERSONAL: MOBILE DEVICE	Revoked	10-02-2014 18:40:23	10-02-2017 18:40:23
	t-esinfpr5	PERSONAL: SECURE EMAIL GATEWAY	Revoked	10-02-2014 18:07:23	10-02-2017 18:07:23
	t-esinfpr5	PERSONAL: MOBILE DEVICE	Revoked	10-02-2014 18:06:04	10-02-2017 18:06:04
	PRUEBA_SMB2	SHARED: MAILBOX	Active	30-01-2014 16:57:00	30-01-2017 16:57:00
	APLICACION_PRUEBAS	TECHNICAL: DOMAIN CONTROLLER PKCS10	Active	16-01-2014 18:14:30	16-01-2017 18:14:30
	APLICACION_PRUEBAS	TECHNICAL: DOMAIN CONTROLLER PKCS10	Active	16-01-2014 18:10:29	16-01-2017 18:10:29
	t-esinfmpp	PERSONAL: SECURE EMAIL GATEWAY	Active	15-01-2014 16:07:27	15-01-2017 16:07:27
	t-esinfmpp	PERSONAL: MOBILE DEVICE	Active	15-01-2014 16:06:11	15-01-2017 16:06:11
	APLICACION_PRUEBAS	TECHNICAL: APPLICATION PKCS12	Active	15-01-2014 08:52:18	15-01-2017 08:52:18
	t-esinfpr3	PERSONAL: MOBILE DEVICE	Active	15-01-2014 08:48:56	15-01-2017 08:48:56
	BDE_PRUEBA_SMB	SHARED: MAILBOX	Active	15-01-2014 08:21:53	15-01-2017 08:21:53

Figure 37 - Certificates list

The **Export XLS** button generates an Excel document with the details of all the certificates meeting the search criteria.

Click the  button to see the details of a certificate from the list.

3.5. CERTIFICATE REQUESTS

From the **Certificate requests** option you can access to the information about the certificate requests generated at your Central Bank.

Figure 38 - Search certificate requests

Clicking the Search button shows the certificate requests that meet the search criteria

Certificate request list


Detail	Subscriber	Subscriber Type	Certificate Package Type	Request Status	Request Date	Request Reason
	APLICACION_PRUEBAS	Devices	Standard	Completed	24-03-2014 14:52:01	Request
	t-esinfppr5	ESCB Users	Mobile Device	Completed	12-03-2014 17:15:13	Key compromise
	PRUEBAS_EPK	Devices	Standard	Completed	12-03-2014 17:12:14	Request
	t-esinfdbcx	ESCB Users	Provisional	Cancelled	26-02-2014 17:42:57	Request
	t-esinfppr4	ESCB Users	Provisional	Completed	26-02-2014 17:31:29	Request
	ESCB-PKI_LDAP	Devices	Standard	Completed	19-02-2014 09:03:29	Request
	ESCB-PKI_LDAP	Devices	Standard	Completed	19-02-2014 09:00:43	Request
	ESCB-PKI_LDAP	Devices	Standard	Completed	19-02-2014 08:58:08	Request
	SEE PROJECT USER 120	Shared Mailbox	Shared Mailbox	Completed	11-02-2014 16:28:59	Request
	t-esinfppr5	ESCB Users	Gateway	Completed	10-02-2014 18:20:17	Request
	t-esinfppr5	ESCB Users	Mobile Device	Completed	10-02-2014 18:20:08	Request
	t-esinfppr5	ESCB Users	Gateway	Completed	10-02-2014 18:07:56	Request
	t-esinfppr5	ESCB Users	Mobile Device	Completed	10-02-2014 18:06:39	Request
	PRUEBA_SMB2	Shared Mailbox	Shared Mailbox	Completed	30-01-2014 16:55:02	Request
	t-esinfppr3	ESCB Users	Gateway	Cancelled	27-01-2014 16:15:39	Request
	APLICACION_PRUEBAS	Devices	Advanced	Completed	16-01-2014 18:15:25	Request
	APLICACION_PRUEBAS	Devices	Advanced	Completed	16-01-2014 18:09:39	Request
	t-esinfmpp	ESCB Users	Gateway	Completed	15-01-2014 16:08:04	Request
	t-esinfmpp	ESCB Users	Mobile Device	Completed	15-01-2014 16:06:50	Request
	APLICACION_PRUEBAS	Devices	Standard	Completed	15-01-2014 08:51:43	Key compromise

1 | 2 | 3 | 4 | 5 | 6 | 7 | 8

Export XLS Details of Search

Figure 39 - Certificate requests list

The **Export XLS** button generates an Excel document with the details of all the certificate requests meeting the search criteria.

Click the  button to see the details of a certificate request from the list.

3.6. EVENTS

From the **Events** option you can access to the security events generated at the ESCB-PKI system for your Central Bank.

Figure 40 - Search events

Clicking the Search button shows the security events that meet the search criteria

Detail	Who (ESCB userid)	What (action)	On subscriber	On certificate type	When
	infvfg	Issue certificate package.	INF_ESCB-PKI		13-04-2014 10:44:58
	infmpp	Approve shared mailbox certificate request.	INF_ESCB-PKI		13-04-2014 10:30:33
	infvfg	Register new shared mailbox certificate request.	INF_ESCB-PKI		13-04-2014 10:28:04
	infmpp	Approve shared mailbox certificate request.	DisplayName		13-04-2014 10:21:26
	infmpp	Approve shared mailbox certificate request.	qalvixSharedMailbox		13-04-2014 10:19:24
	t-esqlorcgx2	Issue TOKEN-BASED certificate package.	t-esqlorcgx2		11-04-2014 10:50:06
	t-esqlorcgx2	Begin TOKEN-BASED certificate package issuance.	t-esqlorcgx2		11-04-2014 10:48:09
	qlorcgx	Enable remote download.	t-esqlorcgx2		11-04-2014 10:42:40
	qlorcgx	Modify device serial number.	t-esqlorcgx2		11-04-2014 10:42:34
	qlorcgx	Enable remote download.	t-esqlorcgx2		11-04-2014 10:41:32
	qlorcgx	Register certificate package request.	t-esqlorcgx2		11-04-2014 10:39:42
	qlorcgx	Register new user.	t-esqlorcgx2		11-04-2014 10:36:59
	qlorcgx	Register new user.	t-esqlorcgx		11-04-2014 10:35:59
	qlorcgx_local	Issue a STANDARD certificate package.	qlorcgx_local		10-04-2014 18:00:50
	qlorcgx_local	Generation of the terms and conditions document.	qlorcgx_local		10-04-2014 18:00:23
	qlorcgx	Enable remote download.	usuarionew		10-04-2014 17:56:01
	qlorcgx	Modify device serial number.	usuarionew		10-04-2014 17:55:55
	qlorcgx	Register provisional certificate package request.	usuarionew		10-04-2014 17:55:49

Figure 41 - Event list

The **Export XLS** button generates an Excel document with the details of all the security events meeting the search criteria.

Click the  button to see the details of a security event from the list

Trace detail

User security information	
User identifier	infmpp
Security groups	[APPR_ESCB-PKI_RegistrationOfficer]
Security roles	[ROLE_RO, ROLE_SMCAUDIT, ROLE_SMCCERACT, ROLE_SMCCERAUD, ROLE_SMCCERREV, ROLE_SMCCERSUS, ROLE_SMCREQAPP, ROLE_SMCREQAUD, ROLE_SMCREQCAN, ROLE_SMCTYC, ROLE_USRCERAUD, ROLE_USRCFACT, ROLE_USRCPREV, ROLE_USRCPSUS, ROLE_USRCPT, ROLE_USRREAD, ROLE_USRREQAUD, ROLE_USRREQPROVISIONAL]
Security domain	[11]

Trace information	
Transaction identifier	ESCB_PKI_cba7b43e-3058-4628-8e0e-41b104da23d0
Event code	STATE_CHANGE
Date	13-04-2014 10:30:33
Application	epkmain
Priority code	INFO
Level	HIGH
Action type	RESULT
Source	SHARED_MAILBOX
Entity type	CERTIFICATE_REQUEST
Entity identifier	214
Entity domain	11
Message	Approve shared mailbox certificate request.
Arguments	<pre> -----INPUT----- HttpServletRequest Request URL=http://t-ra-epk.bde.es:443/epkmain/sharedmailbox/request/approve.html Method=GET RequestedSessionId=[id=JmkBzStCkAq8uBbcSYlpgE, isRequestedSessionIdFromCookie=true, isRequestedSessionIdFromURL=false, isRequestedSessionIdValid=true] Session=[id=JmkBzStCkAq8uBbcSYlpgE, creationTime=1397376882327, lastAccessedTime=1397377795183, maxInactiveInterval=2100] Headers=[Accept=application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */* , Accept-Encoding=gzip, deflate, Accept-Language=es-ES, Host=t-ra-epk.bde.es:443, Referer=https://t-ra-epk.bde.es/epkmain/sharedmailbox/request/detail.html?id=214, User-Agent=Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET CLR 1.1.4322; .NET4.0C; .NET4.0E) , Via=HTTP/1.1 t-ra-epk.bde.es:443, X-ESCB-IAM-AUTHLEVEL=7, X-ESCB-IAM-UD=infmpp, x-escb-iam-roles=APPR_ESCB-PKI_RegistrationOfficer, iv_server_name=bdenredit02-webseald-tamsvc02.bde.es, Cookie=RSESSIONID=0000JmkBzStCkAq8uBbcSYlpgE:15qvg4lh, \$WSIS=false, \$WSSC=http, \$WSPR=HTTP/1.1, \$WSRA=172.20.181.33, \$WSRH=172.20.181.33, \$WSSN=t-ra-epk.bde.es, \$WSSP=443, Surrogate-Capability=WS-ESI="ESI/1.0+", _WS_HAPRT_WLMVERSION=-1] Parameters=[] -----OUTPUT----- redirect/sharedmailbox/request/detail.html </pre>

[Back to event list](#)

Figure 42 - Event details

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.

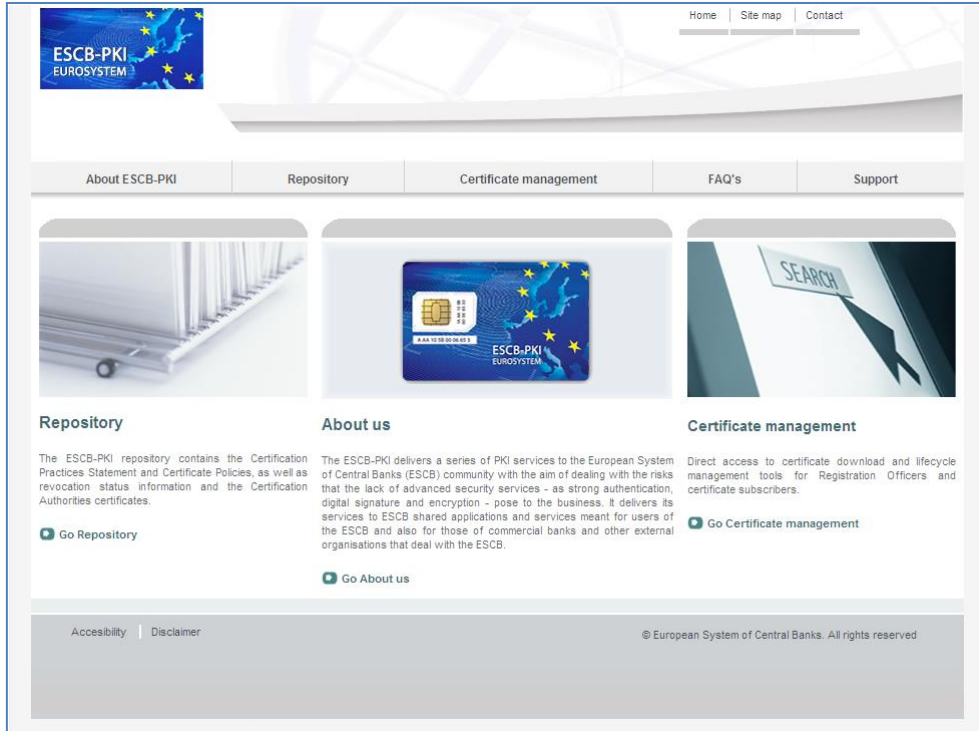


Figure 43 - ESCB-PKI Website

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.