BANCO DE ESPAÑA
Eurosistema

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI PROJECT

ESCB-PKI REGISTRATION AUTHORITY APPLICATION

AUDITOR'S MANUAL

VERSION 3.1

ECB-Restricted
07-Nov-2024

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 *http* links to *https*

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.

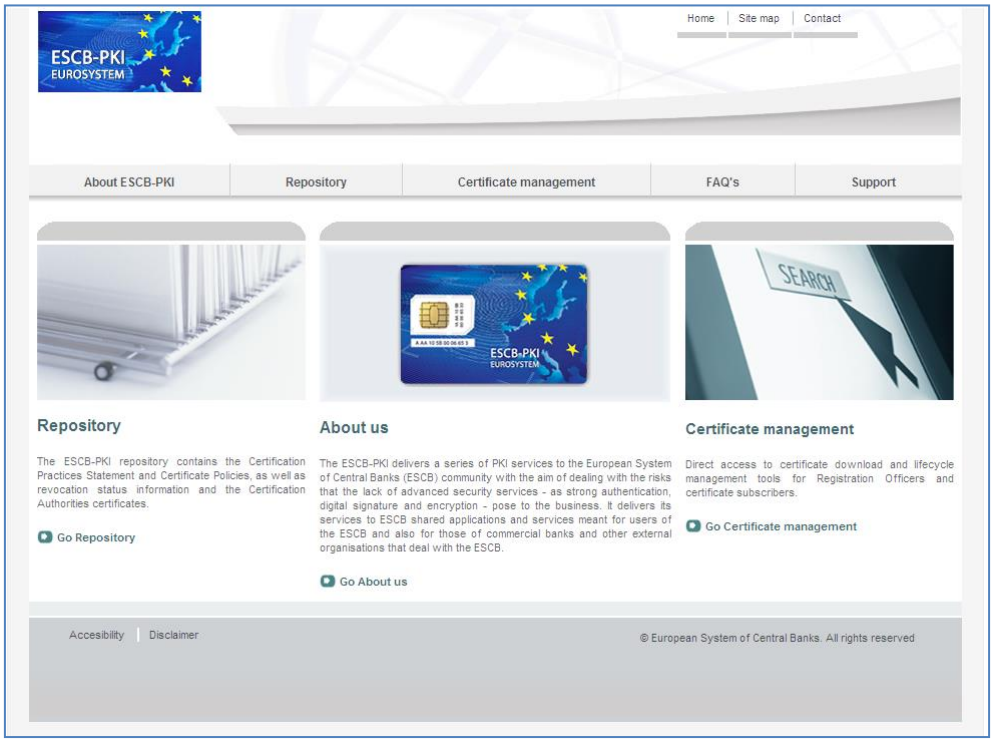

Figure 1 - ESCB-PKI Website

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

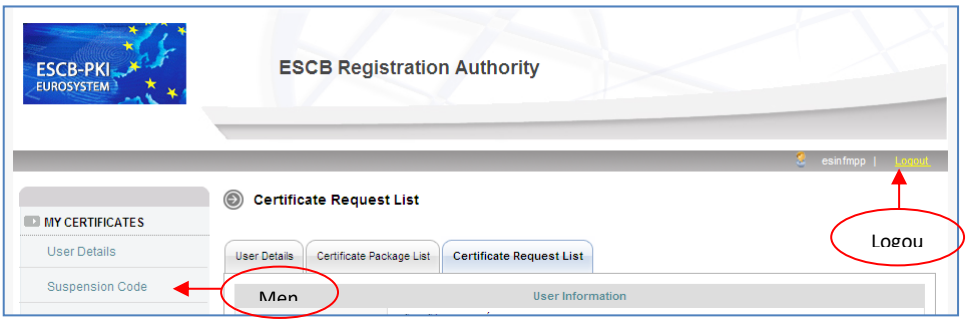

Figure 4 - Certificate management

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

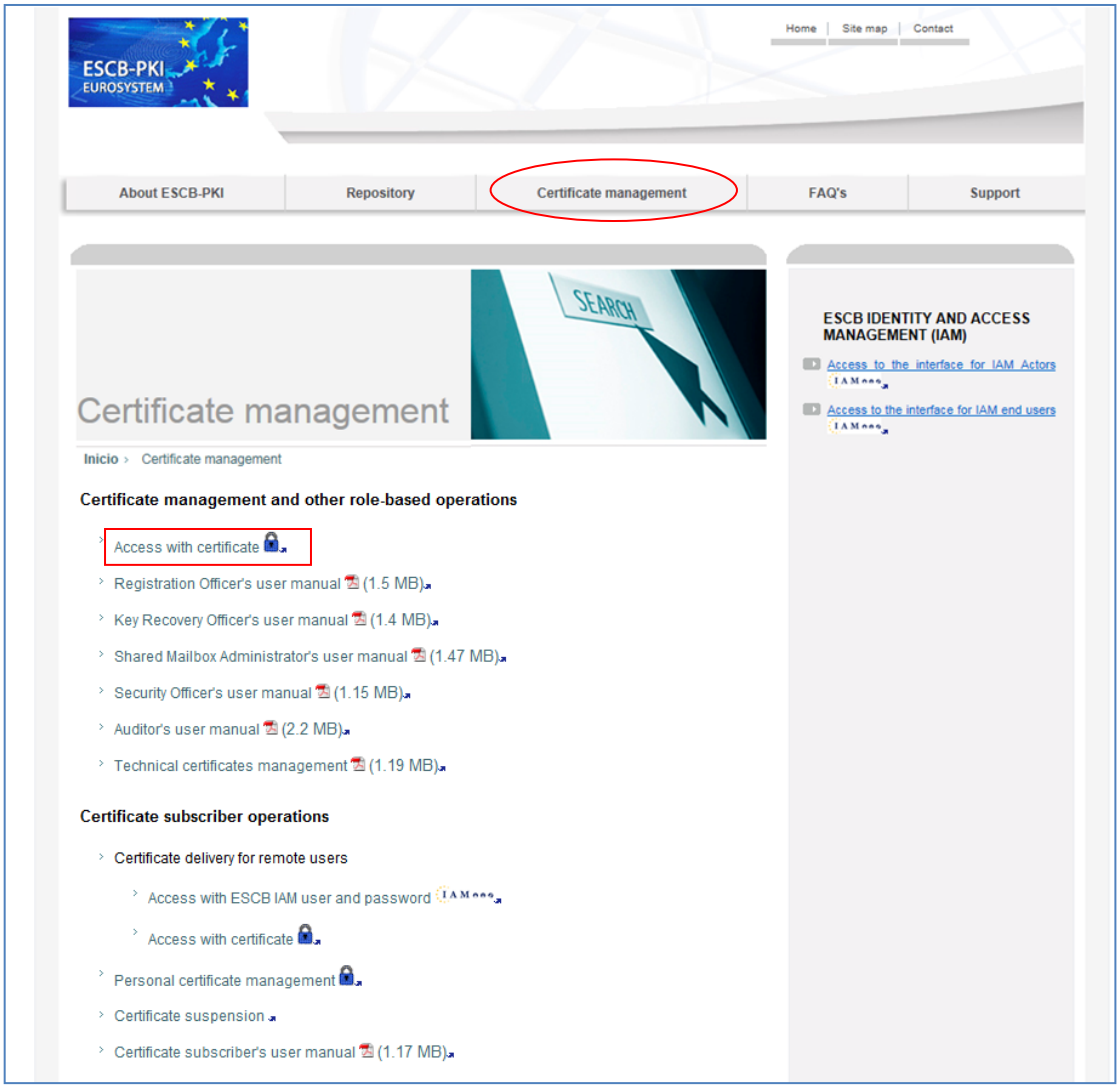

Figure 5 - ESCB-PKI Website - Registration Authority Application

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

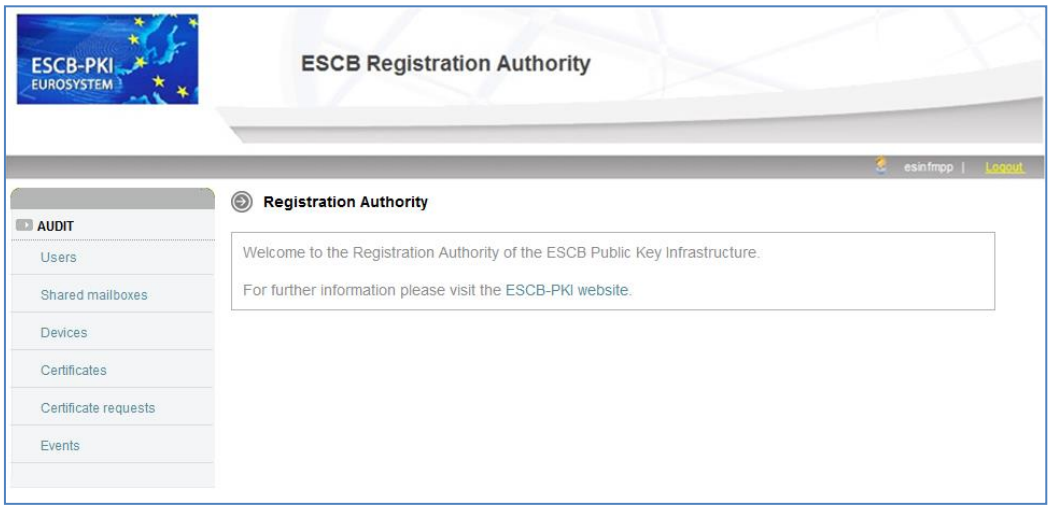

Figure 6 - Auditor menu

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.

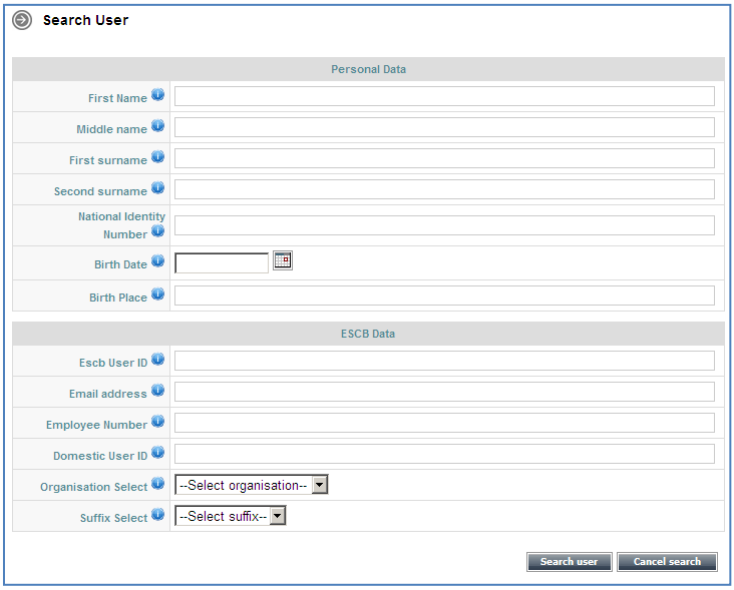

Figure 7 - Certificates management. Search user option

Press the ***Search user*** button

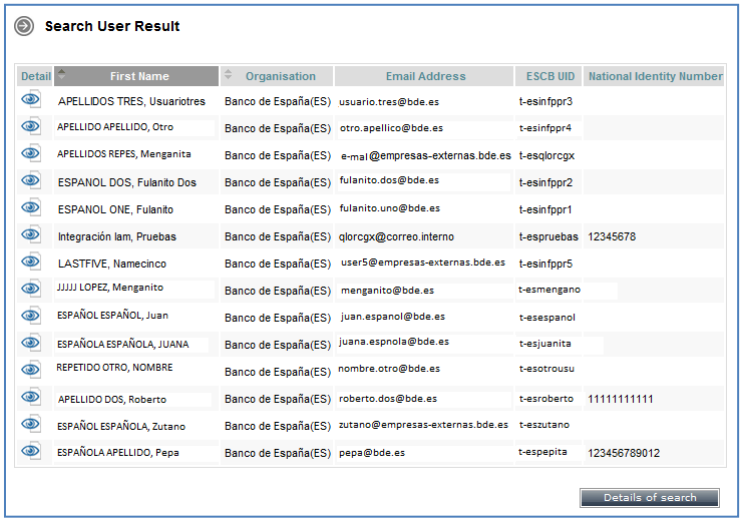

Figure 8 - Organisation user list

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

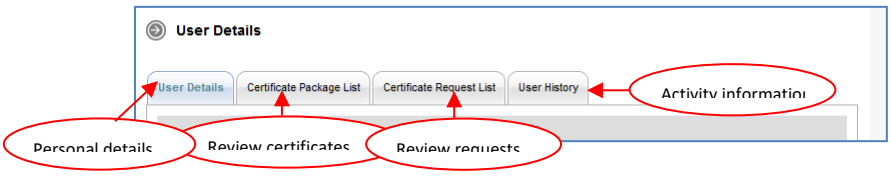

Figure 9 - User details

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.

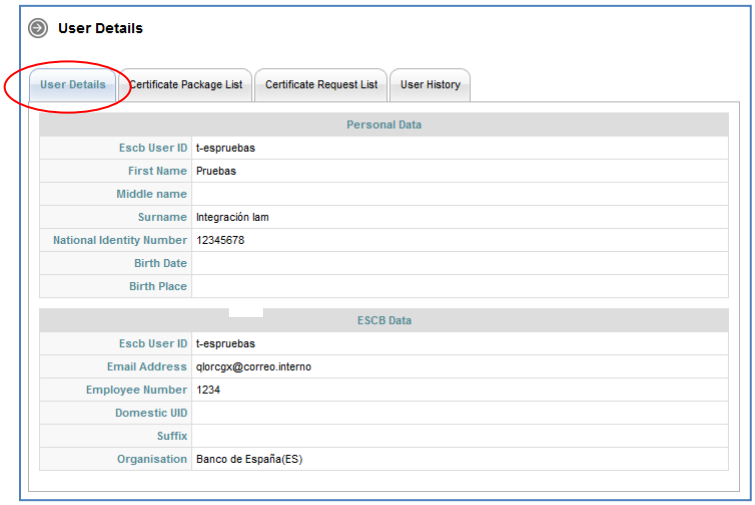

Figure 9 - User details

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

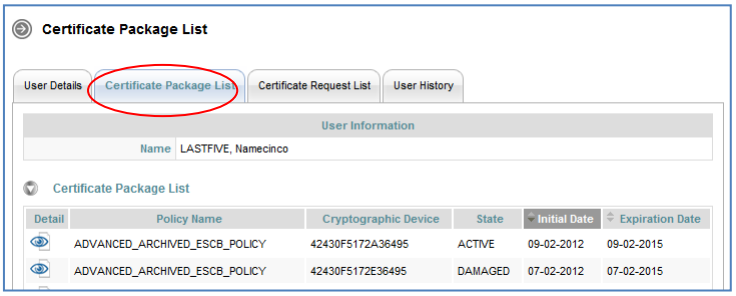

Figure 10 - Certificate list

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:

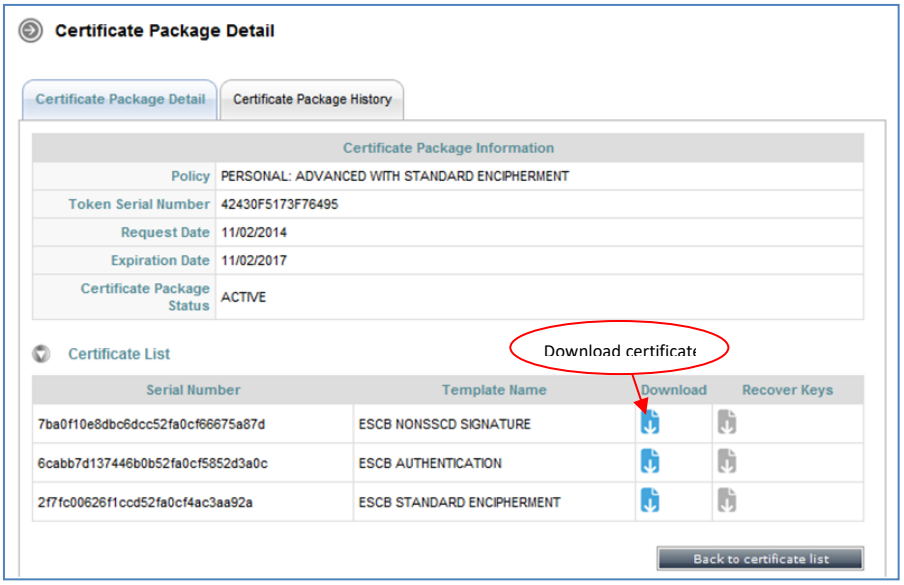

Figure 11 - Certificate details

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.

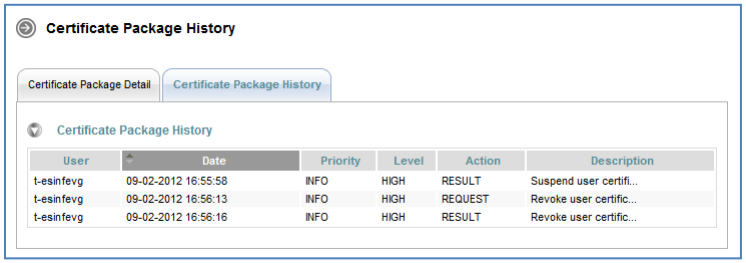

Figure 12 - Certificate activity

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

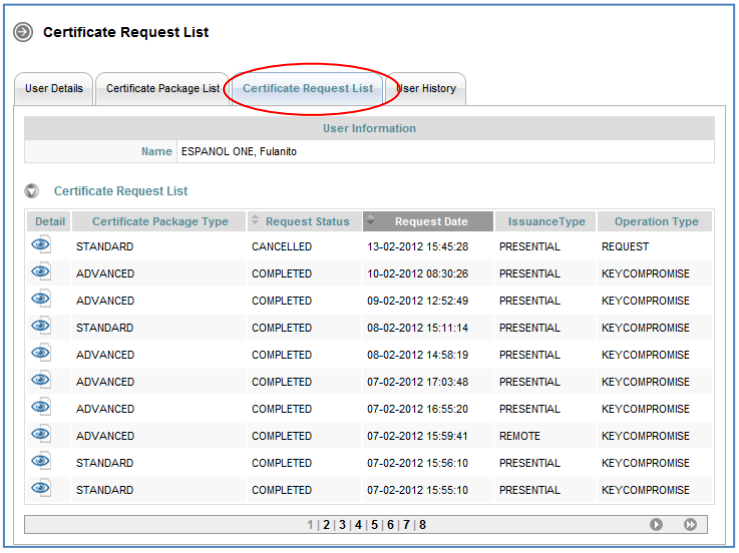

Figure 13 - Certificate requests list

Clicking the button the details of the certificate request are displayed

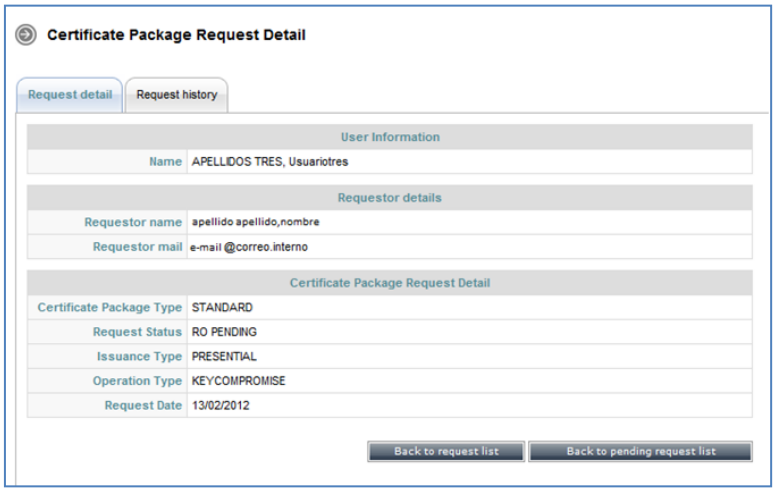

Figure 14 - Certificate request details

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.

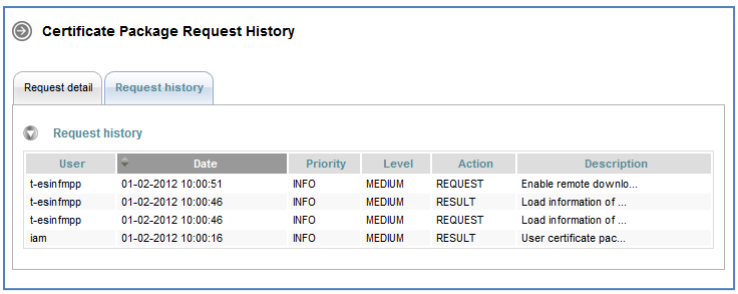

Figure 15 - Request activity

3.1.4. USER HISTORY

Displays all the activity related to the user.

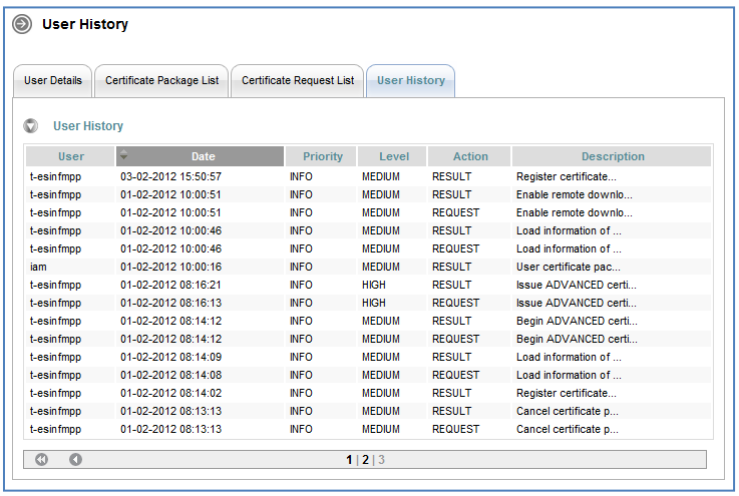

Figure 16 - User activity

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.

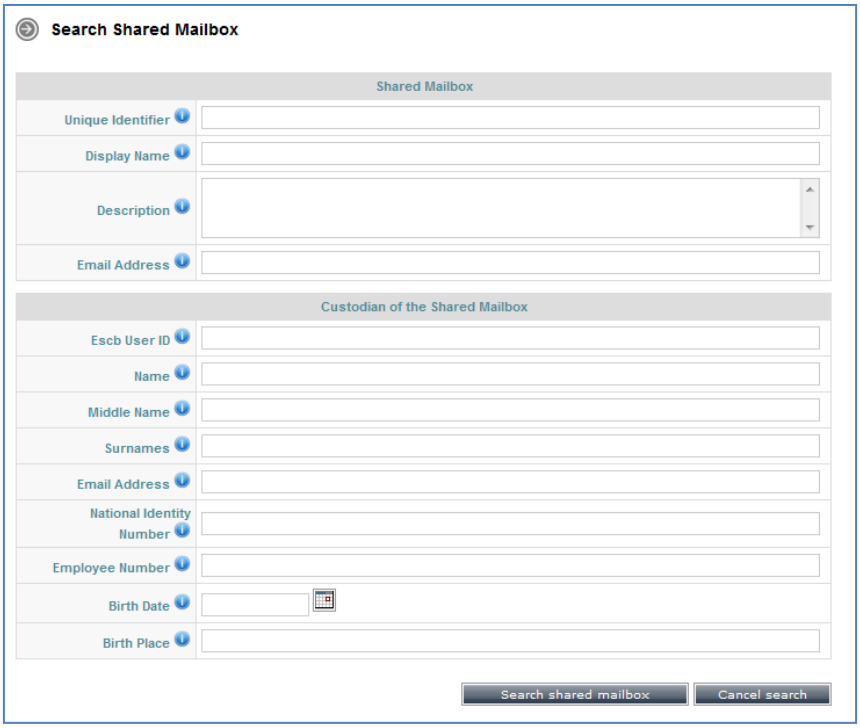

Figure 17 - Search shared mailbox

Press the ***Search shared mailbox*** button

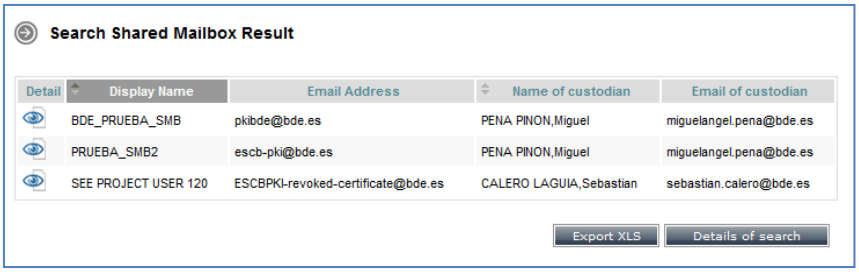

Figure 18 - Shared mailbox list

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

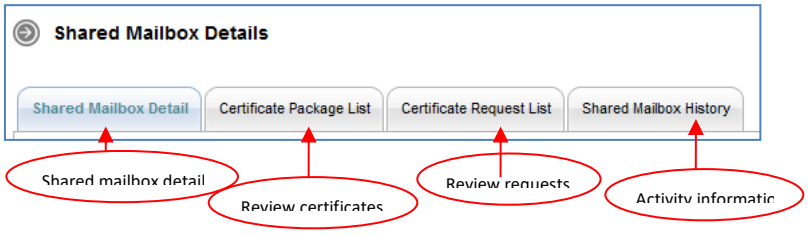

Figure 19 - Shared mailbox details

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.)

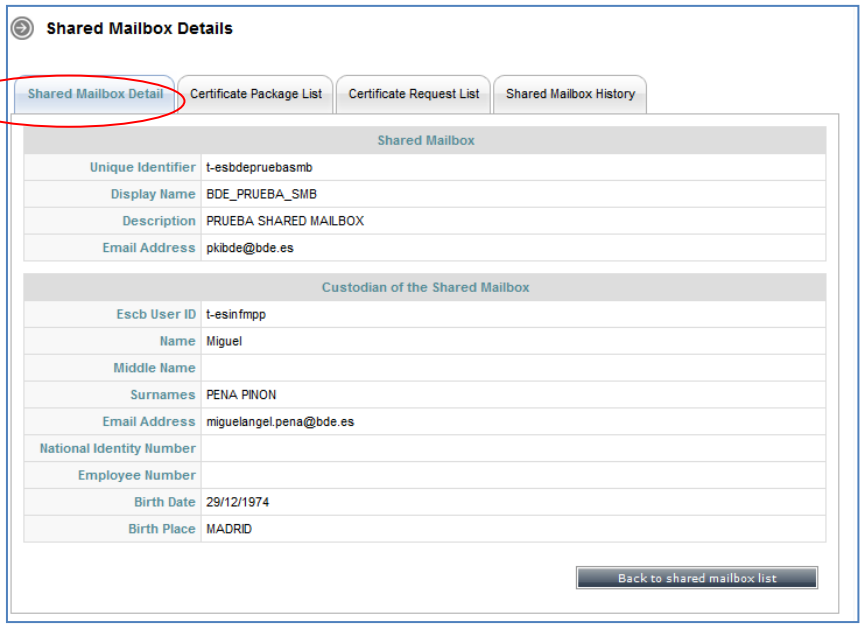

Figure 20 - Shared mailbox details

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

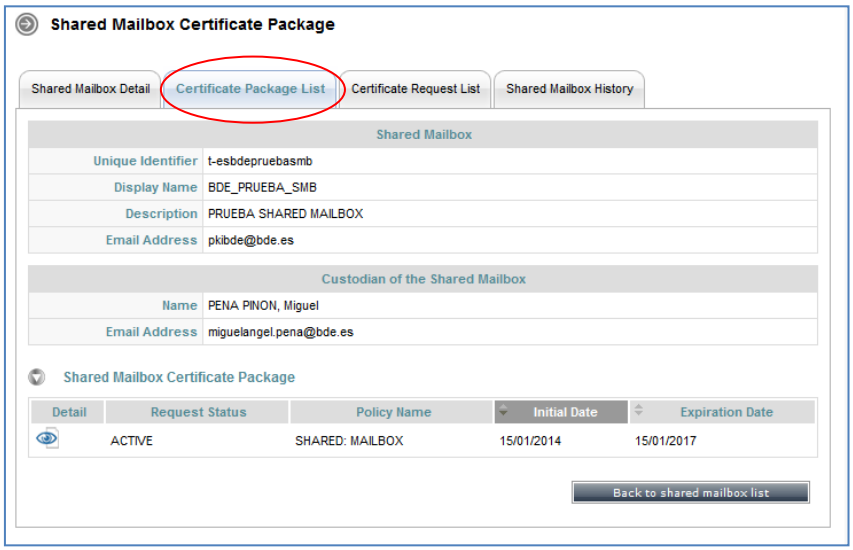

Figure 21 - Shared mailbox certificate package list

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

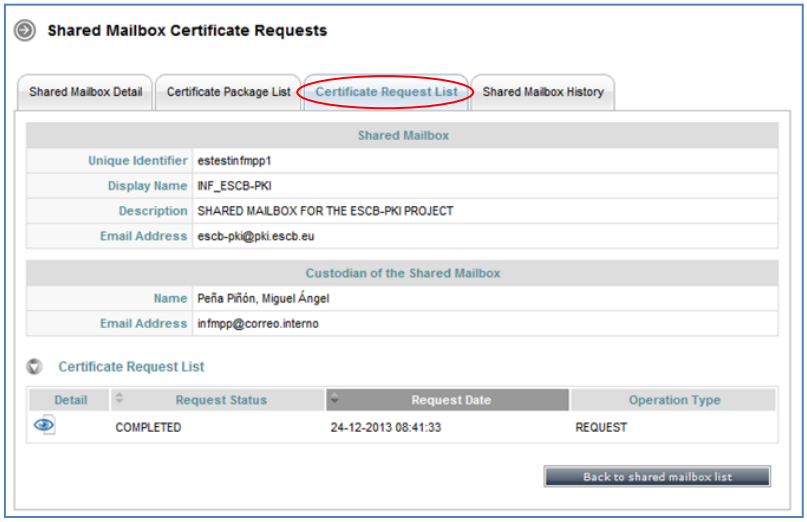

Figure 22 - Shared mailbox certificate requests list

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

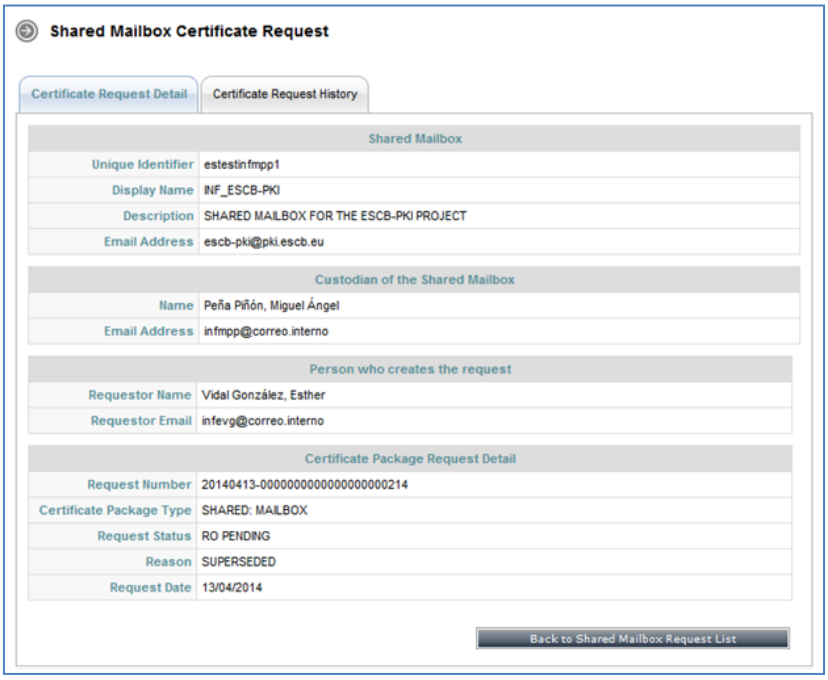

Figure 23 - Shared mailbox certificate request details

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.

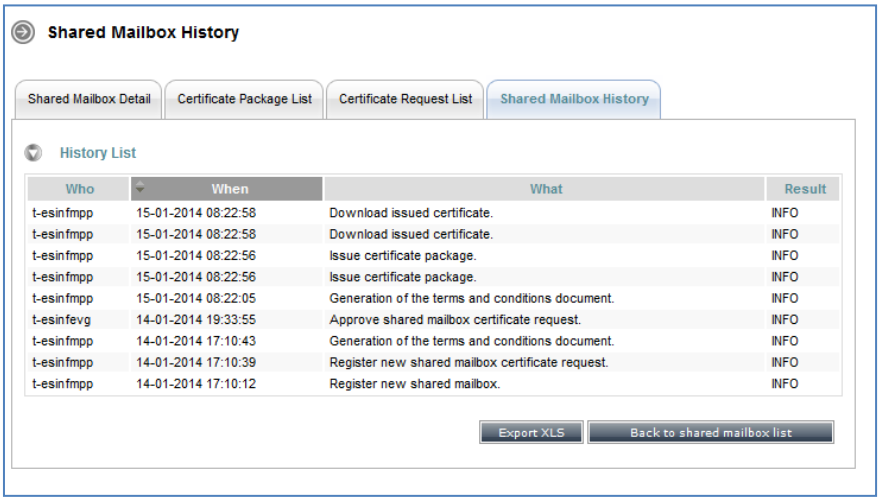

Figure 24 - Shared mailbox activity

3.3. SEARCH DEVICES

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

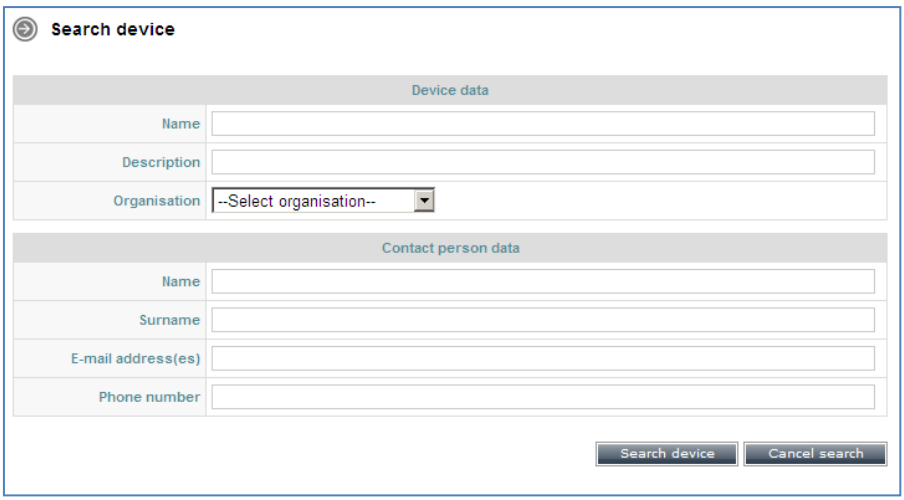

Figure 25 - Search device

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:

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:

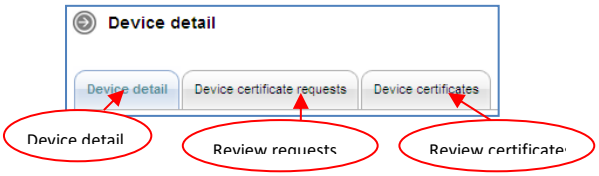

Figure 27 - Device detail

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

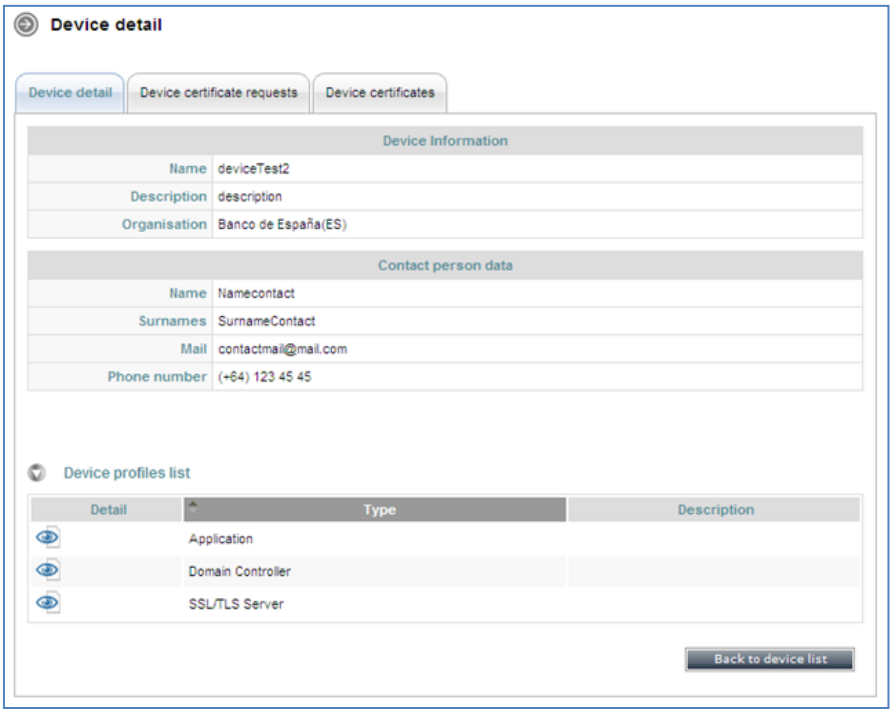

Figure 28 - Device detail tab

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.

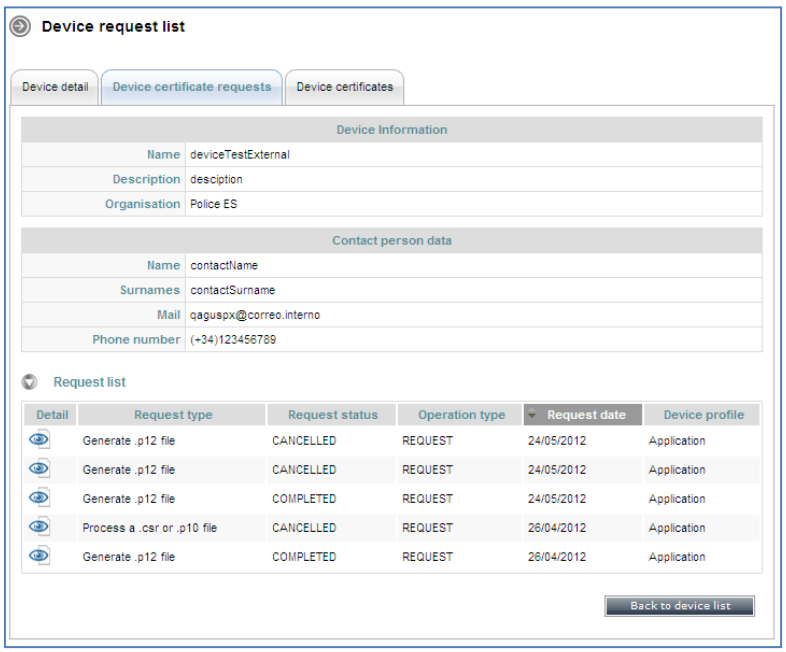

Figure 29 - Device request list

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.

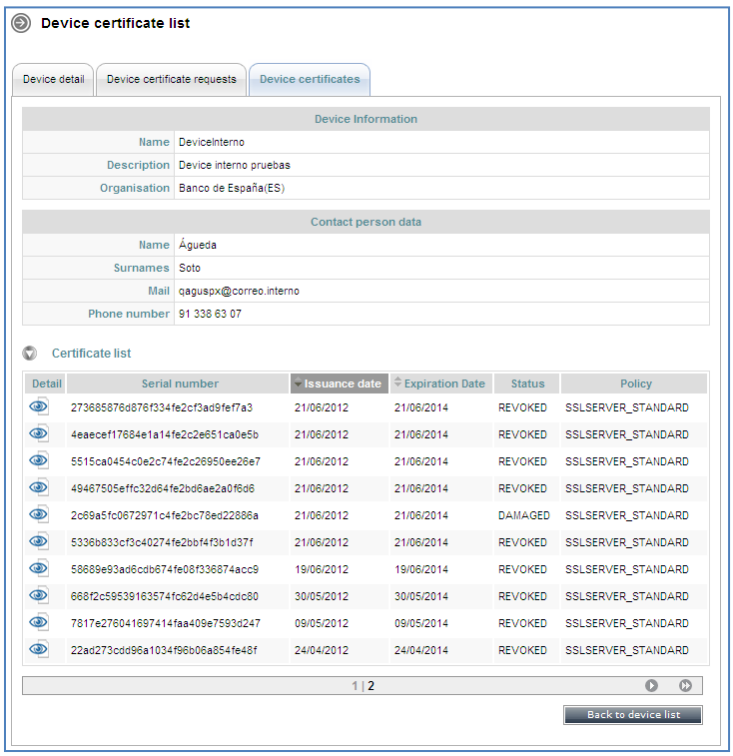

Figure 30 - Device certificate list

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:

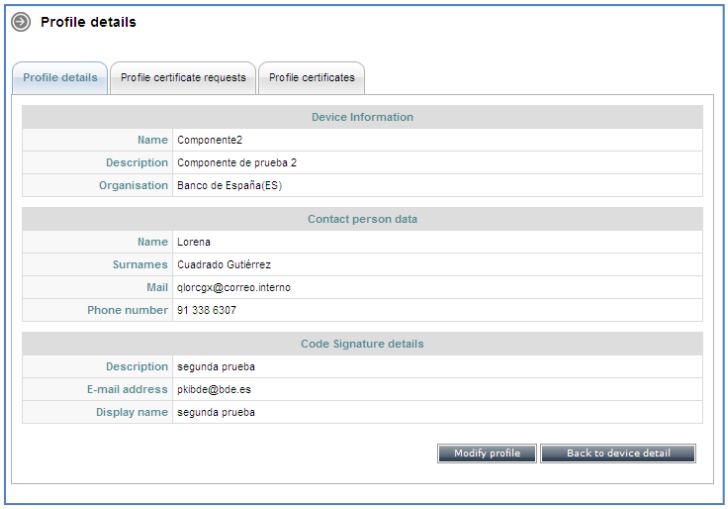

Figure 31 - Device profile details

3.3.4.2. Profile certificate requests

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

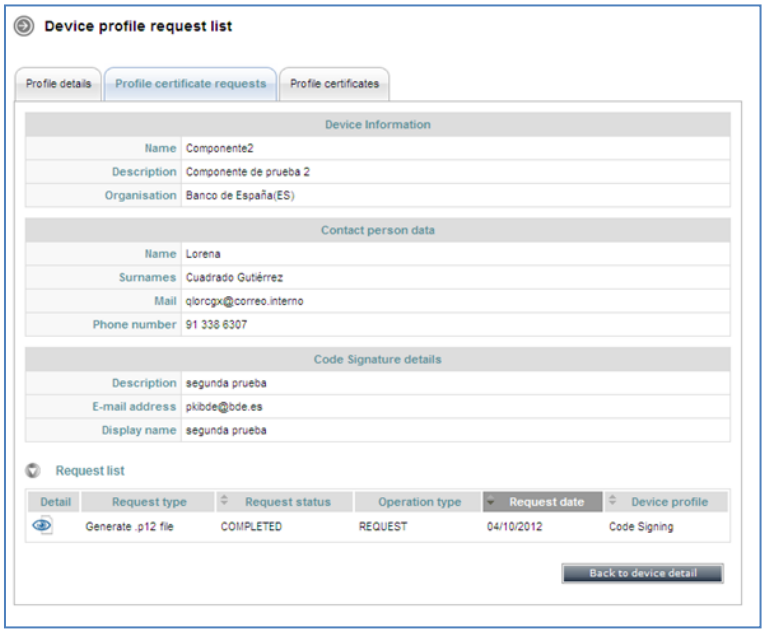

Figure 32 - Device certificate requests

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

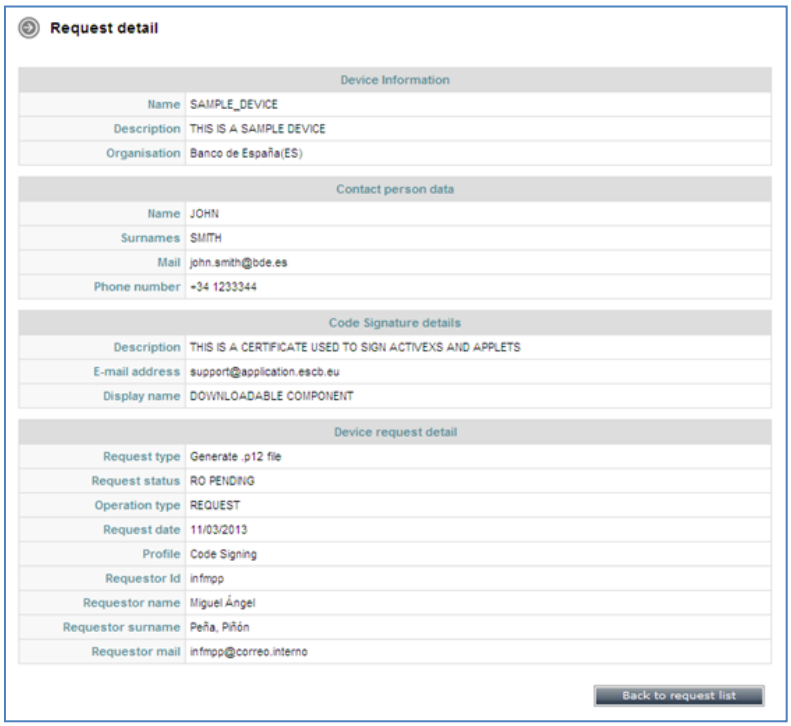

Figure 33 - Device certificate request detail

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.

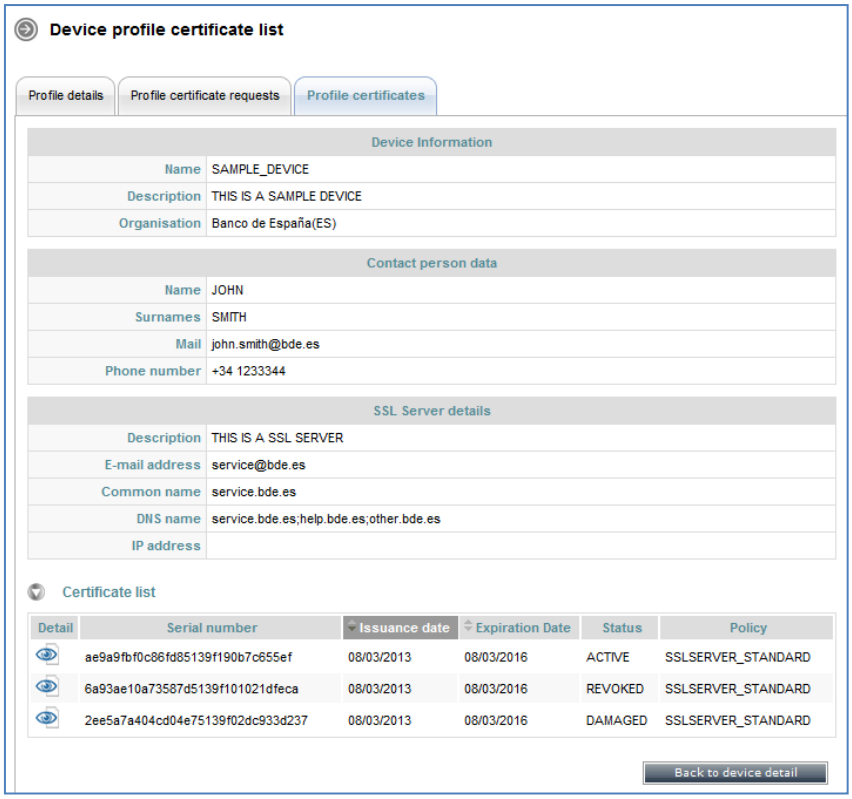

Figure 34 - Device certificates

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

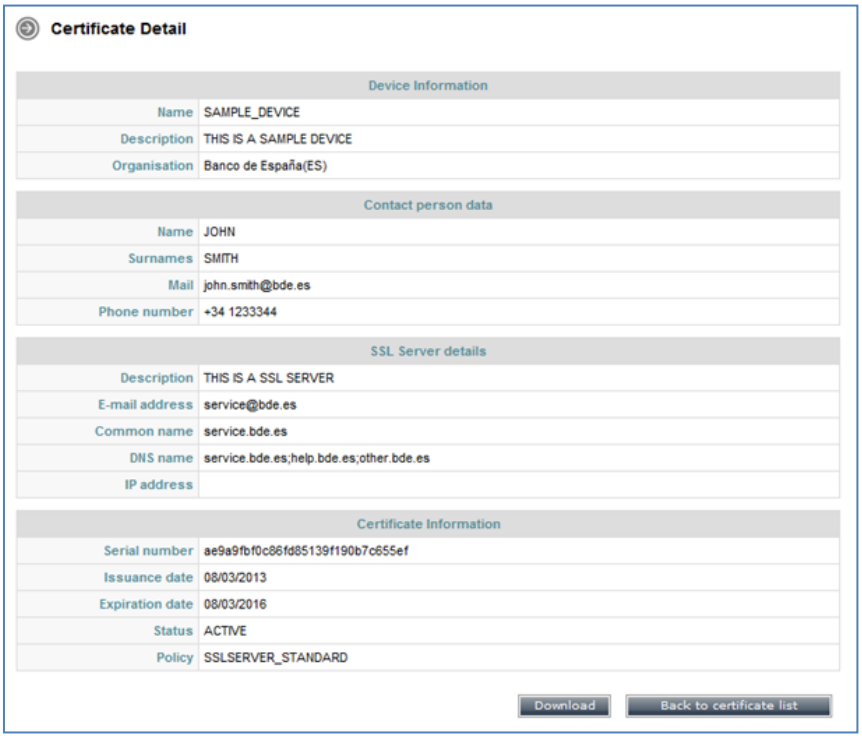

Figure 35 - Device certificate detail

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.

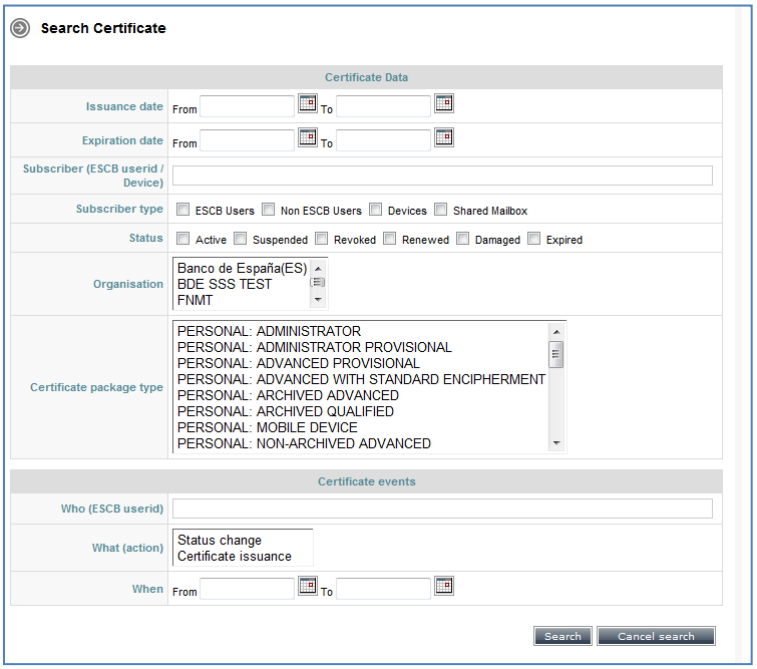

Figure 36 - Search certificates

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

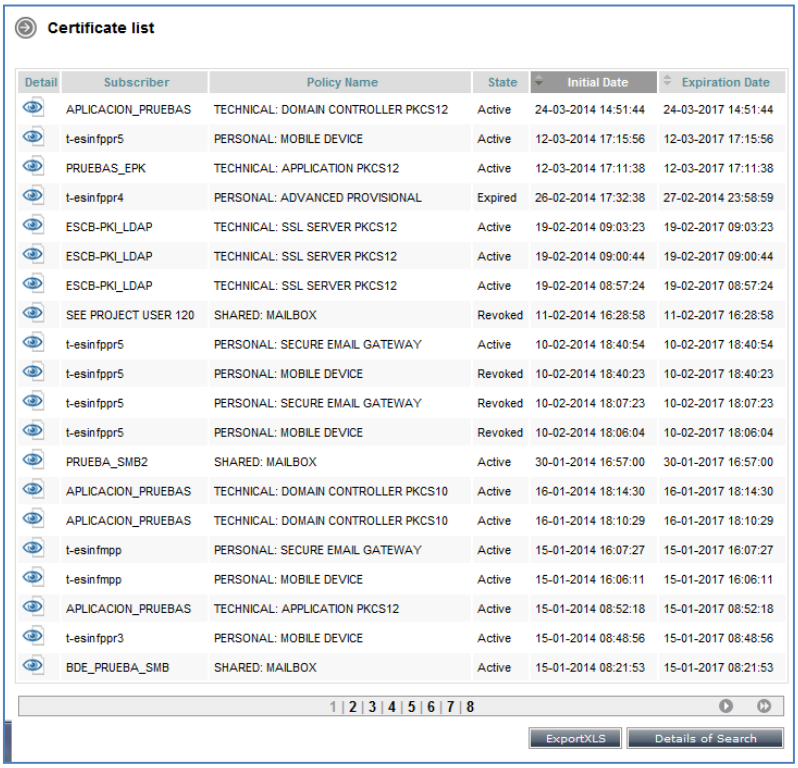

Figure 37 - Certificates list

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.

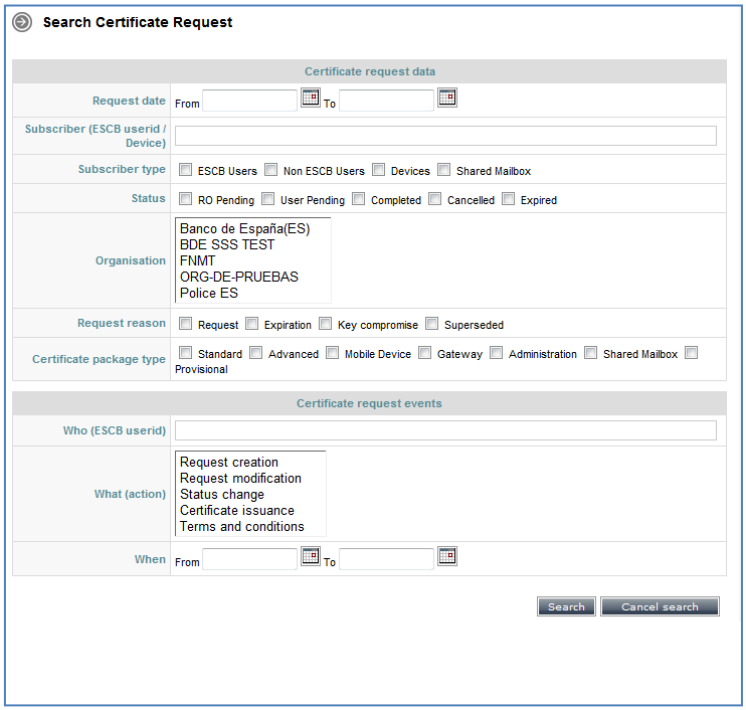

Figure 38 - Search certificate requests

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

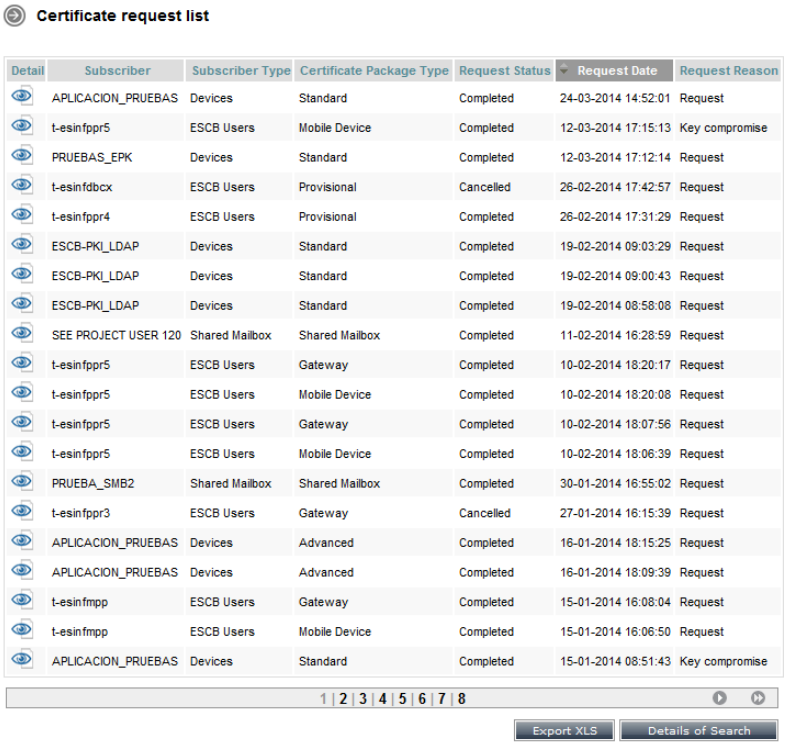

Figure 39 - Certificate requests list

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.

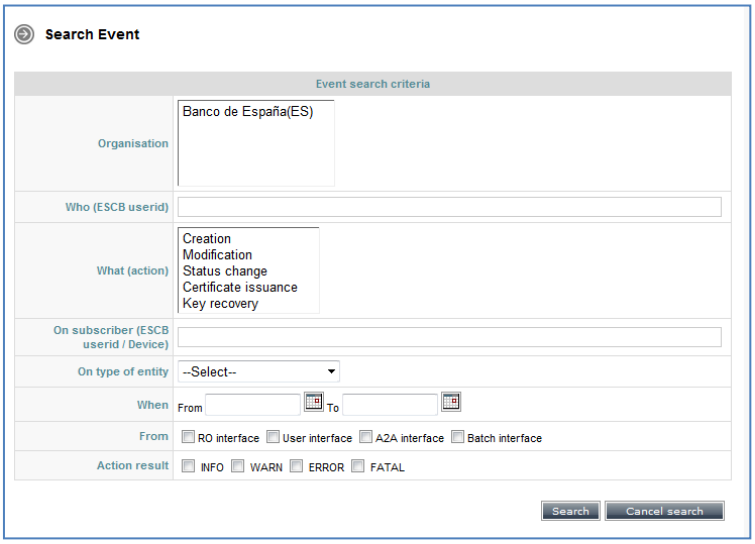

Figure 40 - Search events

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

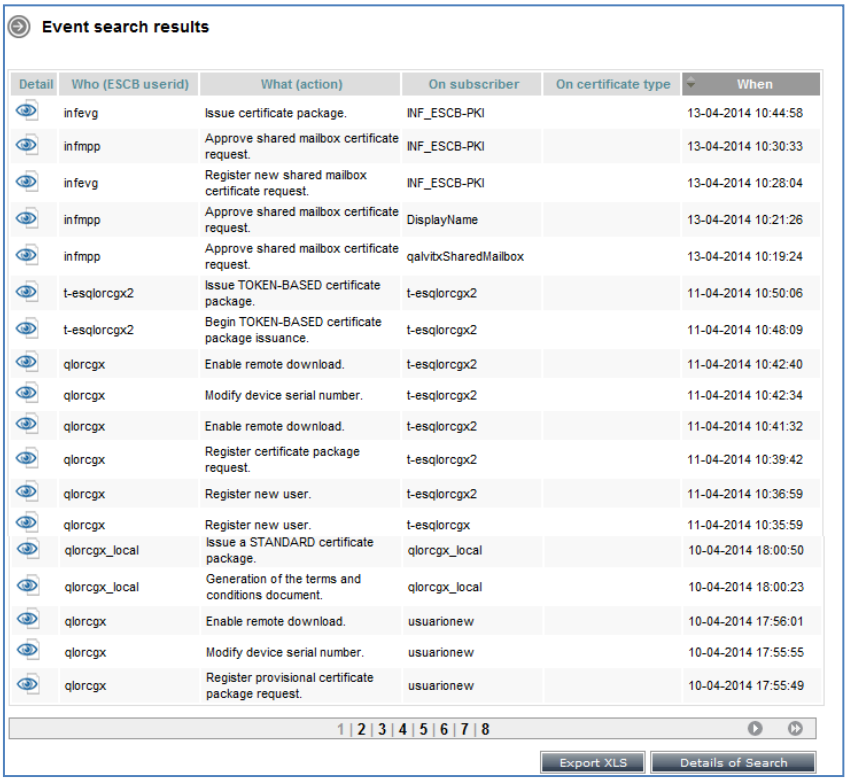

Figure 41 - Event list

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

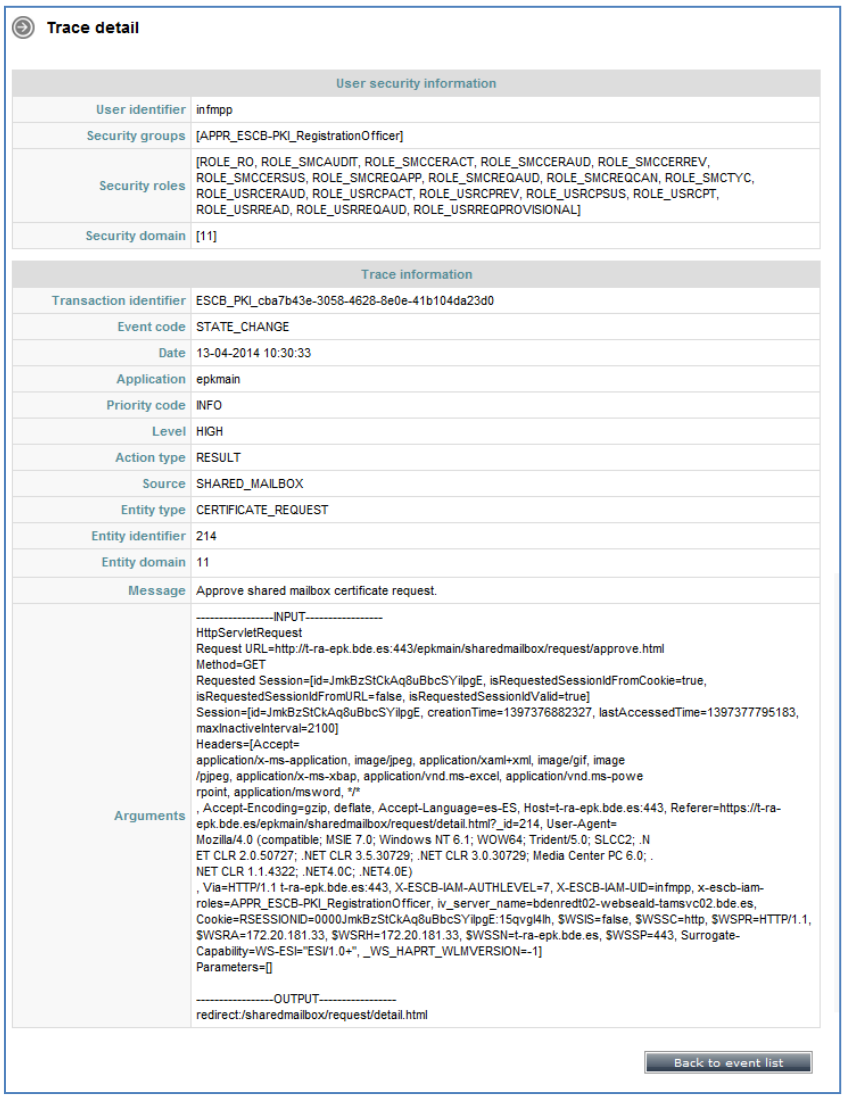

Figure 42 - Event details

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.

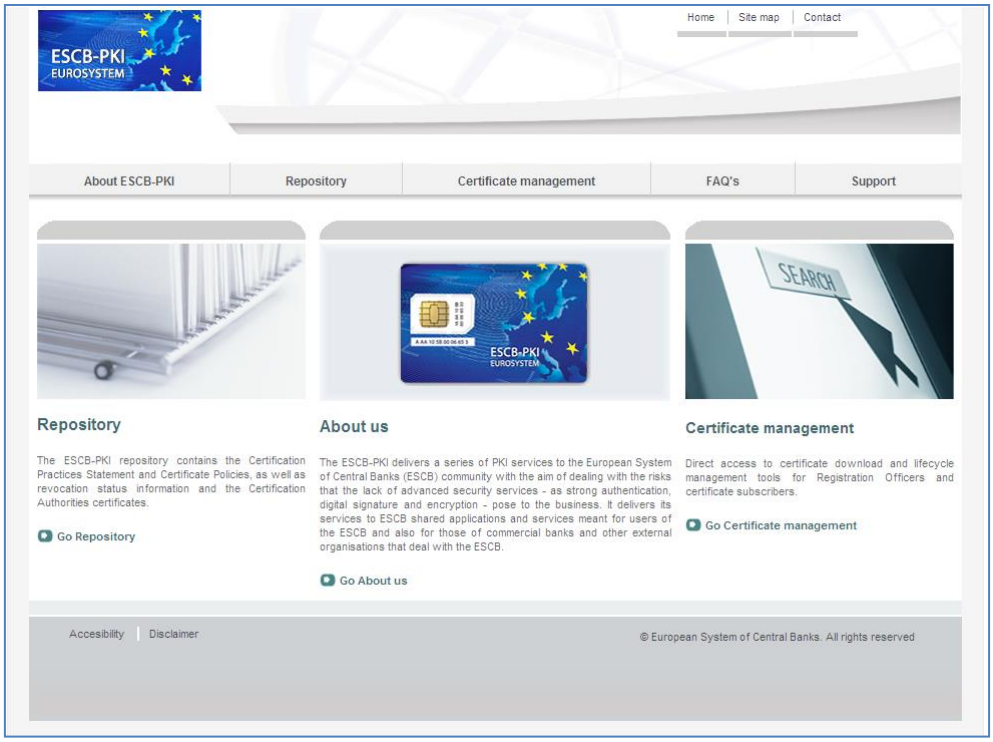

Figure 43 - ESCB-PKI Website

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.