BANCO DE ESPAÑA
Eurosistema

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI PROJECT

ESCB-PKI REGISTRATION AUTHORITY APPLICATION

SECURITY OFFICER’S MANUAL

VERSION 3.1

ECB-Restricted
07-Nov-2024

TABLE OF CONTENTS

TABLE OF ILLUSTRATIONS

Project name:	**ESCB-PKI**
Author:	ESCB-PKI Project team
File name:	ESCB-PKI - RA Application Security 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	15-04-2013	Initial version
2.0	Final	11-09-2018	Added software key recovery option for organisations
3.0	Final	15.11.2021	Compatibility with other browsers
3.1	Final	07.11.2024	Update *http* links to *https*

GLOSSARY AND ACRONYMS

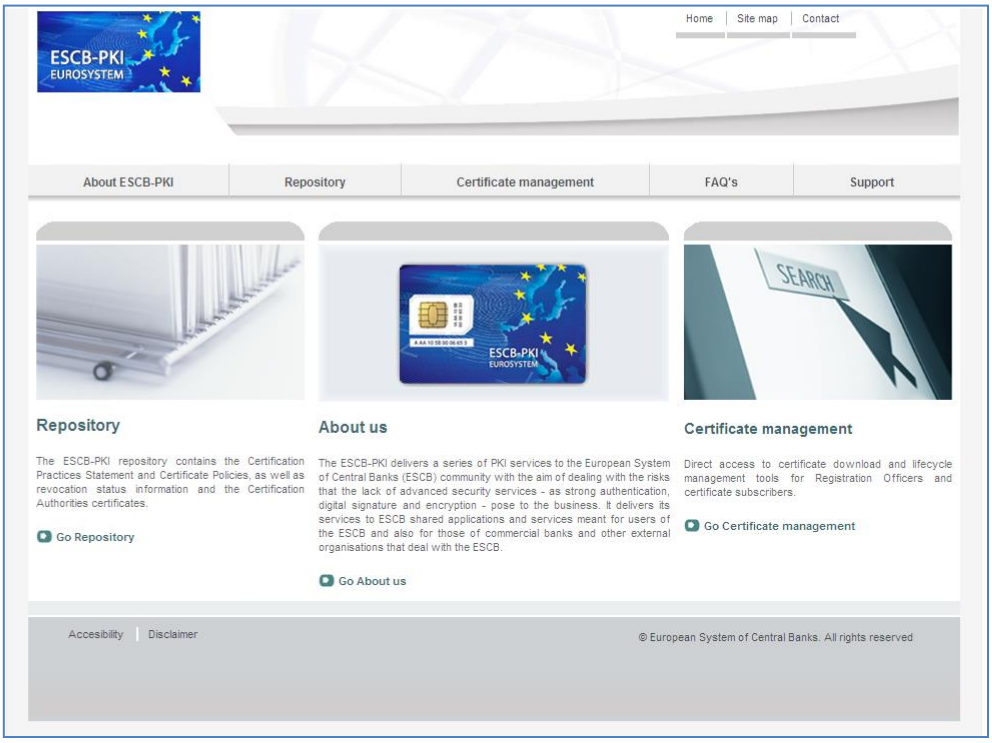
Acronym	Definition
CA	Certificate Authority
CB	ESCB Central Bank (ECB or NCB)
CP	Certification Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
ECB	European Central Bank
ESCB	European System of Central Banks, including the ECB and the NCBs of all States member of the European 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
KRO	Key Recovery Officer
LIA	Local Identity Administrator
NCB	National Central Bank
PKI	Public Key Infrastructure
SO	Security Officer
RA	Registration Authority
RO	Registration Officer
RO4EO	Registration Officers for External Organisations
UPN	User Principal Name

1. INTRODUCTION

This document aims at providing Security Officers (SO) information on how to use the ESCB-PKI Registration Authority application to set several security parameters.

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.



Repository

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

About us

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

Certificate management

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

© European System of Central Banks. All rights reserved

Figure 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.

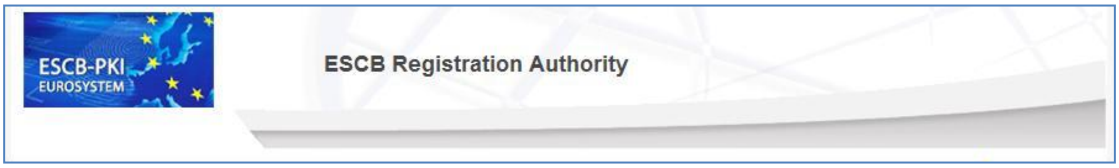


Figure 2 - Production frame

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

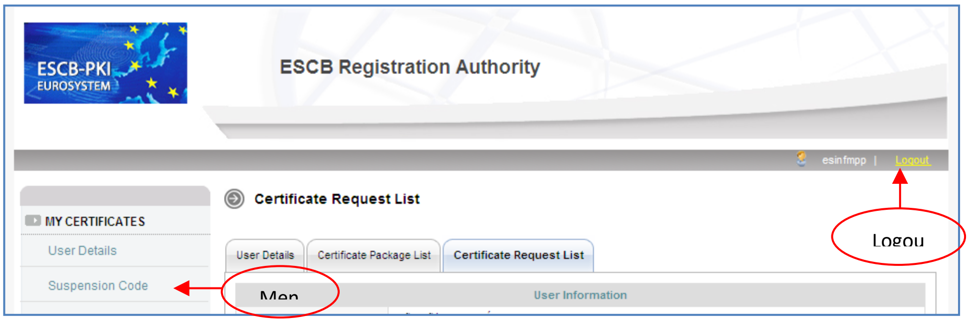
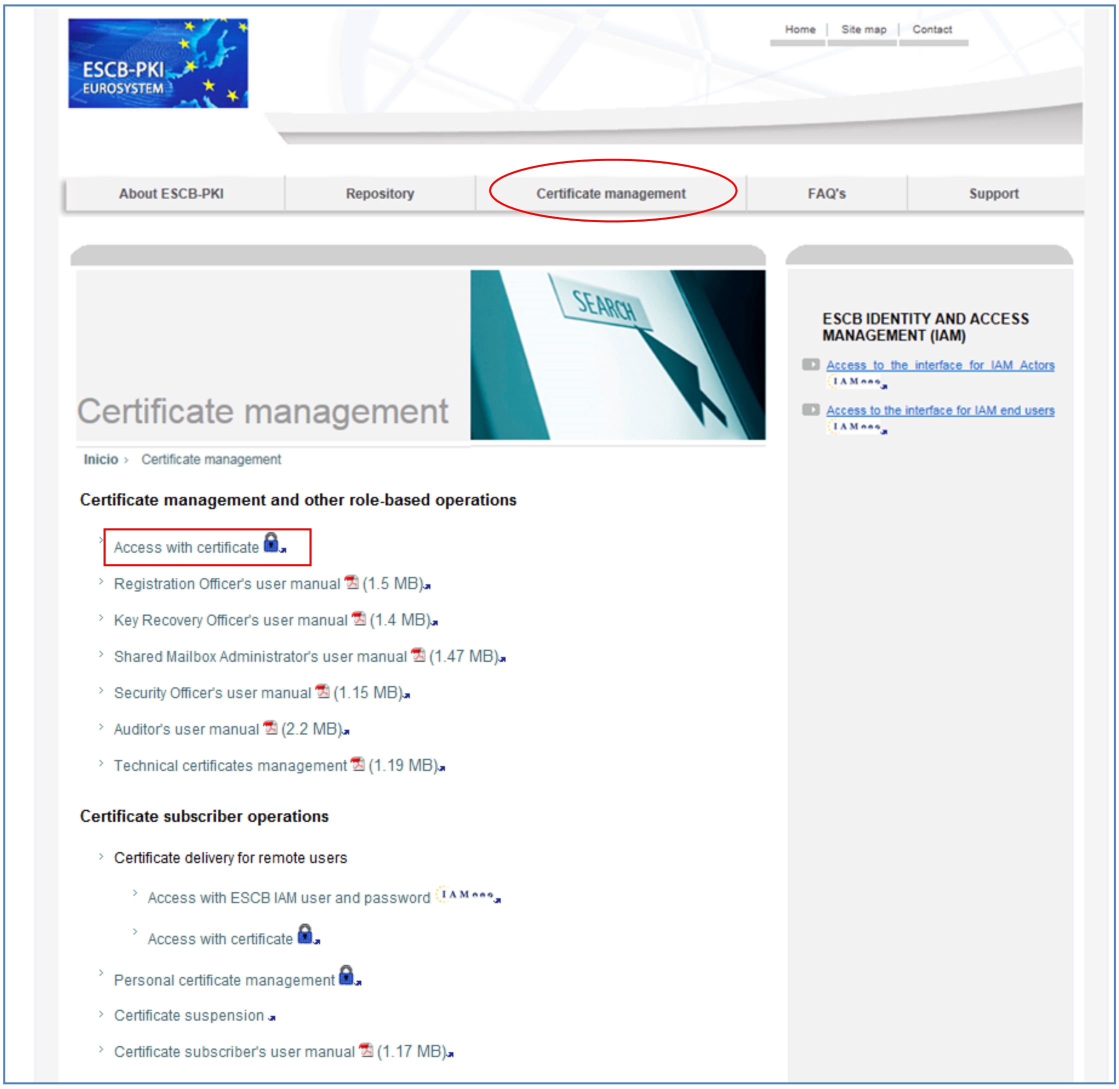


Figure 4 - General layout

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



Certificate management

Inicio › Certificate management

Certificate management and other role-based operations

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

Certificate subscriber operations

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

ESCB IDENTITY AND ACCESS MANAGEMENT (IAM)

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

Figure 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 to set some security parameters.

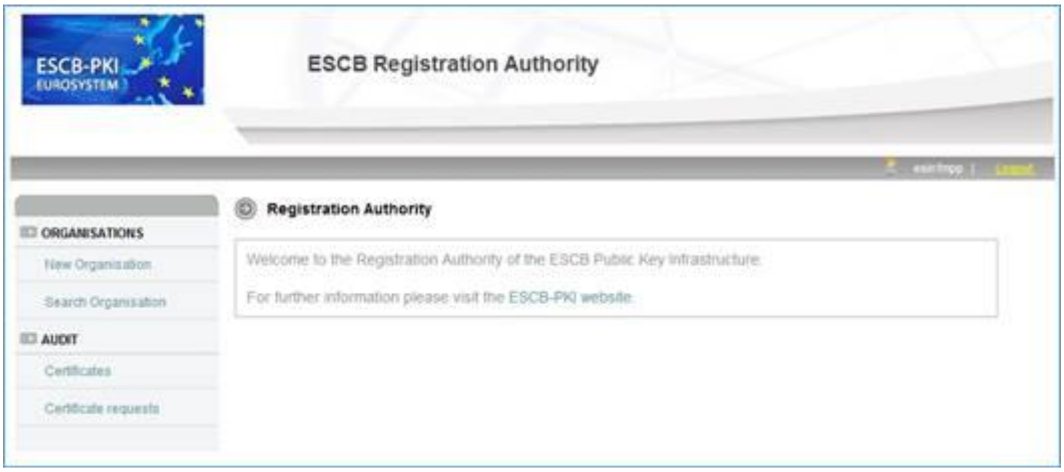
3. ESCB-PKI RA: SECURITY OFFICER TASKS

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.

If you have been granted the role of Security Officer (SO) you may:

- Register new organisations below your Central Bank. This process is required to manage certificates for external users.
- Search organisations that are below your Central Bank and modify some information for that organization. This option also enables you to define some security parameters for your Central Bank such as the key recovery options.
- Review and obtain reports of the certificates, certificate packages and certificate requests that are being managed in your organisation.

Security Officer menu



Welcome to the Registration Authority of the ESCB Public Key Infrastructure

For further information please visit the ESCB-PKI website

Figure 6 - Security Officer menu

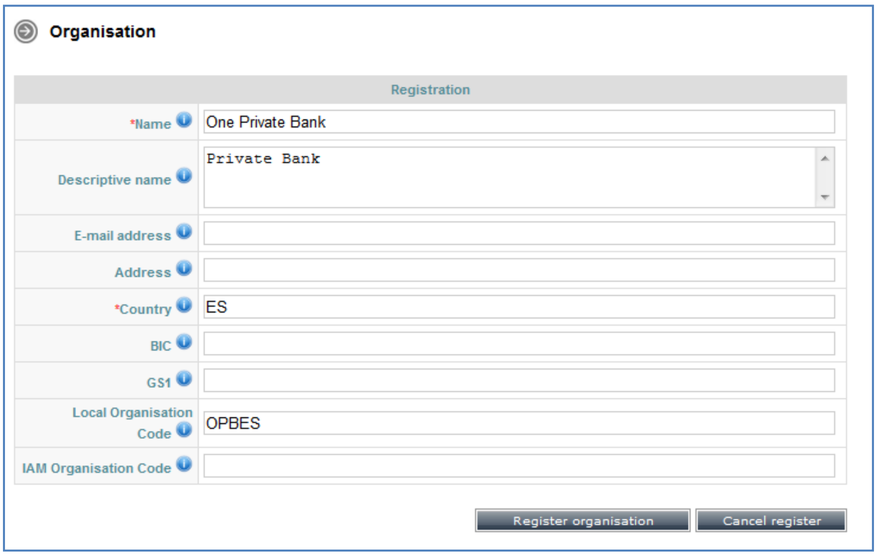
The following options will be available in the left frame menu:

- ***New Organisation*** To register external organisations below your Central Bank
- ***Search Organisation*** To modify the details of your Central Bank or the external organisations that have been registered below your Central Bank
- ***Audit > Certificates*** To show the certificates from your Central Bank
- ***Audit > Certificate Requests*** To show the certificate requests from your Central Bank

Next sections of this document will further develop these options.

3.1. REGISTER AN ORGANISATION

The ***New Organisation*** option allows you to register a new external organisation below your Central Bank. Registration Officers for External Organisations (RO4EO) from your Central Bank will be able to manage certificates for users from this organisation.



Organisation

Registration	
*Name	One Private Bank
Descriptive name	Private Bank
E-mail address	
Address	
*Country	ES
BIC	
GS1	
Local Organisation Code	OPBES
IAM Organisation Code	

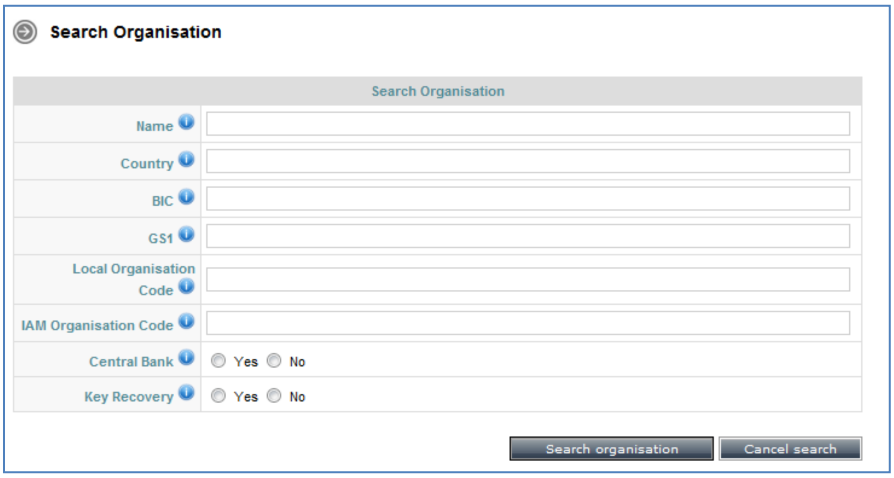
Figure 7 - New organisation

The fields that are available are the following (fields marked with an asterisk * are mandatory):

- ***Name*** Name of the external organisation
- ***Descriptive name*** Additional information to identify the external organisation. This information will be included in the Terms and Conditions document
- ***E-mail address*** E-mail address of the external organisation. This information will be included in the Terms & Conditions document
- ***Address*** Postal address of the external organisation. This information will be included in the Terms & Conditions document
- ***Country*** Country code of the external organisation (e.g. 'ES')
- ***BIC*** Business Identifier Code (aka as SWIFT code) of the external organisation
- ***GS1*** GS1 code of the external organisation
- ***Local Organisation Code*** Unique identifier used within your Central Bank to uniquely identify the external organisation
- ***IAM Organisation Code*** Unique identifier used by the IAM system to uniquely identify the external organisation

3.2. SEARCH ORGANISATION

The ***Search Organisation*** option provides an interface to search your Central Bank or an external organisation that has been registered below your CB in the ESCB-PKI system.



Search Organisation

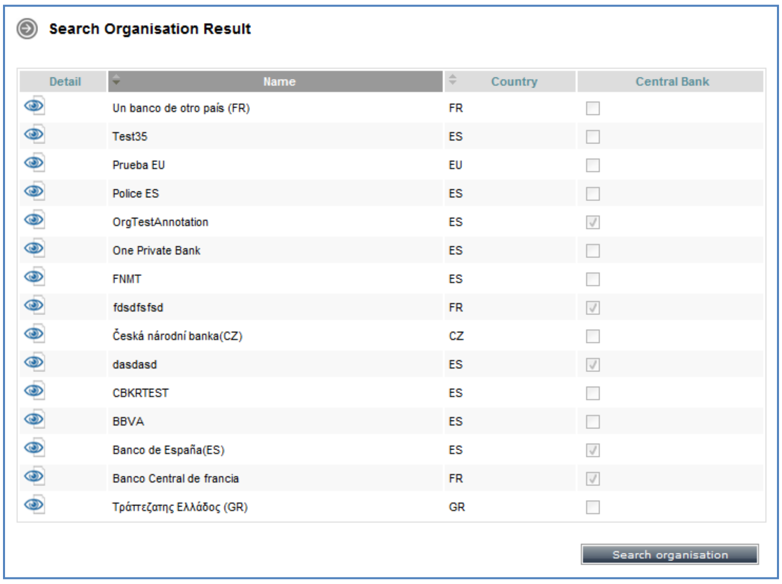
Search Organisation	
Name	
Country	
BIC	
GS1	
Local Organisation Code	
IAM Organisation Code	
Central Bank	○ Yes ○ No
Key Recovery	○ Yes ○ No

Figure 8 - Search organisation

You will be able to search by any field that identifies the organisation (see section 3.1), including the following:

- ***Central Bank*** Indicate if the organisation is a Central Bank or an external organisation
- ***Key Recovery*** Describes if the organisation has enabled the key recovery option (only possible for Central Banks)

Click the ***Search organisation*** button

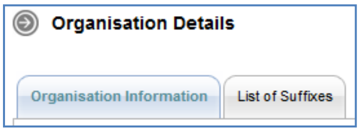


Search Organisation Result

Detail	Name	Country	Central Bank
👁	Un banco de otro país (FR)	FR	□
👁	Test35	ES	□
👁	Prueba EU	EU	□
👁	Police ES	ES	□
👁	OrgTestAnnotation	ES	☑
👁	One Private Bank	ES	□
👁	FNMT	ES	□
👁	fdsdfsfsd	FR	☑
👁	Česká národní banka(CZ)	CZ	□
👁	dasdasd	ES	☑
👁	CBKRTEST	ES	□
👁	BBVA	ES	□
👁	Banco de España(ES)	ES	☑
👁	Banco Central de francia	FR	☑
👁	Τράπεζατης Ελλάδος (GR)	GR	□

Figure 9 - Organisation list

Click the 👁 button to see the organisation details:

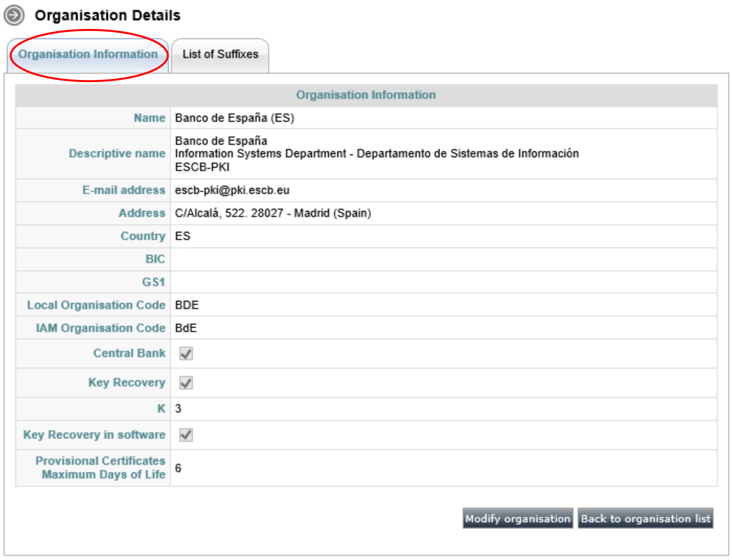


Organisation Details

Figure 10 - Organisation list

3.2.1. ORGANISATION INFORMATION

Clicking this tab displays the organisation attributes and security parameters (only in the case of Central Banks) and enables you to modify them.

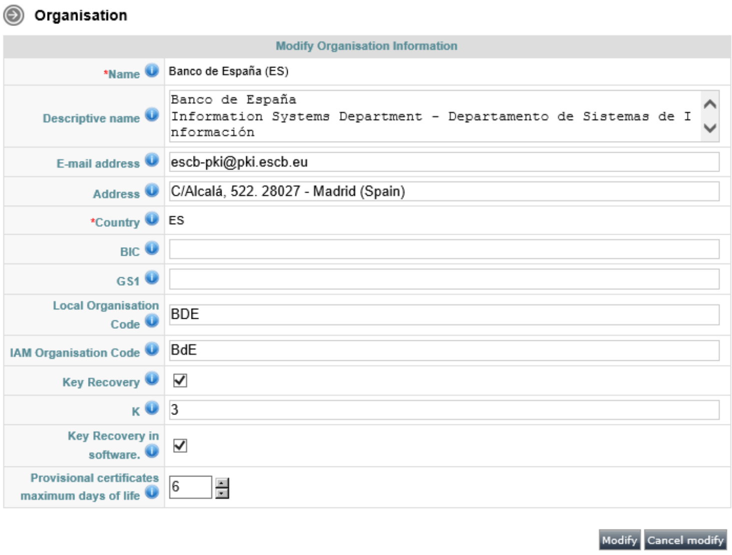


Organisation Details

Organisation Information	
Name	Banco de España (ES)
Descriptive name	Banco de España Information Systems Department - Departamento de Sistemas de Información ESCB-PKI
E-mail address	escb-pki@pki.escb.eu
Address	C/Alcalá, 522. 28027 - Madrid (Spain)
Country	ES
BIC	
GS1	
Local Organisation Code	BDE
IAM Organisation Code	BdE
Central Bank	☑
Key Recovery	☑
K	3
Key Recovery in software	☑
Provisional Certificates Maximum Days of Life	6

Figure 11 - Organisation details

Click the ***Modify organisation*** button.



Organisation

Modify Organisation Information	
*Name	Banco de España (ES)
Descriptive name	Banco de España Information Systems Department - Departamento de Sistemas de I nformación
E-mail address	escb-pki@pki.escb.eu
Address	C/Alcalá, 522. 28027 - Madrid (Spain)
*Country	ES
BIC	
GS1	
Local Organisation Code	BDE
IAM Organisation Code	BdE
Key Recovery	☑
K	3
Key Recovery in software.	☑
Provisional certificates maximum days of life	6

Figure 12 - Modify organisation details

Apart from the fields described in section 3.1, you will be able to change the following fields:

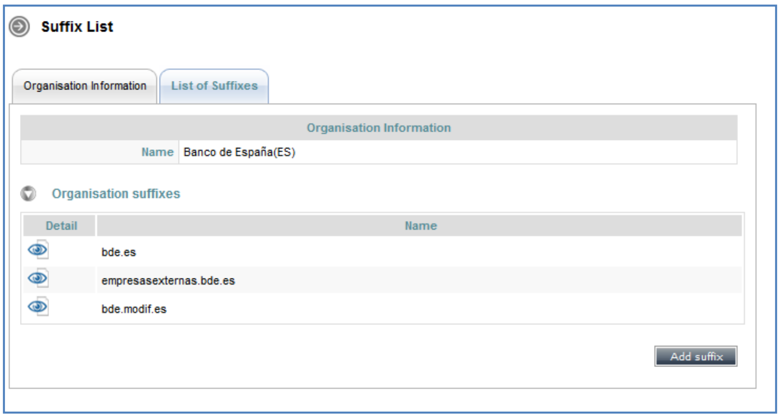
- ***Key Recovery*** Indicates if the organisation will use the key recovery feature (only possible for Central Banks).
- ***K*** In case that the Key Recovery feature has been enabled, this field indicates the number of Key Recovery Officers (KRO) necessary to recover an encryption private key without the participation of the certificate subscriber. The minimum value is 2.
- ***Key Recovery in software*** Indicates if the organisation will use the key recovery in software (Key Recovery Officers would be able to recover an encryption

certificate in a PKCS#12 file) feature (only possible if Key Recovery is enabled).

- ***Provisional certificates maximum days of life*** This field establishes the maximum days of life that a Registration Officer can set for a provisional certificate in the moment of issuance.

3.2.2. LIST OF SUFFIXES

This option is only available for Central Banks. Clicking this tab displays the list of Windows suffixes that are available at the organisation and enables you to modify them. Windows suffixes are used to define the User Principal Name (UPN) attribute included in the authentication certificate of the advanced certificate package. The UPN is equivalent to *UserId@Suffix* and it is required to enable the Windows smartcard logon feature.



Suffix List

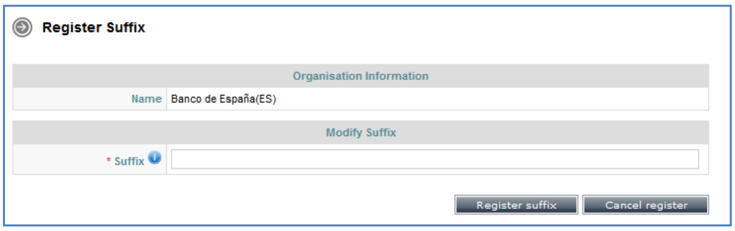
Organisation Information	
Name	Banco de España(ES)

Organisation suffixes

Detail	Name
👁	bde.es
👁	empresasexternas.bde.es
👁	bde.modif.es

Figure 13 - List of suffixes

Click the ***Add suffix*** button to register a new suffix for the organisation



Register Suffix

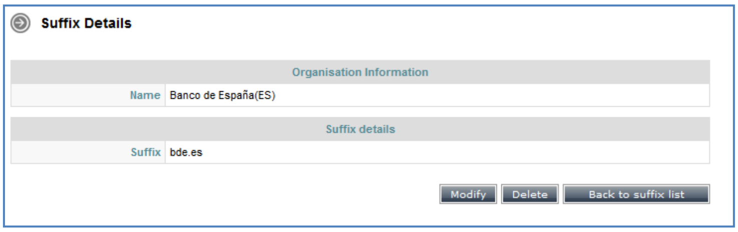
Organisation Information	
Name	Banco de España(ES)

Modify Suffix	
* Suffix	

Figure 14 - Register suffix

You can add as many suffixes as required. Take into account that the first suffix from the list will be used as default for all the users from the organisation. Nevertheless, an ESCB-PKI Local Identity Administrator will be able to assign a particular user a different suffix from the list.

Clicking the 👁 button of the list of suffixes enables you to see the suffix details



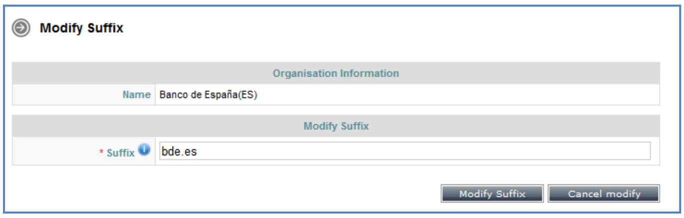
Suffix Details

Organisation Information	
Name	Banco de España(ES)

Suffix details	
Suffix	bde.es

Figure 15 - Suffix details

The ***Modify*** button enables you to modify the suffix



Modify Suffix

Organisation Information

Name	Banco de España(ES)

Modify Suffix

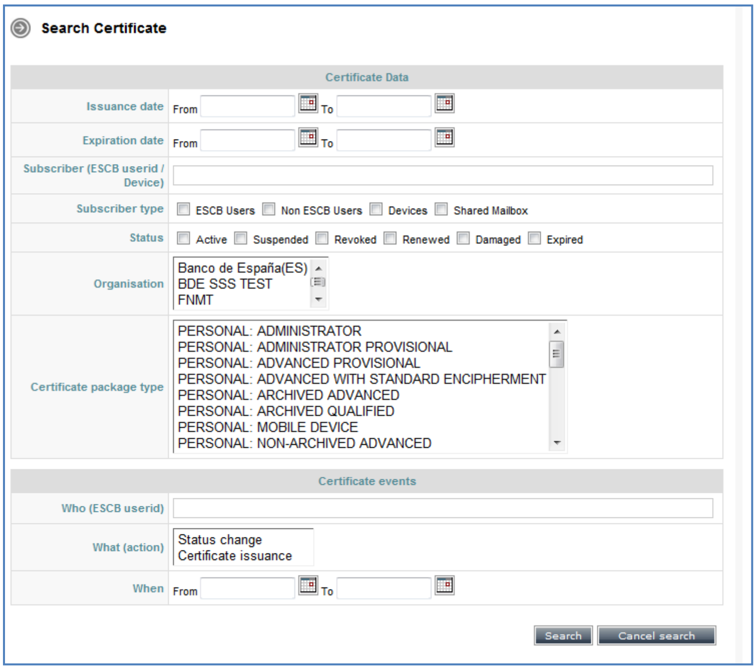
* Suffix	bde.es

Figure 16 - Modify suffix

The ***Delete*** button enables you to delete the suffix.

3.3. CERTIFICATES AUDIT

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



Search Certificate

Certificate Data

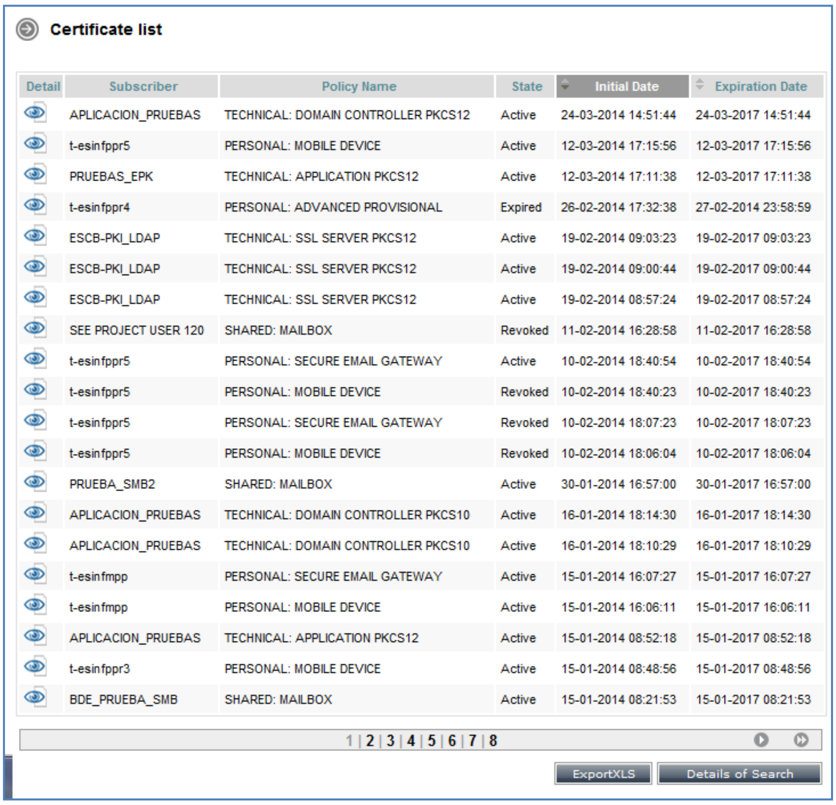
Issuance date	From ______ To ______
Expiration date	From ______ To ______
Subscriber (ESCB userid / Device)	
Subscriber type	□ ESCB Users □ Non ESCB Users □ Devices □ Shared Mailbox
Status	□ Active □ Suspended □ Revoked □ Renewed □ Damaged □ Expired
Organisation	Banco de España(ES) BDE SSS TEST FNMT
Certificate package type	PERSONAL: ADMINISTRATOR PERSONAL: ADMINISTRATOR PROVISIONAL PERSONAL: ADVANCED PROVISIONAL PERSONAL: ADVANCED WITH STANDARD ENCIPHERMENT PERSONAL: ARCHIVED ADVANCED PERSONAL: ARCHIVED QUALIFIED PERSONAL: MOBILE DEVICE PERSONAL: NON-ARCHIVED ADVANCED

Certificate events

Who (ESCB userid)	
What (action)	Status change Certificate issuance
When	From ______ To ______

Figure 17 - Search certificates

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



Certificate list

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-esinfppr5	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-esinfppr4	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-esinfppr5	PERSONAL: SECURE EMAIL GATEWAY	Active	10-02-2014 18:40:54	10-02-2017 18:40:54
👁	t-esinfppr5	PERSONAL: MOBILE DEVICE	Revoked	10-02-2014 18:40:23	10-02-2017 18:40:23
👁	t-esinfppr5	PERSONAL: SECURE EMAIL GATEWAY	Revoked	10-02-2014 18:07:23	10-02-2017 18:07:23
👁	t-esinfppr5	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-esinfppr3	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

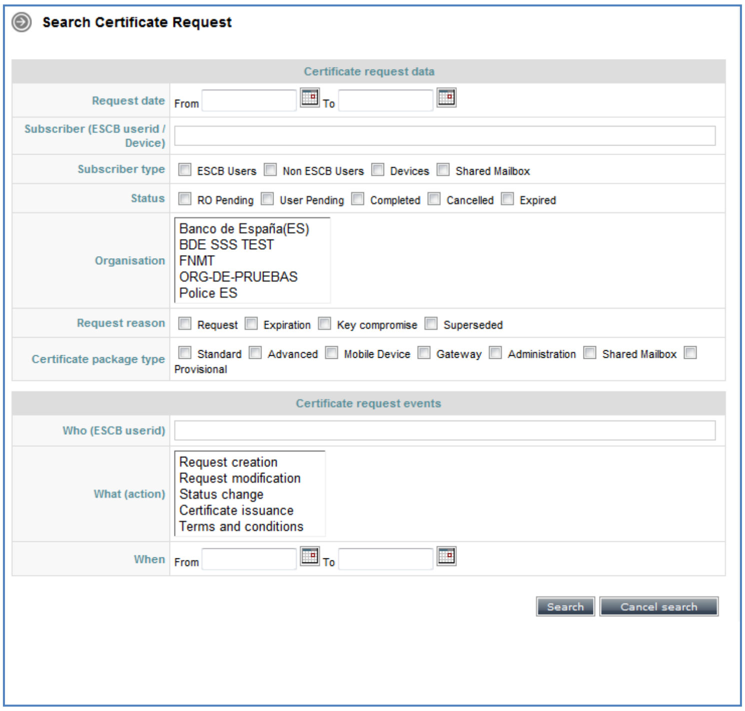
Figure 18 - Certificates list

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.

3.4. CERTIFICATE REQUESTS AUDIT

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

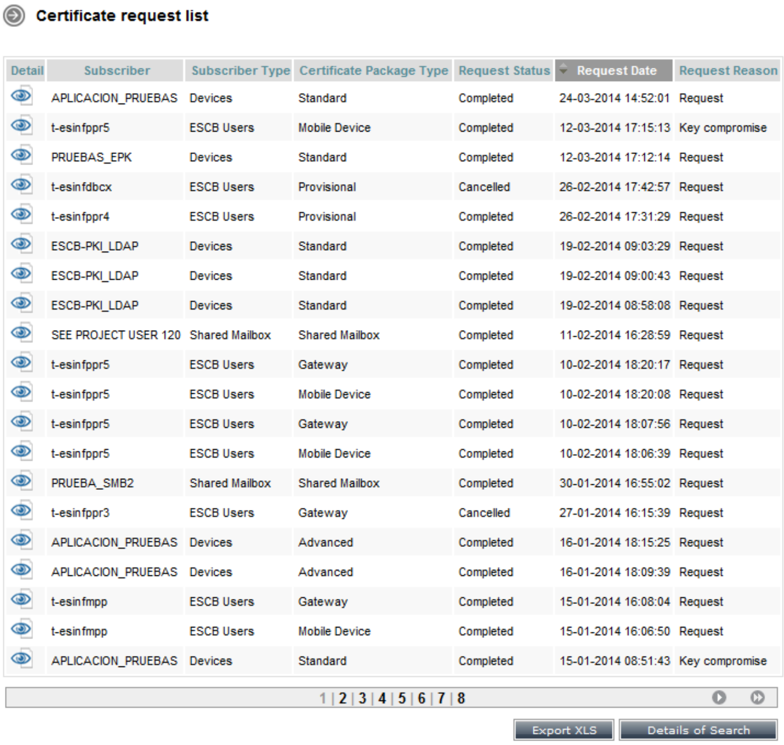


Search Certificate Request

Certificate request data	
Request date	From ____ To ____
Subscriber (ESCB userid / Device)	____
Subscriber type	□ ESCB Users □ Non ESCB Users □ Devices □ Shared Mailbox
Status	□ RO Pending □ User Pending □ Completed □ Cancelled □ Expired
Organisation	Banco de España(ES) BDE SSS TEST FNMT ORG-DE-PRUEBAS Police ES
Request reason	□ Request □ Expiration □ Key compromise □ Superseded
Certificate package type	□ Standard □ Advanced □ Mobile Device □ Gateway □ Administration □ Shared Mailbox □ Provisional
Certificate request events	
Who (ESCB userid)	____
What (action)	Request creation Request modification Status change Certificate issuance Terms and conditions
When	From ____ To ____

Figure 19 - 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

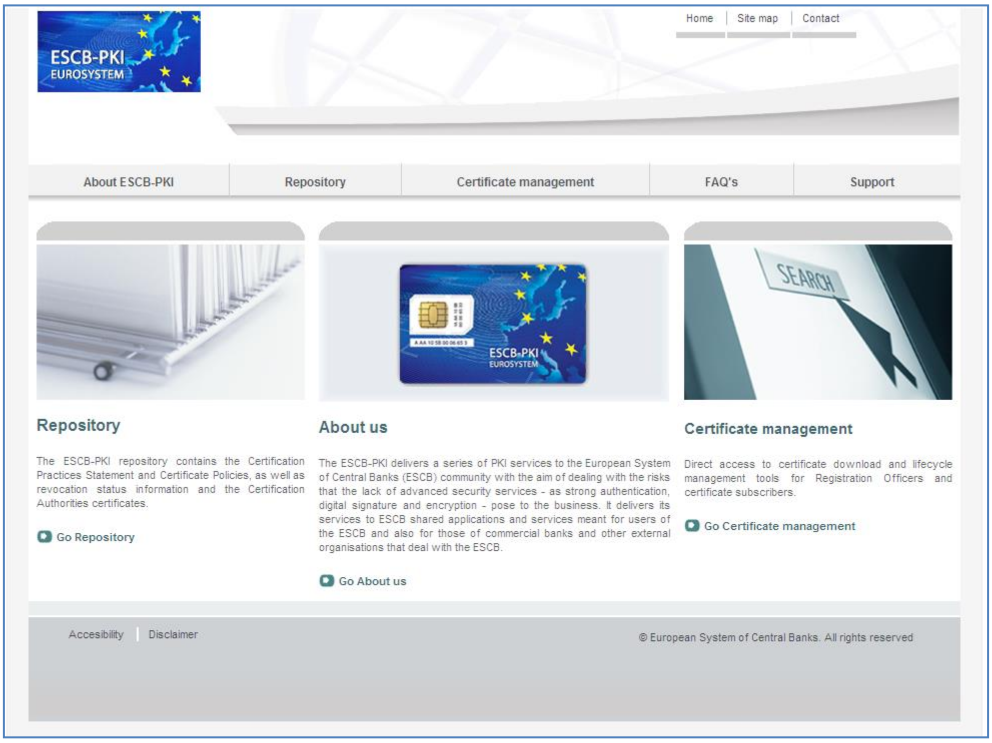
Figure 20 - Certificate requests list

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.

4. MORE INFORMATION ABOUT ESCB-PKI

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



Repository

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

About us

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

Certificate management

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

© European System of Central Banks. All rights reserved

Figure 21 - 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.