

ECB - Restricted

TABL	E O	FΟ	ON.	TEN	ITS
17.00					

GI	LOSSAI	RY A	ND ACRONYMS	6
1.	Intro	oducti	on	7
	1.1.	The E	ESCB-PKI Website	7
2.	The	ESCE	3-PKI Registration Authority application	8
	2.1.	Syste	em requirements	8
	2.2.	Layo	ut	8
	2.3.	Acce	SS	10
3.	ESC	B-PK	I RA: auditor tasks	11
	3.1.	Searc	ch users	12
	3.1.2	L.	User details	14
	3.1.2	2.	Certificate package list	15
	3.1.3	3.	Certificate request list	17
	3.1.4	1.	User history	19
	3.2.	Searc	ch shared mailboxes	20
	3.2.2	L.	Shared mailbox details	22
	3.2.2	2.	Certificate package list	23
	3.2.3	3.	Certificate request list	24
	3.2.4	1.	Shared mailbox history	26
	3.3.	Searc	ch devices	27
	3.3.2	L.	Device details	28
	3.3.2	2.	Device certificate requests	29
	3.3.3	3.	Device certificates	30
	3.3.4	1.	Device profiles	31
	3.3.4	1.1.	Profile details	31
	3.3.4	1.2.	Profile certificate requests	31
	3.3.4	1.3.	Profile certificates	32
	3.4.	Certi	ficates	34
	3.5.	Certi	ficate requests	36
	3.6.	Even	ts	38
4.	Mor	e info	rmation 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	
СВ	ESCB Central Bank (ECB or NCB)	
СР	Certification Policy	
CPS	Certification Practice Statement	
CRL	Certificate Revocation List	
ECB	European Central Bank	
ESCR	European System of Central Banks, including the ECB and the NCBs of all States	
ESCB	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.

About ESCB-PKI	Descriptions Constitution of a state of a state of a state	54.01-	C
	Repository Certificate management	FAQ's	Support
		SE	ARCU
			- unch
1 and 1	AAA 10 58 00 06 65 7 📩 🔶 😽		
-	ESCB-PKI EUROSYSTEM		
0			
			la la
Repository	Aboutus		
copository	Aboutus	Certificate mana	agement
(opository	About us	Certificate mana	agement
he ESCB-PKI repository contains the Certificate Policies as y	Cation The ESCB-PKI delivers a series of PKI services to the European System	Direct access to cert	agement
he ESCB-PKI repository contains the Certificate Policies, as v actices Statement and Certificate Policies, as v avocation status information and the Certifi	ADULT US cation The ESCB-PKI delivers a series of PKI services to the European System refl as of Central Banks (ESCB) community with the aim of dealing with the risks cation that the lack of advanced security services - as strong authentication.	Certificate mana Direct access to cer management tools fi certificate subscribers.	agement tificate download and lifecycl or Registration Officers an
he ESCB-PKI repository contains the Certif ractices Statement and Certificate Policies, as v vocation status information and the Certif uthorities certificates.	cation The ESCB-PKI delivers a series of PKI services to the European System vel as of Central Banks (ESCB) community with the aim of dealing with the risks cation that the lack of advanced security services - as strong authentication, digital signature and encryption - pose to the business. It delivers its	Certificate mana Direct access to cert management tools fi certificate subscribers.	agement tificate download and lifecycl or Registration Officers an
he ESCB-PKI repository contains the Certif ractices Statement and Certificate Policies, as v vocation status information and the Certif uthorities certificates.	ADULT US costion The ESCE-PkI delivers a series of PKI services to the European System vertices as of Central Banks (ESCB) community with the aim of dealing with the risks costion that the lack of advanced security services - as strong authentication, digital signature and encryption - pose to the business. It delivers is services to ESCB shared applications and services meant for users of the ESCB and also for those of commercial banks and other external	Certificate mana Direct access to cert management tools fi certificate subscribers. Go Certificate ma	agement tificate download and lifecycl or Registration Officers an anagement
he ESCB-PKI repository contains the Certif ractices Statement and Certificate Policies, as a vocation status information and the Certif uthorities certificates. Go Repository	ADULT US cation The ESCB-Pki delivers a series of PKI services to the European System verteals of Central Banks (ESCB) community with the aim of dealing with the risks cation 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 ESCE.	Certificate mana Direct access to cert management tools fi certificate subscribers. Go Certificate ma	agement tificate download and lifecycl or Registration Officers an anagement
he ESCB-PKI repository contains the Certif ractices Statement and Certificate Policies, as vocation status information and the Certif uthorities certificates. Go Repository	About us cation The ESCB-PKI delivers a series of PKI services to the European System vel as of Central Banks (ESCB) community with the aim of dealing with the risks cation that the lack of advanced security services - as strong authentication, digital signature and encryption - pose to the business. It delivers fis 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 mana Direct access to cert management tools fi certificate subscribers. Go Certificate ma	agement tificate download and lifecycl or Registration Officers an anagement
 ESCB-PKI repository contains the Certificaties Statement and Certificate Policies, as vocation status information and the Certification and the Certification of the	About us cation The ESCB-PKI delivers a series of PKI services to the European System vel as of Central Banks (ESCB) community with the aim of dealing with the risks cation 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. C Go About us	Certificate mana Direct access to cert management tools fi certificate subscribers. Go Certificate ma	agement tificate download and lifecyc or Registration Officers ar anagement

Figure 1 - ESCB-PKI Website

To access to the ESCB-PKI services, open your web browser and type the following URL address, <u>https://pki.escb.eu/</u>. 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
- <u>Native application required to manage certificates in a smart card.</u>
- One of the following <u>web extensions</u> of your choice, according to your browser preferences:
 - o <u>Mozilla Firefox ESCB-PKI Certificate Enrollment extension</u>.
 - o <u>Chrome and Edge ESCB-PKI Certificate Enrollment extension</u>.

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

ECB - Restricted

ESCB-PKI	ESCB Registration Authority	
		ACCEPTANCE
	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

ESCB-PKI EUROSYSTEM	ESCB Registration Authority	
MY CERTIFICATES	© Certificate Request List	🧟 esinfmpp Longout
User Details Suspension Code	User Details Certificate Package List Certificate Request List Mon User Information	Logou

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
 - o 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

ESCB-PKI	ESCB Registration Authority		Ċ
		💈 esinfmpp	Logout
(Registration Authority		
AUDIT			
Users	Welcome to the Registration Authority of the ESCB Public Key Infrastructure.		
Shared mailboxes	For further information please visit the ESCB-PKI website.		
Devices			
Certificates			
Certificate requests			
Events			

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.

	Personal Data
First Name 🔍	
Middle name 🔍	
First surname 🔍	
Second surname 🔍	
National Identity Number 🔍	
Birth Date 🔍	
Birth Place 🔍	
	ESCB Data
Escb User ID 🔍	
Email address 🔍	
Employee Number 🔍	
Domestic User ID 🔍	
Organisation Select 🔍	Select organisation 💌
Suffix Select 🤍	Select suffix

Figure 7 - Certificates management. Search user option

Press the *Search user* button

Detail	🗢 First Name	Organisation	Email Address	ESCB UID	National Identity Numbe
٩	APELLIDOS TRES, Usuariotres	Banco de España(ES)	usuario.tres@bde.es	t-esinfppr3	
٩	APELLIDO APELLIDO, Otro	Banco de España(ES)	otro.apellico@bde.es	t-esinfppr4	
۲	APELLIDOS REPES, Menganita	Banco de España(ES)	e-mal@empresas-externas.bde.es	t-esqlorcgx	
٩	ESPANOL DOS, Fulanito Dos	Banco de España(ES)	fulanito.dos@bde.es	t-esinfppr2	
٢	ESPANOL ONE, Fulanito	Banco de España(ES)	fulanito.uno@bde.es	t-esinfppr1	
٢	Integración lam, Pruebas	Banco de España(ES)	qlorcgx@correo.interno	t-espruebas	12345678
٢	LASTFIVE, Namecinco	Banco de España(ES)	user5@empresas-externas.bde.es	t-esinfppr5	
٢	JJJJJ LOPEZ, Menganito	Banco de España(ES)	menganito@bde.es	t-esmengano	
٢	ESPAÑOL ESPAÑOL, Juan	Banco de España(ES)	juan.espanol@bde.es	t-esespanol	
٢	ESPAÑOLA ESPAÑOLA, JUANA	Banco de España(ES)	juana.espnola@bde.es	t-esjuanita	
٢	REPETIDO OTRO, NOMBRE	Banco de España(ES)	nombre.otro@bde.es	t-esotrousu	
٢	APELLIDO DOS, Roberto	Banco de España(ES)	roberto.dos@bde.es	t-esroberto	1111111111
٩	ESPAÑOL ESPAÑOLA, Zutano	Banco de España(ES)	zutano@empresas-externas.bde.es	t-eszutano	
0	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

	liser Details
Perconal det:	User Details Certificate Package List Certificate Request List User History Activity information
	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.

er Details Certificate Pa	Ickage List Certificate Request List User History
	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	qlorcgx@correo.interno
Employee Number	1234
Domestic UID	

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

User Deta	ils Certificate Package Lis Certificate	e Request List User Histor	y		
		User Information			
	Name LASTFIVE, Namecinco				
🗊 Ce	rtificate Package List				
Detail	Policy Name	Cryptographic Device	State	Initial Date	Expiration Date
۲	ADVANCED_ARCHIVED_ESCB_POLICY	42430F5172A36495	ACTIVE	09-02-2012	09-02-2015

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:

Certificate Package Detail	Certificate Package H	istory		
	Ce	ertificate Package Information		
Policy	PERSONAL: ADVANCE	D WITH STANDARD ENCIPHERMENT		
Token Serial Number	42430F5173F76495			
Request Date	11/02/2014			
Expiration Date	11/02/2017			
Certificate Package Status	ACTIVE			
Certificate List		Downlo	ad certificate	>
Serial Num	iber	Template Name	Download	Recover Keys
7ba0f10e8dbc6dcc52fa0cf66	675a87d	ESCB NONSSCD SIGNATURE		1,
6cabb7d137446b0b52fa0cf58	52d3a0c	ESCB AUTHENTICATION	•	6
2f7fc00626f1ccd52fa0cf4ac3	aa92a	ESCB STANDARD ENCIPHERMENT	B i	l)

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.

rtificate Packa	ge Detail Certificate Package	History			
	-				
Certificat	e Package History				
Certificat	e Package History	Priority	Level	Action	Description
) Certificat	Package History Date Date	Priority	Level	Action	Description
User User esinfevg	e Package History	Priority	Level HIGH	Action RESULT	Description Suspend user certifi
Certificat User esinfevg esinfevg	Package History Date 09-02-2012 16:55:58 09-02-2012 16:56:13	Priority NFO NFO	Level HIGH HIGH	Action RESULT REQUEST	Description Suspend user certifi Revoke user certific

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

ser Det	ails Certificate Package List	Certificate Request L	ist ser History		
		User li	nformation		
	Name ESPANOL O	NE, Fulanito			
Ce	rtificate Request List				
Detail	Certificate Package Type	Request Status	♦ Request Date	IssuanceType	Operation Type
٩	STANDARD	CANCELLED	13-02-2012 15:45:28	PRESENTIAL	REQUEST
٩	ADVANCED	COMPLETED	10-02-2012 08:30:26	PRESENTIAL	KEYCOMPROMISE
۲	ADVANCED	COMPLETED	09-02-2012 12:52:49	PRESENTIAL	KEYCOMPROMISE
۲	STANDARD	COMPLETED	08-02-2012 15:11:14	PRESENTIAL	KEYCOMPROMISE
۲	ADVANCED	COMPLETED	08-02-2012 14:58:19	PRESENTIAL	KEYCOMPROMISE
۲	ADVANCED	COMPLETED	07-02-2012 17:03:48	PRESENTIAL	KEYCOMPROMISE
۲	ADVANCED	COMPLETED	07-02-2012 16:55:20	PRESENTIAL	KEYCOMPROMISE
٢	ADVANCED	COMPLETED	07-02-2012 15:59:41	REMOTE	KEYCOMPROMISE
٢	STANDARD	COMPLETED	07-02-2012 15:56:10	PRESENTIAL	KEYCOMPROMISE
0	STANDARD	COMPLETED	07-02-2012 15:55:10	PRESENTIAL	KEYCOMPROMISE

Figure 13 - Certificate requests list

Clicking the *a* button the details of the certificate request are displayed

Request detail Request h	istory
	User Information
Name	APELLIDOS TRES, Usuariotres
	Requestor details
Requestor name	apellido apellido, nombre
Requestor mail	e-mail@correo.interno
	Certificate Package Request Detail
Certificate Package Type	STANDARD
Request Status	RO PENDING
Issuance Type	PRESENTIAL
Operation Type	KEYCOMPROMISE
Request Date	13/02/2012

Figure 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.

equest detail	Request history				
Reduest	history				
V Request	history	Priority	Level	Action	Description
User User t-esinfmpp	Date 01-02-2012 10:00:51	Priority 1 NFO	Level	Action REQUEST	Description Enable remote downlo
User User t-esinfmpp t-esinfmpp	Date 01-02-2012 10:00:51 01-02-2012 10:00:46	Priority 1 INFO 6 INFO	Level MEDIUM MEDIUM	Action REQUEST RESULT	Description Enable remote downlo Load information of
User User t-esin fmpp t-esin fmpp t-esin fmpp	history	Priority 1 INFO 6 INFO 5 INFO	Level MEDIUM MEDIUM MEDIUM	Action REQUEST RESULT REQUEST	Description Enable remote downlo Load information of Load information of

Figure 15 - Request activity

3.1.4. USER HISTORY

Displays all the activity related to the user.

er Details	Certificate Package List	Certificate Request List	User His	tory	
) User Hi	story				
User		Priority	Level	Action	Description
-esinfmpp	03-02-2012 15:50:57	INFO	MEDIUM	RESULT	Register certificate
-esinfmpp	01-02-2012 10:00:51	INFO	MEDIUM	RESULT	Enable remote downlo
-esinfmpp	01-02-2012 10:00:51	INFO	MEDIUM	REQUEST	Enable remote downlo
-esinfmpp	01-02-2012 10:00:46	INFO	MEDIUM	RESULT	Load information of
-esinfmpp	01-02-2012 10:00:46	INFO	MEDIUM	REQUEST	Load information of
am	01-02-2012 10:00:16	INFO	MEDIUM	RESULT	User certificate pac
-esinfmpp	01-02-2012 08:16:21	INFO	HIGH	RESULT	Issue ADVANCED certi
-esinfmpp	01-02-2012 08:16:13	INFO	HIGH	REQUEST	Issue ADVANCED certi
-esinfmpp	01-02-2012 08:14:12	INFO	MEDIUM	RESULT	Begin ADVANCED certi
-esinfmpp	01-02-2012 08:14:12	INFO	MEDIUM	REQUEST	Begin ADVANCED certi
-esinfmpp	01-02-2012 08:14:09	INFO	MEDIUM	RESULT	Load information of
-esinfmpp	01-02-2012 08:14:08	INFO	MEDIUM	REQUEST	Load information of
-esinfmpp	01-02-2012 08:14:02	INFO	MEDIUM	RESULT	Register certificate
-esinfmpp	01-02-2012 08:13:13	INFO	MEDIUM	RESULT	Cancel certificate p
esinfmon	01-02-2012 08:13:13	INFO	MEDIUM	REQUEST	Cancel certificate p

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.

	Shared Mailbox
Unique Identifier 🔍	
Display Name 🔍	
Description 🔍	
Email Address 🔍	
	Custodian of the Shared Mailbox
Escb User ID 🔍	
Name 🔍	
Middle Name 🔍	
Surnames 🔍	
Email Address 🔍	
National Identity Number 🔍	
Employee Number 🔍	
Birth Date 🔍	
Birth Place 🕕	

Figure 17 - Search shared mailbox

Press the *Search shared mailbox* button

)etail	Display Name	Email Address	Name of custodian	Email of custodian
۲	BDE_PRUEBA_SMB	pkibde@bde.es	PENA PINON, Miguel	miguelangel.pena@bde.es
۲	PRUEBA_SMB2	escb-pki@bde.es	PENA PINON, Miguel	miguelangel.pena@bde.es
۲	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

Shared Mailbox Details	
Shared Mailbox Detail Certificate Package List Certificate	te Request List Shared Mailbox History
Shared mailhox detail Review certificates	Review requests Activity informat

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 Detail C	ertificate 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-esin fmpp
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

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

ared Mailb	ox Detail Cert	ificate Packag	ge List Certificate Request L	ist Shared Mailbox His	tory	
			Shared Mailbo	x		
U	nique Identifier	t-esbdeprueb	asmb			
	Display Name	BDE_PRUEBA	_SMB			
	Description	PRUEBA SHA	RED MAILBOX			
	Email Address	pkibde@bde.e	es			
			Custodian of the Share	d Mailbox		
	Name	PENA PINON,	Miguel			
	Email Address	miguelangel.p	ena@bde.es			
Share	d Mailbox Certif	icate Packag	je			
Detail	Request	Status	Policy Name	🔶 🛛 Initial Date	÷	Expiration Date
	ACTIVE		SHARED: MAILBOX	15/01/2014	15/01	1/2017

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

Shared Mailbox D	etail Cert	ficate Package List	Certificate	Request List Shared I	failbox History	
			Sha	ared Mailbox		
Uniqu	e Identifier	estestin fmpp1				
Di	splay Name	INF_ESCB-PKI				
	Description	SHARED MAILBOX	FOR THE ESCE	3-PKI PROJECT		
Em	ail Address	escb-pki@pki.escb	.eu			
			Custodian o	f the Shared Mailbox		
	Name	Peña Piñón, Miguel	Ángel			
Em	ail Address	infmpp@correo.inte	erno			
Certificat	e Request L	st				
Detail	Re	quest Status	÷	Request Date	Operation Type	
3	COMPLETED		24-12-20	013 08:41:33	REQUEST	

Figure 22 - Shared mailbox certificate requests list

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

Certificate Request Detail	Certificate Request History
	Shared Mailbox
Unique Identifier	estestin fmpp1
Display Name	INF_ESCB-PKI
Description	SHARED MAILBOX FOR THE ESCB-PKI PROJECT
Email Address	escb-pki@pki.escb.eu
	Custodian of the Shared Mailbox
Name	Peña Piñón, Miguel Ángel
Email Address	in fmpp@correo.interno
	Person who creates the request
Requestor Name	Vidal González, Esther
Requestor Email	infevg@correo.interno
	Certificate Package Request Detail
Request Number	20140413-000000000000000000214
Certificate Package Type	SHARED: MAILBOX
Request Status	RO PENDING
Reason	SUPERSEDED
Request Date	13/04/2014



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.

hared Mailbox	Detail Certificate Package List	Certificate Request List Shared Mailbox History	
History I	ist		
Who	⇔ When	What	Result
-esinfmpp	15-01-2014 08:22:58	Download issued certificate.	INFO
-esin fmpp	15-01-2014 08:22:58	Download issued certificate.	INFO
-esinfmpp	15-01-2014 08:22:56	Issue certificate package.	INFO
esin fmpp	15-01-2014 08:22:56	Issue certificate package.	INFO
-esinfmpp	15-01-2014 08:22:05	Generation of the terms and conditions document.	INFO
-esinfevg	14-01-2014 19:33:55	Approve shared mailbox certificate request.	INFO
-esinfmpp	14-01-2014 17:10:43	Generation of the terms and conditions document.	INFO
-esinfmpp	14-01-2014 17:10:39	Register new shared mailbox certificate request.	INFO
-esinfmpp	14-01-2014 17:10:12	Register new shared mailbox.	INFO

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.

Search device	
	Device data
Name	
Description	
Organisation	Select organisation
	Contact person data
Name	
Surname	
E-mail address(es)	
Phone number	
	Search device Cancel search

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:

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

Figure 26 - List of devices

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

	Device detail	
	Device detail Device certificate requests Device certificates	
Devic	re detail Review requests Review r	ertificate

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

	ice certif	icate requests	Device certificates	
			Device Information	
	Name	deviceTest2		
Desc	ription	description		
Organi	isation	Banco de Españ	a(ES)	
			Contact person data	
	Name	Namecontact		
Surr	names	SurnameContac	t	
	Mail	contactmail@ma	il.com	
Phone n	umber	(+64) 123 45 45		
Device profiles	list		Туре	Description
Device profiles	list App	lication	Туре	Description
Device profiles Detail	App Dom	lication ain Controller	Туре	Description

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.

levice de	tail Device certif	licate requests	Device certificates	s		
			Device In	formation		
	Name	deviceTestExte	rnal			
	Description	desciption				
	Organisation	Police ES				
			Contact p	erson data		
	Name	contactName				
	Surnames	contactSurnam	e			
	Mail	qaguspx@corr	eo.interno			
	Phone number	(+34)12345678	9			
Rec	juest list					
Detail	Request	type	Request status	Operation type	👻 Request date	Device profile
٢	Generate .p12 file		CANCELLED	REQUEST	24/05/2012	Application
۲	Generate .p12 file		CANCELLED	REQUEST	24/05/2012	Application
٢	Generate .p12 file		COMPLETED	REQUEST	24/05/2012	Application
٢	Process a .csr or .p	10 file	CANCELLED	REQUEST	26/04/2012	Application
0	Generate .p12 file		COMPLETED	REQUEST	26/04/2012	Application

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.

Jevice d	etail Device certific	cate requests	Device certificates			
			Device Inform	nation		
	Name	DeviceInterno				
	Description	Device interno p	pruebas			
	Organisation	Banco de Espa	ña(ES)			
			Contact perso	on data		
	Name	Águeda				
	Surnames	Soto				
	Mail	qaguspx@corn	eo.interno			
	Phone number	91 338 63 07				
Detail	Serial	number		Expiration Date	Status	Policy
Detail	Serial 273685876d876f334f	number fe2cf3ad9fef7a3		Expiration Date 21/06/2014	Status REVOKED	Policy SSLSERVER_STANDARD
Detail () ()	Serial 273685876d876f334f 4eaecef17684e1a14f	number fe2cf3ad9fef7a3 fe2c2e651ca0e5	 Issuance date 21/06/2012 21/06/2012 	 Expiration Date 21/06/2014 21/06/2014 	Status REVOKED REVOKED	Policy SSLSERVER_STANDARD SSLSERVER_STANDARD
Detail () () () () () () () () () ()	Serial 273685876d876f334f 4eaecef17684e1a14f 5515ca0454c0e2c74	number fe2cf3ad9fef7a3 fe2c2e651ca0e5 fe2c26950ee26e	 Issuance date 21/06/2012 21/06/2012 21/06/2012 	 Expiration Date 21/06/2014 21/06/2014 21/06/2014 	Status REVOKED REVOKED REVOKED	Policy SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD
	Serial 273685876d876f334f 4eaecef17684e1a14f 5515ca0454c0e2c74 49467505effc32d64f	number le2cf3ad9fef7a3 le2c2e651ca0e5 fe2c26950ee26e e2bd6ae2a0f6d6	Issuance date 21/06/2012 21/06/2012 21/06/2012 21/06/2012 21/06/2012	 Expiration Date 21/06/2014 21/06/2014 21/06/2014 21/06/2014 	Status REVOKED REVOKED REVOKED REVOKED	Policy SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD
	Serial 273685876d876f334f 4eaecef17684e1a14f 5515ca0454c0e2c74 49467505effc32d64f 2c69a5fc0672971c4f	number fe2cf3ad9fef7a3 fe2c2e651ca0e5 fe2c26950ee26e e2bd6ae2a0f6d6 fe2bc78ed22886	Issuance date 21/06/2012 21/06/2012 21/06/2012 21/06/2012 21/06/2012 a 21/06/2012	Expiration Date 21/06/2014 21/06/2014 21/06/2014 21/06/2014 21/06/2014	Status REVOKED REVOKED REVOKED REVOKED DAMAGED	Policy SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD
	Serial 273685876d876f334f 4eaecef17684e1a14f 5515ca0454c0e2c74 49467505effc32d64f 2c69a5fc0672971c4f 5336b833cf3c40274f	number fe2cf3ad9fef7a3 fe2c2e651ca0e5 fe2c26950ee26e e2bd6ae2a0f6d6 fe2bc78ed22886 fe2bbf4f3b1d37f	 Issuance date 21/06/2012 21/06/2012 21/06/2012 21/06/2012 21/06/2012 21/06/2012 21/06/2012 	Expiration Date 21/06/2014 21/06/2014 21/06/2014 21/06/2014 21/06/2014 21/06/2014	Status REVOKED REVOKED REVOKED REVOKED REVOKED	Policy SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD
	Serial 273665576d676f334f 4eaecef17684e1a14f 5515ca0454c0e2c74 49467505effc32d64f 2c69a5fc0672971c4f 5336b833cf3c40274f 58689e93ad6cdb674	number le2cf3ad9fef7a3 le2c2e651ca0e5 fe2c26950ee26e e2bd6ae2a0f6d6 le2bc78ed22886 le2bbf4f3b1d37f fe08f336874acc	 Issuance date 21/06/2012 21/06/2012 21/06/2012 21/06/2012 21/06/2012 21/06/2012 21/06/2012 91/06/2012 	Expiration Date 21/06/2014 21/06/2014 21/06/2014 21/06/2014 21/06/2014 21/06/2014 21/06/2014	Status REVOKED REVOKED REVOKED DAMAGED REVOKED REVOKED	Policy SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD
	Serial 273685676d87613341 4eaece117684e1a141 5515ca0454c0e2c74 49467505effc32d846 2c69a5fc0672971c41 5336b833cf3c402741 58689e93ad8cdb674 668f2c595391635741	number le2cf3ad9fef7a3 le2c2e651ca0e5 fe2c26950ee26e e2bd6ae2a0f6d6 le2bc78ed22886 fe2bbf4f3b1d37f fe08f336874acc fc62d4e5b4cdc8	 ✓ Issuance date 21/06/2012 b 21/06/2012 21/06/2012 21/06/2012 21/06/2012 21/06/2012 21/06/2012 9 19/06/2012 0 30/05/2012 	Expiration Date 21/06/2014 21/06/2014 21/06/2014 21/06/2014 21/06/2014 21/06/2014 21/06/2014 19/06/2014 30/05/2014	Status REVOKED REVOKED REVOKED DAMAGED REVOKED REVOKED REVOKED	Policy SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD
Detail (a) (b) (c) (c) (c) (c) (c) (c) (c) (c	Serial 273685876d6781344 4eacce117684e1a141 5515ca0454c0e2c74 49467505effc32064f 2c69a5fc0672971c41 5336b833cf3c402741 58689e93ad6cdb674 68672c59539183574f 7817e276041697414	number le2cf3ad9fef7a3 le2c2e651ca0e5 fe2c26950ee26e e2bd6ae2a0f6d6 le2bc78ed22886 fe2bbf4f3b1d37f fe08f336874acc lc62d4e5b4cdc8 faa409e7593d24	Issuance date 21/06/2012 b 21/06/2012 r7 21/06/2012 a 19/06/2012 0 30/05/2012 r7 09/05/2012	Expiration Date 21/06/2014 21/06/2014 21/06/2014 21/06/2014 21/06/2014 21/06/2014 21/06/2014 30/05/2014 09/05/2014	Status REVOKED REVOKED REVOKED DAMAGED REVOKED REVOKED REVOKED	Policy SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD
	Serial 2738587608761334 4eaece117864e1a141 5515ca0454c0e2c74 49467505effc320841 2c69a5fc0672971c41 5336b833cf3c402741 56689e93ad6cdb874 66872c595391635741 7817e276041697414 22ad273cdd96a1034	number le2cf3ad9fef7a3 le2c2e651ca0e5 le2c2e950ee26e e2bd6ae2a0f6d6 le2bc78ed22886 le2bc78ed22886 le2bbf4f3b1d37f 1e08f336874acc le62d4e5b4cdc8 faa409e7593d24 f96b06a854fe48	 Issuance date 21/06/2012 21/06/2012 21/06/2012 21/06/2012 21/06/2012 21/06/2012 91/06/2012 19/06/2012 30/05/2012 30/05/2012 21/04/2012 	Expiration Date 21/06/2014 21/06/2014 21/06/2014 21/06/2014 21/06/2014 21/06/2014 21/06/2014 30/05/2014 30/05/2014 24/04/2014	Status REVOKED REVOKED REVOKED DAMAGED REVOKED REVOKED REVOKED REVOKED	Policy SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD SSLSERVER_STANDARD

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:

Nar	Device Information
Nar	
	Componente2
Descripti	n Componente de prueba 2
Organisati	n Banco de España(ES)
	Contact person data
Nar	Lorena
Surnam	s Cuadrado Gutiérrez
М	ail qlorcgx@correo.interno
Phone numb	er 91 338 6307
	Code Signature details
Descripti	n segunda prueba
E-mail addre	s pkibde@bde.es
Disalauras	an anguinda agusha

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.

rofile details	Profile cert	ficate requests	Profile certificates	5		
			Device In	formation		
	Name	Componente2				
	Description	Componente de p	ueba 2			
	Organisation	Banco de España	(ES)			
			Contact p	erson data		
	Name	Lorena				
Surnames Cuadrado Gutiérre			z			
	Mail	qlorcgx@correo.i	nterno			
	Phone number	91 338 6307				
			Code Signa	ture details		
	Description	segunda prueba				
	E-mail address	pkibde@bde.es				
	Display name	segunda prueba				
Reque	stlist					
Detail	Request typ	e 🗘 Requ	est status	Operation type	Request date	Device profile
ی 💿	enerate .p12 file	COMPLETE	D REC	QUEST	04/10/2012	Code Signing

Figure 32 - Device certificate requests

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

ECB - Restricted

	Device Information
Heres	Device information
Description	
Oceaniantian	I RIS IS A SAMPLE DEVICE
Organisation	Banco de Espana(ES)
	Contact person data
Name	JOHN
Surnames	SMITH
Mail	john.smith@bde.es
Phone number	+34 1233344
	Code Signature detaile
Description	THIS IS A CERTIFICATE LISER TO SIGN ACTIVEYS AND ADDI FTS
E-mail address	
Display name	DOWNLOADABLE COMPONENT
broping name	
	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	infmon@correo_interno

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.

ECB - Restricted

rofile det	ails Profile certifie	cate requests Prot	file certificates			
			Device Inform	nation		
	Name	SAMPLE_DEVICE				
	Description	THIS IS A SAMPLE DE	EVICE			
	Organisation	Banco de España(ES)			
			Contact perso	n data		
	Name	JOHN				
	Surnames	SMITH				
	Mail	john.smith@bde.es				
	Phone number	+34 1233344				
			SSL Server d	etails		
	Description	THIS IS A SSL SERVE	ER			
	E-mail address	service@bde.es				
Common name service.bde.es						
	DNS name	service.bde.es;help.b	ode.es;other.bde.es			
	IP address					
Cer	tificate list					
Detail	Serial	number	♦ Issuance date	$\stackrel{\diamond}{=}$ Expiration Date	Status	Policy
3	ae9a9fbf0c86fd8513	9f190b7c655ef	08/03/2013	08/03/2016	ACTIVE	SSLSERVER_STANDARD
3	6a93ae10a73587d51	39f101021dfeca	08/03/2013	08/03/2016	REVOKED	SSLSERVER_STANDARD
A	200507040404075	1206024-0224227	09/02/2012	09/02/2016	DAMAGED	COLCEDVED CTANDADD

Figure 34 - Device certificates

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

	Device Information
Name	SAMPLE_DEVICE
Description	THIS IS A SAMPLE DEVICE
Organisation	Banco de España(ES)
	Contact person data
Name	NHOL
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	ae9a9fbf0c86fd85139f190b7c655ef
Issuance date	08/03/2013
Expiration date	08/03/2016
Status	ACTIVE
Policy	SSLSERVER_STANDARD

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.

	Certificate Data
Issuance date	From
Expiration date	From To
Ibscriber (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) A BDE SSS TEST (EI) FNMT T
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

Figure 36 - Search certificates

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

)) C	ertificate list				
Detail	Subscriber	Policy Name	State	Initial Date	Expiration Date
3	APLICACION_PRUEBAS	TECHNICAL: DOMAIN CONTROLLER PKCS12	Active	24-03-2014 14:51:44	24-03-2017 14:51:4
۲	t-esinfppr5	PERSONAL: MOBILE DEVICE	Active	12-03-2014 17:15:56	12-03-2017 17:15:
3	PRUEBAS_EPK	TECHNICAL: APPLICATION PKCS12	Active	12-03-2014 17:11:38	12-03-2017 17:11:
3	t-esinfppr4	PERSONAL: ADVANCED PROVISIONAL	Expired	26-02-2014 17:32:38	27-02-2014 23:58:
3	ESCB-PKI_LDAP	TECHNICAL: SSL SERVER PKCS12	Active	19-02-2014 09:03:23	19-02-2017 09:03:
۲	ESCB-PKI_LDAP	TECHNICAL: SSL SERVER PKCS12	Active	19-02-2014 09:00:44	19-02-2017 09:00:
۲	ESCB-PKI_LDAP	TECHNICAL: SSL SERVER PKCS12	Active	19-02-2014 08:57:24	19-02-2017 08:57:
۲	SEE PROJECT USER 120	SHARED: MAILBOX	Revoked	11-02-2014 16:28:58	11-02-2017 16:28
3	t-esinfppr5	PERSONAL: SECURE EMAIL GATEWAY	Active	10-02-2014 18:40:54	10-02-2017 18:40:
۲	t-esinfppr5	PERSONAL: MOBILE DEVICE	Revoked	10-02-2014 18:40:23	10-02-2017 18:40:
3	t-esinfppr5	PERSONAL: SECURE EMAIL GATEWAY	Revoked	10-02-2014 18:07:23	10-02-2017 18:07:
Ð	t-esinfppr5	PERSONAL: MOBILE DEVICE	Revoked	10-02-2014 18:06:04	10-02-2017 18:06:
۲	PRUEBA_SMB2	SHARED: MAILBOX	Active	30-01-2014 16:57:00	30-01-2017 16:57
3	APLICACION_PRUEBAS	TECHNICAL: DOMAIN CONTROLLER PKCS10	Active	16-01-2014 18:14:30	16-01-2017 18:14:
۲	APLICACION_PRUEBAS	TECHNICAL: DOMAIN CONTROLLER PKCS10	Active	16-01-2014 18:10:29	16-01-2017 18:10:
۲	t-esin fmpp	PERSONAL: SECURE EMAIL GATEWAY	Active	15-01-2014 16:07:27	15-01-2017 16:07:
3	t-esinfmpp	PERSONAL: MOBILE DEVICE	Active	15-01-2014 16:06:11	15-01-2017 16:06:
۲	APLICACION_PRUEBAS	TECHNICAL: APPLICATION PKCS12	Active	15-01-2014 08:52:18	15-01-2017 08:52:
3	t-esinfppr3	PERSONAL: MOBILE DEVICE	Active	15-01-2014 08:48:56	15-01-2017 08:48:
3	BDE_PRUEBA_SMB	SHARED: MAILBOX	Active	15-01-2014 08:21:53	15-01-2017 08:21:
		1 2 3 4 5 6 7	8		0
				ExportXLS	Details of Search

Figure 37 - Certificates list

ECB - Restricted

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

Click the Solution 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.

	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
	Search Cancel search

Figure 38 - Search certificate requests

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

Detail	Subscriber	Subscriber Type	Certificate Package Type	Request Status	Request Date	Request Reaso
٩	APLICACION_PRUEBAS	Devices	Standard	Completed	24-03-2014 14:52:01	Request
٩	t-esinfppr5	ESCB Users	Mobile Device	Completed	12-03-2014 17:15:13	Key compromise
٩	PRUEBAS_EPK	Devices	Standard	Completed	12-03-2014 17:12:14	Request
٢	t-esinfdbcx	ESCB Users	Provisional	Cancelled	26-02-2014 17:42:57	Request
۲	t-esinfppr4	ESCB Users	Provisional	Completed	26-02-2014 17:31:29	Request
٩	ESCB-PKI_LDAP	Devices	Standard	Completed	19-02-2014 09:03:29	Request
٢	ESCB-PKI_LDAP	Devices	Standard	Completed	19-02-2014 09:00:43	Request
۲	ESCB-PKI_LDAP	Devices	Standard	Completed	19-02-2014 08:58:08	Request
٩	SEE PROJECT USER 120	Shared Mailbox	Shared Mailbox	Completed	11-02-2014 16:28:59	Request
۲	t-esinfppr5	ESCB Users	Gateway	Completed	10-02-2014 18:20:17	Request
3	t-esinfppr5	ESCB Users	Mobile Device	Completed	10-02-2014 18:20:08	Request
3	t-esinfppr5	ESCB Users	Gateway	Completed	10-02-2014 18:07:56	Request
3	t-esinfppr5	ESCB Users	Mobile Device	Completed	10-02-2014 18:06:39	Request
3	PRUEBA_SMB2	Shared Mailbox	Shared Mailbox	Completed	30-01-2014 16:55:02	Request
3	t-esinfppr3	ESCB Users	Gateway	Cancelled	27-01-2014 16:15:39	Request
3	APLICACION_PRUEBAS	Devices	Advanced	Completed	16-01-2014 18:15:25	Request
3	APLICACION_PRUEBAS	Devices	Advanced	Completed	16-01-2014 18:09:39	Request
۲	t-esin fmpp	ESCB Users	Gateway	Completed	15-01-2014 16:08:04	Request
۲	t-esin fmpp	ESCB Users	Mobile Device	Completed	15-01-2014 16:06:50	Request
3	APLICACION_PRUEBAS	Devices	Standard	Completed	15-01-2014 08:51:43	Key compromise
			1 2 3 4 5 6 7	8		0 0

Certificate request list

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 $\[ensuremath{\ensu$

3.6. EVENTS

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

Search Event	
	Event search criteria
Organisation	Banco de España(ES)
Who (ESCB userid)	
What (action)	Creation Modification Status change Certificate issuance Key recovery
On subscriber (ESCB userid / Device)	
On type of entity	Select
When	From To
From	RO interface User interface A2A interface Batch interface
Action result	NFO WARN ERROR FATAL
	Search Cancel search

Figure 40 - Search events

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

Ev	ent search result	ts			
Detail	Who (ESCB userid)	What (action)	On subscriber	On certificate type	🗘 When
۲	infevg	Issue certificate package.	INF_ESCB-PKI		13-04-2014 10:44:58
۲	in fmpp	Approve shared mailbox certificate request.	INF_ESCB-PKI		13-04-2014 10:30:33
۲	infevg	Register new shared mailbox certificate request.	INF_ESCB-PKI		13-04-2014 10:28:04
٩	infmpp	Approve shared mailbox certificate request.	DisplayName		13-04-2014 10:21:26
3	infmpp	Approve shared mailbox certificate request.	qalvitxSharedMailbox		13-04-2014 10:19:24
۲	t-esqlorcgx2	Issue TOKEN-BASED certificate package.	t-esqlorcgx2		11-04-2014 10:50:06
٢	t-esqlorcgx2	Begin TOKEN-BASED certificate package issuance.	t-esqlorcgx2		11-04-2014 10:48:09
٩	qlorcgx	Enable remote download.	t-esqlorcgx2		11-04-2014 10:42:40
٢	qlorcgx	Modify device serial number.	t-esqlorcgx2		11-04-2014 10:42:34
۲	qlorcgx	Enable remote download.	t-esqlorcgx2		11-04-2014 10:41:32
۹	qlorcgx	Register certificate package request.	t-esqlorcgx2		11-04-2014 10:39:42
۲	qlorcgx	Register new user.	t-esqlorcgx2		11-04-2014 10:36:59
۲	qlorcgx	Register new user.	t-esqlorcgx		11-04-2014 10:35:59
3	qlorcgx_local	Issue a STANDARD certificate package.	qlorcgx_local		10-04-2014 18:00:50
٢	qlorcgx_local	Generation of the terms and conditions document.	qlorcgx_local		10-04-2014 18:00:23
۲	qlorcgx	Enable remote download.	usuarionew		10-04-2014 17:56:01
3	qlorcgx	Modify device serial number.	usuarionew		10-04-2014 17:55:55
٩	qlorcgx	Register provisional certificate package request.	usuarionew		10-04-2014 17:55:49
		1 2 3	4 5 6 7 8		00
				Export XLS	Details of Search

Figure 41 - Event list

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

User identifier infmpp Security groups [APRR_ESCB-PKI_RegistrationOfficer] ROLE_RO, ROLE_SIMCAUDIT, ROLE_SIMCCERALT, ROLE_SIMCCERAUD, ROLE_SIMCCERREV, ROLE_USRCERAUD, ROLE_USRCEAUD, ROLE_USRCEAUD, ROLE_MICREGUAU, ROLE_SIMCCFOR, ROLE_USRCEAUD, ROLE_USRCEAUD, ROLE_USRCEAUD, ROLE_MISCREGUCAU, ROLE_USRCEAUD, ROLE_U	User identifier Security groups	infmpp
Security groups [APPR_ESCB-PK]_RegistrationOfficer] RoLE_SMCCERBUS, ROLE_SMCREART, ROLE_SMCCERAUD, ROLE_SMCREARD, ROLE_SMCREARD, ROLE_SMCREARD, ROLE_SMCREARD, ROLE_SMCREARD, ROLE_SMCREARD, ROLE_SMCREARD, ROLE_SMCREARD, ROLE_USRREAD, ROLE_USRREAD, ROLE_USRREADD, ROLE, R	Security groups	
Security role POLE_RO, ROLE_SMCAUDIT, ROLE_SMCREGARCT, ROLE_SMCREGAUD, ROLE_SMCCERREV, ROLE_SMCCERSUS, ROLE_SMCREGAPP, ROLE_SMCREGAUD, ROLE_SMCREGAUN, ROLE_USRCREAUN, ROLES, R		[APPR_ESCB-PKI_RegistrationOfficer]
Security domain [11] Transaction identifier ESCB_PKL_cba7b43e-3058-4628-8e0e-41b104da23d0 Transaction identifier ESCB_PKL_cba7b43e-3058-4628-8e0e-41b104da23d0 Event code STATE_CHANGE 10-04-2014 10:30:33 epkmain Application epkmain Priority code NFO Level HIGH Action type RESULT Source SHARED_MALBOX Entity type CERTFICATE_REQUEST Entity domain 11 Message Approve shared mailbox certificate request. Import = NPUT	Security roles	[ROLE_RO, ROLE_SMCAUDIT, ROLE_SMCCERACT, ROLE_SMCCERAUD, ROLE_SMCCERREV, ROLE_SMCCERSUS, ROLE_SMCREGAPP, ROLE_SMCREGAUD, ROLE_SMCREGCAN, ROLE_SMCTYC, ROLE_USRCREAUD, ROLE_USRCPACT, ROLE_USRCPREV, ROLE_USRCPSUS, ROLE_USRCPT, ROLE_USRREAD, ROLE_USRREGAUD, ROLE_USRREGPROVISIONAL]
Trace information Transaction identifier ESCB_PKL_cba7b43e-3058-4628-8e0e-41b104da23d0 Fvent code STATE_CHANGE Date 13-04-2014 10:30:33 Application epkmain Priority code NFO Level HIGH Action type RESULT Source SHARED_MALBOX Entity type CERTFICATE_REQUEST Entity domain 11 Message Approve shared mailbox certificate request. Import = NPUT	Security domain	[11]
Transaction identifier ESCB_PKL_cba7b43e-3058-4628-8e0e-41b104da23d0 Event code STATE_CHANGE 1004-2014 10:30:33 epkmain Application epkmain Priority code NFO Level HIGH Action type RESULT Source SHARED_MALBOX Entity type CERTFICATE_REQUEST Entity domain 11 Message Approve shared mailbox certificate request. Import = number of the special speci special special special special speci spec		Trace information
Event code STATE_CHANGE Event code STATE_CHANGE 13-04-2014 10:30:33 Application epkmain Priority code NFO Level HIGH Action type RESULT Source SHARED_MALBOX Entity type CERTFICATE_REQUEST Entity identifier 214 Entity domain 11 Message Approve shared mailbox certificate request.	Transaction identifier	FSCB_PKL_cha7b43e_3058_4628_8e0e_41b104da23d0
Arguments 13-04-2014 10:30:33 Application epkmain Priority code NFO Level HGH Action type RESULT Source SHARED_MALBOX Entity type CERTFICATE_REQUEST Entity identifier 214 Entity domain 11 Message Approve shared mailbox certificate request.	Event code	STATE CHANGE
Application epimain Priority code NFO Level HIGH Action type RESULT Source SHARED_MAILBOX Entity type CERTIFICATE_REQUEST Entity identifier 214 Interview Approve shared mailbox certificate request. Image: Interview Interview Message Approve shared mailbox certificate request. Image: Interview Interview HipSerview Interview Headurest URL=http://h-ra-epi.bde.es:443/epimain/sharedmailbox/request/approve.html Method-GET Requested SessionIfd=ImMBZSICkAq8uBbcSY/lipgE, isRequestedSessionIdFromCookie=true, asRequested SessionIdFromULT-false, isRequestedSessionId/avalid=true] Session=Id=J-mikBZSICkAq8uBbcSY/lipgE, creationTime=1397376882327, lastAccessedTime=13973777951 maxinactiveInterval=2100) Headers=[Accept=application/xms-ma-pplication, image/jeg, application/xmim=sexcel, application/xms-ma-powerpoint, application/xms-ma-pplication, image/jeg, application/xms-ma-powerpoint, application/may ord, v ⁺ Accept-Encoding=gzip, deflate, Accept-Language=es-ES, Host=t-ra-epk.bde.es.443, Refere=https://t-ra-epk.bde.es/43, Refere=https://t-ra-epk.bde.es/43, Refere=https://t-ra-epk.bde.es/43, Refere=https://t-ra-epk.bde.es/43, Refere=https://t-ra-epk.bde.es/43, Refere=https://t-ra-epk.bde.es/43, Sio729, MET (LR 3.0.30729, MET (LR 3.0.50729, MET (LR 3.0.5072	Date	13.04.2014 10:30:33
Priority code NFO Level HIGH Action type RESULT Source SHARED_MALBOX Entity type CERTFICATE_REQUEST Entity domain 11 Message Approve shared mailbox certificate request. Image: Start St	Application	ankmain
Action type RESULT Action type RESULT Source SHARED_MALBOX Entity type CERTFICATE_REQUEST Entity identifier 214 Entity identifier 214 Interfease Season and the season of	Application	
Action type RESULT Source SHARED_MALBOX Entity type CERTFICATE_REQUEST Entity identifier 214 Entity identifier 214 Image: State Stat	Filonity code	
Action type RESULT Source SHARED MALBOX Entity type CERTFICATE_REQUEST Entity identifier 214 Entity domain 11 Message Approve shared mailbox certificate request.	A stime to a	
Source ShAkED_IMALEDXX Entity type CERTFICATE_REQUEST Entity identifier 214 Entity domain 11 Message Approve shared mailbox certificate request.	Action type	RESULT
Arguments Arguments Arguments Accept-Encoding-spic deflate, Accept-Language-es-ES, Host=t-ra-epk.bde.es/443, Referer=https://t-ra-epk.bde.es/443, X-ESCB-IAM-AUTHLEVEL=7, X-ESCB-IAM-AUTHLEVEL=7, X-ESCB-IAM-AUTHLEVEL=7, X-ESCB-IAM-AUTHLEVEL=7, X-ESCB-IAM-AUTHLEVEL=7, X-ESCB-IAM-AUTHLEVEL=7, X-ESCB-IAM, SWSSR-I417, 2005	Source	STARED_MAILBOX
Entity identitier 214 Entity domain 11 Message Approve shared mailbox certificate request.	Entity type	
Entity domain 11 Message Approve shared mailbox certificate request.	Entity identifier	214
Message Approve shared mailbox certificate request.	Entity domain	11
HPUT	Message	Approve shared mailbox certificate request.
Capability=WS-ESI="ESI/1.0+", _WS_HAPRT_WLMVERSION=-1] Parameters=[]	Arguments	Intro Jime Jimes HttpServiefRequest Request URL=http://r-ra-epk.bde.es:443/epkmain/sharedmailbox/request/approve.html Method=GET Requested Session=[id=JmkBzStCkAq8uBbcSYilpgE, isRequestedSessionIdVaid=true] Session=[id=JmkBzStCkAq8uBbcSYilpgE, isRequestedSessionIdVaid=true] Session=[id=JmkBzStCkAq8uBbcSYilpgE, creationTime=1397376882327, lastAccessedTime=1397377951 maxinactiveInterval=2100] Headers=[Accept= application/x-ms-application, image/igeg, application/xami+xml, image/igf, image /pipeg, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powe rpoint, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powe rpoint, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.sperite wpbication/x=scippeg rpl.bde.sciPkmain/sharedmailbox/request/delai.htm?_id=214, User-Agent= Mozilla/4.0 (compatible; MSE 7.0; Windows NT 6.1; WOW64, Trident/5.0; SLCC2; N ET CLR 2.0 SO727, NET CLR 3.5 S30729; NET CLR 3.0:30729; Media Center PC 6.0; VIa=TTTT1.1 t-ra-epk.bde es:443, X-ESCB-IAM-AUTH_EVEL=7, X-ESCB-IAM-UID=infmpp, x-escb-iam-rolesAPRE_ESCB-PKLRegistrationOfficer, iserver_name=bdenredt02-webseald-tamsvc02.bde.es, Cookie=RSESSIOND=0000JmkBzStCkAq8uBbcSYlipgE:15qvg4h, SWISE=false, \$WSSC=http, \$W/SPR+HTT Capability=WS-ESI=TEVI1.0+*, _WS_HAPRT_WLMVERSION=-1]

Figure 42 - Event details

4. MORE INFORMATION ABOUT ESCB-PKI

For further information see the ESCB-PKI Website, <u>https://pki.escb.eu/</u> (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.