BANCO DE ESPAÑA
Eurosistema

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI PROJECT

ESCB-PKI REGISTRATION AUTHORITY APPLICATION

REGISTRATION OFFICER'S MANUAL

VERSION 4.2

ECB-Restricted
22-October-2024

TABLE OF CONTENTS

TABLE OF ILLUSTRATIONS

Project name:	**ESCB-PKI**
Author:	ESCB-PKI Project team
File name:	ESCB-PKI - RA Application Registration Officer's Manual v.4.2.docx
Version:	4.2
Date of issue:	22.10.2024
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**
0.01	Draft	07.10.2011	Initial version
0.10	Draft	20.10.2011	Several additions
0.13	Draft	28.11.2011	BdE Revision
1.0	Draft	22.02.2012	Version distributed at the workshop
1.1	Final	13.03.2012	Final version
1.2	Final	01.06.2012	Minor modifications
1.3	Final	15.04.2014	Introduction of new certificate types
2.0	Final	11.09.2018	BdE Revision
3.0	Final	15.11.2021	Compatibility with other browsers
4.0	Final	20.12.2022	Terms and Conditions acceptance procedure update
4.1	Final	31.12.2023	Updated http links to ESCB-PKI website to https
4.2	Final	22.10.2024	Face-to-face certificate delivery for local users' procedure

GLOSSARY AND ACRONYMS

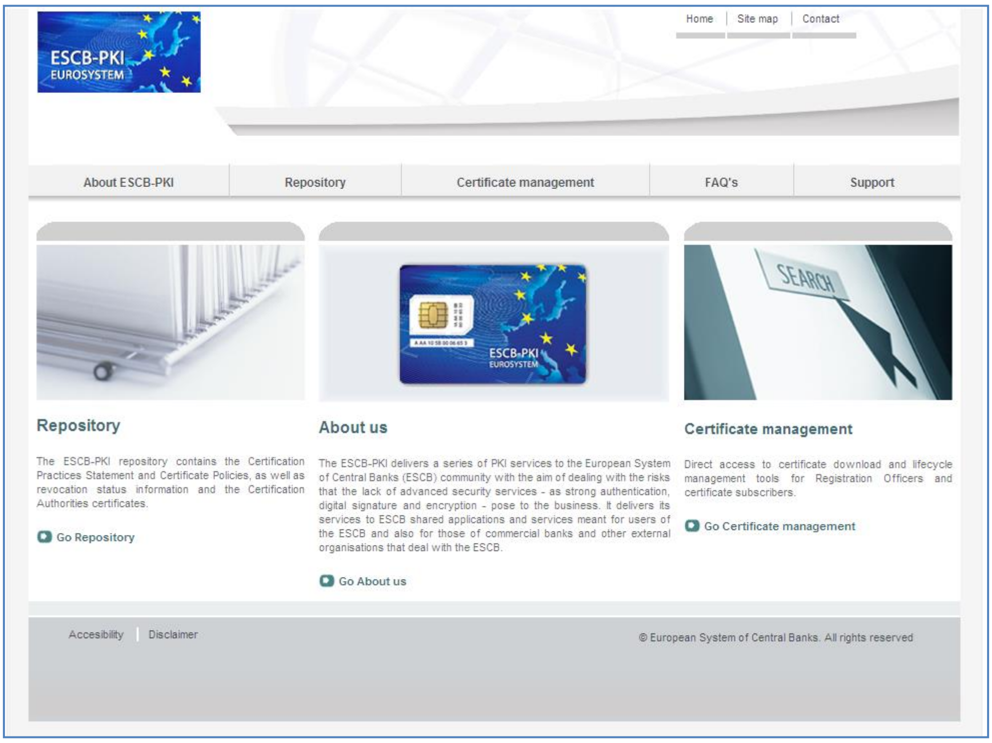
Acronym	Definition
CA	Certificate Authority
CB	ESCB Central Bank (ECB or NCB)
CP	Certification Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
ECB	European Central Bank
ESCB	European System of Central Banks, including the ECB and the NCBs of all States member of the European 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
SMA	Shared Mailbox Administrator

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.



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:

- 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.

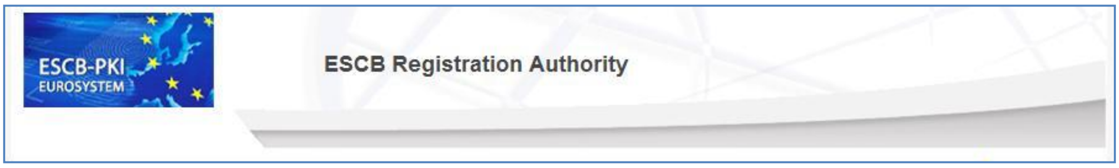


Figure 2 - Production frame

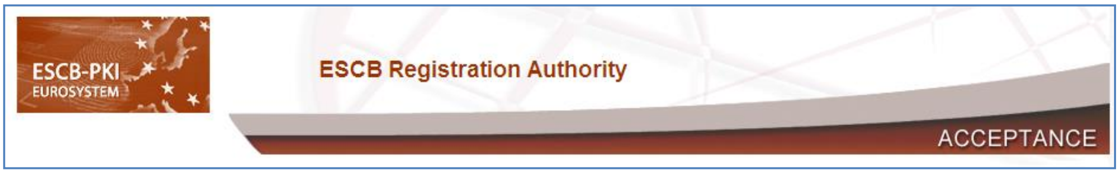


Figure 3 - Acceptance frame

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

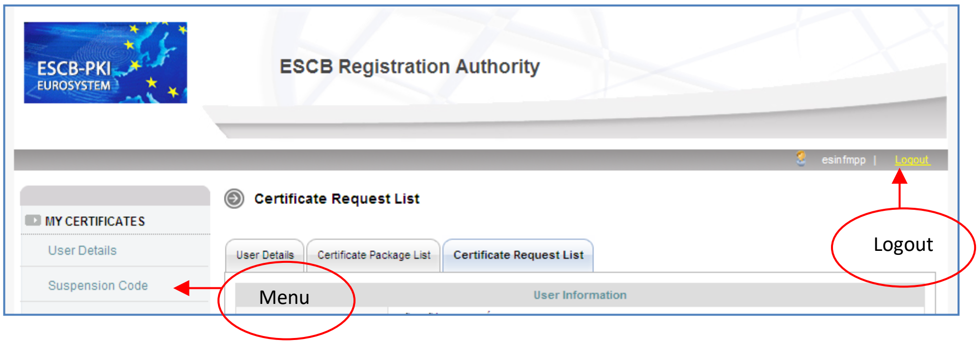
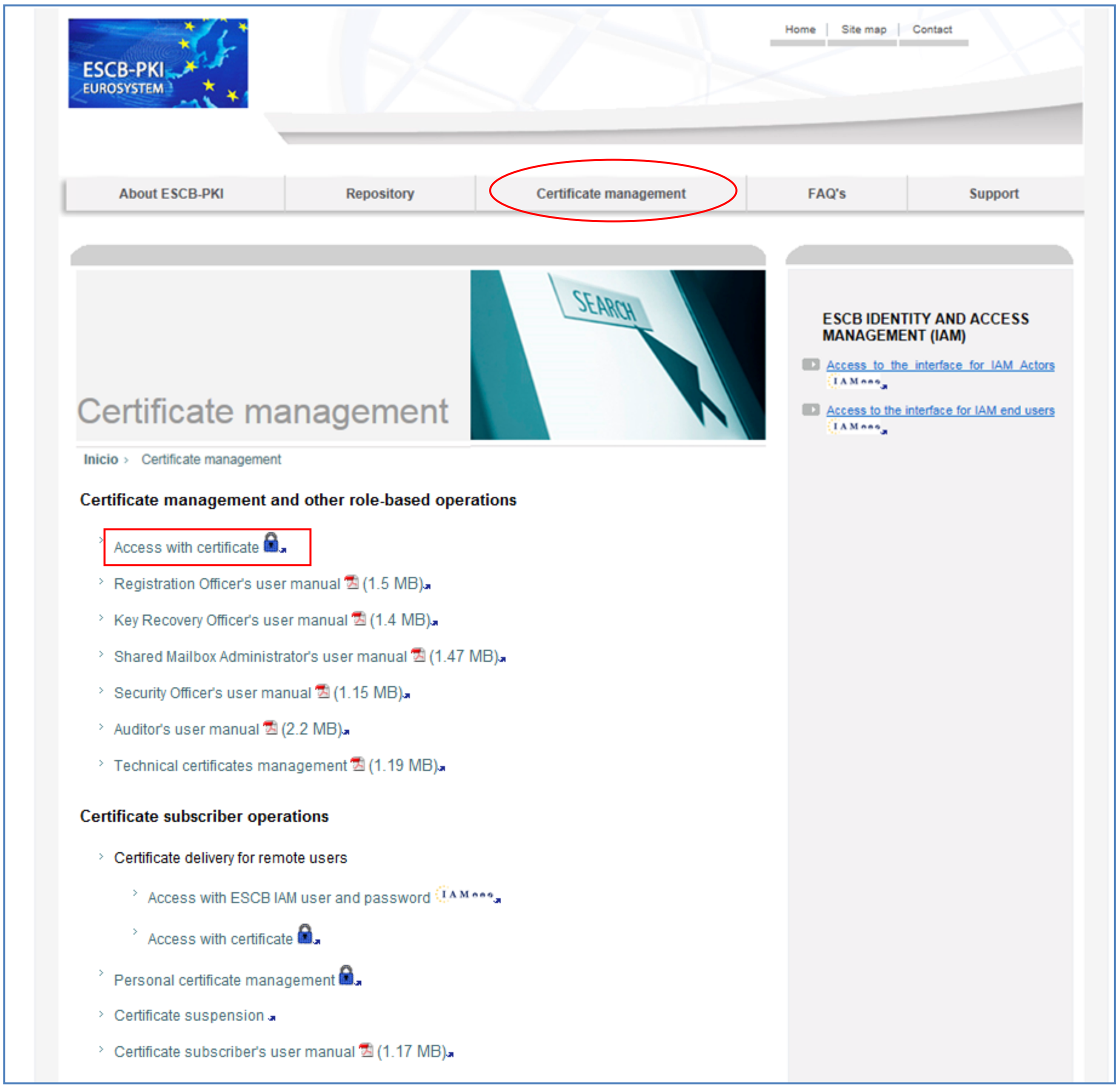


Figure 4 - Certificate management

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



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.

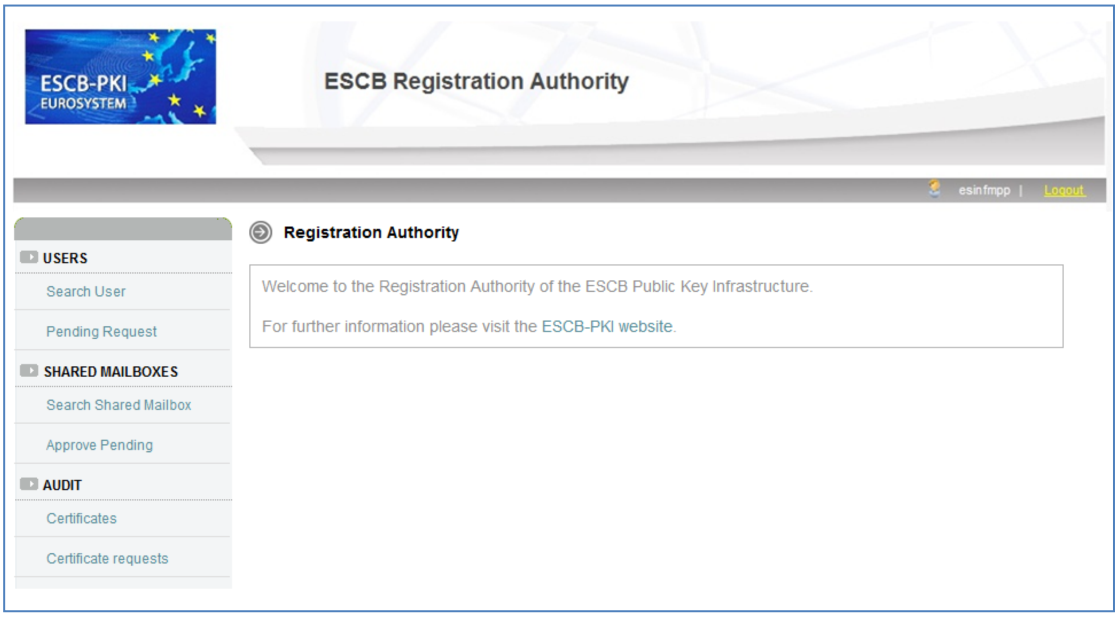
3. ESCB-PKI RA: CERTIFICATE MANAGEMENT

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 and shared mailboxes pertaining to your organization which have applied for ESCB-PKI certificates. For every user or shared mailbox in the list you may perform the following operations.
  - Check the registered personal data
  - Manage her/his requests
    - Cancel the request
    - Allow/disallow remote download of the certificates
    - Download the certificates
    - Obtain a copy of the Terms and Conditions form associated with that request
  - Manage her/his certificates
    - Suspend/reactivate certificates
    - Revoke certificates
- Check your organization’s pending certificate requests for personal and shared mailbox certificates and perform the following operations.
  - Cancel the request
  - Allow/disallow remote download of the certificates
  - Download the certificates
  - Obtain a copy of the term and conditions form associated to every request
- Review and obtain reports of the certificates and certificate requests that have been managed in your organization.

Certificate management menu



Welcome to the Registration Authority of the ESCB Public Key Infrastructure.

For further information please visit the ESCB-PKI website.

Figure 6 - Certificate management

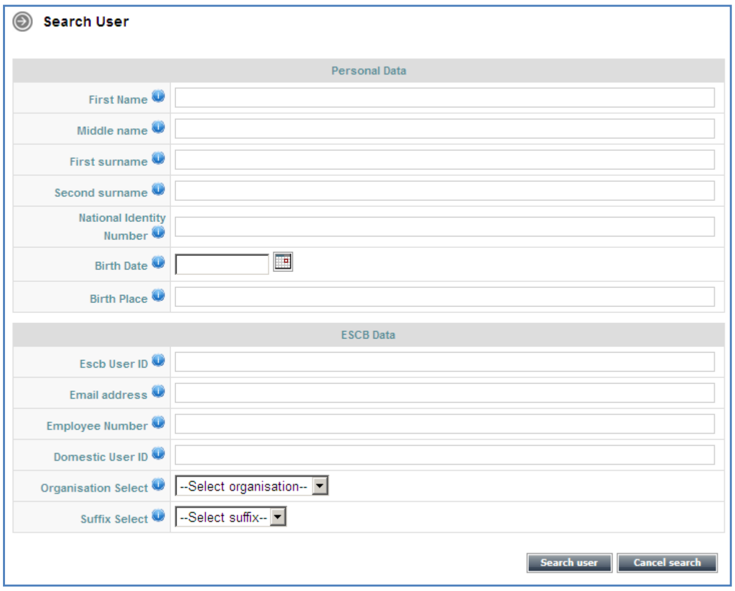
The following options will be available in the left frame menu:

- ***Users > Search users*** To select users from your Central Bank
- ***Users > Pending Request*** To show all personal certificate pending requests from your Central Bank
- ***Shared mailboxes > Search shared mailboxes*** To select shared mailboxes from your Central Bank
- ***Shared mailboxes > Approve Pending*** To show all shared mailbox certificate pending requests from 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 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 organization which have applied for ESCB-PKI certificates. Several filtering criteria can be applied to narrow the search.



Search User

Personal Data

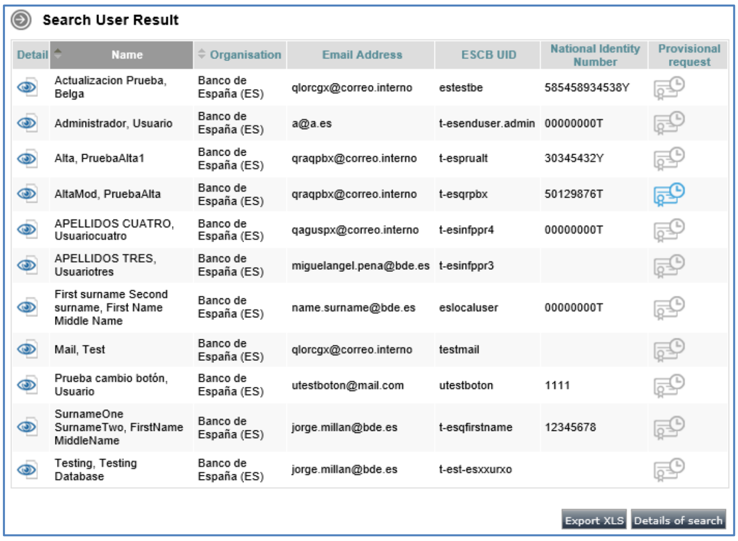
First Name	
Middle name	
First surname	
Second surname	
National Identity Number	
Birth Date	
Birth Place	

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



Search User Result

Detail	Name	Organisation	Email Address	ESCB UID	National Identity Number	Provisional request
	Actualizacion Prueba, Belga	Banco de España (ES)	qlorcgx@correo.interno	estestbe	585458934538Y	
	Administrador, Usuario	Banco de España (ES)	a@a.es	t-esenduser.admin	00000000T	
	Alta, PruebaAlta1	Banco de España (ES)	qraqpbx@correo.interno	t-esprualt	30345432Y	
	AltaMod, PruebaAlta	Banco de España (ES)	qraqpbx@correo.interno	t-esqrpbx	50129876T	
	APELLIDOS CUATRO, Usuariocuatro	Banco de España (ES)	qaguspx@correo.interno	t-esinfppr4	00000000T	
	APELLIDOS TRES, Usuariotres	Banco de España (ES)	miguelangel.pena@bde.es	t-esinfppr3		
	First surname Second surname, First Name Middle Name	Banco de España (ES)	name.surname@bde.es	eslocaluser	00000000T	
	Mail, Test	Banco de España (ES)	qlorcgx@correo.interno	testmail		
	Prueba cambio botón, Usuario	Banco de España (ES)	utestboton@mail.com	utestboton	1111	
	SurnameOne SurnameTwo, FirstName MiddleName	Banco de España (ES)	jorge.millan@bde.es	t-esqfirstname	12345678	
	Testing, Testing Database	Banco de España (ES)	jorge.millan@bde.es	t-est-esxxurxo		

Figure 8 - Organisation user list

From this list you can:

- Request provisional certificates for a given user, clicking the certificate-with-time icon in blue ( ). This option will only appear in the case of a user with active certificate packages that are based on a smartcard or USB token, if this is not the case, the icon will be greyed out and unusable. See section 3.2.4 for further information.

- 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

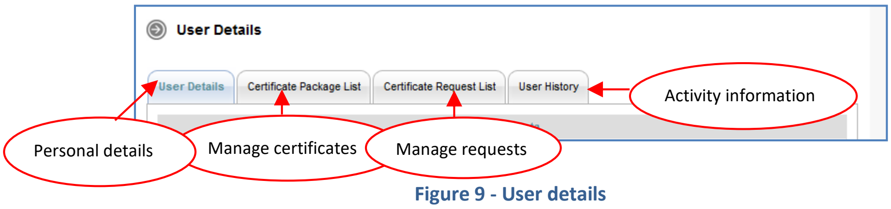


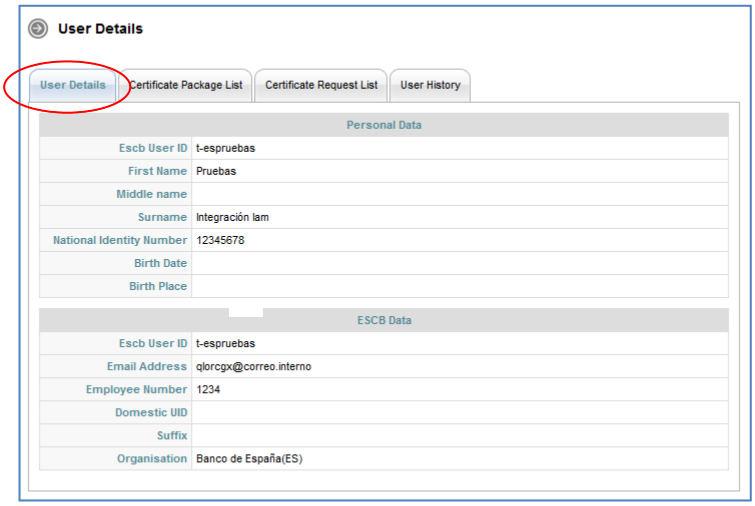
Figure 9 - User details

The following operations may be executed:

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

3.1.1. USER DETAILS

Clicking on this tab the user attributes (first name, surname, user-id, etc.) and the information of the organization they belong to are displayed.



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

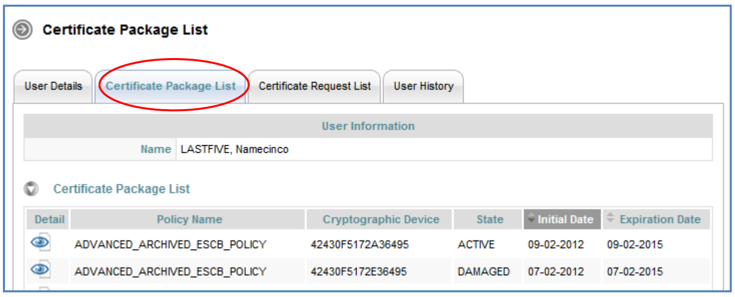
ESCB Data	
Escb User ID	t-espruebas
Email Address	qlorcgx@correo.interno
Employee Number	1234
Domestic UID	
Suffix	
Organisation	Banco de España(ES)

Figure 10 - 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



Certificate Package List

User Information	
Name	LASTFIVE, Namecinco

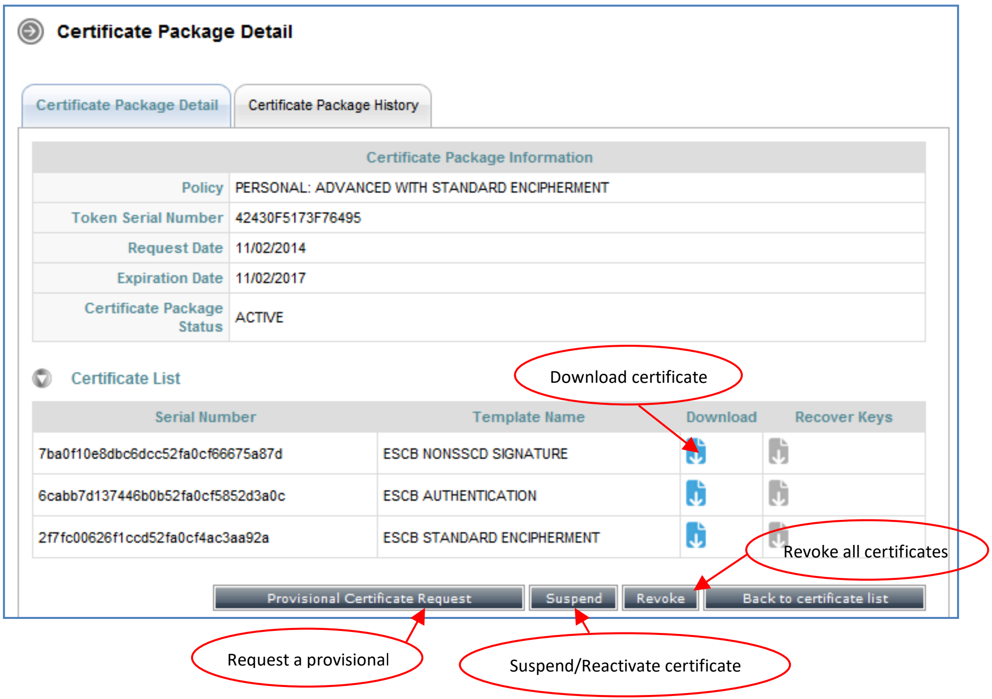
Certificate Package List

Detail	Policy Name	Cryptographic Device	State	Initial Date	Expiration Date
👁	ADVANCED_ARCHIVED_ESCB_POLICY	42430F5172A36495	ACTIVE	09-02-2012	09-02-2015
👁	ADVANCED_ARCHIVED_ESCB_POLICY	42430F5172E36495	DAMAGED	07-02-2012	07-02-2015

Figure 11 - 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 Information	
Policy	PERSONAL: ADVANCED WITH STANDARD ENCIPHERMENT
Token Serial Number	42430F5173F76495
Request Date	11/02/2014
Expiration Date	11/02/2017
Certificate Package Status	ACTIVE

Certificate List

Serial Number	Template Name	Download	Recover Keys
7ba0f10e8dbc6dcc52fa0cf66675a87d	ESCB NONSSCD SIGNATURE	⬇	⬇
6cabb7d137446b0b52fa0cf5852d3a0c	ESCB AUTHENTICATION	⬇	⬇
2f7fc00626f1ccd52fa0cf4ac3aa92a	ESCB STANDARD ENCIPHERMENT	⬇	⬇

Download certificate

Revoke all certificates

Request a provisional

Suspend/Reactivate certificate

Figure 12 - Certificate details

And request 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 suspension/reactivation***[1]

  Clicking the ***Suspend/Reactivate*** button you will suspend/reactivate all the certificates contained in this package.

- ***Provisional certificate request***

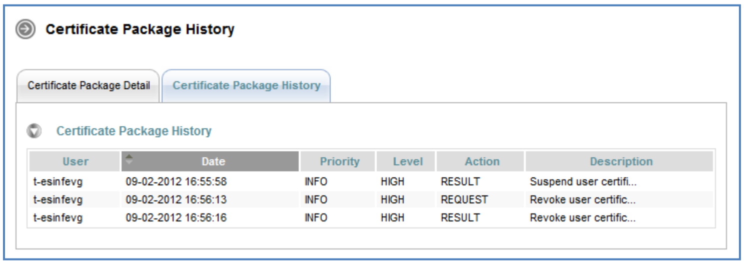
  Clicking the ***Provisional Certificate Request*** button will initiate the process to request a provisional certificate. This option will only appear in the case of certificate packages that are based on a smartcard or USB token. See section 3.2.4 for further information.

- ***Certificate revocation***

  Clicking the ***Revoke*** button you will revoke all the certificates contained in this package.

- ***Certificate Package History***

  This tab shows the activity associated with this certificate package.


Certificate Package History
Certificate Package Detail
Certificate Package History
Certificate Package History

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

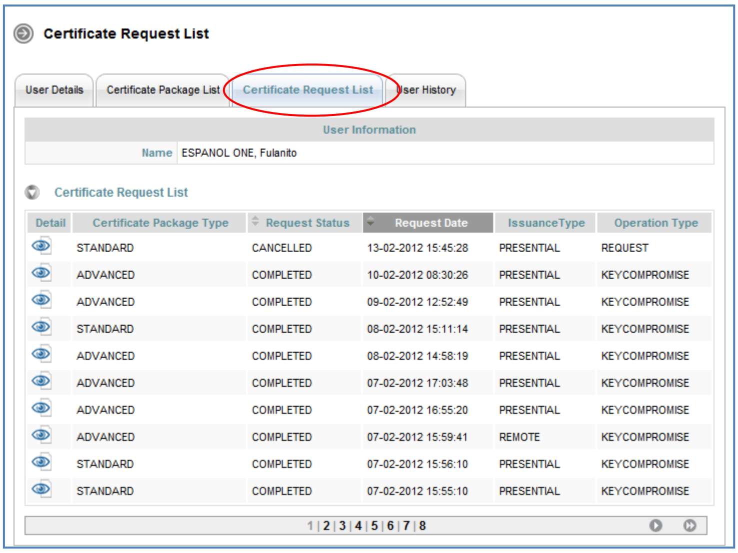
Figure 13 - Certificate activity

[1] A suspended certificate will be revoked after 60 days of its suspension.

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



Certificate Request List

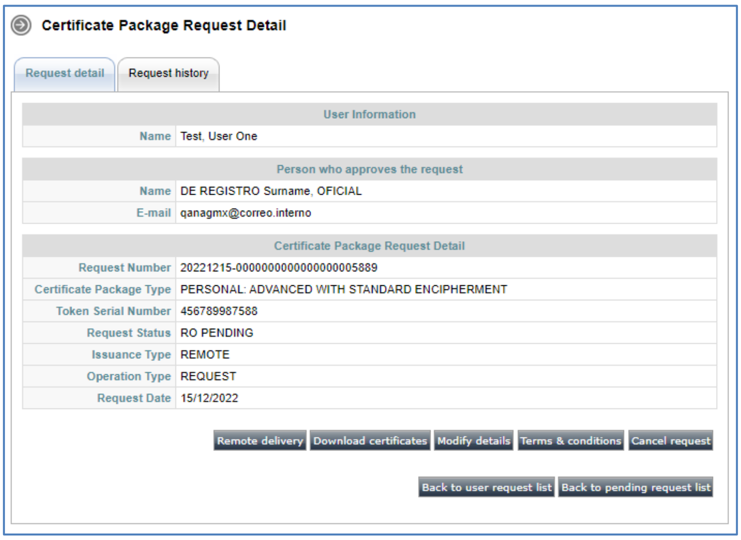
User Information	
Name	ESPANOL ONE, Fulanito

Certificate Request List

Detail	Certificate Package Type	Request Status	Request Date	IssuanceType	Operation Type
👁	STANDARD	CANCELLED	13-02-2012 15:45:28	PRESENTIAL	REQUEST
👁	ADVANCED	COMPLETED	10-02-2012 08:30:26	PRESENTIAL	KEYCOMPROMISE
👁	ADVANCED	COMPLETED	09-02-2012 12:52:49	PRESENTIAL	KEYCOMPROMISE
👁	STANDARD	COMPLETED	08-02-2012 15:11:14	PRESENTIAL	KEYCOMPROMISE
👁	ADVANCED	COMPLETED	08-02-2012 14:58:19	PRESENTIAL	KEYCOMPROMISE
👁	ADVANCED	COMPLETED	07-02-2012 17:03:48	PRESENTIAL	KEYCOMPROMISE
👁	ADVANCED	COMPLETED	07-02-2012 16:55:20	PRESENTIAL	KEYCOMPROMISE
👁	ADVANCED	COMPLETED	07-02-2012 15:59:41	REMOTE	KEYCOMPROMISE
👁	STANDARD	COMPLETED	07-02-2012 15:56:10	PRESENTIAL	KEYCOMPROMISE
👁	STANDARD	COMPLETED	07-02-2012 15:55:10	PRESENTIAL	KEYCOMPROMISE

Figure 14 - Certificate requests list

Clicking the 👁 button the details of the certificate request are displayed (by default the *"Request detail"* tab is opened).



Certificate Package Request Detail

User Information	
Name	Test, User One

Person who approves the request	
Name	DE REGISTRO Surname, OFICIAL
E-mail	qanagmx@correo.interno

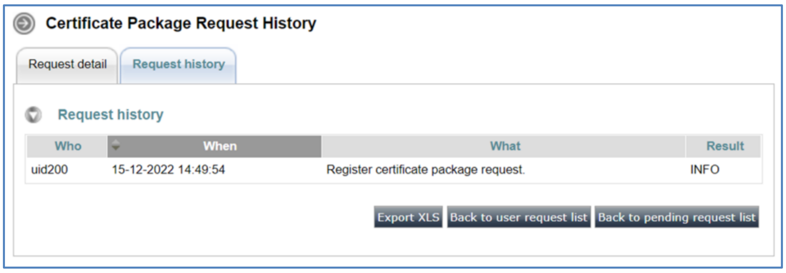
Certificate Package Request Detail	
Request Number	20221215-00000000000000000005889
Certificate Package Type	PERSONAL: ADVANCED WITH STANDARD ENCIPHERMENT
Token Serial Number	456789987588
Request Status	RO PENDING
Issuance Type	REMOTE
Operation Type	REQUEST
Request Date	15/12/2022

Figure 15 - Certificate request details

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

- ***Remote delivery*** To enable/disable Remote certificate delivery
- ***Download certificates*** To generate and download the certificates (see section 3.2)
- ***Modify details*** To update the certificate request details (e.g. the serial number of the token or smartcard)
- ***Terms and Conditions*** To check if the subscriber has signed the *Terms and Conditions* document (see section 3.2.5)
- ***Cancel request*** To cancel the request
- ***Back to user request list*** To go back to the selected user requests list
- ***Back to pending requests list*** To go back to your organization pending requests list

There is also a *“**Request history**”* tab which shows the activity associated to this certificate package.



Certificate Package Request History

Request history

Who	When	What	Result
uid200	15-12-2022 14:49:54	Register certificate package request.	INFO

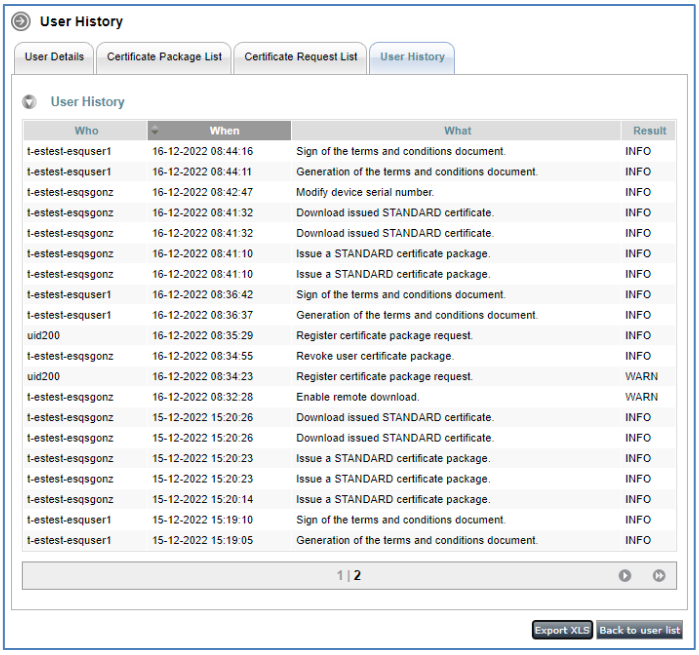
Figure 16 - Request activity

You may select the following operations:

- ***Export XLS*** To export the history in a XLS file
- ***Back to user request list*** To go back to the selected user requests list
- ***Back to pending requests list*** To go back to your organization pending requests list

3.1.4. USER HISTORY

Displays all the activity related to the user.



Who	When	What	Result
t-estest-esquser1	16-12-2022 08:44:16	Sign of the terms and conditions document.	INFO
t-estest-esquser1	16-12-2022 08:44:11	Generation of the terms and conditions document.	INFO
t-estest-esqsgonz	16-12-2022 08:42:47	Modify device serial number.	INFO
t-estest-esqsgonz	16-12-2022 08:41:32	Download issued STANDARD certificate.	INFO
t-estest-esqsgonz	16-12-2022 08:41:32	Download issued STANDARD certificate.	INFO
t-estest-esqsgonz	16-12-2022 08:41:10	Issue a STANDARD certificate package.	INFO
t-estest-esqsgonz	16-12-2022 08:41:10	Issue a STANDARD certificate package.	INFO
t-estest-esquser1	16-12-2022 08:36:42	Sign of the terms and conditions document.	INFO
t-estest-esquser1	16-12-2022 08:36:37	Generation of the terms and conditions document.	INFO
uid200	16-12-2022 08:35:29	Register certificate package request.	INFO
t-estest-esqsgonz	16-12-2022 08:34:55	Revoke user certificate package.	INFO
uid200	16-12-2022 08:34:23	Register certificate package request.	WARN
t-estest-esqsgonz	16-12-2022 08:32:28	Enable remote download.	WARN
t-estest-esqsgonz	15-12-2022 15:20:26	Download issued STANDARD certificate.	INFO
t-estest-esqsgonz	15-12-2022 15:20:26	Download issued STANDARD certificate.	INFO
t-estest-esqsgonz	15-12-2022 15:20:23	Issue a STANDARD certificate package.	INFO
t-estest-esqsgonz	15-12-2022 15:20:23	Issue a STANDARD certificate package.	INFO
t-estest-esqsgonz	15-12-2022 15:20:14	Issue a STANDARD certificate package.	INFO
t-estest-esquser1	15-12-2022 15:19:10	Sign of the terms and conditions document.	INFO
t-estest-esquser1	15-12-2022 15:19:05	Generation of the terms and conditions document.	INFO

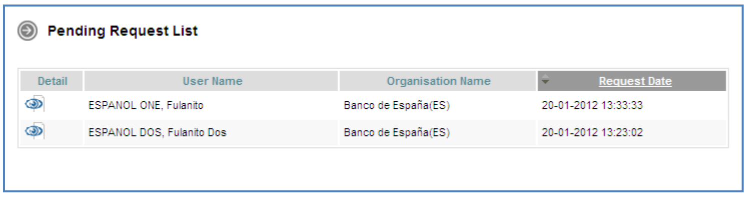
Figure 17 - User activity

You may select the following operations:

- ***Export XLS*** To export the user history into a XLS file
- ***Back to user list*** To go back to the user list

3.2. PENDING REQUEST LIST OPTION

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

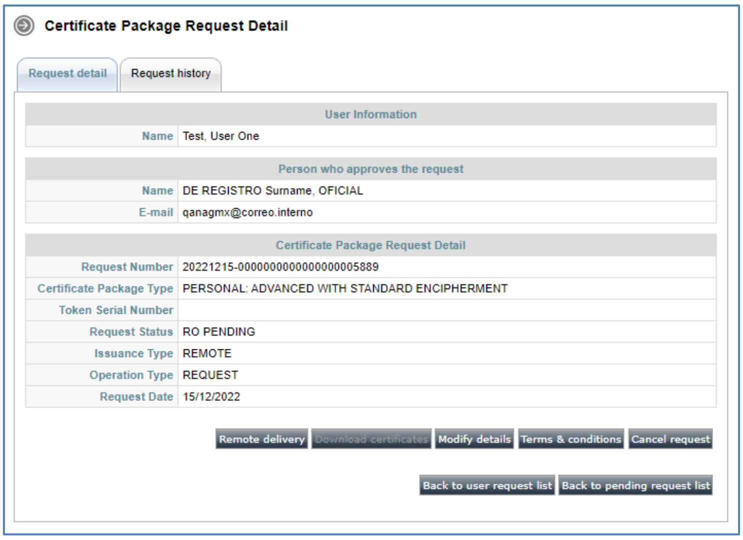


Pending Request List

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

Figure 18 - Pending requests list

Clicking the 👁 button, further details of the request will be displayed. This page is equally shown when opening a user's certificate request list and clicking the 👁 button to enter the certificate details page (section 3.1.3).



Certificate Package Request Detail

User Information	
Name	Test, User One

Person who approves the request	
Name	DE REGISTRO Surname, OFICIAL
E-mail	qanagmx@correo.interno

Certificate Package Request Detail	
Request Number	20221215-00000000000000000005889
Certificate Package Type	PERSONAL: ADVANCED WITH STANDARD ENCIPHERMENT
Token Serial Number	
Request Status	RO PENDING
Issuance Type	REMOTE
Operation Type	REQUEST
Request Date	15/12/2022

Figure 19 - Request detail

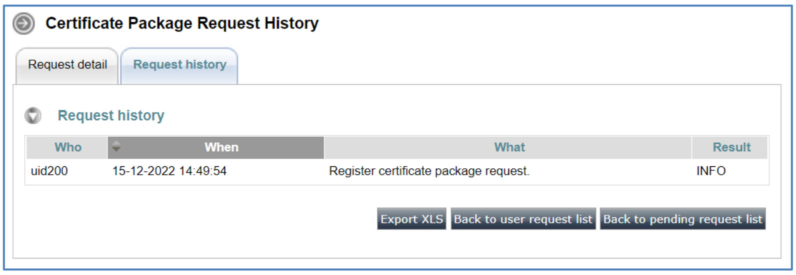
The status of the request can be:

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

You may select the following operations:

– ***Remote delivery***	To enable/disable Remote certificate delivery
– ***Download certificates***	To generate and download the certificates (see section 3.2)
– ***Modify details***	To update the certificate request details (e.g. the serial number of the token or smartcard)
– ***Terms and Conditions***	To check if the subscriber has signed the *Terms and Conditions* document (see section 3.2.5)
– ***Cancel request***	To cancel the request
– ***Back to user request list***	To go back to the selected user requests list
– ***Back to pending requests list***	To go back to your organization pending requests list

The *"**Request history**"* tab shows the activity associated to this certificate package.


Certificate Package Request History
Request detail
Request history
Request history

Who	When	What	Result
uid200	15-12-2022 14:49:54	Register certificate package request.	INFO

Export XLS
Back to user request list
Back to pending request list

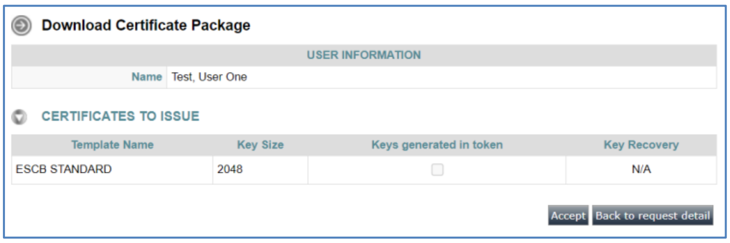
Figure 20 - Request history

You may select the following operations:

–	***Export XLS***	To export the history in a XLS file
–	***Back to user request list***	To go back to the selected user requests list
–	***Back to pending requests list***	To go back to your organization pending requests list

3.2.1. GENERATE AND DOWNLOAD SOFTWARE-BASED CERTIFICATES

The next figure shows the information displayed when you click the Download button for a software-based (i.e. standard, mobile device, or secure e-mail gateway) certificate:



Download Certificate Package

USER INFORMATION	
Name	Test, User One

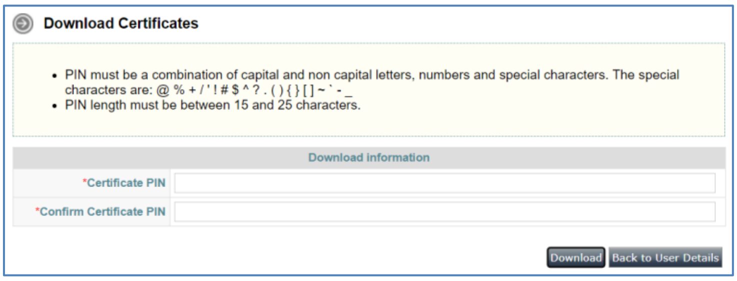
CERTIFICATES TO ISSUE

Template Name	Key Size	Keys generated in token	Key Recovery
ESCB STANDARD	2048	□	N/A

Figure 21 - Software-based certificate download

1. To initiate the process you must click the ***Accept*** button.

2. Then you will be requested to set a PIN code to protect the certificate and the keys generated



Download Certificates

- PIN must be a combination of capital and non capital letters, numbers and special characters. The special characters are: @ % + / ' ! # $ ^ ? . ( ) { } [ ] ~ ` - _
- PIN length must be between 15 and 25 characters.

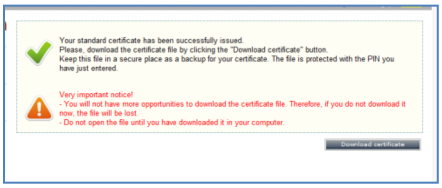
Download information	
*Certificate PIN	
*Confirm Certificate PIN	

Figure 22 - File protection PIN

Ask the user to type her/his selected PIN

- PIN length must be between 15 and 25 characters.
- PIN is a combination of capital and non capital letters, numbers and special characters (special characters are @ % + / ‘ ! # $ ^ ? . ( ) { } [ ] ~ ` - _)

3. Click the ***Download*** button. The certificate will be generated



Your standard certificate has been successfully issued.
Please, download the certificate file by clicking the "Download certificate" button.
Keep this file in a secure place as a backup for your certificate. The file is protected with the PIN you have just entered.

Very important notice!
- You will not have more opportunities to download the certificate file. Therefore, if you do not download it now, the file will be lost.
- Do not open the file until you have downloaded it in your computer.

Figure 23 - Standard certificate generated

4. Click the ***Download certificate*** button to store the certificate.

5. A File Download dialog box will pop up. Click the **SAVE** button to download the keys.

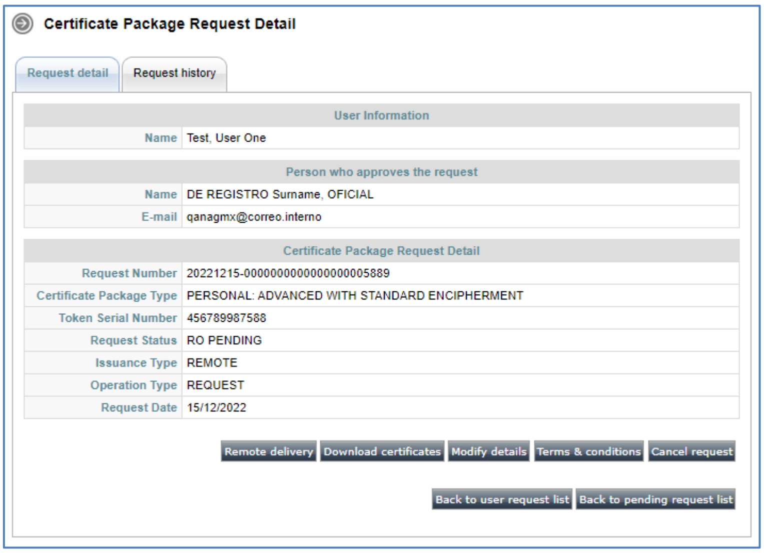
⚠ **Important notice!**
If you select the **OPEN** option (instead of **SAVE**) Windows will automatically start the installation of the certificate in your PC.

The certificate will be saved, protected by the PIN, to ensure that only the user and no one else can access to the private key.

6. Handle the file to the user and recommend to her/him to keep this file as a backup copy of her/his certificate after the installation. This will permit her/him to recover the certificate in the future in case it gets damaged.

3.2.2. GENERATE AND DOWNLOAD TOKEN-BASED CERTIFICATES

Next figure shows the information displayed for a token-based (i.e. advanced or administrator) certificate:



User Information	
Name	Test, User One

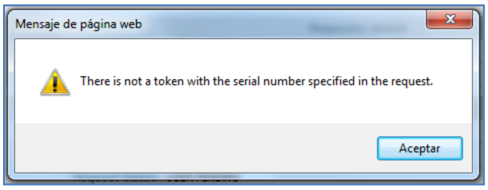
Person who approves the request	
Name	DE REGISTRO Surname, OFICIAL
E-mail	qanagmx@correo.interno

Certificate Package Request Detail	
Request Number	20221215-00000000000000000005889
Certificate Package Type	PERSONAL: ADVANCED WITH STANDARD ENCIPHERMENT
Token Serial Number	456789987588
Request Status	RO PENDING
Issuance Type	REMOTE
Operation Type	REQUEST
Request Date	15/12/2022

Figure 24 - Token-based certificates request

1. Insert the **user personal secure token** in the reader and Click the ***Download*** button.

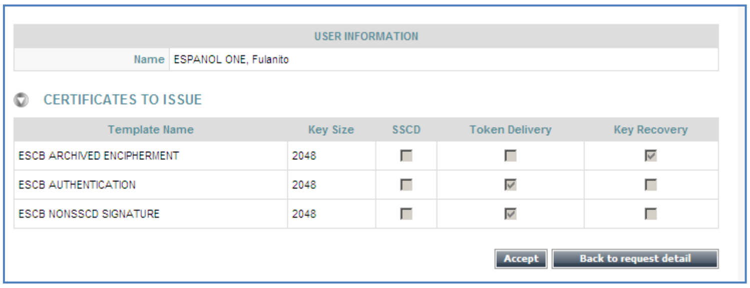
   If the serial number of the token is not the one indicated in the request an error pop-up window will be displayed.



There is not a token with the serial number specified in the request.

Figure 25 - Invalid token

   If the right token has been used the information about the certificates to be issued will be displayed.



USER INFORMATION	
Name	ESPANOL ONE, Fulanito

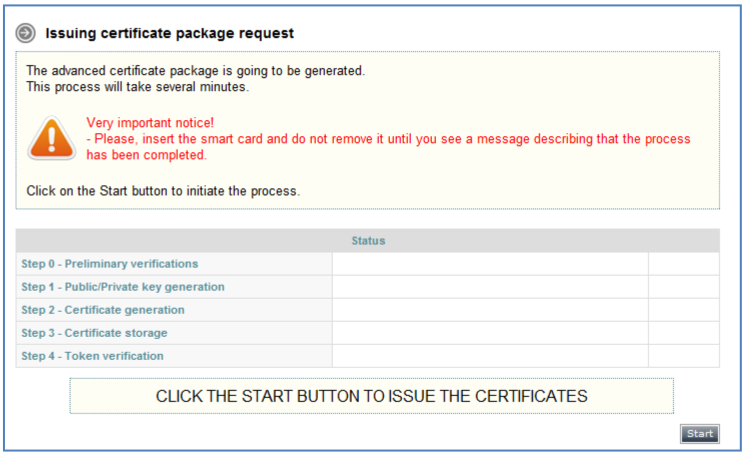
CERTIFICATES TO ISSUE

Template Name	Key Size	SSCD	Token Delivery	Key Recovery
ESCB ARCHIVED ENCIPHERMENT	2048	□	□	☑
ESCB AUTHENTICATION	2048	□	☑	□
ESCB NONSSCD SIGNATURE	2048	□	☑	□

Figure 26 - Token-based certificates download process

2. To initiate the process, click the ***Accept*** button. The whole process will take a few minutes because, depending on the certificate package type, several key-pairs may be generated and stored in the

token (e.g. in the case of advanced certificates, three key pairs will be generated: authentication, signature and encryption).



Issuing certificate package request

The advanced certificate package is going to be generated.
This process will take several minutes.

Very important notice!
- Please, insert the smart card and do not remove it until you see a message describing that the process has been completed.

Click on the Start button to initiate the process.

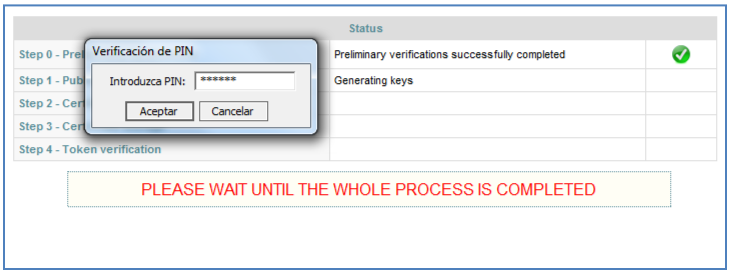
	Status	
Step 0 - Preliminary verifications		
Step 1 - Public/Private key generation		
Step 2 - Certificate generation		
Step 3 - Certificate storage		
Step 4 - Token verification		

CLICK THE START BUTTON TO ISSUE THE CERTIFICATES

Figure 27 - Advanced certificates generation

3. Click the ***Start*** button.

4. The system will prompt for the PIN of the token. Ask the user to enter it.



	Status	
Step 0 - Pre	Preliminary verifications successfully completed	✓
Step 1 - Pub	Generating keys	
Step 2 - Cer		
Step 3 - Cer		
Step 4 - Token verification		

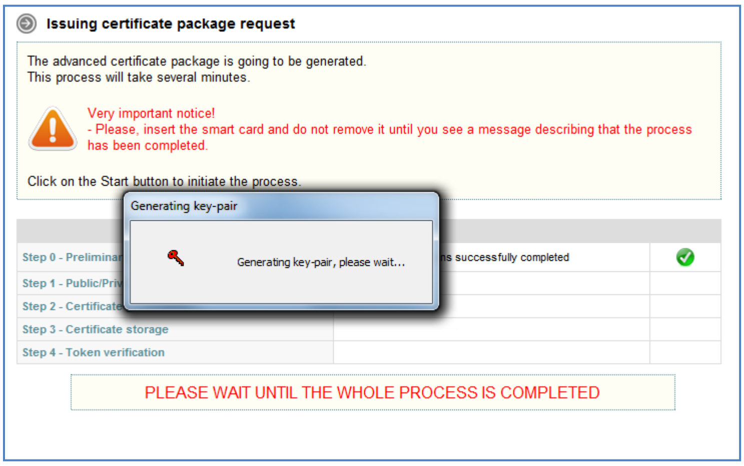
Verificación de PIN

Introduzca PIN: ******

PLEASE WAIT UNTIL THE WHOLE PROCESS IS COMPLETED

Figure 28 - Introduce PIN code

The key-pairs will be generated into the secure token.



Issuing certificate package request

The advanced certificate package is going to be generated.
This process will take several minutes.

Very important notice!
- Please, insert the smart card and do not remove it until you see a message describing that the process has been completed.

Click on the Start button to initiate the process.

Step 0 - Preliminar	s successfully completed	✓
Step 1 - Public/Priv		
Step 2 - Certificate		
Step 3 - Certificate storage		
Step 4 - Token verification		

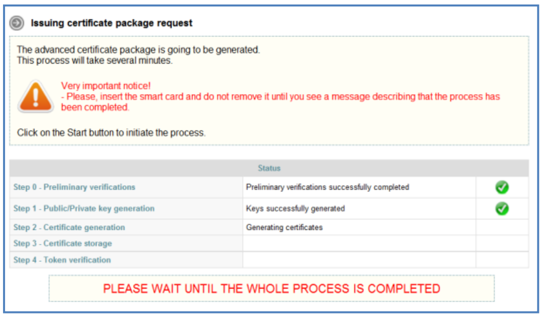
Generating key-pair

Generating key-pair, please wait...

PLEASE WAIT UNTIL THE WHOLE PROCESS IS COMPLETED

Figure 29 - Public/private keys generation

You will be informed when the keys have already been generated.



Issuing certificate package request

The advanced certificate package is going to be generated.
This process will take several minutes.

Very important notice!
- Please, insert the smart card and do not remove it until you see a message describing that the process has been completed

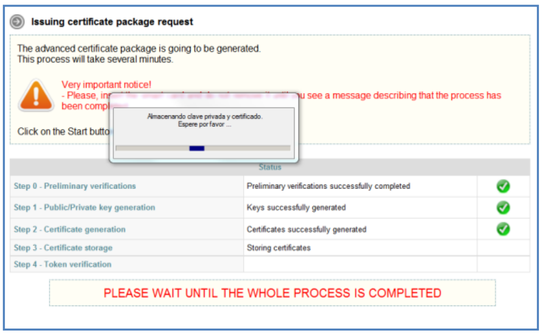
Click on the Start button to initiate the process.

	Status	
Step 0 - Preliminary verifications	Preliminary verifications successfully completed	✓
Step 1 - Public/Private key generation	Keys successfully generated	✓
Step 2 - Certificate generation	Generating certificates	
Step 3 - Certificate storage		
Step 4 - Token verification		

PLEASE WAIT UNTIL THE WHOLE PROCESS IS COMPLETED

Figure 30 - Token-based certificates successfully generated

The system will generate the certificates and will store them in the token.



Issuing certificate package request

The advanced certificate package is going to be generated.
This process will take several minutes.

Very important notice!
- Please, in... ...u see a message describing that the process has been compl...

Click on the Start butto...

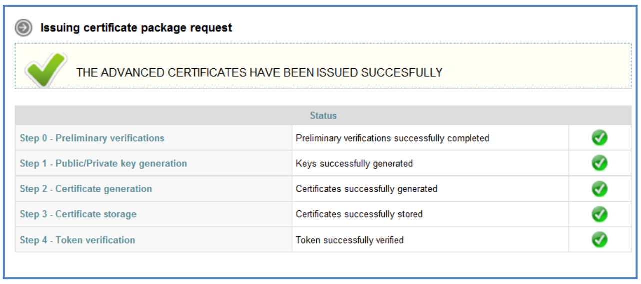
Almacenando clave privada y certificado.
Espere por favor ...

	Status	
Step 0 - Preliminary verifications	Preliminary verifications successfully completed	✓
Step 1 - Public/Private key generation	Keys successfully generated	✓
Step 2 - Certificate generation	Certificates successfully generated	✓
Step 3 - Certificate storage	Storing certificates	
Step 4 - Token verification		

PLEASE WAIT UNTIL THE WHOLE PROCESS IS COMPLETED

Figure 31 - Storing certificates

The keys and the certificates will then be available in the token.



Issuing certificate package request

THE ADVANCED CERTIFICATES HAVE BEEN ISSUED SUCCESFULLY

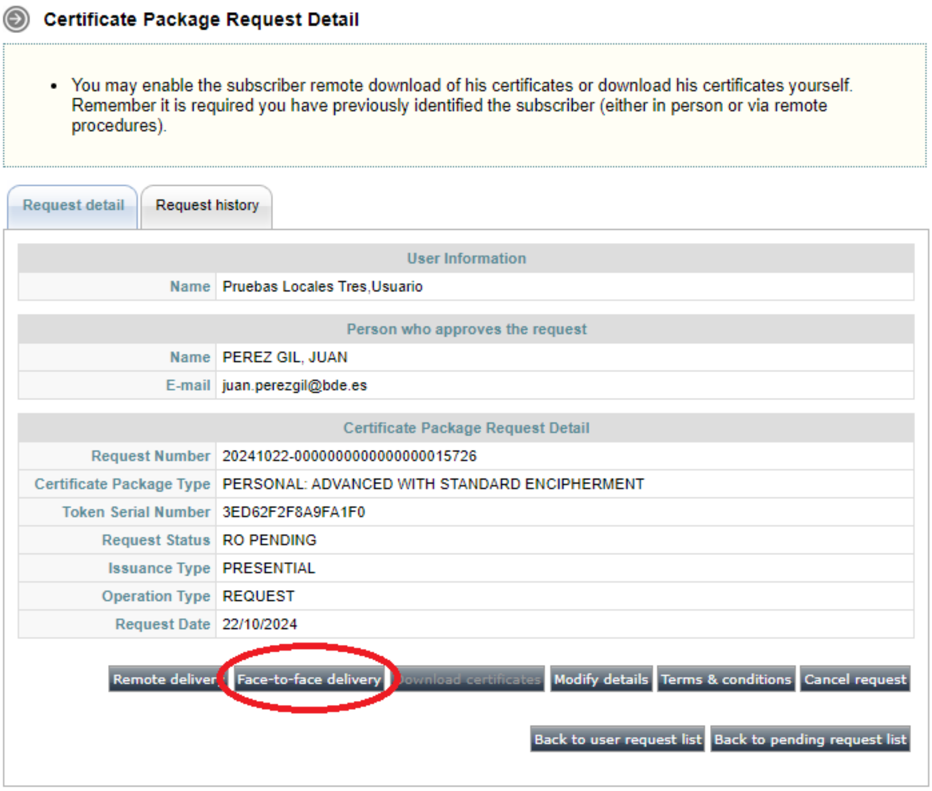
	Status	
Step 0 - Preliminary verifications	Preliminary verifications successfully completed	✓
Step 1 - Public/Private key generation	Keys successfully generated	✓
Step 2 - Certificate generation	Certificates successfully generated	✓
Step 3 - Certificate storage	Certificates successfully stored	✓
Step 4 - Token verification	Token successfully verified	✓

Figure 32 - Token-based certificates successfully stored

3.2.3. FACE-TO-FACE DELIVERY OF TOKEN-BASED CERTIFICATES FOR NON ESCB/SSM USERS

This use case applies when a Registration Officer for External Organizations (RO4EO) needs to issue a token-based certificate for a non ESCB/SSM user (also known as “Local User”), but do not want the subscriber to be able to download it themselves. The RO4EO will be the one in charge of downloading the certificates inside the token.

For this purpose, the *Face-to-face delivery* use case was created. Instead of enabling the *Remote delivery*, the RO4EO should click on the *Face-to-face delivery* button.



Certificate Package Request Detail

- You may enable the subscriber remote download of his certificates or download his certificates yourself. Remember it is required you have previously identified the subscriber (either in person or via remote procedures).

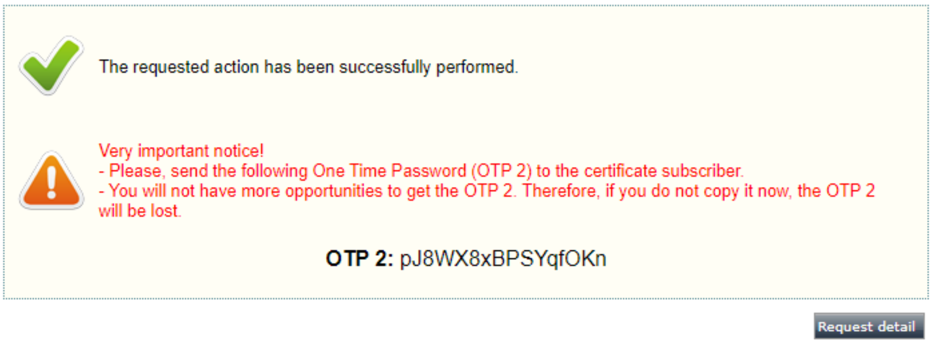
User Information	
Name	Pruebas Locales Tres,Usuario

Person who approves the request	
Name	PEREZ GIL, JUAN
E-mail	juan.perezgil@bde.es

Certificate Package Request Detail	
Request Number	20241022-0000000000000000015726
Certificate Package Type	PERSONAL: ADVANCED WITH STANDARD ENCIPHERMENT
Token Serial Number	3ED62F2F8A9FA1F0
Request Status	RO PENDING
Issuance Type	PRESENTIAL
Operation Type	REQUEST
Request Date	22/10/2024

Figure 33 – Face-to-face delivery option

Then, as the subscriber is a Local user, an OTP2 will be shown. The RO4EO must deliver it to the subscriber who will use it, together with the OTP1 that they received, to access the ESCB-PKI Registration Authority.



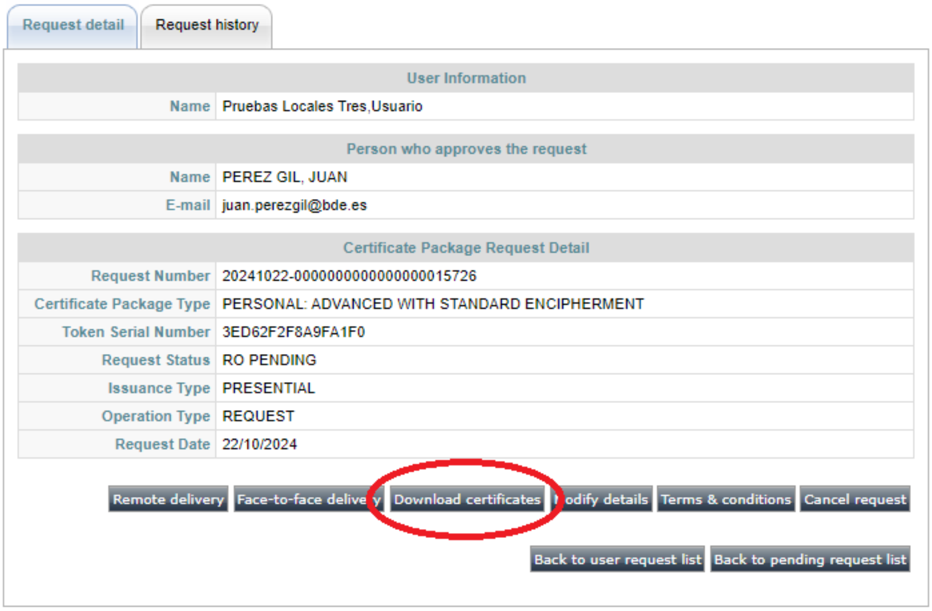
The requested action has been successfully performed.

Very important notice!
- Please, send the following One Time Password (OTP 2) to the certificate subscriber.
- You will not have more opportunities to get the OTP 2. Therefore, if you do not copy it now, the OTP 2 will be lost.

OTP 2: pJ8WX8xBPSYqfOKn

Figure 34 – OTP2 shown to the Registration Officer for External Organizations

Once the subscriber signs the Terms and Conditions document, then <u>only the Registration Officer for External Organizations will be able to download the certificates</u>. Now the *Download certificates* button appears as enabled, and the certificate download process can be performed as described in point *"3.2.2 - GENERATE AND DOWNLOAD TOKEN-BASED CERTIFICATES".*



User Information	
Name	Pruebas Locales Tres,Usuario
Person who approves the request	
Name	PEREZ GIL, JUAN
E-mail	juan.perezgil@bde.es
Certificate Package Request Detail	
Request Number	20241022-0000000000000000015726
Certificate Package Type	PERSONAL: ADVANCED WITH STANDARD ENCIPHERMENT
Token Serial Number	3ED62F2F8A9FA1F0
Request Status	RO PENDING
Issuance Type	PRESENTIAL
Operation Type	REQUEST
Request Date	22/10/2024

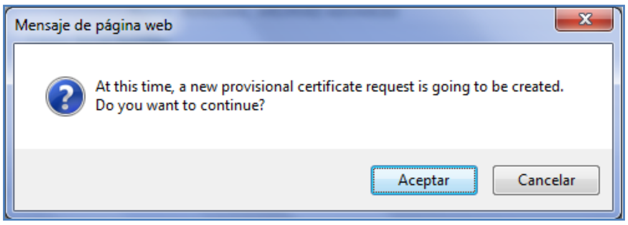
Figure 35 – Download certificates button enabled once the subscriber signs the T&C document

3.2.4. GENERATE AND DOWNLOAD PROVISIONAL CERTIFICATES

In case that the subscriber of token-based certificates (i.e. advanced and administrator) has forgotten his smartcard or token at home, provisional certificates can be requested and downloaded on a provisional token.

The process to request a provisional certificate is the following:

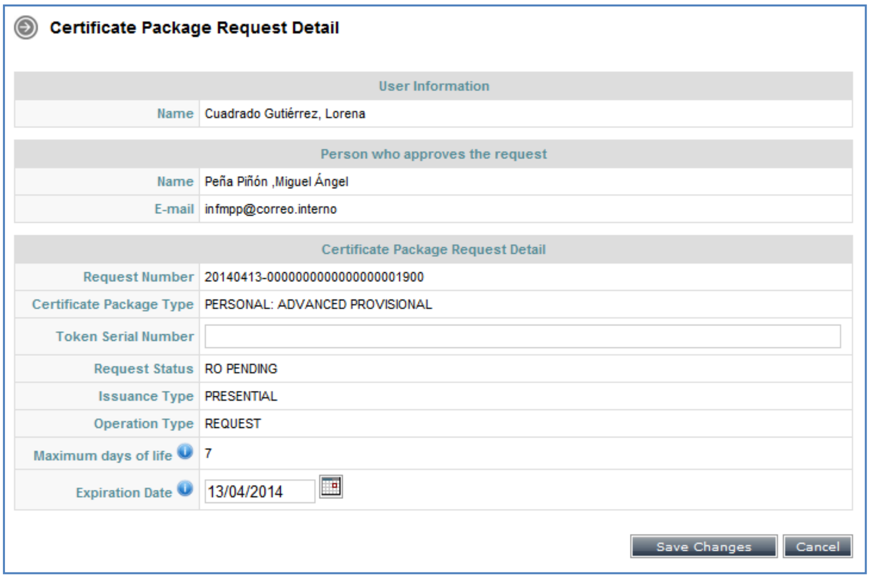
1. Locate the certificate package linked to the smartcard that he has forgotten and click the **Provisional Certificate Request** button (see section 3.1.2 for further information) or search the user and click the **Provisional Certificate Request** button directly from the search results (see section 3.1 for further information). The following message will be shown:



At this time, a new provisional certificate request is going to be created.
Do you want to continue?

Figure 36 - Provisional certificate request confirmation

2. The certificate request details will be displayed:



Certificate Package Request Detail

User Information	
Name	Cuadrado Gutiérrez, Lorena
Person who approves the request	
Name	Peña Piñón ,Miguel Ángel
E-mail	infmpp@correo.interno
Certificate Package Request Detail	
Request Number	20140413-0000000000000000001900
Certificate Package Type	PERSONAL: ADVANCED PROVISIONAL
Token Serial Number	
Request Status	RO PENDING
Issuance Type	PRESENTIAL
Operation Type	REQUEST
Maximum days of life	7
Expiration Date	13/04/2014

Figure 37 - Provisional certificate request details

3. You can modify the following details:

– ***Token serial number*** Enter the provisional token serial number

– ***Expiration date*** Enter the expiration date for the provisional certificate. By default, the certificate will expire at the end of the day when the certificate is being requested. You can select any maximum days of life that is below the number defined globally by your Central Bank's Security Officer

Once that you have modified the details click the **Save Changes** button.

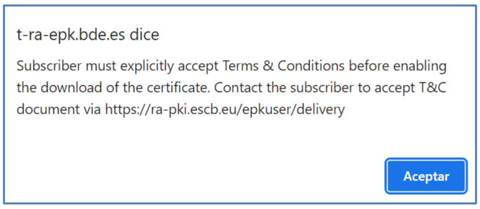
4. Proceed to download the provisional certificate in the provisional token as described for token-based certificates (see section 3.2.2)

3.2.5. VERIFY TERMS AND CONDITIONS ACCEPTANCE

Before delivering a certificate, users must formally accept their responsibilities by signing the Terms and Conditions document online. This option will allow you to check if the user has signed the Terms and Conditions document or not.

After clicking the ***Terms and Conditions*** button a dialog box will pop up.

In case the subscriber has not signed the document yet, the following pop up would appear:

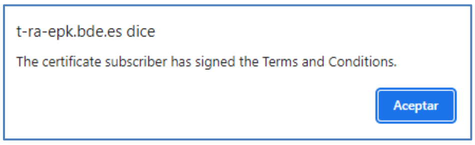


t-ra-epk.bde.es dice

Subscriber must explicitly accept Terms & Conditions before enabling the download of the certificate. Contact the subscriber to accept T&C document via https://ra-pki.escb.eu/epkuser/delivery

Figure 38 - Terms and Conditions not accepted yet pop up

If the subscriber has accepted and signed the Terms and Conditions document, then the pop up would look like this:



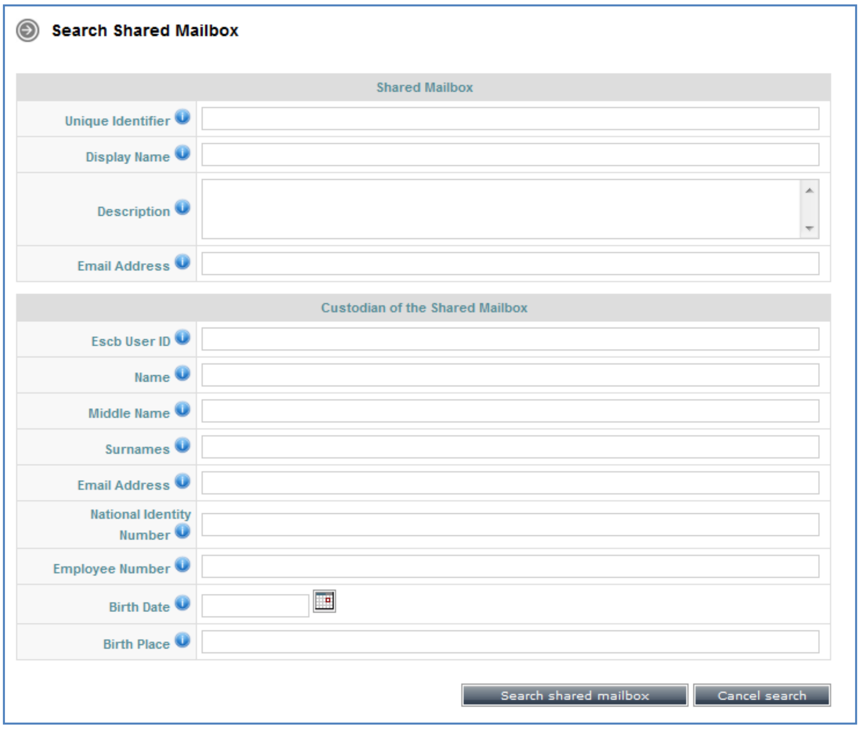
t-ra-epk.bde.es dice

The certificate subscriber has signed the Terms and Conditions.

Figure 39 - Terms and Conditions already accepted yet pop up

3.3. SEARCH SHARED MAILBOX

From the ***Search Shared Mailbox*** 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.



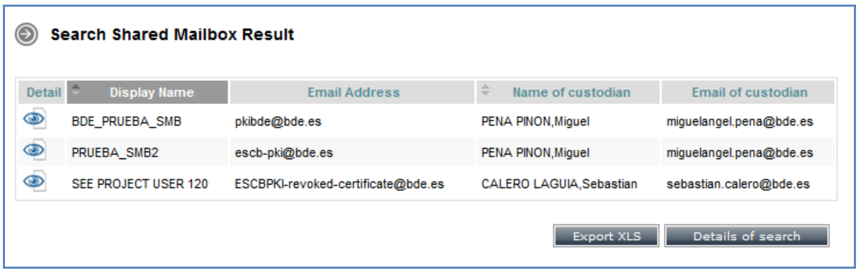
Search Shared Mailbox

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 40 - Search shared mailbox

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

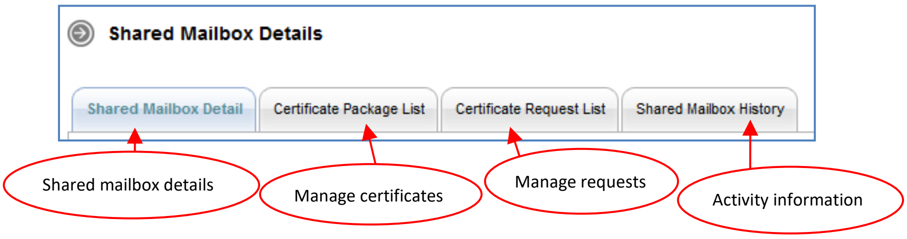


Search Shared Mailbox Result

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

Figure 41 - 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

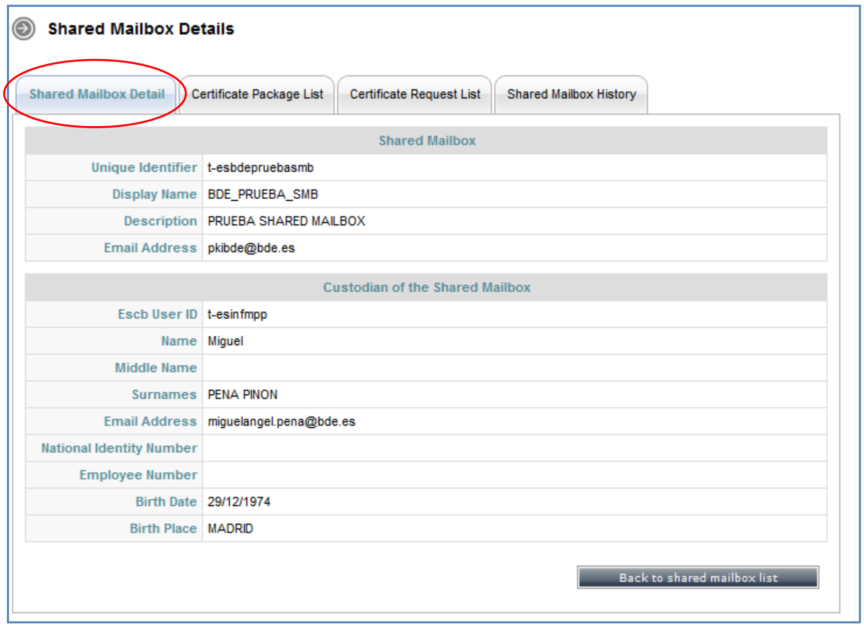
Figure 42 - Shared mailbox details

The following operations may be executed:

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

3.3.1. SHARED MAILBOX DETAILS

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



Shared Mailbox Details

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

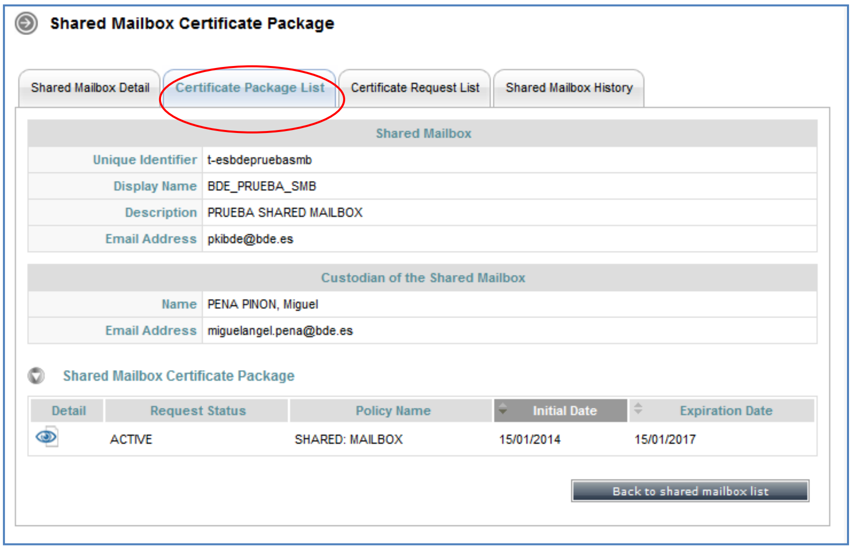
Custodian of the Shared Mailbox	
Escb User ID	t-esinfmpp
Name	Miguel
Middle Name	
Surnames	PENA PINON
Email Address	miguelangel.pena@bde.es
National Identity Number	
Employee Number	
Birth Date	29/12/1974
Birth Place	MADRID

Figure 43 - Shared mailbox details

3.3.2. 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



Shared Mailbox Certificate Package

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	
Name	PENA PINON, Miguel
Email Address	miguelangel.pena@bde.es

Shared Mailbox Certificate Package

Detail	Request Status	Policy Name	Initial Date	Expiration Date
	ACTIVE	SHARED: MAILBOX	15/01/2014	15/01/2017

Figure 44 - 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:

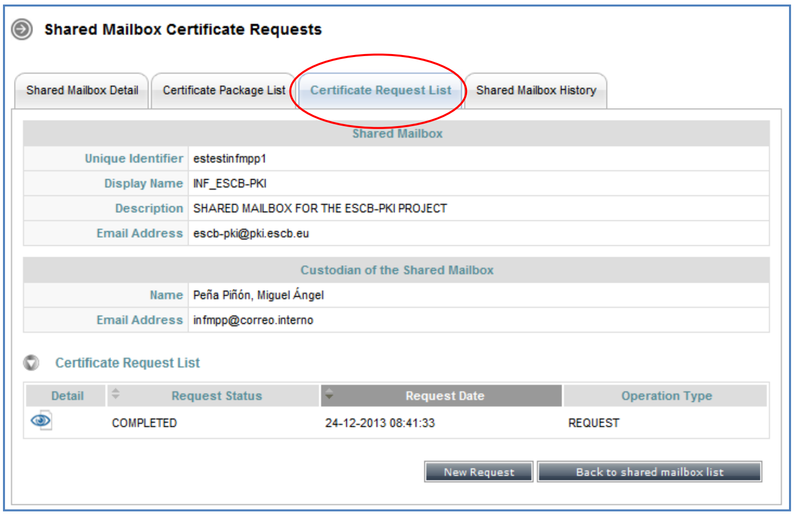
- ***Certificate download*** Clicking the button a copy of the certificate (**only public information**) will be downloaded to be locally stored in a file (a .cer file containing the certificate). It is important to notice that the private key will not be provided.
- ***Certificate suspension/reactivation***[2] Clicking the ***Suspend/Reactivate*** button you will suspend/reactivate the certificate.
- ***Certificate revocation*** Clicking the ***Revoke*** button you will revoke the certificate.
- ***Certificate Package History*** This tab shows the activity associated with this certificate.

[2] A suspended certificate will be revoked after 60 days of its suspension.

3.3.3. 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	
Unique Identifier	estestinfmpp1
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	infmpp@correo.interno

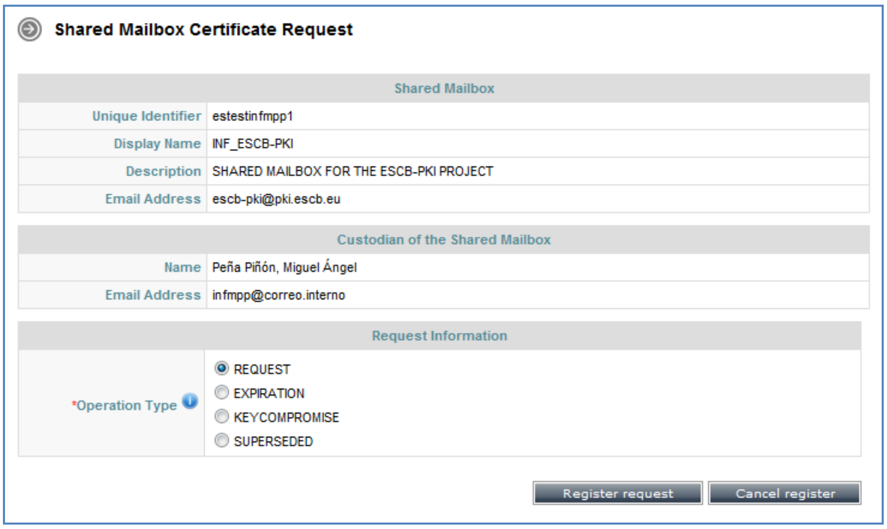
Certificate Request List

Detail	Request Status	Request Date	Operation Type
	COMPLETED	24-12-2013 08:41:33	REQUEST

Figure 45 - Shared mailbox certificate requests list

Clicking the **New Request** button initiates the request of a new certificate for the shared mailbox.

Very important: in order to ensure the 4-eyes principle, a different person that the one who requests the certificate for the shared mailbox has to approve the requests. However, only the requestor will be allowed to process the request (i.e. to download the certificate), once that it has been approved.



Shared Mailbox	
Unique Identifier	estestinfmpp1
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	infmpp@correo.interno

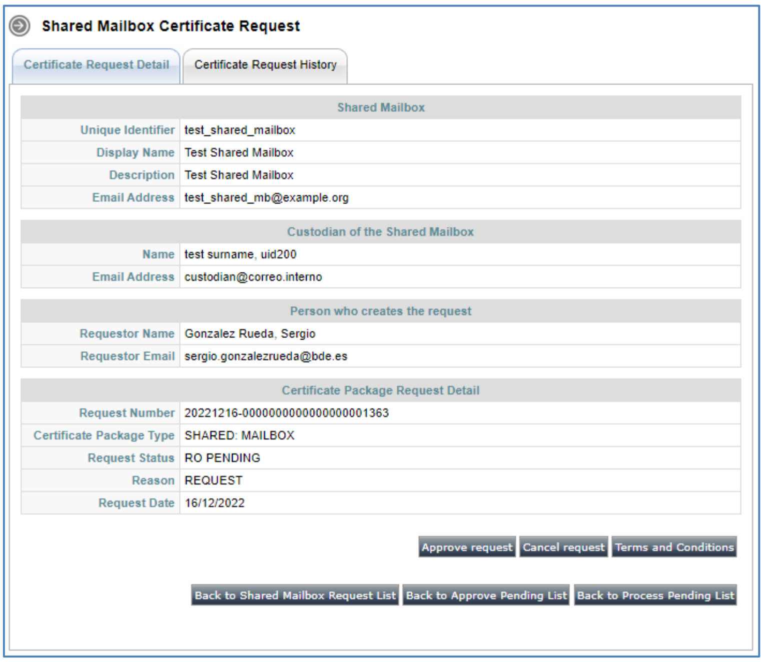
Request Information	
*Operation Type	● REQUEST ○ EXPIRATION ○ KEYCOMPROMISE ○ SUPERSEDED

Figure 46 - New shared mailbox certificate request

You have to indicate the reason of the new request:

- ***Request*** This is the first time that a certificate is being requested for this shared mailbox
- ***Expiration*** This shared mailbox has got a certificate that is going to expire soon
- ***Key compromise*** The private key linked to the certificate that this shared mailbox has got has been compromised
- ***Superseded*** This shared mailbox has got a certificate that has been superseded (e.g some of the information included in the certificate has changed)

In the certificate list tab, you can click the 👁 button to access the certificate request details:


Shared Mailbox Certificate Request
Certificate Request Detail
Certificate Request History
Approve request
Cancel request
Terms and Conditions
Back to Shared Mailbox Request List
Back to Approve Pending List
Back to Process Pending List

Shared Mailbox	
Unique Identifier	test_shared_mailbox
Display Name	Test Shared Mailbox
Description	Test Shared Mailbox
Email Address	test_shared_mb@example.org

Custodian of the Shared Mailbox	
Name	test surname, uid200
Email Address	custodian@correo.interno

Person who creates the request	
Requestor Name	Gonzalez Rueda, Sergio
Requestor Email	sergio.gonzalezrueda@bde.es

Certificate Package Request Detail	
Request Number	20221216-0000000000000000001363
Certificate Package Type	SHARED: MAILBOX
Request Status	RO PENDING
Reason	REQUEST
Request Date	16/12/2022

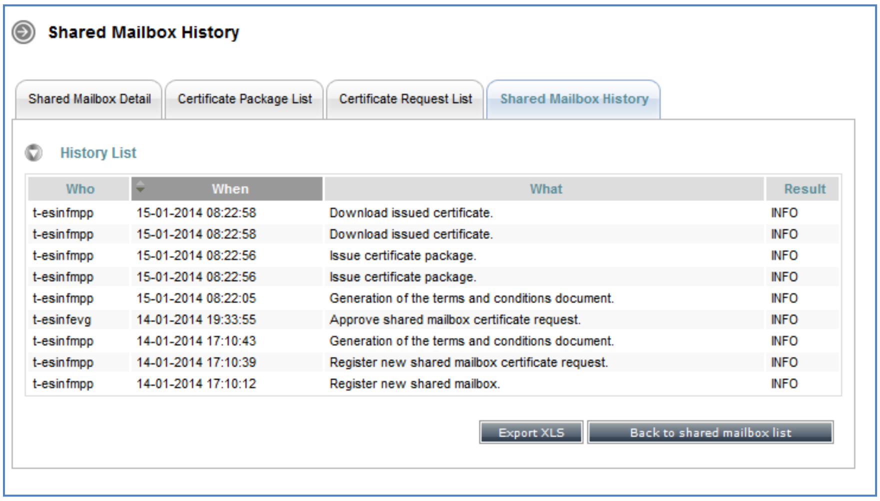
Figure 47 - Shared mailbox certificate request details

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

- ***Terms and Conditions*** To check if the shared mailbox custodian has signed the *Terms and Conditions* document
- ***Approve request*** To approve the certificate request (very important: to ensure the 4-eyes principle, only a different person than the one that created the request can approve it)
- ***Process request*** To process the certificate request and download the certificate once it has been approved (very important: only the person that requested the certificate can download it once that the request has been approved)
- ***Cancel request*** To cancel the certificate request
- ***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.

3.3.4. SHARED MAILBOX HISTORY

Displays all the activity related to the shared mailbox.

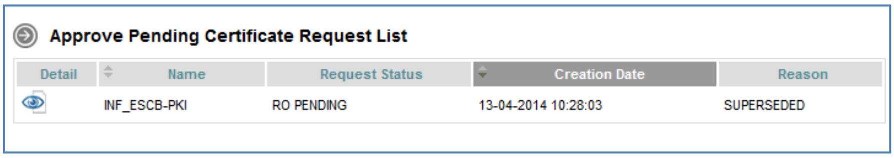


Who	When	What	Result
t-esinfmpp	15-01-2014 08:22:58	Download issued certificate.	INFO
t-esinfmpp	15-01-2014 08:22:58	Download issued certificate.	INFO
t-esinfmpp	15-01-2014 08:22:56	Issue certificate package.	INFO
t-esinfmpp	15-01-2014 08:22:56	Issue certificate package.	INFO
t-esinfmpp	15-01-2014 08:22:05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

Figure 48 - Shared mailbox activity

3.4. APPROVE PENDING SHARED MAILBOX CERTIFICATE REQUESTS

From the ***Shared mailbox > Approve pending*** option you can access to all pending shared mailbox certificate requests for your Central Bank.

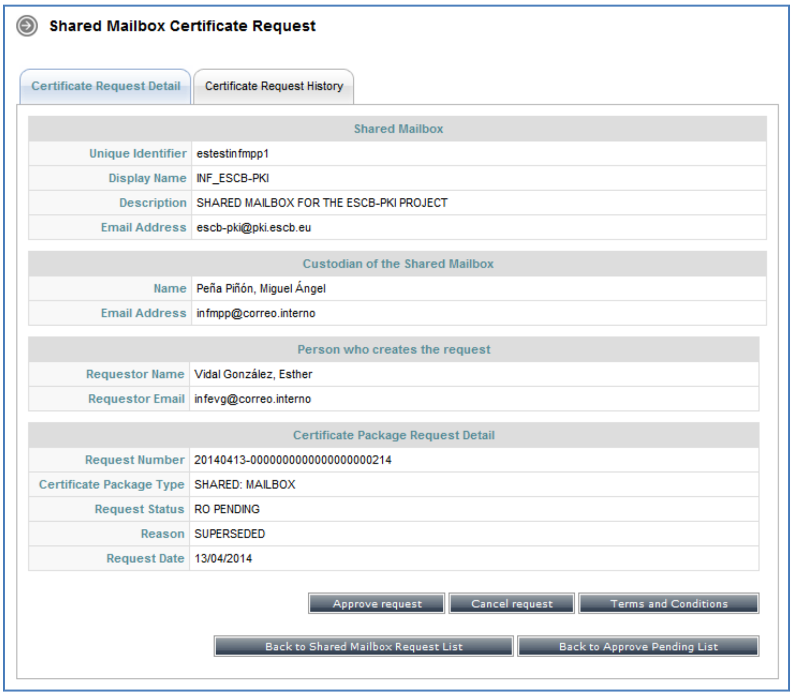


Approve Pending Certificate Request List

Detail	Name	Request Status	Creation Date	Reason
👁	INF_ESCB-PKI	RO PENDING	13-04-2014 10:28:03	SUPERSEDED

Figure 49 - Shared mailbox certificate requests pending to approve

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



Shared Mailbox Certificate Request

Shared Mailbox	
Unique Identifier	estestinfmpp1
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	infmpp@correo.interno

Person who creates the request	
Requestor Name	Vidal González, Esther
Requestor Email	infevg@correo.interno

Certificate Package Request Detail	
Request Number	20140413-0000000000000000000214
Certificate Package Type	SHARED: MAILBOX
Request Status	RO PENDING
Reason	SUPERSEDED
Request Date	13/04/2014

Approve request
Cancel request
Terms and Conditions
Back to Shared Mailbox Request List
Back to Approve Pending List

Figure 50 - Shared mailbox certificate request detail

The status of the request can be:

- ***RO-Pending*** A Registration Officer has to approve the request
- ***User-Pending*** The shared mailbox certificate requestor can generate and download the certificates. A different person acting as RO has already approved the request

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

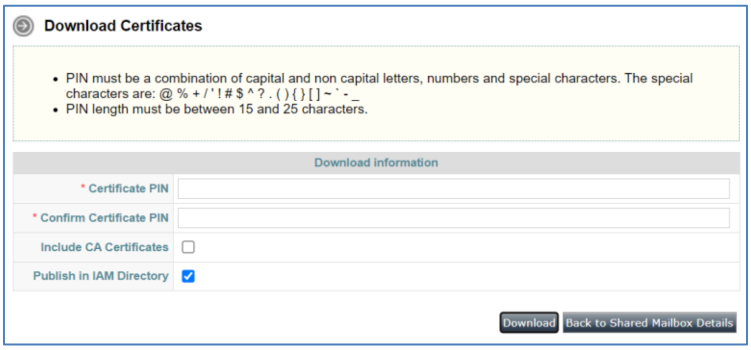
- ***Terms and Conditions*** To check if the shared mailbox custodian has signed the *Terms and Conditions* document
- ***Approve request*** To approve the certificate request (very important: to ensure the 4-eyes principle, only a different person than the one that created the request can approve it)
- ***Process request*** To process the certificate request once that it has been approved and download the certificate (very important: only the person that requested the certificate can download it once that the request has been approved)

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

3.4.1. GENERATE AND DOWNLOAD SHARED MAILBOX CERTIFICATES

This section describes how to download a shared mailbox certificate. This process is initiated only by the person who requested the certificate and once that another person, acting as Registration Officer, has approved the request.

1. The process is initiated by clicking the ***Process Request*** button from the shared mailbox certificate request details. This can be done only by the person who requested the certificate. The following screen will be shown:



Download Certificates

- PIN must be a combination of capital and non capital letters, numbers and special characters. The special characters are: @ % + / ' ! # $ ^ ? . ( ) { } [ ] ~ ` - _
- PIN length must be between 15 and 25 characters.

Download information	
* Certificate PIN	
* Confirm Certificate PIN	
Include CA Certificates	□
Publish in IAM Directory	☑

Figure 51 - Download shared mailbox certificate

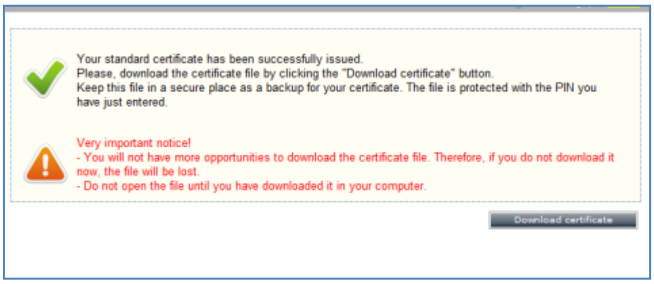
Enter a PIN to protect the shared mailbox certificate file

- PIN length must be between 15 and 25 characters.
- PIN is a combination of capital and non capital letters, numbers and special characters (special characters are @ % + / ‘ ! # $ ^ ? . ( ) { } [ ] ~ ` - _)

Check the *Include CA Certificates* option if you wish that the certificate file includes the certificates of the root and subordinate CAs

Check the *Publish in IAM Directory* option if you wish that a copy of the certificate (only the public part) is published in IAM Directory so that the certificate is automatically mapped to the corresponding IAM account

2. Click the ***Download*** button. The certificate will be generated



Your standard certificate has been successfully issued.
Please, download the certificate file by clicking the "Download certificate" button.
Keep this file in a secure place as a backup for your certificate. The file is protected with the PIN you have just entered.

Very important notice!
- You will not have more opportunities to download the certificate file. Therefore, if you do not download it now, the file will be lost.
- Do not open the file until you have downloaded it in your computer.

Figure 52 - Shared mailbox certificate generated

3. Click the ***Download certificate*** button to store the certificate.

4. A File Download dialog box will pop up. Click the **SAVE** button to download the keys.

   ⚠ **Important notice!**
   If you select the **OPEN** option (instead of **SAVE**) Windows will automatically start the installation of the certificate in your PC.

The certificate will be saved, protected by the PIN, to ensure that only the shared mailbox custodian and authorised users can access to the private key.

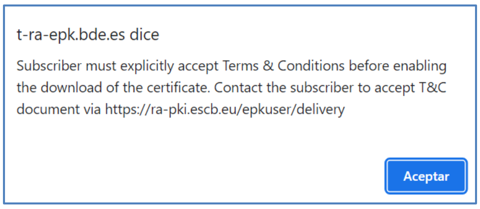
5. Handle the file to the shared mailbox custodian and recommend him to keep this file as a backup copy of the certificate. This will permit him to recover the certificate in the future and to provide a copy to the authorised users.

3.4.2. VERIFY TERMS AND CONDITIONS ACCEPTANCE

Before delivering a certificate, shared mailbox custodians must formally accept their responsibilities by signing the Terms and Conditions document online. This option will allow you to check if the user has signed the Terms and Conditions document or not.

After clicking the ***Terms and Conditions*** button a dialog box will pop up.

In case the custodian has not signed the document yet, the following pop up would appear:

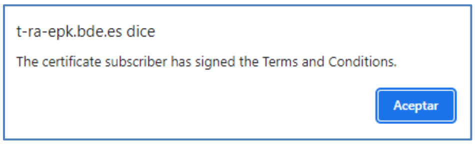


t-ra-epk.bde.es dice

Subscriber must explicitly accept Terms & Conditions before enabling the download of the certificate. Contact the subscriber to accept T&C document via https://ra-pki.escb.eu/epkuser/delivery

Figure 53 - Terms and Conditions not accepted yet pop up

If the custodian has accepted and signed the Terms and Conditions document, then the pop up would look like this:



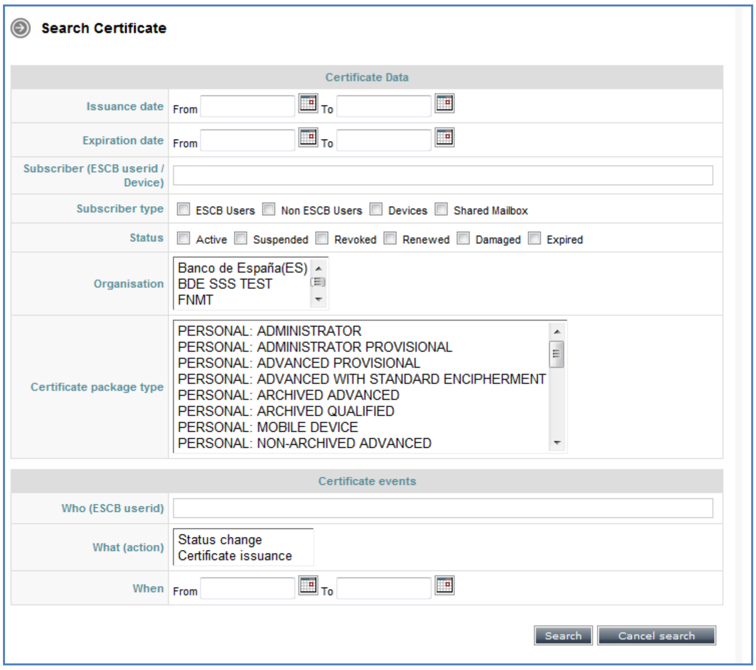
t-ra-epk.bde.es dice

The certificate subscriber has signed the Terms and Conditions.

Figure 54 - Terms and Conditions already accepted pop up

3.5. CERTIFICATES AUDIT

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

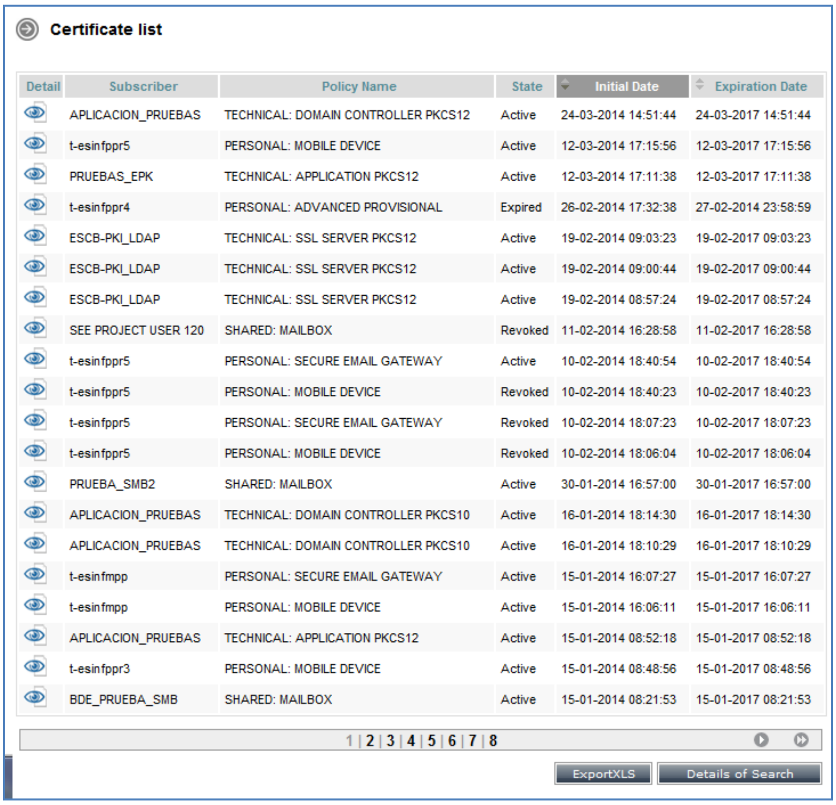


Search Certificate

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 55 - 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

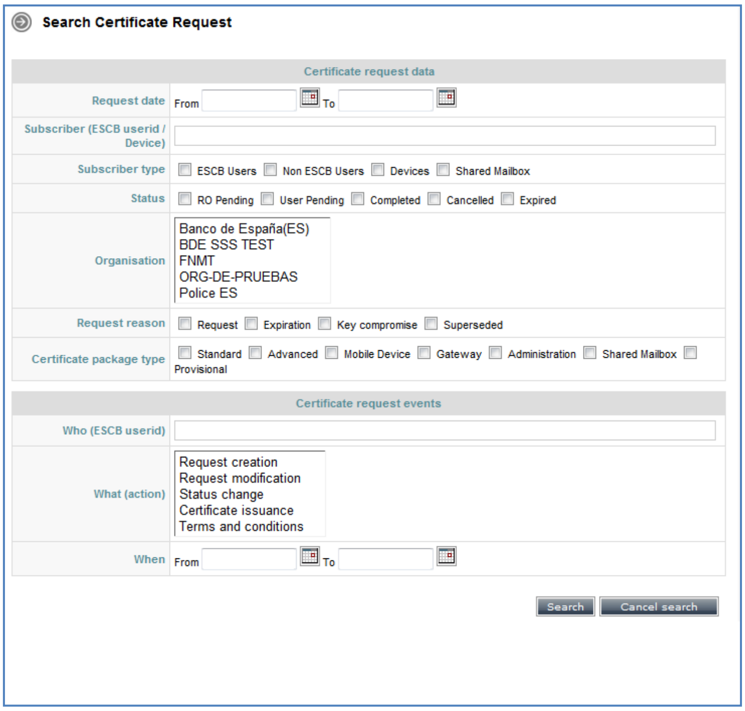
Figure 56 - Certificates list

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.

3.6. CERTIFICATE REQUESTS AUDIT

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

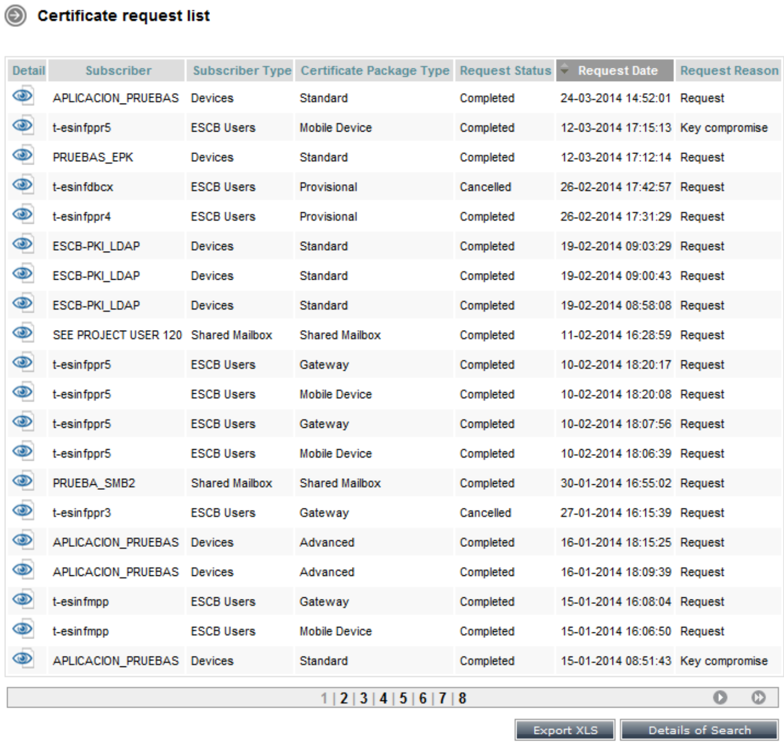


Search Certificate Request

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 57 - 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

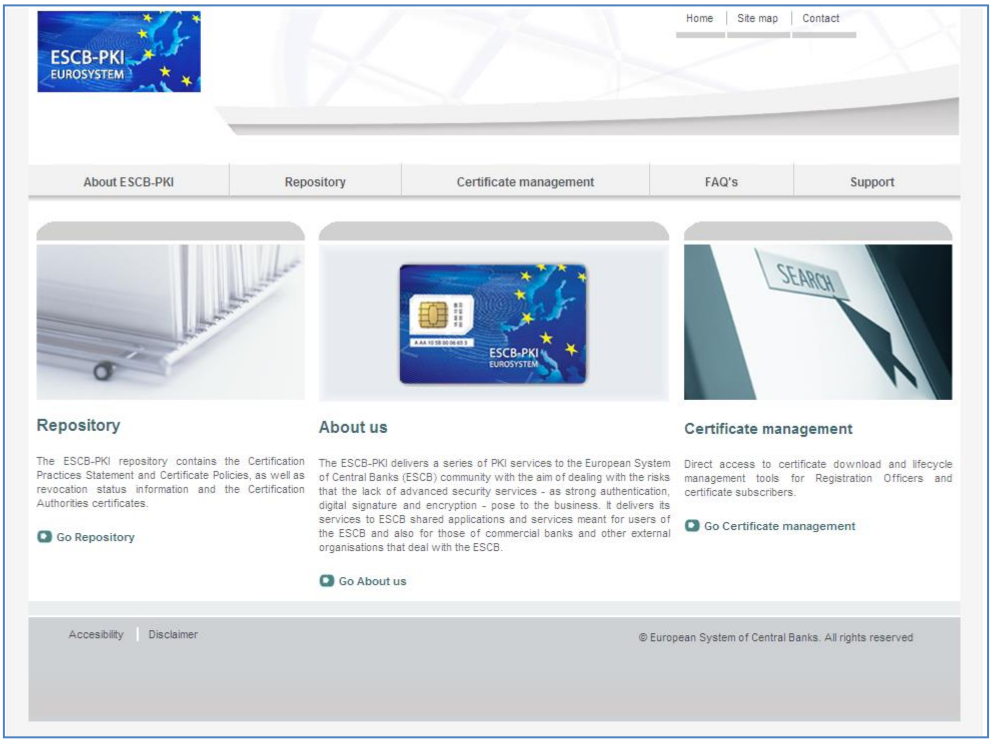
Figure 58 - Certificate requests list

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 59 - 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.