

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI PROJECT



ESCB-PKI REGISTRATION AUTHORITY APPLICATION

SUBSCRIBER'S MANUAL

VERSION 4.1

TABLE OF CONTENTS

GLOSSARY AND ACRONYMS 5

1. Introduction 6

 1.1. The ESCB-PKI Website 6

2. The ESCB-PKI Registration Authority application 7

 2.1. System requirements 7

 2.2. Layout 7

 2.3. Access 9

 2.3.1. Certificate delivery for remote users 10

 2.3.2. Personal certificate management 11

 2.3.3. Certificate suspension 12

3. User details 13

4. Certificate requests 14

 4.1. Sign Terms and Conditions 15

 4.2. Generate and download software-based certificates 17

 4.3. Generate and download token-based certificates 18

5. Certificates 22

6. Suspension code 24

7. More information about ESCB-PKI 25

8. Annex 1. Table of operations 26

TABLE OF ILLUSTRATIONS

Figure 1 - ESCB-PKI Website..... 6

Figure 2 - Production frame..... 7

Figure 3 - Acceptance frame 8

Figure 4 - Certificate management 8

Figure 5 - ESCB-PKI Website - Registration Authority Application..... 9

Figure 6 - Certificate request list 10

Figure 7 - Personal certificates management 11

Figure 8 - Certificate List 12

Figure 9 - User details 13

Figure 10 - Register personal information 13

Figure 11 - Certificate request list 14

Figure 12 - Certificate request details..... 14

Figure 13 - Terms and Conditions acceptance form..... 16

Figure 14 - Software-based certificate download 17

Figure 15 - File protection PIN..... 17

Figure 16 - Software-based certificate generated 17

Figure 17 - Token-based certificate request 18

Figure 18 - Invalid token 18

Figure 19 - Token-based certificates download..... 19

Figure 20 - Token-based certificates generation..... 19

Figure 21 - Introduce PIN code 19

Figure 22 - Public/private keys generation..... 20

Figure 23 - Token-based certificates successfully generated..... 20

Figure 24 - Storing certificates 20

Figure 25 - Token-based certificates successfully stored 20

Figure 26 - Certificate list..... 22

Figure 27 - Certificate details 22

Figure 28 - Set the suspension code 24

Project name:	ESCB-PKI
Author:	ESCB-PKI Project team
File name:	ESCB-PKI - RA Application Subscriber's Manual v.4.1.docx
Version:	4.1
Date of issue:	20.12.2022
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
0.02	Draft	20.10.2011	Several additions
0.03	Draft	31.10.2011	BdE Revision
0.12	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	29.10.2012	Adaptation to the legal framework
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

GLOSSARY AND ACRONYMS

Acronym	Definition
CA	Certificate Authority
CB	ESCB Central Bank (ECB or NCB)
CP	Certification Policies
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 (whatever 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
RO	Registration Officer
RA	Registration Authority

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 that delivers a series of PKI services to ESCB and non-ESCB members.

1.1. THE ESCB-PKI WEBSITE

From this Website you can have access to the ESCB-PKI services and you can also find additional information connected to certificate management, token management and Public Key Infrastructures.

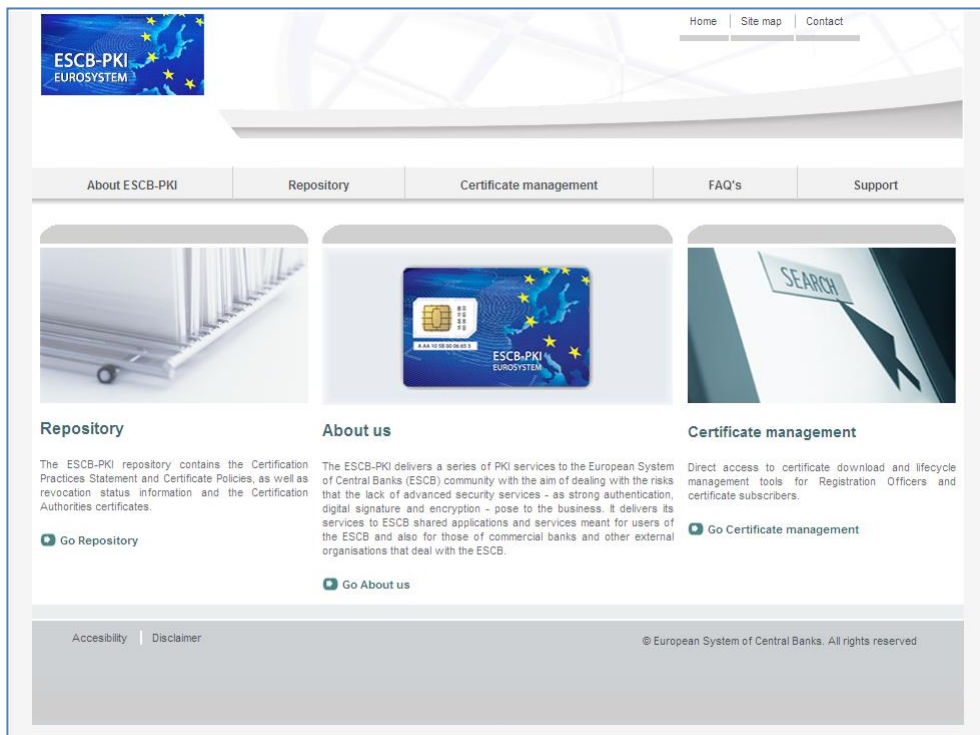


Figure 1 - ESCB-PKI Website

To access to the ESCB-PKI services, open your web browser and type the following URL address, <https://pki.escb.eu/>. You will find the following information:

- **About ESCB-PKI** Generic information with regards to the ESCB-PKI services
- **Repository** ESCB-PKI public information: Certificate Practice Statement (CPS) document, Certificate Policy (CP) documents, Certificate Authority (CA)certificates , Certificate Revocation Lists (CRLs), etc.
- **Certificate management** ESCB-PKI Registration Authority application and guidelines
- **FAQ** Frequently Asked Questions
- **Support** Software needed to manage ESCB-PKI tokens and utilities to test ESCB-PKI certificates

2. THE ESCB-PKI REGISTRATION AUTHORITY APPLICATION

2.1. SYSTEM REQUIREMENTS

The following software is required to use the ESCB Registration Authority application:

- ESCB-PKI Smartcard drivers
- Native application required to manage certificates in a smart card.
- One of the following web extensions of your choice, according to your browser preferences:
 - Mozilla Firefox ESCB-PKI Certificate Enrollment extension.
 - Chrome and Edge ESCB-PKI Certificate Enrollment extension.

Instructions on the installation of the aforementioned software are available in the ESCB-PKI User guide - Browser configuration, which may be downloaded from the ESCB-PKI portal support area:

<https://pki.escb.eu/epkweb/en/support.html>

The following browsers have been thoroughly tested and are therefore recommended:

- Internet Explorer 11
- Google Chrome 94
- Mozilla Firefox 92
- Microsoft Edge 95

Note. - “JavaScript” and “Cookies” must be enabled in the web browser for the application to work properly.

2.2. LAYOUT

Please be aware that two different ESCB-PKI 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.

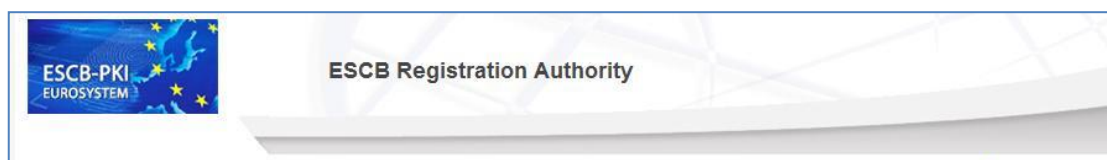


Figure 2 - Production frame



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

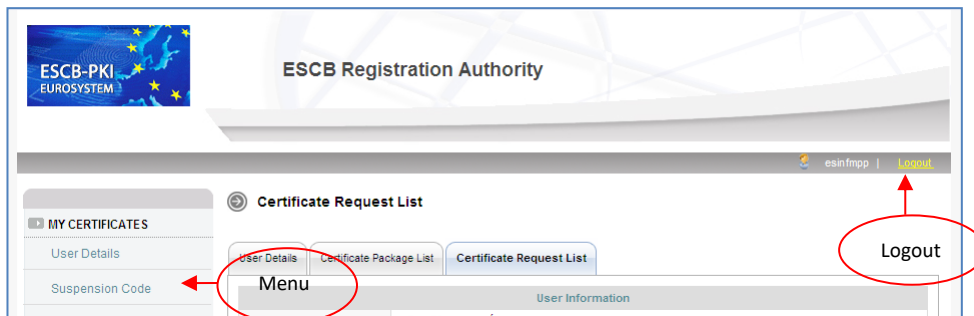


Figure 4 - Certificate management

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 to certificate subscribers

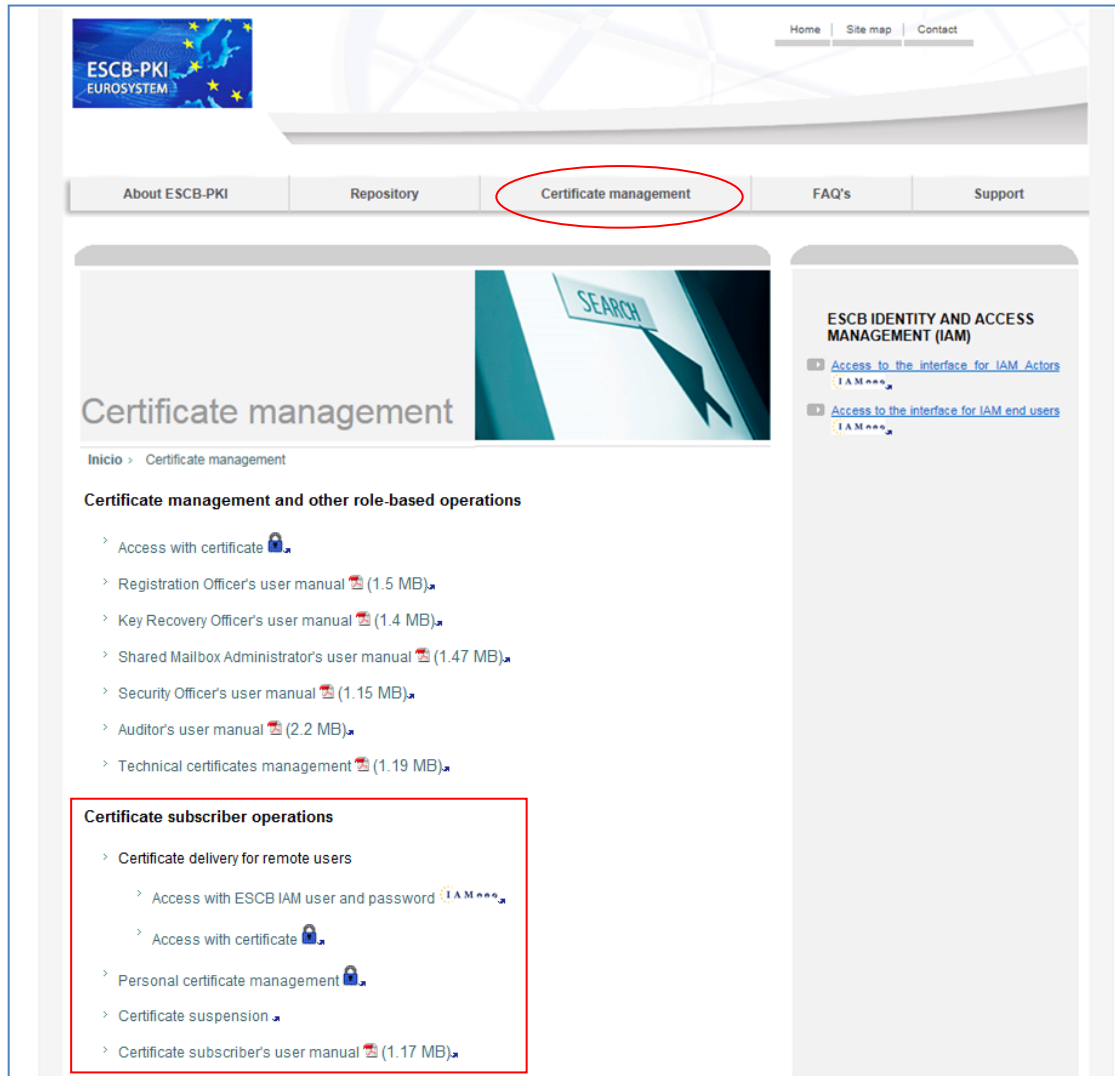


Figure 5 - ESCB-PKI Website - Registration Authority Application

There are three different links available to ESCB-PKI subscribers:

Link	Use this option when you ...	Credentials required
Certificate delivery for remote users	.. do not have any CAF-compliant certificate to authenticate, for example, the first time you request a certificate or when your personal secure token is lost or stolen	IAM user-id and password OR ESCB accepted certificate (CAF compliant)
Personal certificate management	.. have an advanced CAF-compliant certificate (i.e. your token based ESCB-PKI certificate) to authenticate	ESCB accepted advanced certificate (CAF compliant)
Certificate suspension	... want to suspend your certificates and you do not have any CAF-compliant certificate to authenticate (i.e. token lost or stolen) and you do not remember your IAM password	IAM user-id and your personal ESCB-PKI suspension code

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

2.3.1. CERTIFICATE DELIVERY FOR REMOTE USERS

You will use this link to manage your certificates and certificate requests when you do not have any CAF-compliant certificate to authenticate. This link will initially display all certificate requests currently associated with you and their status:

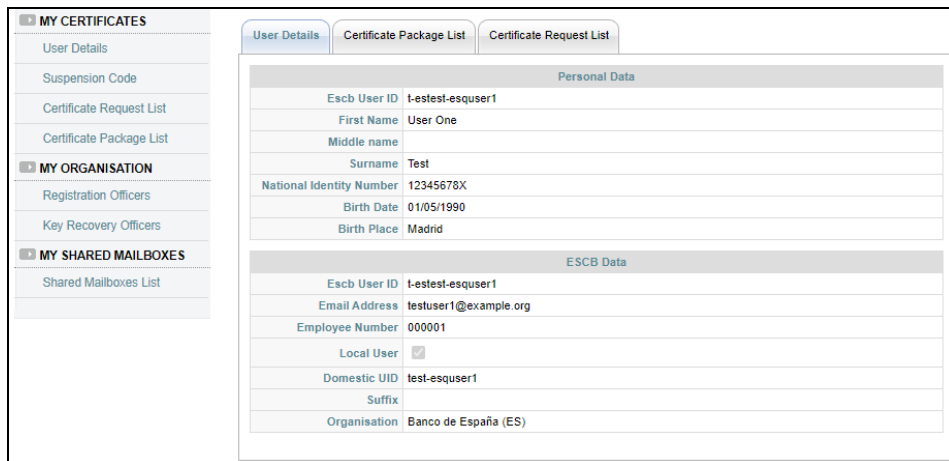


Figure 6 - Certificate request list

The following options will be available from the left frame menu (or from the tabs):

- **User Details** Selecting this option you will be able to check your personal information and manage your personal certificates and certificate requests
- **Suspension code** This option will allow you to set your personal suspension code

- **Certificate Request list** Selecting this option you will be able to check your certificate requests and perform the following operations
 - Cancel the request
 - Download your certificates provided an RO has authorized you the remote download
- **Certificate Package list** Selecting this option you will be able to check your certificates and perform the following operations
 - Suspend your certificates in case you suspect they have been compromised

Next chapters will further elaborate on these options.

2.3.2. PERSONAL CERTIFICATE MANAGEMENT

You will use this link to manage your certificates and certificate requests when you have a CAF-compliant certificate to authenticate. This link will initially display your personal data:

Personal Data	
Escb User ID	l-estest-esquser1
First Name	User One
Middle name	
Surname	Test
National Identity Number	12345678X
Birth Date	01/05/1990
Birth Place	Madrid

ESCB Data	
Escb User ID	l-estest-esquser1
Email Address	testuser1@example.org
Employee Number	000001
Local User	<input checked="" type="checkbox"/>
Domestic UID	test-esquser1
Suffix	
Organisation	Banco de España (ES)

Figure 7 - Personal certificates management

Four options will be available from the left frame menu (or from the tabs):

- **User Details** Selecting this option you will be able to check your personal information and manage your personal certificates and certificate requests
- **Suspension code** This option will allow you to set your personal suspension code
- **Certificate Request list** Selecting this option you will be able to check your certificate requests and perform the following operations
 - Cancel the request
 - Download your certificates provided an RO has authorized you the remote download
- **Certificate Package list** Selecting this option you will be able to check your certificates and perform the following operations
 - Suspend your certificates in case you suspect they have been compromised
 - Recover your old encryption keys

Next chapters will further elaborate on these options.

2.3.3. CERTIFICATE SUSPENSION

You will use this link to suspend your ESCB-PKI certificates when you do not have any CAF-compliant certificate to authenticate (i.e. token lost or stolen) and you do not remember your IAM password. This link will display ESCB-PKI certificates currently associated with your user-id and their status:

The screenshot shows a web interface for 'MY CERTIFICATES'. On the left is a navigation menu with 'Certificates' selected. The main content area is titled 'Certificate Package List' and includes a 'User Information' section with the name 'ESPAÑOL ONE, Fulanto'. Below this is a table listing certificate packages.

Detail	Policy Name	Cryptographic Device	State	Initial Date	Expiration Date
	ADVANCED_ARCHIVED_ESCB_POLICY	42430F5172A36495	ACTIVE	10-02-2012	10-02-2015
	ADVANCED_ARCHIVED_ESCB_POLICY	42430F5172A36495	REVOKED	09-02-2012	09-02-2015
	STANDARD_ESCB_POLICY		REVOKED	08-02-2012	08-02-2015

Figure 8 - Certificate List

One option will be available from the left frame menu

- **Certificates**
 - Check your certificates and perform the following operations
 - Suspend your certificates in case you suspect they have been compromised

Next chapters will further elaborate on this option.

3. USER DETAILS

Displays the user attributes (first name, surname, user-id, etc.) and the information of the organisation you belong to.

The screenshot shows a web interface titled "UserDetails" with three tabs: "User Details" (highlighted with a red circle), "Certificate Package List", and "Certificate Request List". Below the tabs are two data tables.

Personal Data	
Escb User ID	uid200
First Name	name
Middle name	middlename
Surname	surname
National Identity Number	
Birth Date	
Birth Place	

ESCB Data	
Escb User ID	uid200
Email Address	qtamomx@correo.interno
Employee Number	
Local Upn	
Organisation	Banco de España (ES)

Figure 9 - User details

NOTE: User attributes not completed

Before issuing any certificate the RA application must ensure that all the personal information required to uniquely identify you is registered in the system.

In particular the place and date of birth and/or the number of your identification document (i.e. national identity number, passport number, driver license number, etc.) could be missing, as this information is not registered in the IAM directory and therefore not imported by ESCB-PKI system.

In this event, the application will prompt you to introduce either your national identity number or your place and date of birth.

The screenshot shows a form titled "User birth information register". At the top, there is a yellow warning box with a red triangle icon containing an exclamation mark. The text in the box reads: "The following fields are missing: - National identification number - Birth place and birth date". Below this, it says: "At least one of these fields is required to identify a user before issuing ESCB-PKI certificates. Please, complete the information to continue."

The form is divided into two sections:

- User information:** Contains a field for "Name" with the value "F name, Surname".
- Pending information:** Contains three fields:
 - "National Identity Number": A text input field.
 - "Birth Date and Birth Place": A section containing two sub-fields: "Birth Date" (with a calendar icon) and "Birth Place" (with a location pin icon).

A "Register" button is located at the bottom right of the form.

Figure 10 - Register personal information

4. CERTIFICATE REQUESTS

This option displays all certificate requests currently associated with you

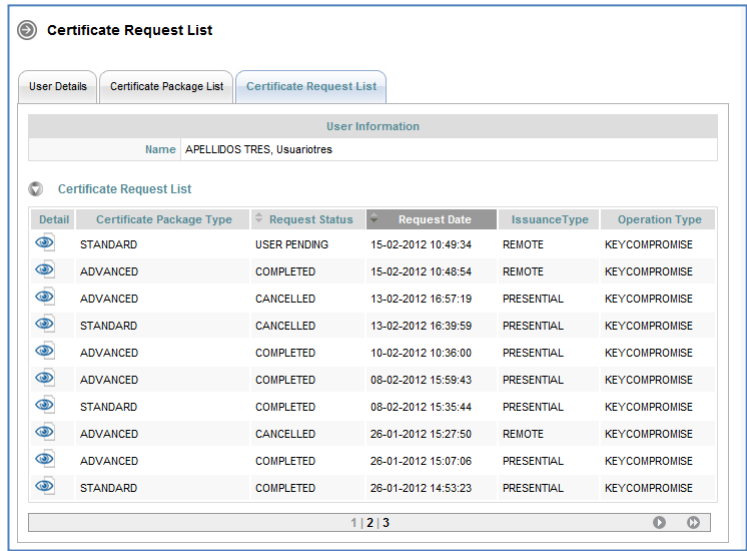


Figure 11 - Certificate request list

and their status:

- **Completed** The request has been processed and certificates have been generated
- **Cancelled** The request has been cancelled
- **Expired** The request has expired
- **RO-Pending** The RO shall still process the request or Terms and Conditions document must be signed
- **User-Pending** The user can generate and download the certificates. The RO has already handled the request and has allowed a remote download

Clicking the button the details of the certificate request are displayed

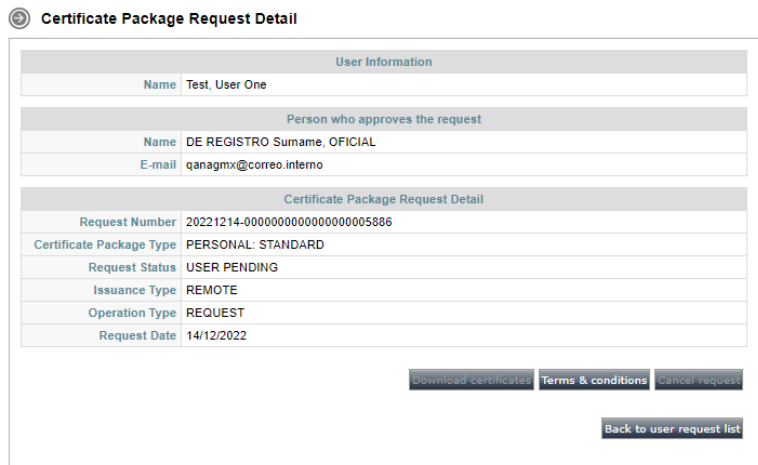


Figure 12 - Certificate request details

You may choose from the following operations:

- **Terms and Conditions** If the request is still in RO_PENDING state the **Terms and Conditions** button will be available in order to sign the Terms and Conditions document online
- **Certificate generation/download** If the status of the request is **User-Pending** a **Download** button will be available to generate and download the certificates
- **Modify device** To update the serial number of the device if necessary (this button will be only available for advanced certificate requests when the status of the request is Ro-pending)
- **Cancel request** If the status of the request is **RO-Pending** the **Cancel request** button will be available to cancel this request

4.1. SIGN TERMS AND CONDITIONS

You must formally accept your responsibilities by signing the Terms and Conditions document, this option will let you do this. When clicking on the “Terms & conditions” button, the document will appear as shown in the next figure. You have to accept the checkbox “I have read and agree to the Terms and Conditions” and then click on the “Sign” button to complete the signature.

4.2. GENERATE AND DOWNLOAD SOFTWARE-BASED CERTIFICATES

This option will only be available if the status of the request is **User-Pending**. The next figure shows the information displayed when you select the download button for standard certificates.

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	<input type="checkbox"/>	N/A

Accept Back to request detail

Figure 14 - Software-based certificate download

- To initiate the process you must click the **Accept** button.
- 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	<input type="text"/>
*Confirm Certificate PIN	<input type="text"/>


Download Back to user request list Back to User Details


Figure 15 - File protection PIN

Type your selected PIN:

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

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


 Your software-based certificate has been issued successfully. 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.

Download certificate

Figure 16 - Software-based 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 recommended procedure is to save this file, keep it as a backup copy and, afterwards, start the installation process (opening the file). Detailed information for the installation process is available at "User guide: importing and exporting standard certificates" document which is available in the ESCB-PKI Website.

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

6. Keep this file as a backup copy of the certificate. This will permit you to recover the certificate in the future, in case it gets damaged.

4.3. GENERATE AND DOWNLOAD TOKEN-BASED CERTIFICATES

This option will only be available if the status is **User-Pending**.



The screenshot shows a web form titled "Certificate Package Request Detail". It is divided into three sections:

- User Information:** Name: APELLIDOS TRES, Usuariotres
- Requestor details:** Requestor name: Apellido1 Apellido2, Peticionario; Requestor mail: petionario.apellido1@bde.es
- Certificate Package Request Detail:** Certificate Package Type: ADVANCED; Cryptographic Device: 0000481555AF131E; Request Status: USER PENDING; Issuance Type: REMOTE; Operation Type: KEYCOMPROMISE; Request Date: 15/02/2012

At the bottom of the form, there are three buttons: "Download", "Terms and conditions", and "Back to request list".

Figure 17 - Token-based certificate request

1. Insert your 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.

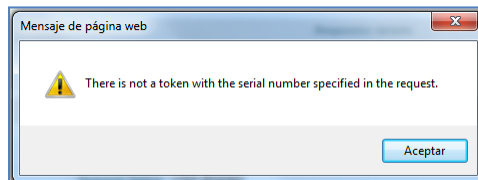


Figure 18 - Invalid token

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

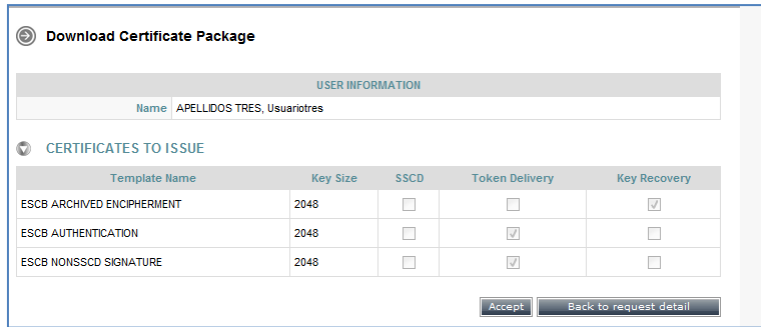


Figure 19 - Token-based certificates download

- In order to initiate the process, click the **Accept** button. The whole process will take a few minutes because, in the case of the advanced certificate package, three key-pairs will be generated (authentication, encryption and signing) and stored in your token.

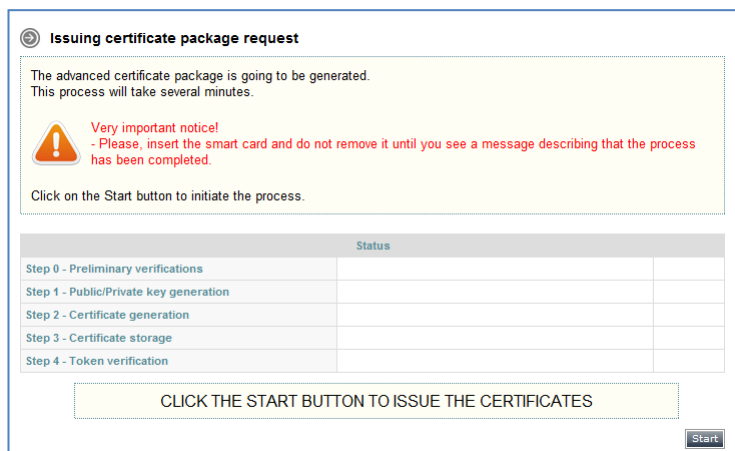


Figure 20 - Token-based certificates generation

- Click the **Start** button.
- The system will prompt you to enter the PIN of the token.

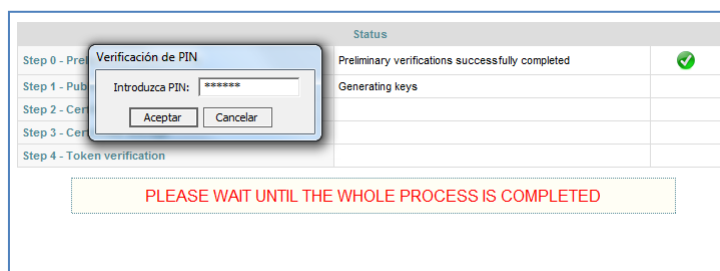


Figure 21 - Introduce PIN code

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

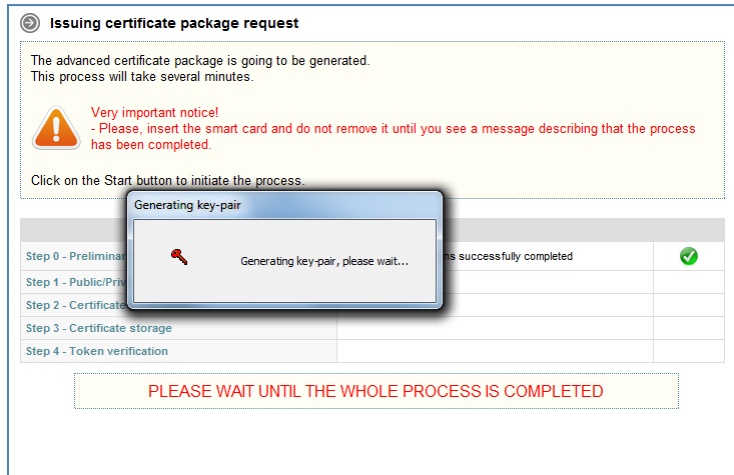


Figure 22 - Public/private keys generation

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

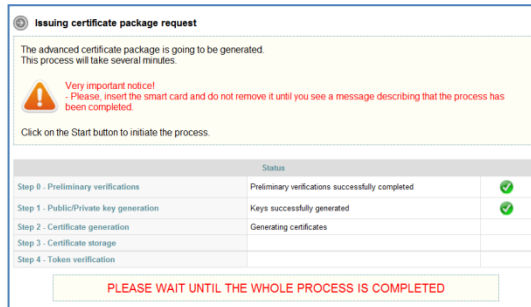


Figure 23 - Token-based certificates successfully generated

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

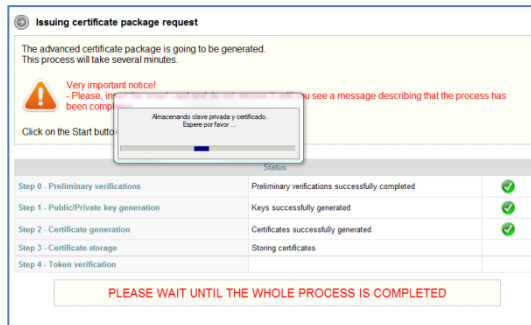


Figure 24 - Storing certificates

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

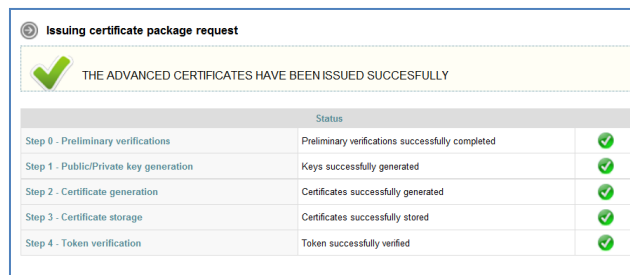


Figure 25 - Token-based certificates successfully stored

5. CERTIFICATES

Displays all ESCB-PKI certificates currently associated with your user-id

User Information					
Name: ESPANOL ONE, Fulanito					
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
	STANDARD_ESCB_POLICY		ACTIVE	08-02-2012	08-02-2015
	ADVANCED_ARCHIVED_ESCB_POLICY	42430F5172A36495	REVOKED	08-02-2012	08-02-2015
	ADVANCED_ARCHIVED_ESCB_POLICY	42430F5172A36495	REVOKED	07-02-2012	07-02-2015

Figure 26 - Certificate list

and their status:

- **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

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.

After clicking a certificate package the certificate details will be displayed:

Certificate Package Detail

Certificate Package Information

Policy	QUALIFIED_ARCHIVED_ESCB_POLICY
Cryptographic Device	021029BB80121A1A
Expiration Date	23/01/2015
Request Date	23/01/2012
Certificate Package Status	ACTIVE

Certificate List

Serial Number	Template Name	Download	Recover Keys
2555eb1e0fb47eab4f1da01800f1d6fb	ESCB AUTHENTICATION		
4cc8034b7632a4a34f1da019b943ae6b2	ESCB SSCD SIGNATURE		
4fb28f98e33181074f1da0179d6a80ae	ESCB ARCHIVED ENCIPHERMENT		

Download certificate
Recover Key

Suspend all certificates

Figure 27 - Certificate details

And you may 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 your certificate). It is important to notice that the private key will not be provided

- **Key recovery** This option will only be activated (blue color) for encryption certificates if the key recovery option has been authorised by your Central Bank

NOTE. - Only available from the **Personal Certificate management** link

- **Certificate suspension** Clicking this button you will suspend all the certificates contained in this package. When the action is processed the certificate validity is suspended temporarily

NOTE. - **Certificate reactivation must be requested by an ESCB-PKI Registration Officer**

6. SUSPENSION CODE

Bear in mind that the suspension code will be the only way to identify you if your personal secure token is lost or stolen and you do not remember your IAM password. You will use this code to request the suspension of your certificates.

From the Suspension Code option you can set your personal suspension code.

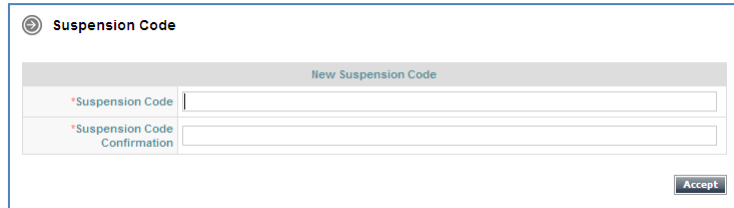
The screenshot shows a web form titled "Suspension Code" with a back arrow icon. Below the title is a header "New Suspension Code". There are two input fields: the first is labeled "*Suspension Code" and the second is labeled "*Suspension Code Confirmation". Both fields have a red asterisk indicating a required field. At the bottom right of the form is a button labeled "Accept".

Figure 28 - Set the suspension code

- Type your suspension code and then click the **Accept** button.
 - Length must be between 8 and 15 characters.
 - Must be a combination of capital and non-capital letters, numbers and special characters (special characters are: @ % + / ! # \$ ^ ? . () { } [] ~ ` - _)

7. MORE INFORMATION ABOUT ESCB-PKI

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

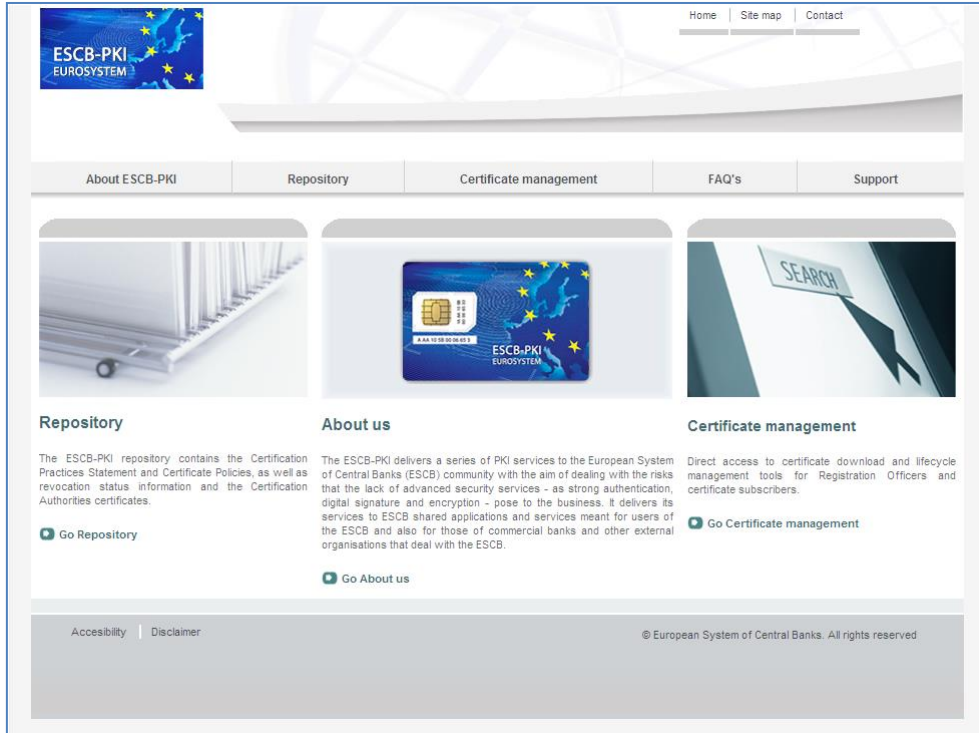


Figure 29 - ESCB-PKI Website

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.

8. ANNEX 1. TABLE OF OPERATIONS

Menu options		RA application links		
		Certificate delivery for remote users	Personal certificate management	Certificate suspension
User Details		✓	✓	
Certificate Request	Term and conditions	✓	✓	
	Certificate generation and download	✓	✓	
	Modify device	✓	✓	
	Cancel request	✓	✓	
Suspension Code			✓	
Certificates	Certificate download	✓	✓	✓
	Certificate suspension	✓	✓	✓
	Key recovery		✓	