BANCO DE ESPAÑA
Eurosistema

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI PROJECT

TECHNICAL CERTIFICATES MANAGEMENT

VERSION 3.1

ECB-Restricted
07-Nov-2024

TABLE OF CONTENTS

TABLE OF ILLUSTRATIONS

Project name:	ESCB-PKI
Author:	ESCB-PKI Project team
Document:	Technical certificates management
Version:	3.1
Date of issue:	07.11.2024
Status:	Final
Approved by:	
Distribution:	

RELEASE NOTES

In order to follow the current status of this document, the following matrix is provided. The numbers mentioned in the column “Release number” refer to the current version of the document.

Release number	**Status**	**Date of issue**	**Revisions**
1.0	Final	7.03.2013	Initial version
1.1	Final	15.04.2014	Update of the ESCB-PKI website
1.2	Final	28.07.2016	Number of possible DNS for certificates updated to 10
2.0	Final	11.09.2018	BdE Revision
3.0	Final	15.11.2021	Compatibility with other browsers and removal of SHA-1 algorithm as optional
3.1	Final	07.11.2024	Update *http* links to *https*

GLOSSARY AND ACRONYMS

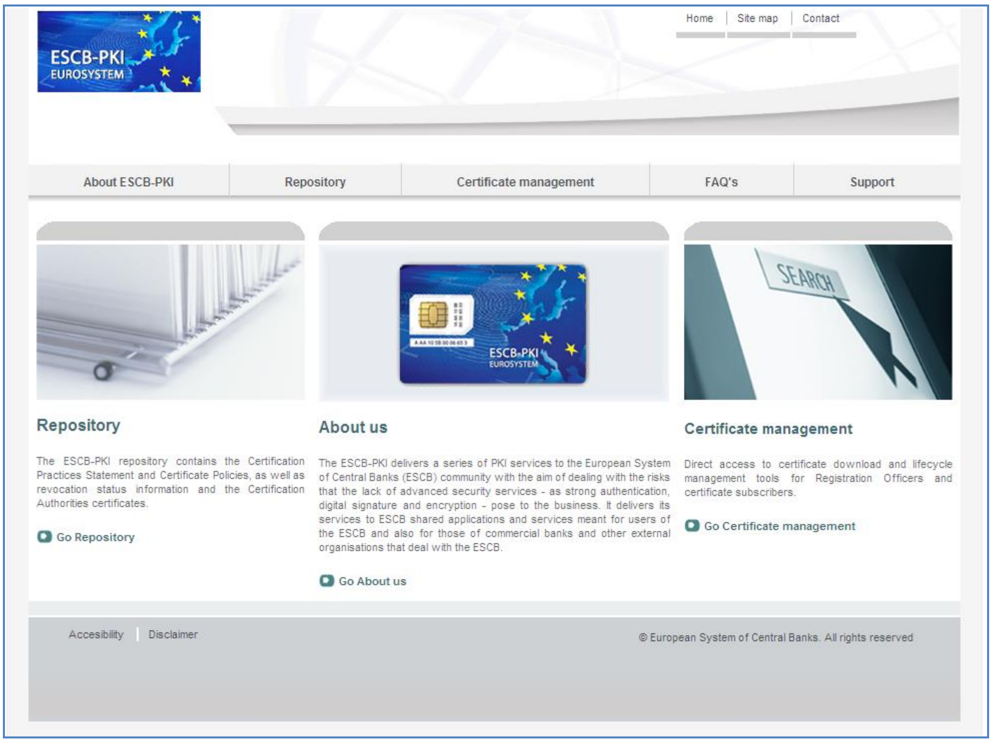
Acronym	Definition
CSR	Certificate Signing Request
ESCB-PKI	European System of Central Banks - Public Key Infrastructure
FAQ	Frequently Asked Questions
PKCS#10	Public Key Cryptographic Standard #10: Certification Request Standard
PKCS#12	Public Key Cryptographic Standard #12: Personal Information Exchange Syntax Standard
PKI	Public Key Infrastructure

1. INTRODUCTION

The present document aims at providing information on how to manage technical certificates with the ESCB-PKI Registration Authority application developed as part of the ESCB-PKI project.

1.1. THE ESCB-PKI WEBSITE

From the ESCB-PKI website you can get access to the ESCB-PKI services and find additional information related 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.

Go Repository

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.

Go About us

Certificate management

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

Go Certificate management

Accesibility | Disclaimer

© 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 REGISTRATION AUTHORITY APPLICATION

2.1. SYSTEM REQUIREMENTS

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

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

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

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

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

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

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

2.2. LAYOUT

Please be aware that two different ESCB-PKI services environments are available to ESCB-PKI users: acceptance and production. Each environment has a different frame colour so the customer can easily see the difference and use the one that better suits their intended usage; furthermore, the acceptance environment includes the “acceptance” label in the upper right position indicating that the acceptance environment is the one being accessed.

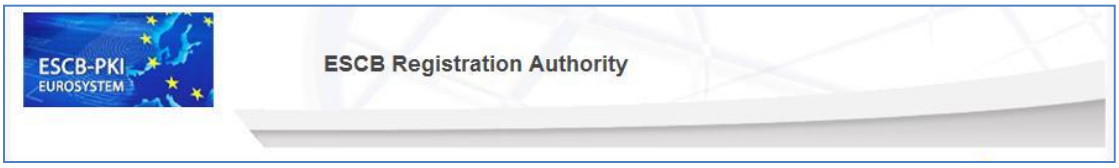


Figure 2 - Production frame

Figure 3 - Acceptance frame

After logging in the RA application, the following features are always available to the user:

- A menu on the left frame to facilitate quick access to all available options
- A Logout button in the upper-right corner to end the user session

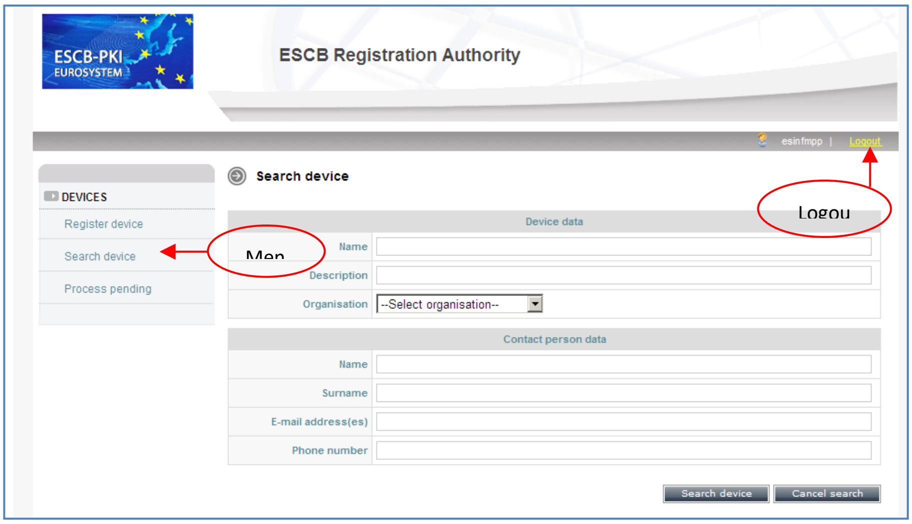
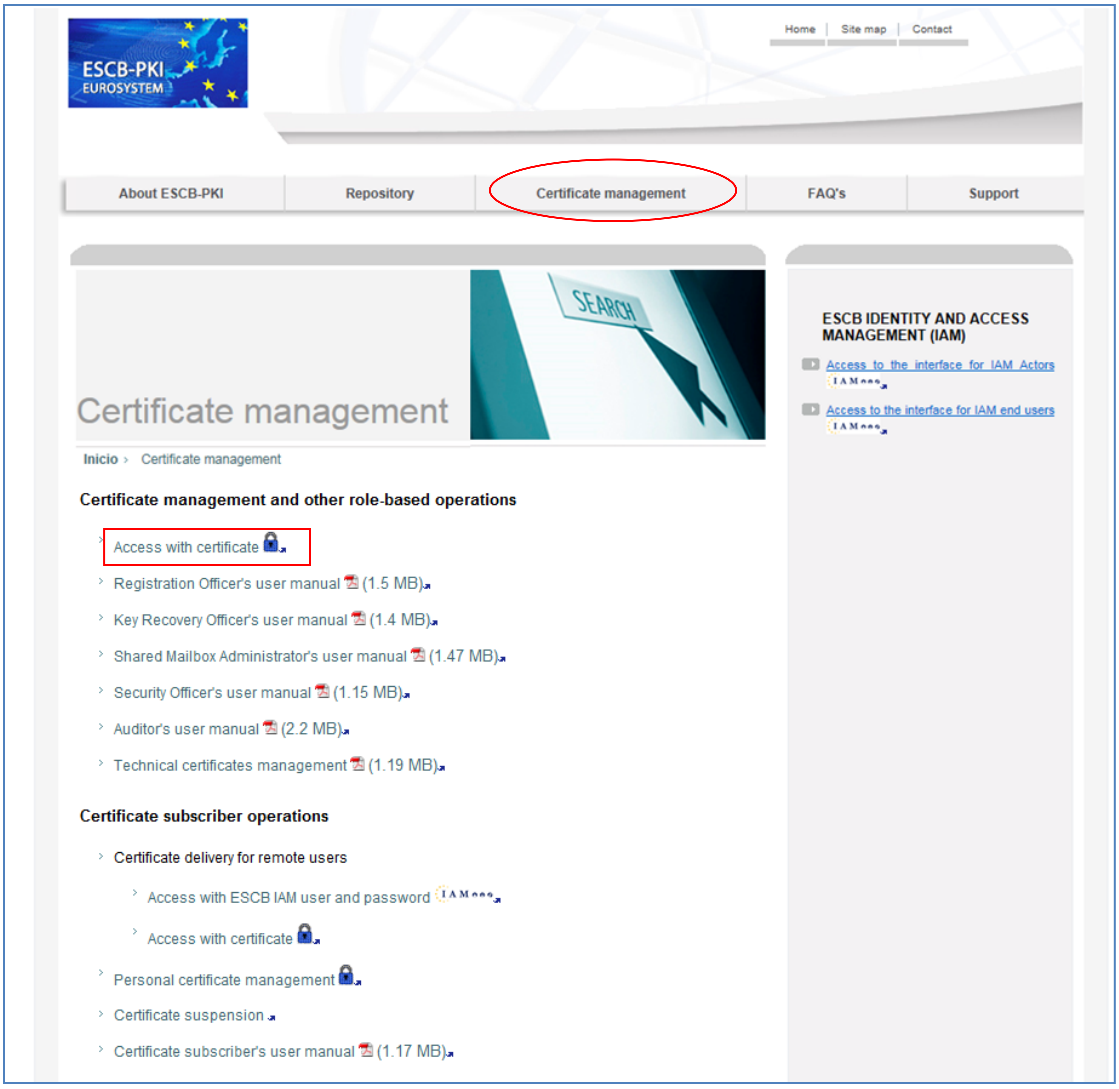


Figure 4 - Certificate Management

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

3. TYPES OF TECHNICAL CERTIFICATES

The following technical certificate types are provided by the ESCB-PKI system:

1) Application certificate: used by an automated process to authenticate, encrypt and sign information in application-to-application communications and secure e-mail (S/MIME). This type of certificate is available to Central Banks and also external organisations to communicate with ESCB services.

2) SSL/TLS certificate: used to implement an SSL/TLS connection with single on mutual authentication.

3) IPsec certificate: used to implement IPsec connectivity.

4) Code signing certificate: used to digitally sign software components such as Applets, ActiveX, .NET assemblies, etc.

5) Domain controller certificate: can be used by Central Banks that want to implement smart card logon in a Windows domain using the ESCB-PKI system.

3.1. DEVICES AND DEVICE PROFILES

The ESCB-PKI literature differentiates between the following elements:

1) **Device**. Any technical component that requires an ESCB-PKI technical certificate is known as "device" in the ESCB-PKI system. The following attributes define a device within the ESCB-PKI system:

   - Name and description
   - Central Bank or external organisation to which the device belongs to
   - Contact person. This is the person that is responsible for the lifecycle management of the certificates issued for the technical component

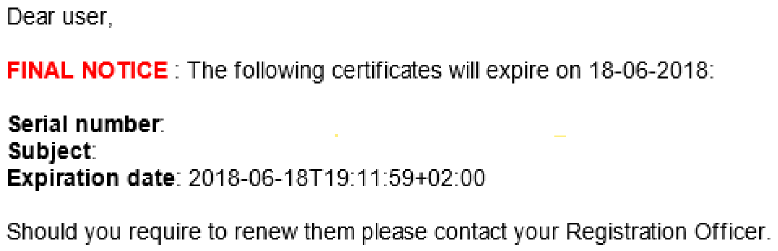
2) **Device profiles**. One or several "device profiles" can be defined for each device. The types of device profiles are equivalent to the types of technical certificates that the ESCB-PKI system provides:

   - Application profile (for devices of Central Banks and external organisations)
   - Code signing profile (only for Central Bank devices)
   - SSL server profile (only for Central Bank devices)
   - IPsec profile (only for Central Bank devices)
   - Domain controller profile (only for Central Bank devices)

3.2. TECHNICAL CERTIFICATES EXPIRATION

Technical certificates are issued with an expiration date, 3 years after the issuing date.

When the expiration date is close the contact person will receive emails indicating the certificate which will expire and the expiration date for it. The final notification, warning the contact person that the expiration date is very close and that the renewal should be made as soon as possible, looks like this:



Dear user,

FINAL NOTICE : The following certificates will expire on 18-06-2018:

Serial number:
Subject:
Expiration date: 2018-06-18T19:11:59+02:00

Should you require to renew them please contact your Registration Officer.

4. APPLICATION ROLES REQUIRED TO MANAGE TECHNICAL CERTIFICATES

The ESCB-PKI system is protected by the IAM infrastructure. Therefore, the ESCB-PKI application roles are granted or revoked by means of the IAM Identity Management system. Refer to IAM literature for further information.

This section describes the two application roles available to manage technical certificates at the ESCB-PKI system. The roles are not incompatible, therefore a given individual can be granted both roles, if required.

4.1. TECHNICAL CERTIFICATE SUBSCRIBER (TCS)

This role is in charge of requesting and retrieving certificates for technical components (e.g. servers, SSL accelerators, applications, etc.). This role will be typically assigned to IT experts from the Central Bank.

They interact with the ESCB-PKI system to:

- Define technical components in the ESCB-PKI system and their associated certificate profiles
- Request certificates for the profiles that have been defined for the technical component
- Process the certificate request (i.e. obtain the certificates) once a Registration Officer for Technical Component has approved the request

4.2. REGISTRATION OFFICER FOR TECHNICAL COMPONENTS (RO4TC)

This role is in charge of managing technical certificate requests that have been carried out by the Technical Certificate Subscribers.

They interact with the ESCB-PKI system to:

- Approve or reject technical certificate requests
- Revoke, suspend and reactivate technical certificates
- Review and obtain reports of the technical certificates and certificate requests that have been managed in your organisation.

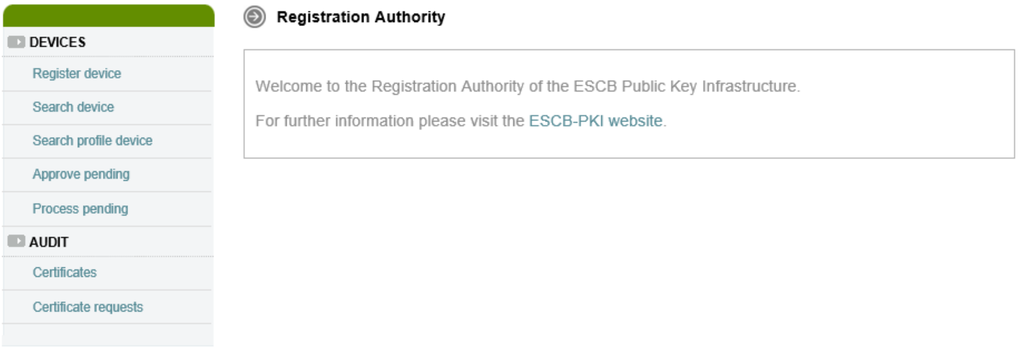
5. TECHNICAL CERTIFICATE MANAGEMENT

Both roles, TCS and RO4TC, use the same web interface, the Registration Authority application.

The following features are available (in bracket the role required):

- Register a new device that will need technical certificates (TCS)
- Review the list of devices belonging to your Central Bank, or to an external organisation that is subordinated to your Central Bank (TCS or RO4TC). For every device you will be able to perform the following operations:
  - Review the device information (TCS or RO4TC)
  - Modify the device information (TCS)
  - Create and modify one or several profiles for the device (TCS). The list of profiles available are the following:
    - Application (for devices of Central Banks and external organisations)
    - Code signing (only for Central Bank devices)
    - SSL/TLS server (only for Central Bank devices)
    - IPsec (only for Central Bank devices)
    - Domain controller (only for Central Bank devices)
  - Request certificates for the device profiles (TCS)
  - Approve or reject certificate requests (RO4TC)
  - Process certificate issuance (TCS)
  - Revoke, suspend and activate certificates (RO4TC)
- Review and obtain reports of the shared mailbox certificates and certificate requests that have been managed in your organisation (RO4TC).

Technical 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 - Technical certificate management menu

The following options are available in the left frame menu (in bracket, the role required to see the option):

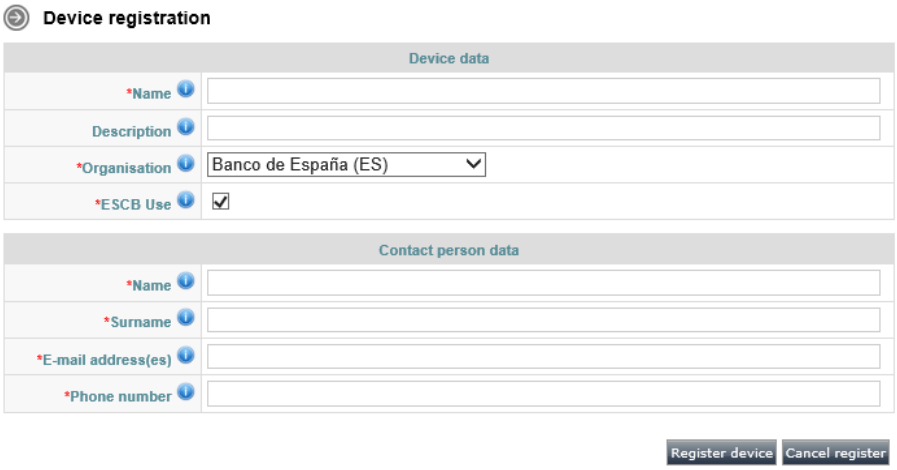
- ***Register device*** Register a new device in the ESCB-PKI system (TCS)
- ***Search device and search profile*** Search an existing device (TCS or RO4TC) and search an existing device profile (TCS or RO4TC)
- ***Approve pending*** Approve pending certificate requests (RO4TC)
- ***Process pending*** Process pending certificate issuances, once that the request has been approved (TCS)

- ***Audit > Certificates*** To show the technical certificates from your Central Bank
- ***Audit > Certificate Requests*** To show the technical certificate requests from your Central Bank

Next sections of this chapter will further develop these options.

5.1. REGISTER DEVICES

From the ***Register devices*** option you can register new devices into the ESCB-PKI system. You can register devices that belong to your Central Bank or to an external organisation that is subordinated to your CB. It is required to have been granted the TCS role for this purpose.



Device registration

Device data	
*Name	
Description	
*Organisation	Banco de España (ES)
*ESCB Use	☑
Contact person data	
*Name	
*Surname	
*E-mail address(es)	
*Phone number	

Figure 7 – Device registration

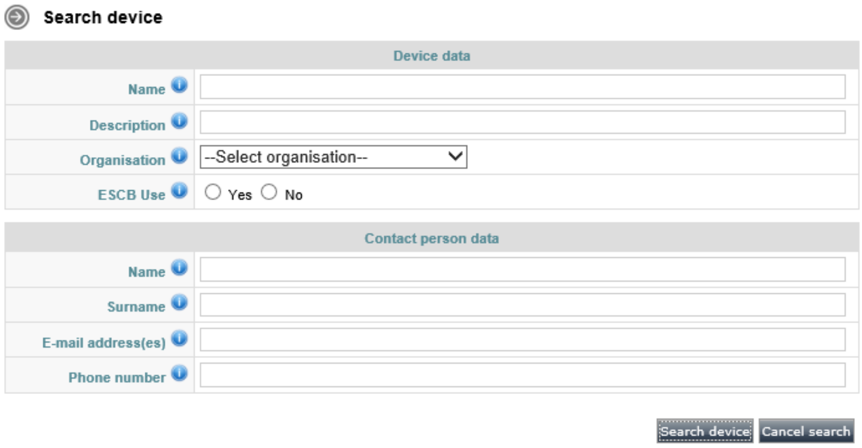
The information required to register a device is the following:

- **Name**: name of the device. No white spaces are allowed
- **Description**: description of the device
- **Organisation**: the name of the Central Bank or an external organisation[1] subordinated to the Central Bank
- **ESCB Use**: whether the certificate purpose is to be used in the context of the ESCB or local usage
- **Contact person**: personal information about the person in charge of the device. The e-mail address attribute will be used for lifecycle notifications (e.g. expiration warnings). Several e-mail addresses can be introduced, separated with the semicolon (“;”) character

[1] The Security Officer role can define new external organisations subordinated to the Central Bank

5.2. SEARCH DEVICES AND SEARCH PROFILES

From the ***Search devices*** option you can search devices that have been previously registered. Both, the TCS and RO4TC, can search devices.



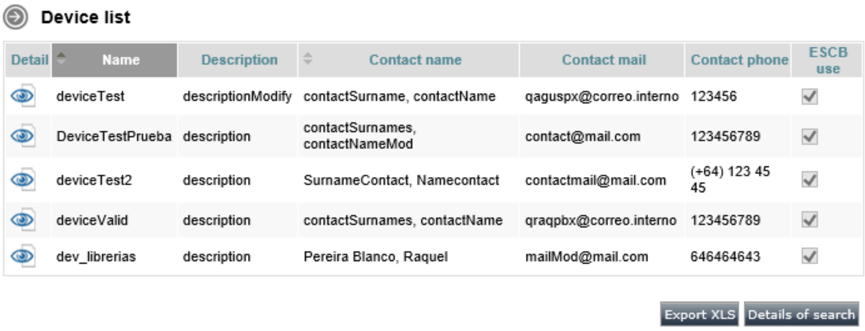
Search device

Device data	
Name	
Description	
Organisation	--Select organisation--
ESCB Use	○ Yes ○ No

Contact person data	
Name	
Surname	
E-mail address(es)	
Phone number	

Figure 8 – Search device

It is possible to use any device or contact person attribute to search. Once clicked the “Search device” button, the list of devices that follow the search criteria is shown:

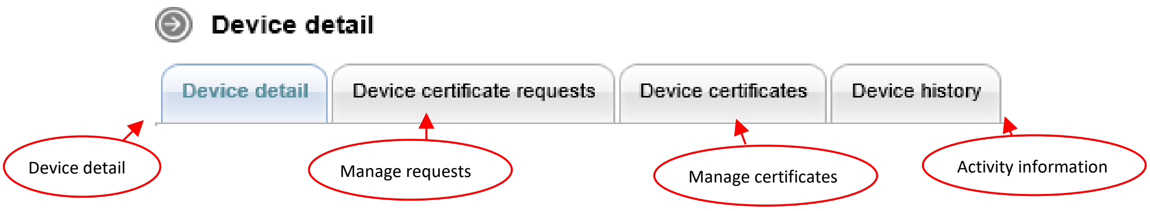


Device list

Detail	Name	Description	Contact name	Contact mail	Contact phone	ESCB use
👁	deviceTest	descriptionModify	contactSurname, contactName	qaguspx@correo.interno	123456	☑
👁	DeviceTestPrueba	description	contactSurnames, contactNameMod	contact@mail.com	123456789	☑
👁	deviceTest2	description	SurnameContact, Namecontact	contactmail@mail.com	(+64) 123 45 45	☑
👁	deviceValid	description	contactSurnames, contactName	qraqpbx@correo.interno	123456789	☑
👁	dev_librerias	description	Pereira Blanco, Raquel	mailMod@mail.com	646464643	☑

Figure 9 – List of devices

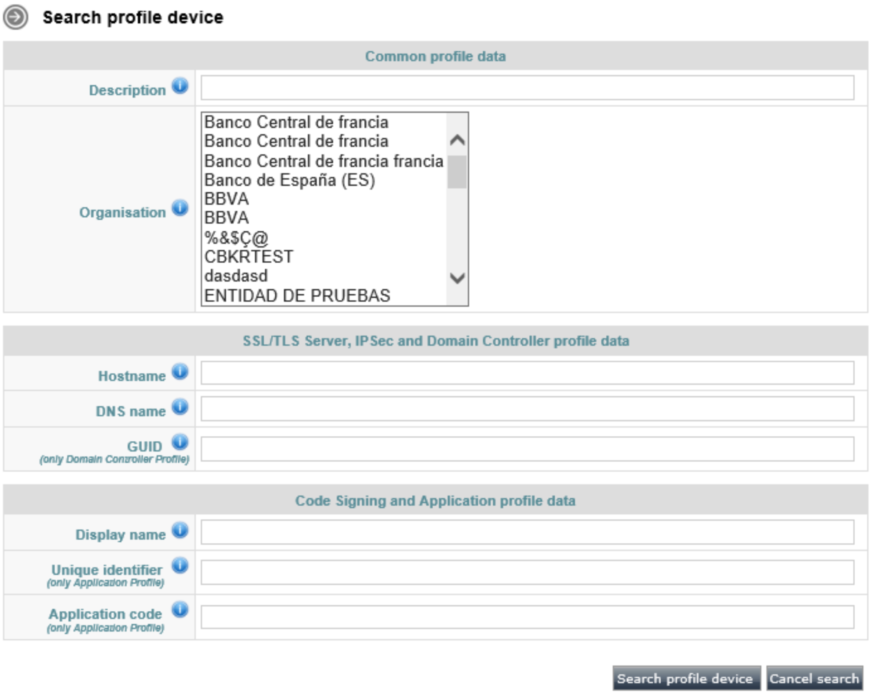
Clicking the eye icon (👁) the device details will be displayed. From this menu you can manage the device details, profiles and certificates:



Device detail

Figure 10 – Device detail

From the ***Search profiles*** option you can search directly profiles that have been previously registered. Both, the TCS and RO4TC, can search profiles.

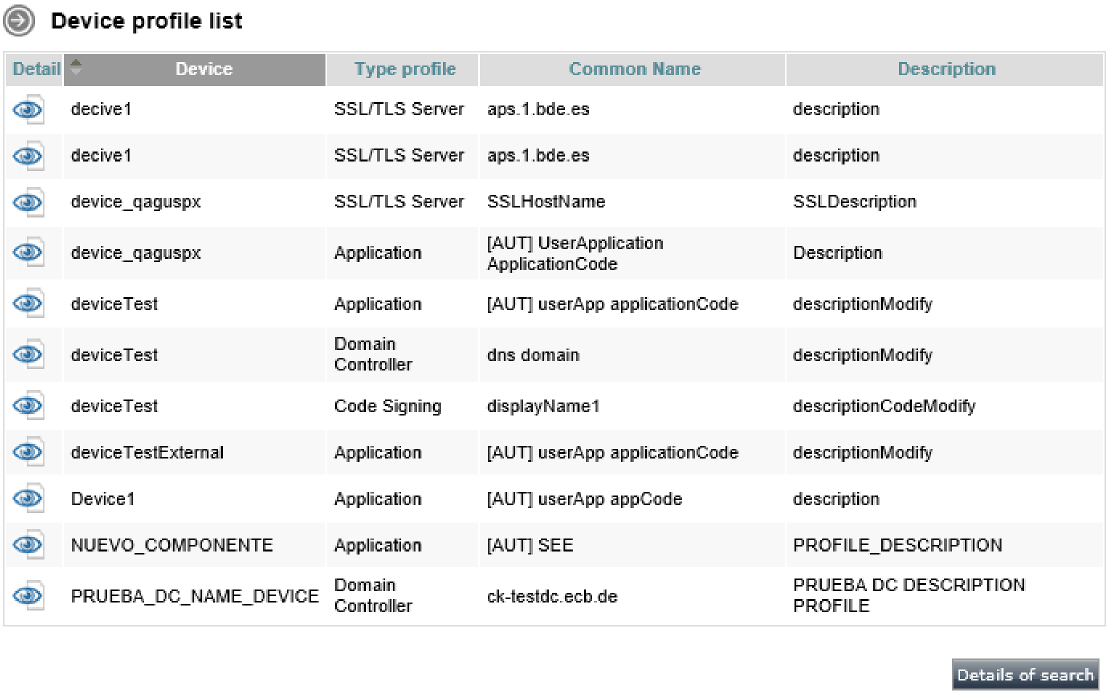


Search profile device

Common profile data	
Description	
Organisation	Banco Central de francia Banco Central de francia Banco Central de francia francia Banco de España (ES) BBVA BBVA %&$Ç@ CBKRTEST dasdasd ENTIDAD DE PRUEBAS
SSL/TLS Server, IPSec and Domain Controller profile data	
Hostname	
DNS name	
GUID (only Domain Controller Profile)	
Code Signing and Application profile data	
Display name	
Unique identifier (only Application Profile)	
Application code (only Application Profile)	

Figure 11 – Search profile

It is possible to use any device or contact person attribute to search. Once clicked the "Search profile device" button, the list of profiles that follow the search criteria is shown:



Device profile list

Detail	Device	Type profile	Common Name	Description
👁	decive1	SSL/TLS Server	aps.1.bde.es	description
👁	decive1	SSL/TLS Server	aps.1.bde.es	description
👁	device_qaguspx	SSL/TLS Server	SSLHostName	SSLDescription
👁	device_qaguspx	Application	[AUT] UserApplication ApplicationCode	Description
👁	deviceTest	Application	[AUT] userApp applicationCode	descriptionModify
👁	deviceTest	Domain Controller	dns domain	descriptionModify
👁	deviceTest	Code Signing	displayName1	descriptionCodeModify
👁	deviceTestExternal	Application	[AUT] userApp applicationCode	descriptionModify
👁	Device1	Application	[AUT] userApp appCode	description
👁	NUEVO_COMPONENTE	Application	[AUT] SEE	PROFILE_DESCRIPTION
👁	PRUEBA_DC_NAME_DEVICE	Domain Controller	ck-testdc.ecb.de	PRUEBA DC DESCRIPTION PROFILE

Figure 12 – List of profiles

Clicking the eye icon (👁) the profile details will be displayed. From this menu you can manage the profile details, requests and certificates:

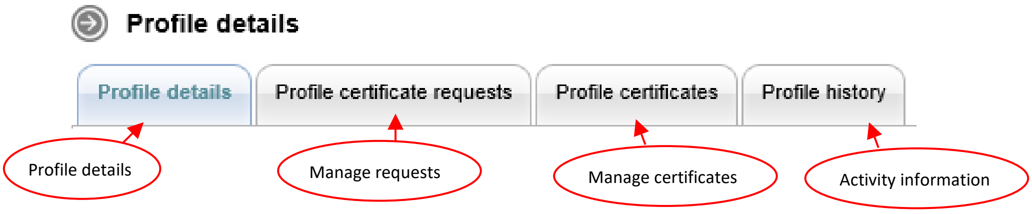
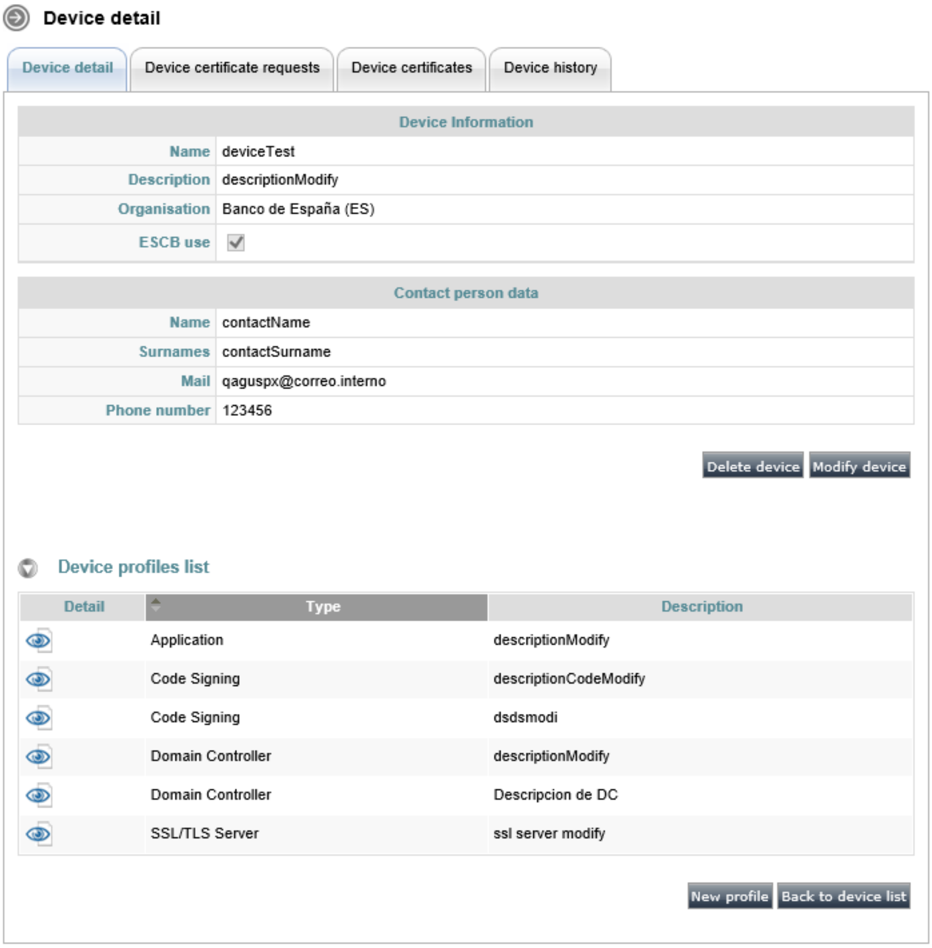


Figure 13 – Profile detail

5.2.1. DEVICE DETAILS

This tab allows performing the following operations:

- Modify the device and contact person information (TCS)
- Create profiles for the device (TCS)
- Access the details of the different device profiles (TCS or RO4TC)
- Delete the device (RO4TC)



Device detail

Device Information	
Name	deviceTest
Description	descriptionModify
Organisation	Banco de España (ES)
ESCB use	☑

Contact person data	
Name	contactName
Surnames	contactSurname
Mail	qaguspx@correo.interno
Phone number	123456

Device profiles list

Detail	Type	Description
👁	Application	descriptionModify
👁	Code Signing	descriptionCodeModify
👁	Code Signing	dsdsmodi
👁	Domain Controller	descriptionModify
👁	Domain Controller	Descripcion de DC
👁	SSL/TLS Server	ssl server modify

Figure 14 - Device detail tab

The ***Modify device*** button takes to the device registration screen (see section 5.1). All the device and contact person attributes are editable but the Organisation, which will only be editable if the device does not yet have certificates.

The ***Delete device*** button asks the user to confirm he is sure about it before proceeding to the deletion. A device being deleted will have the following effect:

- Any pending certificate request will be cancelled.
- The device will be marked as deleted, therefore it will no longer be accessible.
- Any active certificate will NOT be revoked.

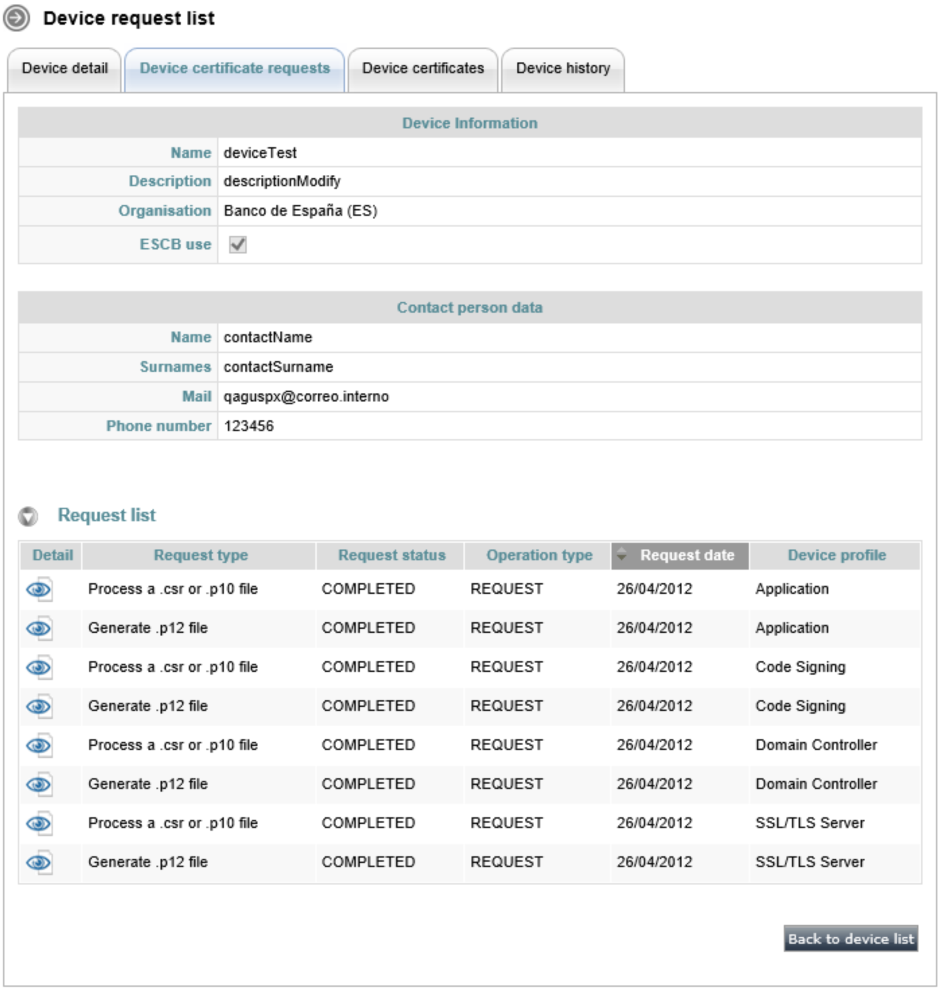
Would you need to be able to access again a previously deleted device, contact the ESCB-PKI mailbox at escb-pki@pki.escb.eu.

The ***New profile*** button takes to the “new profile device” screen (see section 5.2.4.1).

The eye icon (👁) under the “device profile list” allows displaying the profile details (see section 5.2.4.2).

5.2.2. DEVICE CERTIFICATE REQUESTS

This tab allows watching the details of the certificate requests of all the profiles associated to the device. Both, the TCS and RO4TC, can display device certificate requests.



Device request list

Device Information	
Name	deviceTest
Description	descriptionModify
Organisation	Banco de España (ES)
ESCB use	☑

Contact person data	
Name	contactName
Surnames	contactSurname
Mail	qaguspx@correo.interno
Phone number	123456

Request list

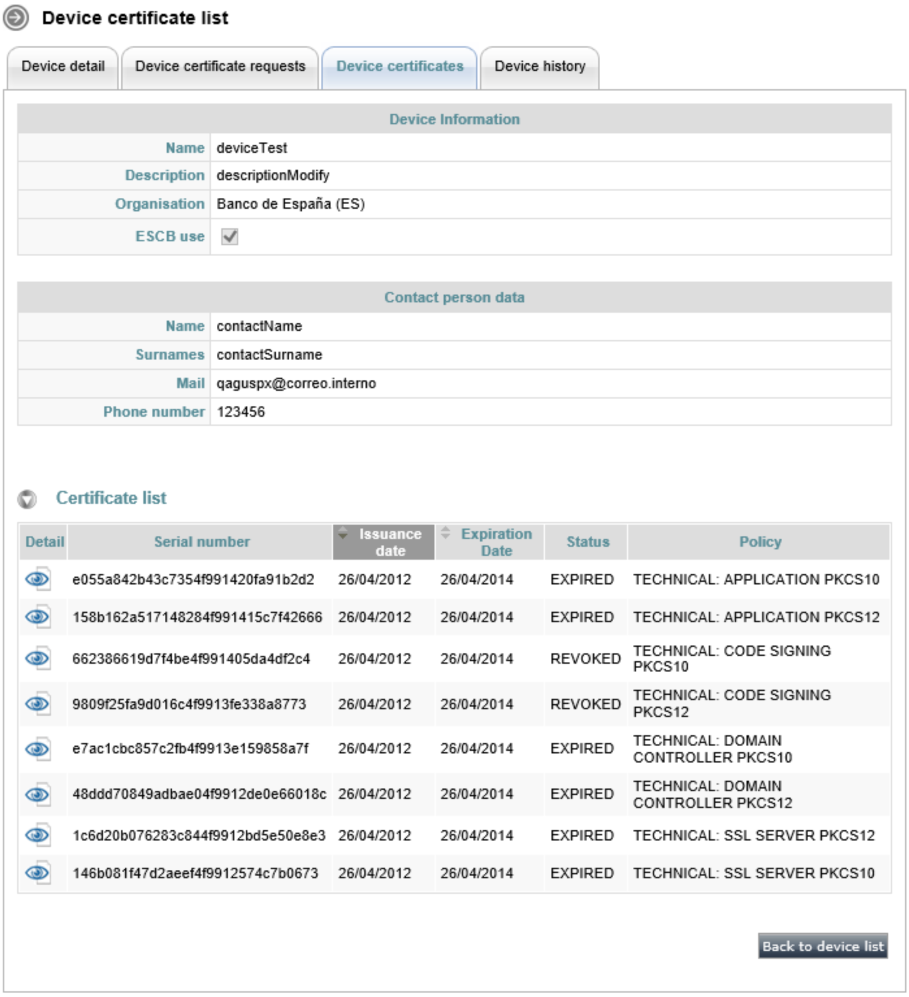
Detail	Request type	Request status	Operation type	Request date	Device profile
👁	Process a .csr or .p10 file	COMPLETED	REQUEST	26/04/2012	Application
👁	Generate .p12 file	COMPLETED	REQUEST	26/04/2012	Application
👁	Process a .csr or .p10 file	COMPLETED	REQUEST	26/04/2012	Code Signing
👁	Generate .p12 file	COMPLETED	REQUEST	26/04/2012	Code Signing
👁	Process a .csr or .p10 file	COMPLETED	REQUEST	26/04/2012	Domain Controller
👁	Generate .p12 file	COMPLETED	REQUEST	26/04/2012	Domain Controller
👁	Process a .csr or .p10 file	COMPLETED	REQUEST	26/04/2012	SSL/TLS Server
👁	Generate .p12 file	COMPLETED	REQUEST	26/04/2012	SSL/TLS Server

Figure 15 - Device request list

The eye icon (👁) under the "request list" takes to the "request detail" screen (see section 5.2.4.3)

5.2.3. DEVICE CERTIFICATES

This tab allows watching the details of the certificates of all the profiles associated to the device. Both, the TCS and RO4TC, can display device certificates.



Device Information	
Name	deviceTest
Description	descriptionModify
Organisation	Banco de España (ES)
ESCB use	☑

Contact person data	
Name	contactName
Surnames	contactSurname
Mail	qaguspx@correo.interno
Phone number	123456

Certificate list

Detail	Serial number	Issuance date	Expiration Date	Status	Policy
👁	e055a842b43c7354f991420fa91b2d2	26/04/2012	26/04/2014	EXPIRED	TECHNICAL: APPLICATION PKCS10
👁	158b162a517148284f991415c7f42666	26/04/2012	26/04/2014	EXPIRED	TECHNICAL: APPLICATION PKCS12
👁	662386619d7f4be4f991405da4df2c4	26/04/2012	26/04/2014	REVOKED	TECHNICAL: CODE SIGNING PKCS10
👁	9809f25fa9d016c4f9913fe338a8773	26/04/2012	26/04/2014	REVOKED	TECHNICAL: CODE SIGNING PKCS12
👁	e7ac1cbc857c2fb4f9913e159858a7f	26/04/2012	26/04/2014	EXPIRED	TECHNICAL: DOMAIN CONTROLLER PKCS10
👁	48ddd70849adbae04f9912de0e66018c	26/04/2012	26/04/2014	EXPIRED	TECHNICAL: DOMAIN CONTROLLER PKCS12
👁	1c6d20b076283c844f9912bd5e50e8e3	26/04/2012	26/04/2014	EXPIRED	TECHNICAL: SSL SERVER PKCS12
👁	146b081f47d2aeef4f9912574c7b0673	26/04/2012	26/04/2014	EXPIRED	TECHNICAL: SSL SERVER PKCS10

Figure 16 - Device certificate list

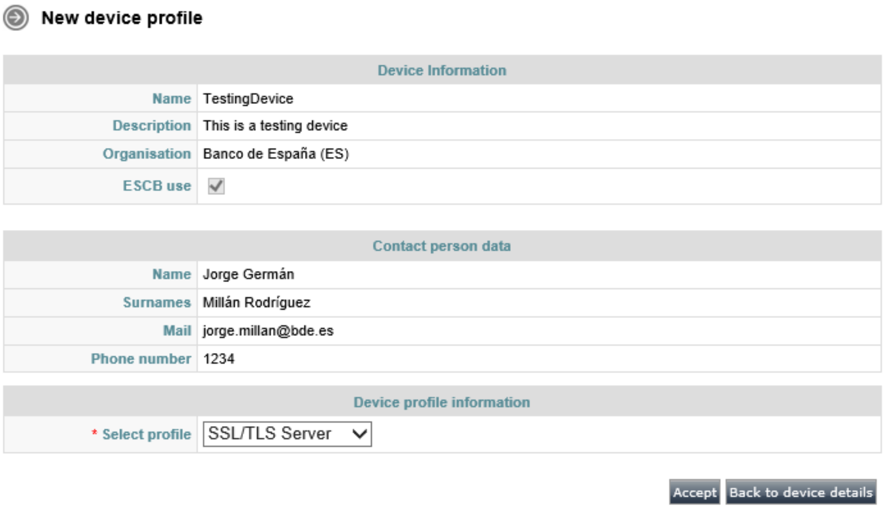
The eye icon (👁) under the “certificate list” takes to the “certificate detail” screen (see section 5.2.4.4)

5.2.4. DEVICE PROFILE MANAGEMENT

The “device details” screen (see section 5.2.1) allows managing profiles for the device.

5.2.4.1. Register device profiles

The “New device profile” screen enables the TCS role to define profiles associated to the device:



New device profile

Device Information	
Name	TestingDevice
Description	This is a testing device
Organisation	Banco de España (ES)
ESCB use	☑

Contact person data	
Name	Jorge Germán
Surnames	Millán Rodríguez
Mail	jorge.millan@bde.es
Phone number	1234

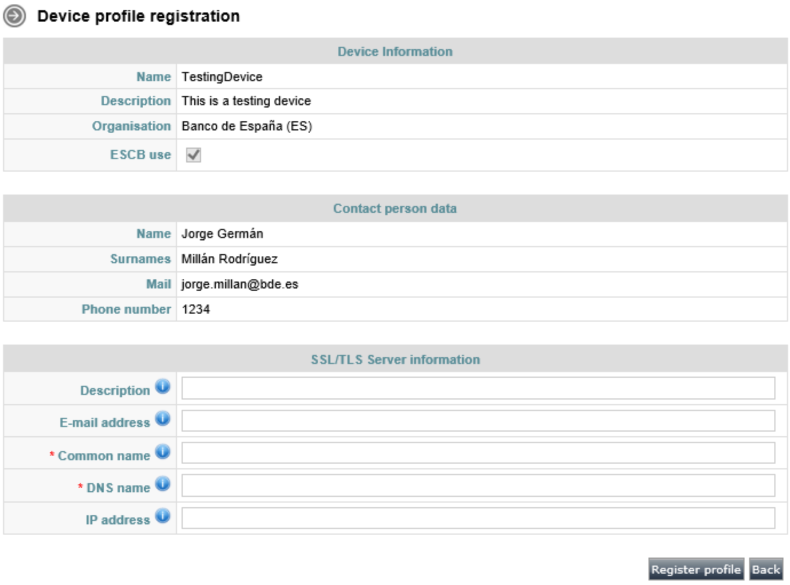
Device profile information	
* Select profile	SSL/TLS Server

Figure 17 - New device profile

The only attribute that has to be selected is the type of profile to create:

- Application (for devices of Central Banks and external organisations)
- Code signing (only for Central Bank devices)
- SSL/TLS server (only for Central Bank devices)
- IPSec (only for Central Bank devices)
- Domain controller (only for Central Bank devices)

After clicking the “Accept” button, the “register profile” screen is shown:



Device profile registration

Device Information	
Name	TestingDevice
Description	This is a testing device
Organisation	Banco de España (ES)
ESCB use	☑

Contact person data	
Name	Jorge Germán
Surnames	Millán Rodríguez
Mail	jorge.millan@bde.es
Phone number	1234

SSL/TLS Server information	
Description	
E-mail address	
* Common name	
* DNS name	
IP address	

Figure 18 - Register device profile

The following fields are common for all types of profiles:

- **Description:** this field can be used to identify the profile being registered
- **E-mail address**: this is an optional field that can be used to include an e-mail address in the certificate. In the case of the application certificate profile, this will be the e-mail address for secure e-mail (S/MIME)

The rest of information to be fulfilled is different depending on the type of profile being registered:

Application

- **Unique identifier**: optional field that can be used to include the unique identifier of a technical account associated to the application. This attribute will be included in the pseudonym (PS) attribute of the certificate's subject
- **Application code**: this field is reserved to include an application identifier that will be included in the certificate. It will be included as part of the common name (CN) attribute of certificate's subject
- **Display name**: this text will be included as part of the common name (CN) attribute of the certificate's subject, next to the application code. The CN will be equal to "[AUT] AAA DISPLAYNAME", being AAA the application code and DISPLAYNAME the value of the display name attribute.

Code signing

- **Display name**: text that will be included in the common name (CN) attribute of the certificate's subject

Domain controller

- **DNS name**: server name, such as it will used in the URL required to access the server (e.g. "pki.escb.eu"). It will be included in the DNSName attribute of the SubjectAltName (SAN) extension of the certificate. In case that more than one name are valid to identify the server, it is possible to include up to 10 names, separated by the semicolon (";") character (e.g. "name1.escb.eu;name2.escb.eu;name3.escb.eu;name4.escb.eu;name5.escb.eu")
- **GUID**: this is the Globally Unique Identifier attribute of the Windows domain controller. The following formats are allowed:
  - Hexadecimal: the bytes have to be typed in the order that they are available at the Active Directory. Examples:
    ```
    0a78f4c552385d4991a319f6fdd27456
    0a 78 f4 c5 52 38 5d 49 91 a3 19 f6 fd d2 74 56
    0a:78:f4:c5:52:38:5d:49:91:a3:19:f6:fd:d2:74:56
    0a-78-f4-c5-52-38-5d-49-91-a3-19-f6-fd-d2-74-56
    ```
  - CLSID: this format can be obtained with the dsquery.exe and ldp.exe Microsoft tools. Examples:
    ```
    {c5f4780a-3852-495d-91a3-19f6fdd27456}
    ```

SSL/TLS server

- **Common name**: text that will be included in the common name (CN) attribute of the certificate. It is typically used to include the server name (e.g. "pki.escb.eu"), but is can be used also to include a descriptive text (e.g. "ESCB-PKI WEBSITE")

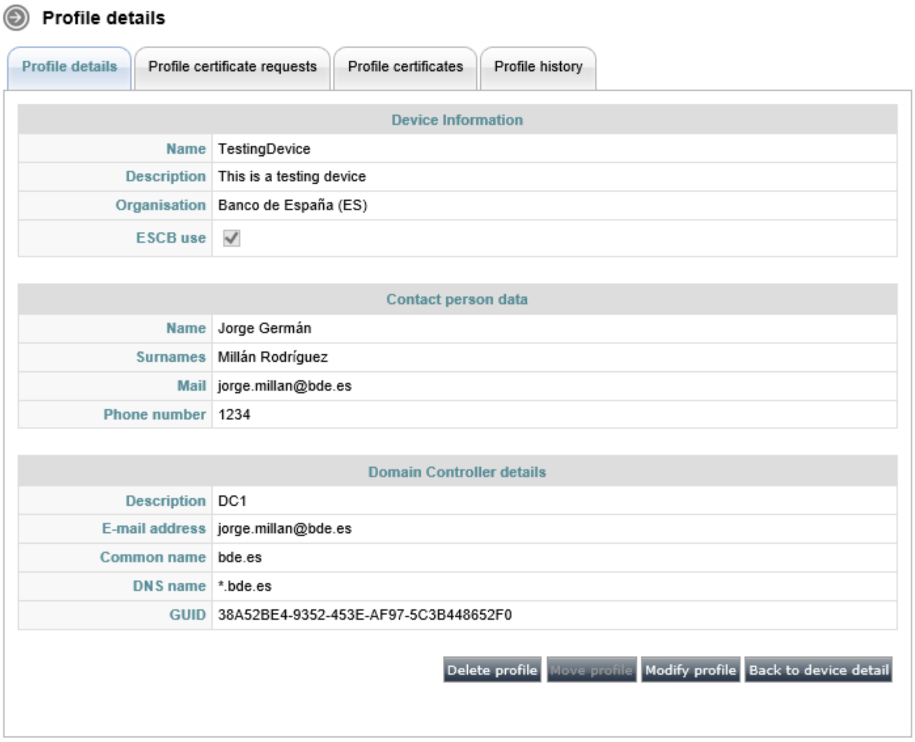
- **DNS name**: the same than for the Domain controller profile
- **IP address:** this is an optional field that can be used to include the IP address of the server

IPSec

- **Common name**: the same than for the SSL/TLS profile
- **DNS name**: the same than for the SSL/TLS profile
- **IP address:** the same than for the SSL/TLS profile

5.2.4.2. Profile details

When a device profile has been created, the profile details screen is shown:



Profile details

Device Information	
Name	TestingDevice
Description	This is a testing device
Organisation	Banco de España (ES)
ESCB use	☑

Contact person data	
Name	Jorge Germán
Surnames	Millán Rodríguez
Mail	jorge.millan@bde.es
Phone number	1234

Domain Controller details	
Description	DC1
E-mail address	jorge.millan@bde.es
Common name	bde.es
DNS name	*.bde.es
GUID	38A52BE4-9352-453E-AF97-5C3B448652F0

Figure 19 - Profile details

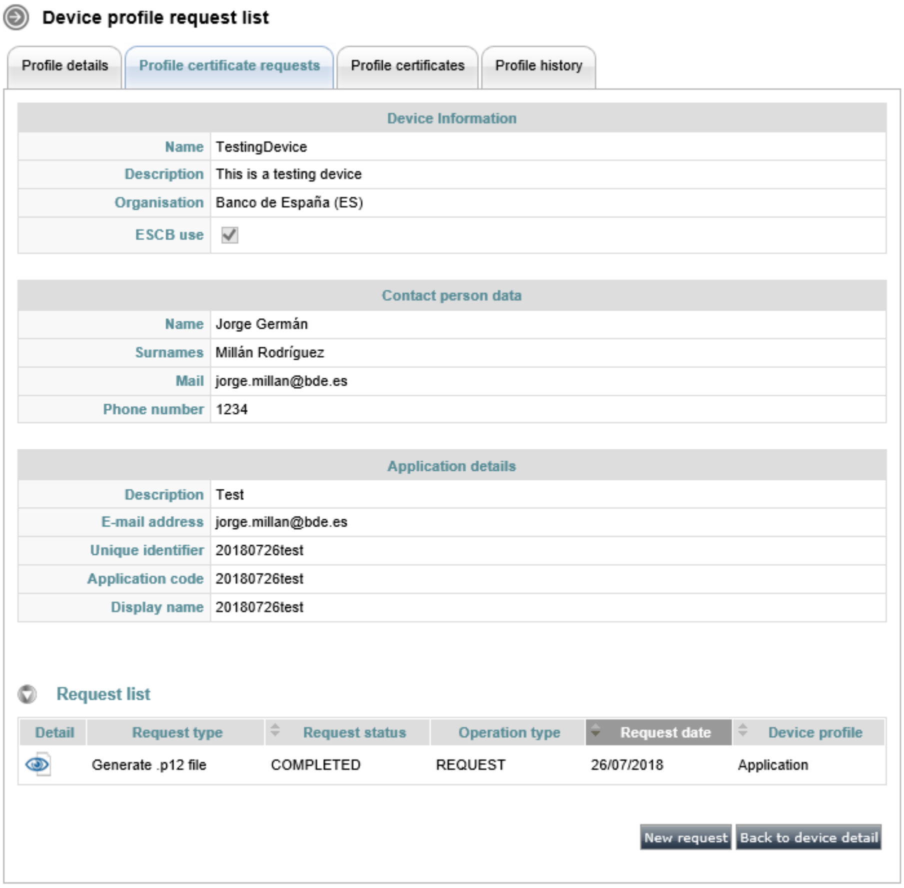
The ***Modify profile*** button takes to the register profile screen (see above) to modify the profile attributes. This button is only available for the TCS role.

The ***Delete profile*** button allows to fully delete a profile. It is only available for the TCS role when the profile does not have associated certificates.

The **Move profile** button allows to move a profile to other device. It is only available for the TCS role when the profile does not have associated certificates.

5.2.4.3. Profile certificate requests

The “profile certificate requests” tab allows displaying the certificate requests associated to the device profile. Additionally the TCS role can create new ones.



Device Information	
Name	TestingDevice
Description	This is a testing device
Organisation	Banco de España (ES)
ESCB use	☑

Contact person data	
Name	Jorge Germán
Surnames	Millán Rodríguez
Mail	jorge.millan@bde.es
Phone number	1234

Application details	
Description	Test
E-mail address	jorge.millan@bde.es
Unique identifier	20180726test
Application code	20180726test
Display name	20180726test

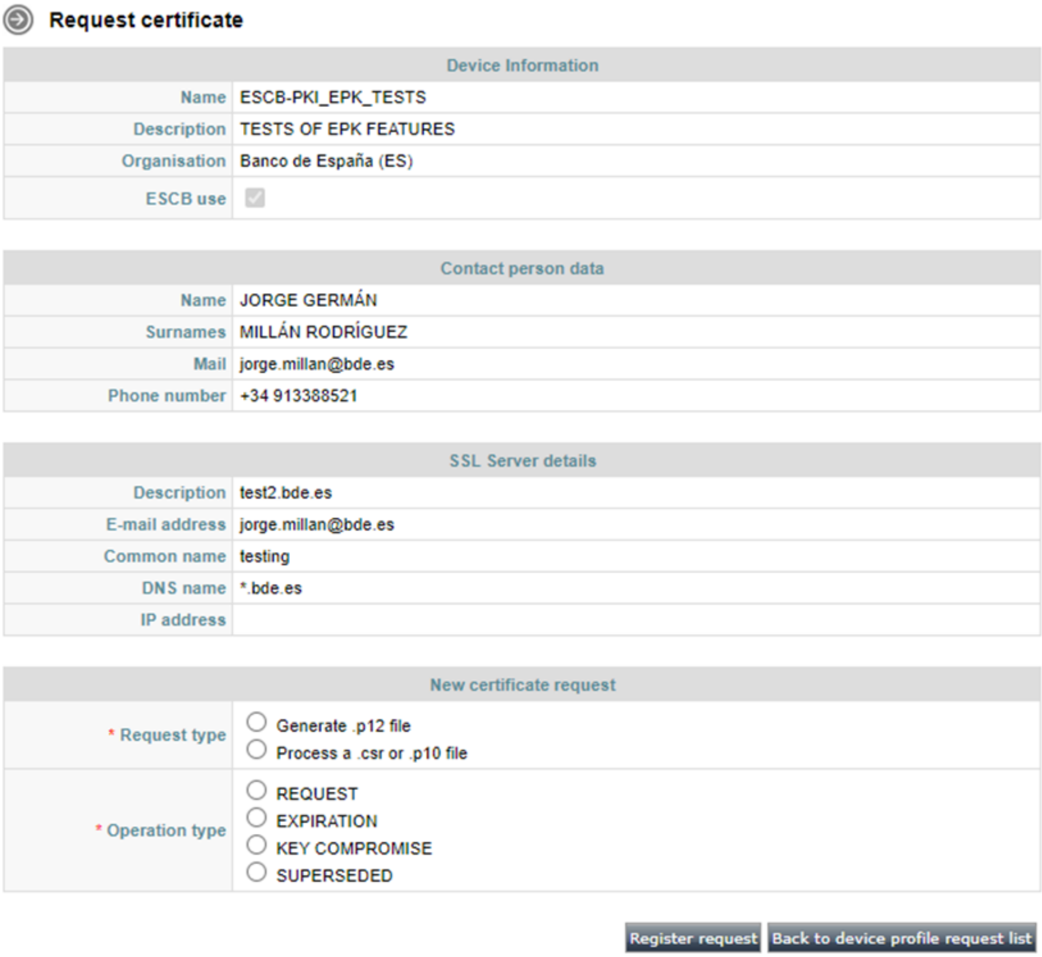
Request list

Detail	Request type	Request status	Operation type	Request date	Device profile
👁	Generate .p12 file	COMPLETED	REQUEST	26/07/2018	Application

Figure 20 - Profile certificate requests

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

The ***New request*** button allows creating new certificate requests for the device profile. This button is only available for the TCS role. When the button is clicked, the “request certificate” screen is shown:



Request certificate

Device Information	
Name	ESCB-PKI_EPK_TESTS
Description	TESTS OF EPK FEATURES
Organisation	Banco de España (ES)
ESCB use	☑

Contact person data	
Name	JORGE GERMÁN
Surnames	MILLÁN RODRÍGUEZ
Mail	jorge.millan@bde.es
Phone number	+34 913388521

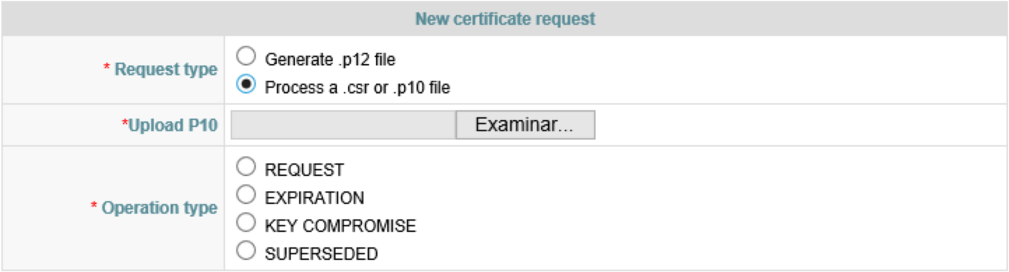
SSL Server details	
Description	test2.bde.es
E-mail address	jorge.millan@bde.es
Common name	testing
DNS name	*.bde.es
IP address	

New certificate request	
* Request type	○ Generate .p12 file ○ Process a .csr or .p10 file
* Operation type	○ REQUEST ○ EXPIRATION ○ KEY COMPROMISE ○ SUPERSEDED

Figure 21 - Request certificate

The following information has to be provided to initiate the request:

- **Request type:** two options are provided:
  - Generate a .p12 file: choose this option if you prefer that the Certification Authority (CA) generates the key pair by means of its Hardware Security Module (HSM). In this case a PKCS#12 file will be delivered to the TCS
  - Process a .csr or .p10 file: choose this option if you prefer to generate the key pair using the key generation options available at the device. In this case, the TCS will have to provide a PKCS#10 (aka Certificate Signing Request, CSR) file (see the screen below)



New certificate request	
* Request type	○ Generate .p12 file ● Process a .csr or .p10 file
*Upload P10	Examinar...
* Operation type	○ REQUEST ○ EXPIRATION ○ KEY COMPROMISE ○ SUPERSEDED

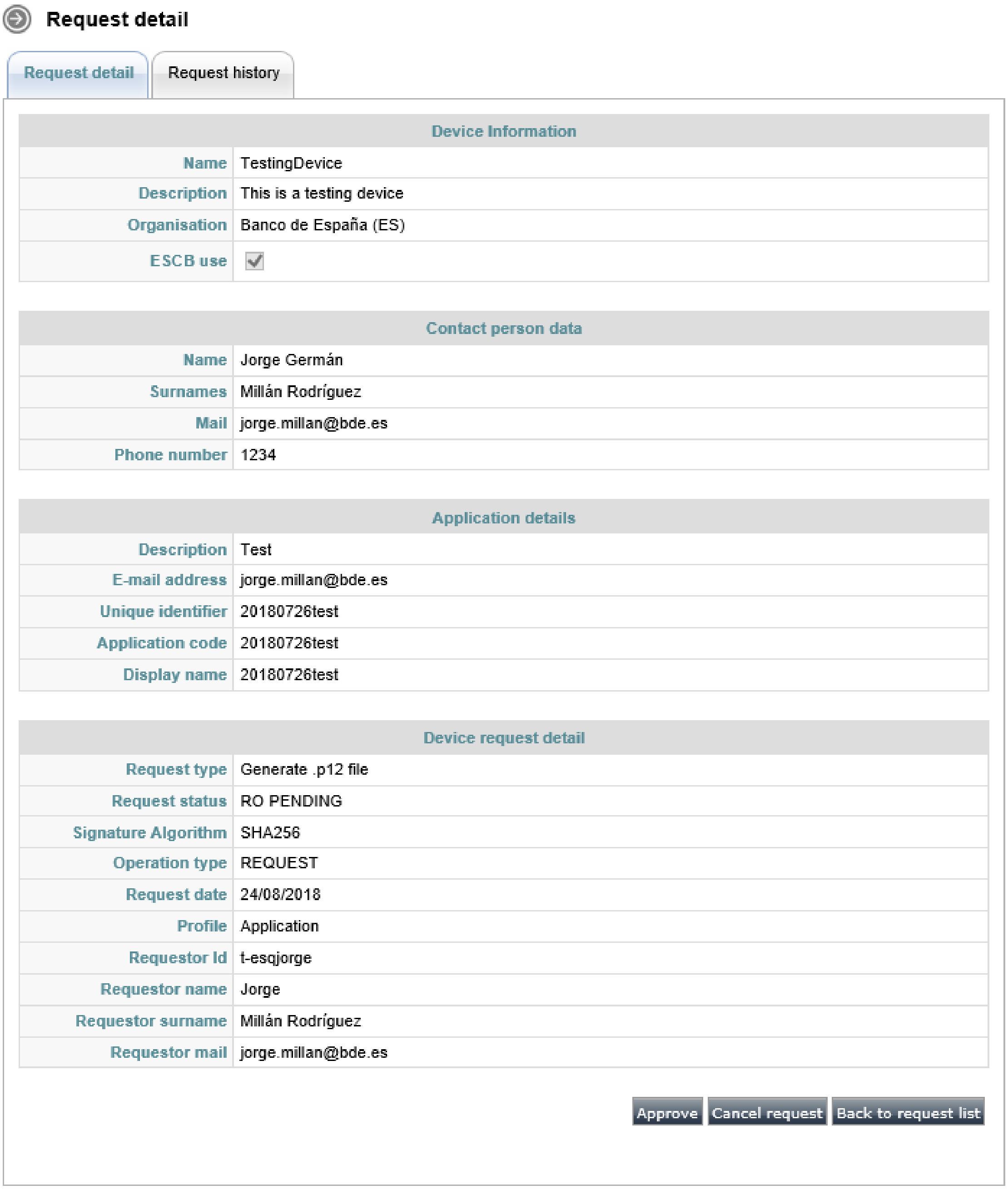
Figure 22 - Request with .csr or .p10 file

CSR files have the following requirements:
- Only RSA keys of 2048 or 4096 bits are allowed
- Only SHA-256 hashing algorithm is allowed
- Other attributes included in the request (e.g. CN, OU, O, etc.) will be ignored

- **Operation type**: choose the reason to request the certificate:
  - REQUEST: this is the first time that a certificate is being request for the device profile
  - EXPIRATION: a previous certificate is about to expire. The old certificate will not be revoked
  - KEY COMPROMISE: a new certificate is required because the private key associated to the previous one has been compromised. The old certificate will be revoked
  - SUPERSEDED: the previous certificate has to be replaced before the expiration date (e.g. some affiliation data has been modified). The old certificate will not be revoked

A given device profile can only have one certificate active at the same time, so it is not possible to request a new certificate if the previous one is not near to its expiration day, unless the “key compromise” or “superseded” options are used. The other exception is the case that different request types are used, since a given device can have one certificate that have been issued with a .p12 file and another one with a .csr or .p10 file.

In the “Request certificate” screen, when the “Register request” button is clicked, the following screen is shown:



Request detail

Device Information	
Name	TestingDevice
Description	This is a testing device
Organisation	Banco de España (ES)
ESCB use	☑

Contact person data	
Name	Jorge Germán
Surnames	Millán Rodríguez
Mail	jorge.millan@bde.es
Phone number	1234

Application details	
Description	Test
E-mail address	jorge.millan@bde.es
Unique identifier	20180726test
Application code	20180726test
Display name	20180726test

Device request detail	
Request type	Generate .p12 file
Request status	RO PENDING
Signature Algorithm	SHA256
Operation type	REQUEST
Request date	24/08/2018
Profile	Application
Requestor Id	t-esqjorge
Requestor name	Jorge
Requestor surname	Millán Rodríguez
Requestor mail	jorge.millan@bde.es

Figure 23 - Request detail

The possible certificate request states are the following:

- RO PENDING: the request has been created and has to be approved (or cancelled) by a RO4TC
- USER PENDING: the request has been approved by a RO4TC and has to be processed by a TCS. The RO4TC can also cancel the request
- CANCEL: the request has been canceled by a RO4TC
- FINISH: the request has been completed
- EXPIRED: the request has expired before completion

The buttons available at the “request detail” screen depend on the status of the certificate request and the role of the user:

- **Approve**: approve the certificate request (RO4TC). If this button is clicked, the certificate request is approved. Afterwards, the TCS will be able to process the request and get the certificate
- **Cancel request**: cancel the certificate request (RO4TC). It this button is clicked the certificate request is cancelled. Therefore, the TCS will not be able to process the request
- **Process**: process the certificate request (TCS). Only the specific TCS that requested the certificate will be able to click this button once that a RO4TC has approved the request

Processing certificate requests

The TCS role is able to process a certificate request only when a RO4TC has approved the request, that is to say, when the request is in the USER PENDING state. In the "request detail" screen (see above), the TCS has to click the "Process" button to process the request.

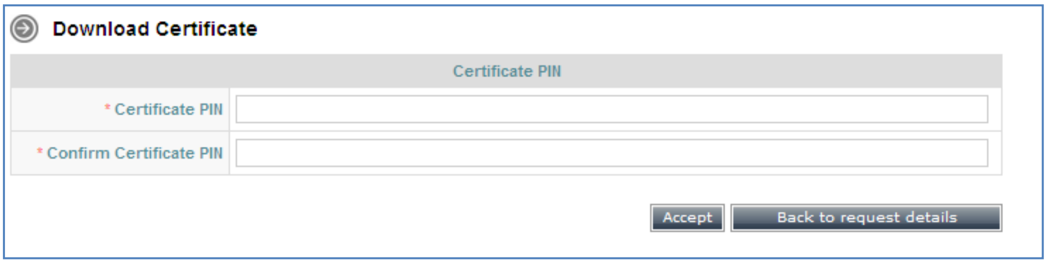
Very important: only the specific TCS that requested the certificate will be able to process the request, once that a RO4TC has approved it.

The next screen is different depending on the request type:

Generate a .p12 file

In case of request of a PKCS#12 file, it is required to enter the PIN to be used to protect the file. The rules are the following:

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



Download Certificate

Certificate PIN

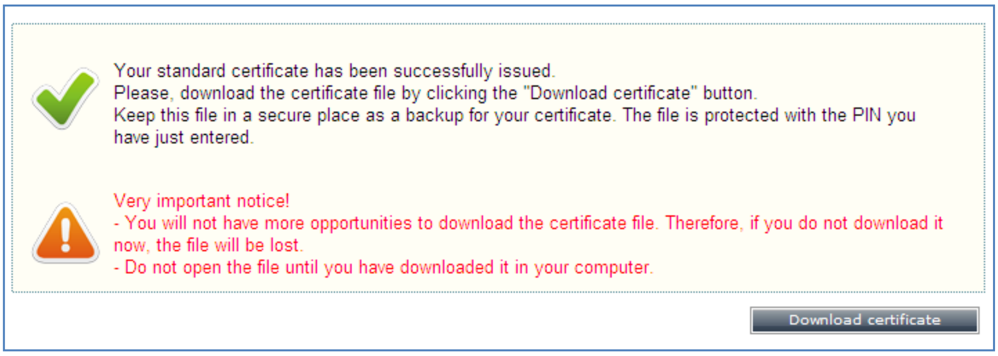
* Certificate PIN	
* Confirm Certificate PIN	

Figure 24 - Process PKCS#12 request

Once that the "Accept" button is clicked, the Certification Authority generates the PKCS#12 and the TCS is able to download the .p12 file (see the "Download certificate" screen below)

Process a .csr or .p10 file

In case of request via a PKCS#10 file (aka Certificate Signing Request, CSR), it will not be required to type a PIN and the TCS will be able to download the certificate (.cer) file:



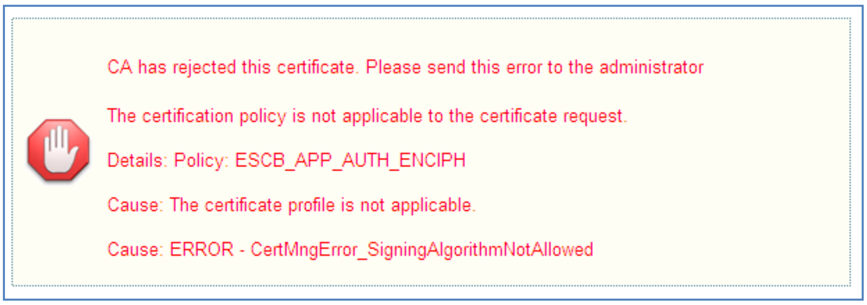
Your standard certificate has been successfully issued.
Please, download the certificate file by clicking the "Download certificate" button.
Keep this file in a secure place as a backup for your certificate. The file is protected with the PIN you have just entered.

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 25 - Download certificate file

Very important: the TCS will be able to download the file only in this screen. Therefore, if the TCS does not click the “Download certificate” button, the file will be lost.

In case that the PKCS#10 (CSR) files does not fulfill the requirements (see above), the CA will reject the request. For example, this is the screen in case that the PKCS#10 has been signed using the MD5 algorithm:



CA has rejected this certificate. Please send this error to the administrator

The certification policy is not applicable to the certificate request.

Details: Policy: ESCB_APP_AUTH_ENCIPH

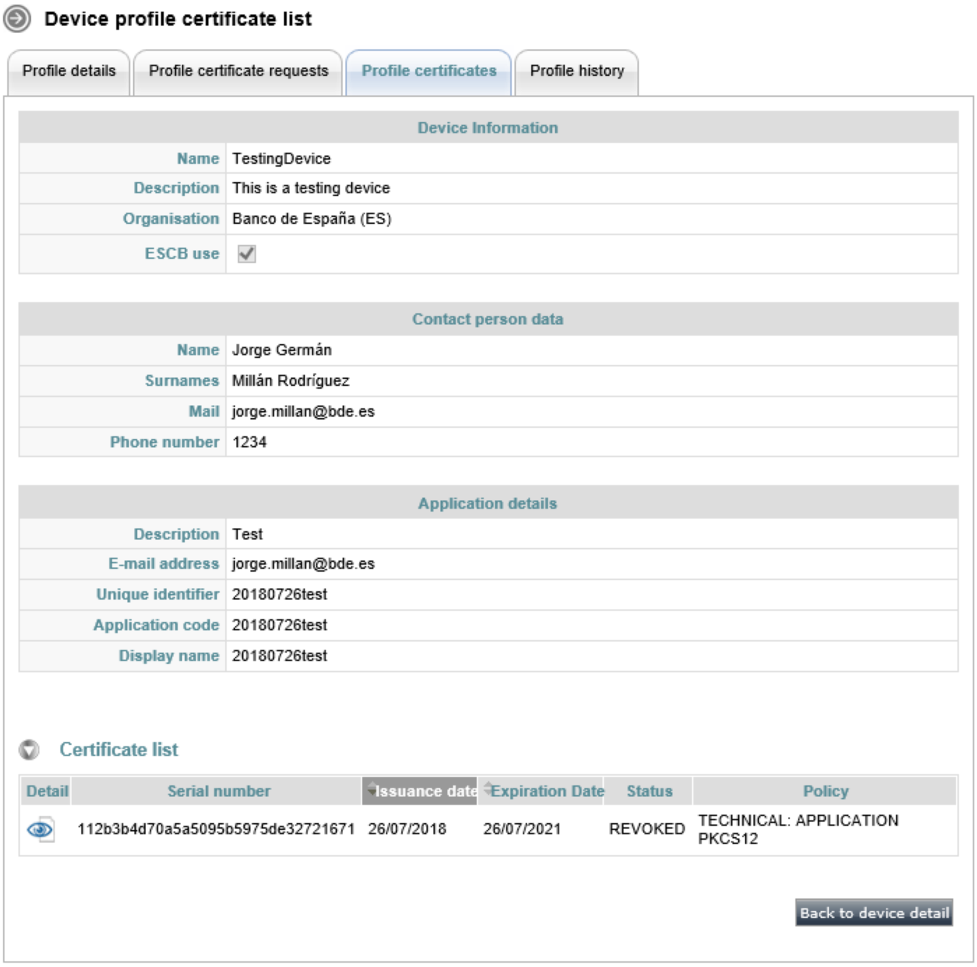
Cause: The certificate profile is not applicable.

Cause: ERROR - CertMngError_SigningAlgorithmNotAllowed

Figure 26 - Download certificate file

5.2.4.4. Profile certificates

The “profile certificates” tab allows displaying the certificates associated to the device. Additionally, the RO4TC can use this tab to revoke, suspend and activate certificates.



Device profile certificate list

Device Information

Name	TestingDevice
Description	This is a testing device
Organisation	Banco de España (ES)
ESCB use	☑

Contact person data

Name	Jorge Germán
Surnames	Millán Rodríguez
Mail	jorge.millan@bde.es
Phone number	1234

Application details

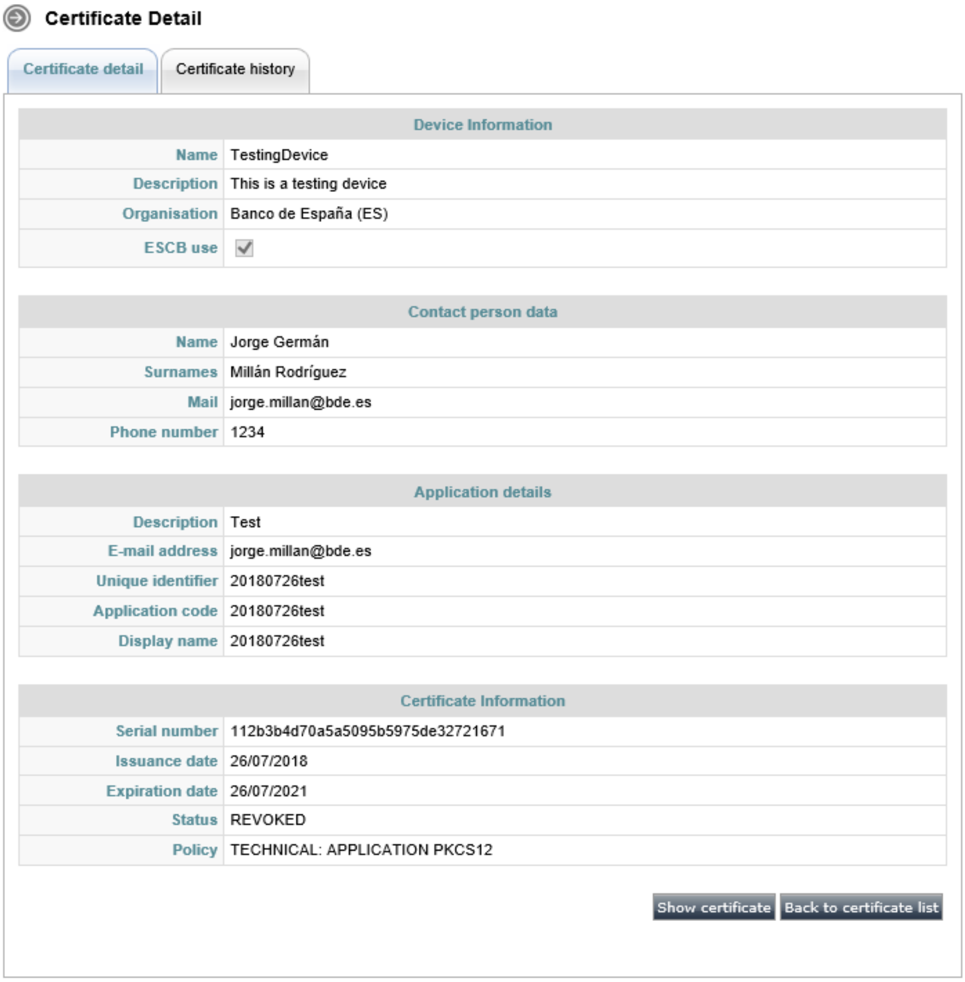
Description	Test
E-mail address	jorge.millan@bde.es
Unique identifier	20180726test
Application code	20180726test
Display name	20180726test

Certificate list

Detail	Serial number	Issuance date	Expiration Date	Status	Policy
	112b3b4d70a5a5095b5975de32721671	26/07/2018	26/07/2021	REVOKED	TECHNICAL: APPLICATION PKCS12

Figure 27 - Profile certificates

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



Certificate Detail

Device Information	
Name	TestingDevice
Description	This is a testing device
Organisation	Banco de España (ES)
ESCB use	☑

Contact person data	
Name	Jorge Germán
Surnames	Millán Rodríguez
Mail	jorge.millan@bde.es
Phone number	1234

Application details	
Description	Test
E-mail address	jorge.millan@bde.es
Unique identifier	20180726test
Application code	20180726test
Display name	20180726test

Certificate Information	
Serial number	112b3b4d70a5a5095b5975de32721671
Issuance date	26/07/2018
Expiration date	26/07/2021
Status	REVOKED
Policy	TECHNICAL: APPLICATION PKCS12

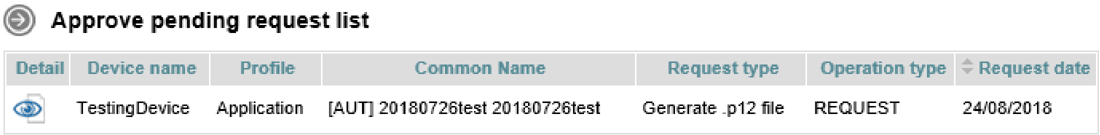
Figure 28 - Certificate detail

The buttons available at the “certificate detail” screen depend on the status of the certificate request and the role of the user:

- **Download**: this button allows the TCS and RO4TC to download a copy of the certificate. Only the .cer file is available and therefore it is not possible to get the .p12 (PKCS#12) file, in case that this request type was used to request the certificate (see section 5.2.4.3)
- **Revoke**: this button allows revoking the certificate. It is only available for to RO4TC when the certificate is not revoked. Certificate revocation cannot be reversed
- **Suspend**: this button allows suspending the certificate. It is only available for to RO4TC when the certificate is not suspended. Certificate suspension is similar to revocation, but it can be reversed
- **Activate**: this button allows activating a certificate. It is only available for to RO4TC when the certificate is suspended. Certificate activation allows enabling a certificate that has been suspended before

5.3. APPROVE AND PROCESS PENDING CERTIFICATE REQUESTS

The **Approve pending** option of the menu on the left enables the RO4TC role to have a direct access to the list of certificate requests that have been introduced by a TCS and that are pending to approve or cancel. Only the RO4TC role can see this option.



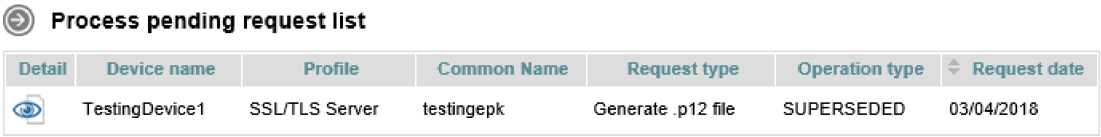
Approve pending request list

Detail	Device name	Profile	Common Name	Request type	Operation type	Request date
👁	TestingDevice	Application	[AUT] 20180726test 20180726test	Generate .p12 file	REQUEST	24/08/2018

Figure 29 - List of certificate requests pending to approve

The eye icon (👁)takes to the “request detail” screen (see section 5.2.4.3)

The **Process pending** option of the menu on the left enables the TCS role to have a direct access to the list of certificate requests that have been approved by a RO4TC and that are pending to process. Only the TCS role can see this option.



Process pending request list

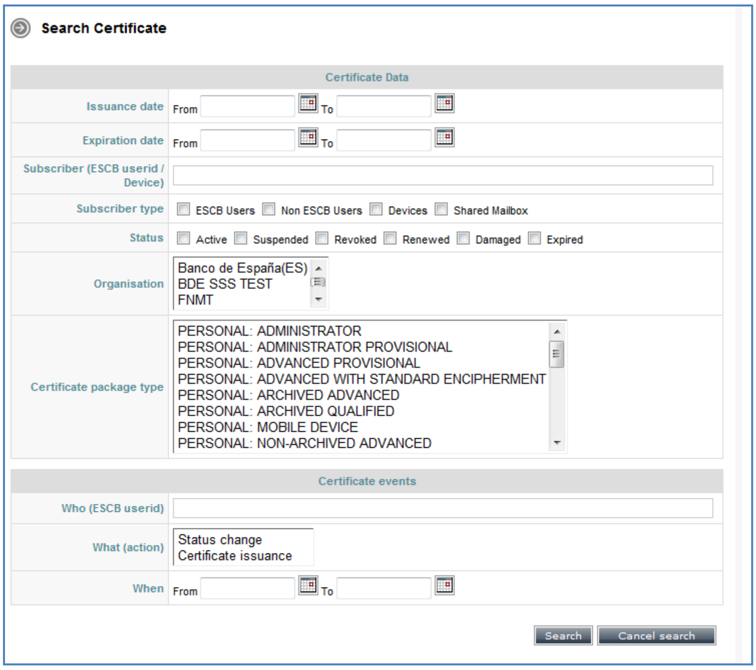
Detail	Device name	Profile	Common Name	Request type	Operation type	Request date
👁	TestingDevice1	SSL/TLS Server	testingepk	Generate .p12 file	SUPERSEDED	03/04/2018

Figure 30 - List of certificate requests pending to process

The eye icon (👁)takes to the “request detail” screen (see section 5.2.4.3)

5.4. CERTIFICATE AUDIT

From the ***Audit > Certificates*** option users with RO4TC role can access to the information about the technical certificates issued for your Central Bank.

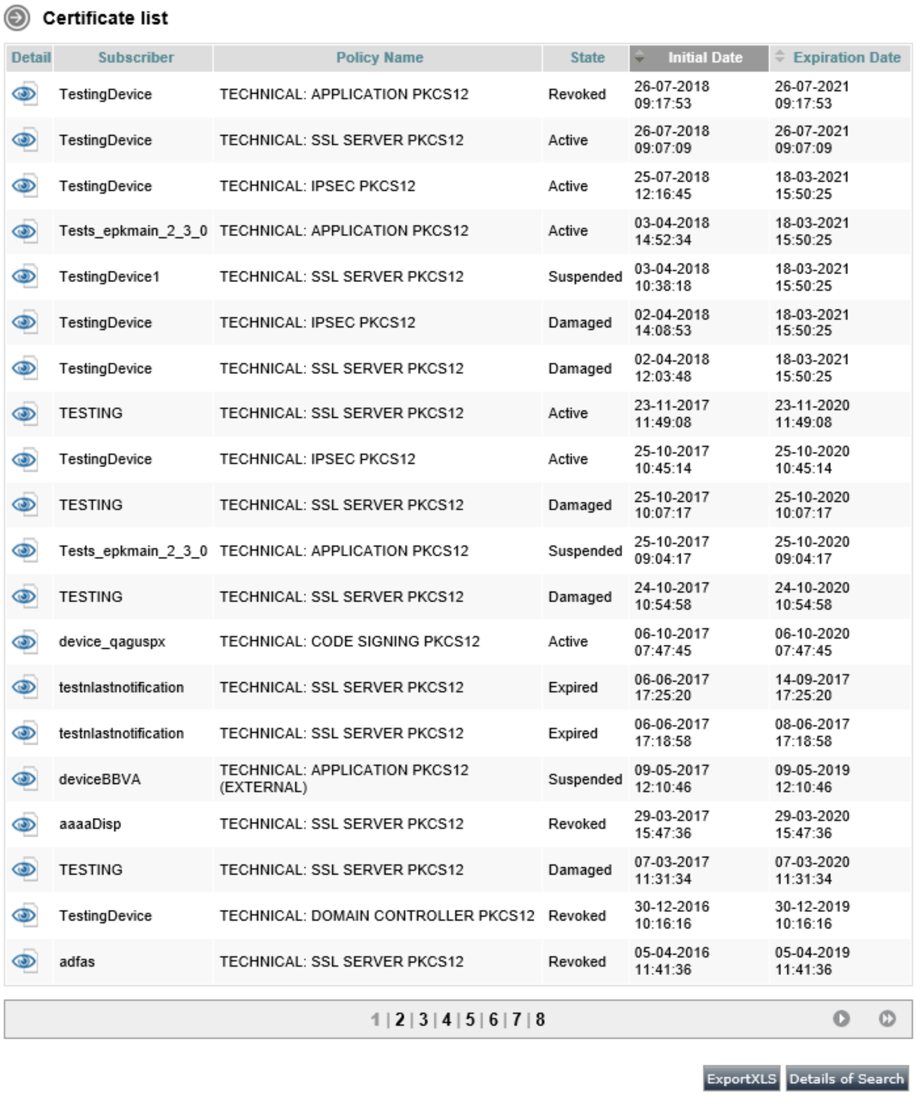


Search Certificate

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 31 - 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
👁	TestingDevice	TECHNICAL: APPLICATION PKCS12	Revoked	26-07-2018 09:17:53	26-07-2021 09:17:53
👁	TestingDevice	TECHNICAL: SSL SERVER PKCS12	Active	26-07-2018 09:07:09	26-07-2021 09:07:09
👁	TestingDevice	TECHNICAL: IPSEC PKCS12	Active	25-07-2018 12:16:45	18-03-2021 15:50:25
👁	Tests_epkmain_2_3_0	TECHNICAL: APPLICATION PKCS12	Active	03-04-2018 14:52:34	18-03-2021 15:50:25
👁	TestingDevice1	TECHNICAL: SSL SERVER PKCS12	Suspended	03-04-2018 10:38:18	18-03-2021 15:50:25
👁	TestingDevice	TECHNICAL: IPSEC PKCS12	Damaged	02-04-2018 14:08:53	18-03-2021 15:50:25
👁	TestingDevice	TECHNICAL: SSL SERVER PKCS12	Damaged	02-04-2018 12:03:48	18-03-2021 15:50:25
👁	TESTING	TECHNICAL: SSL SERVER PKCS12	Active	23-11-2017 11:49:08	23-11-2020 11:49:08
👁	TestingDevice	TECHNICAL: IPSEC PKCS12	Active	25-10-2017 10:45:14	25-10-2020 10:45:14
👁	TESTING	TECHNICAL: SSL SERVER PKCS12	Damaged	25-10-2017 10:07:17	25-10-2020 10:07:17
👁	Tests_epkmain_2_3_0	TECHNICAL: APPLICATION PKCS12	Suspended	25-10-2017 09:04:17	25-10-2020 09:04:17
👁	TESTING	TECHNICAL: SSL SERVER PKCS12	Damaged	24-10-2017 10:54:58	24-10-2020 10:54:58
👁	device_qaguspx	TECHNICAL: CODE SIGNING PKCS12	Active	06-10-2017 07:47:45	06-10-2020 07:47:45
👁	testnlastnotification	TECHNICAL: SSL SERVER PKCS12	Expired	06-06-2017 17:25:20	14-09-2017 17:25:20
👁	testnlastnotification	TECHNICAL: SSL SERVER PKCS12	Expired	06-06-2017 17:18:58	08-06-2017 17:18:58
👁	deviceBBVA	TECHNICAL: APPLICATION PKCS12 (EXTERNAL)	Suspended	09-05-2017 12:10:46	09-05-2019 12:10:46
👁	aaaaDisp	TECHNICAL: SSL SERVER PKCS12	Revoked	29-03-2017 15:47:36	29-03-2020 15:47:36
👁	TESTING	TECHNICAL: SSL SERVER PKCS12	Damaged	07-03-2017 11:31:34	07-03-2020 11:31:34
👁	TestingDevice	TECHNICAL: DOMAIN CONTROLLER PKCS12	Revoked	30-12-2016 10:16:16	30-12-2019 10:16:16
👁	adfas	TECHNICAL: SSL SERVER PKCS12	Revoked	05-04-2016 11:41:36	05-04-2019 11:41:36

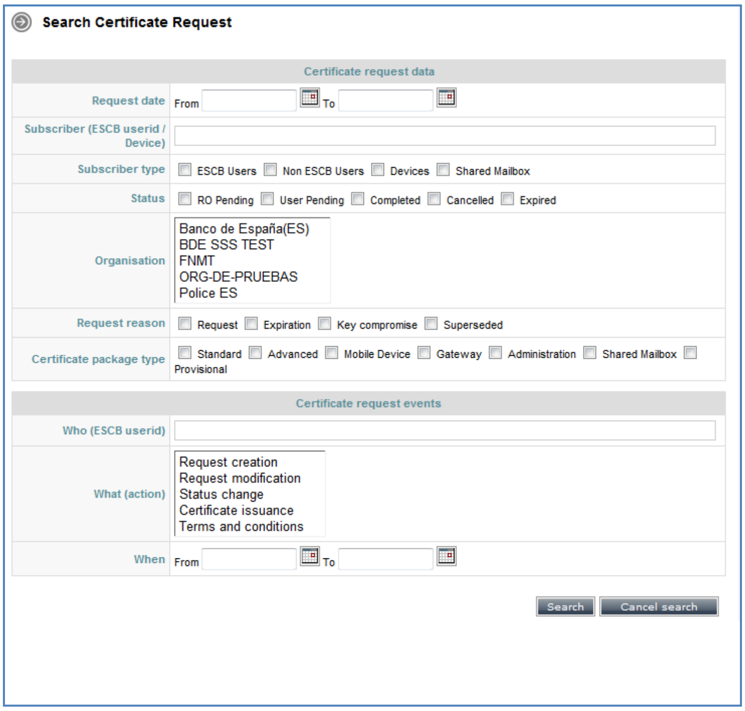
Figure 32 - Certificates list

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.

5.5. CERTIFICATE REQUESTS AUDIT

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

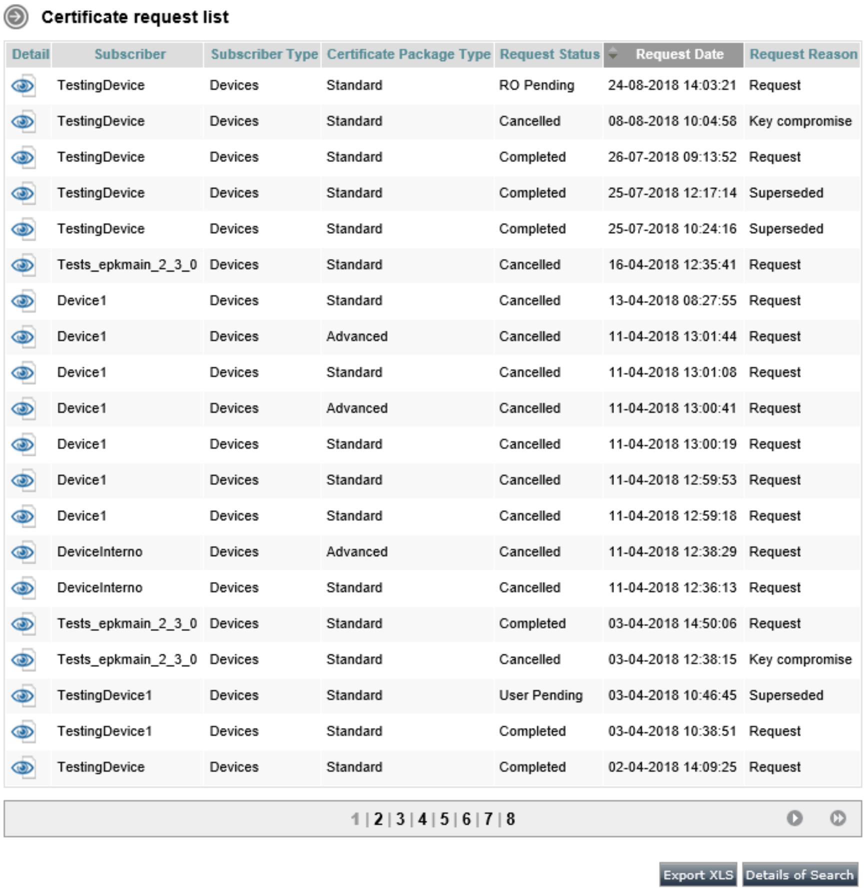


Search Certificate Request

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 33 - 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
👁	TestingDevice	Devices	Standard	RO Pending	24-08-2018 14:03:21	Request
👁	TestingDevice	Devices	Standard	Cancelled	08-08-2018 10:04:58	Key compromise
👁	TestingDevice	Devices	Standard	Completed	26-07-2018 09:13:52	Request
👁	TestingDevice	Devices	Standard	Completed	25-07-2018 12:17:14	Superseded
👁	TestingDevice	Devices	Standard	Completed	25-07-2018 10:24:16	Superseded
👁	Tests_epkmain_2_3_0	Devices	Standard	Cancelled	16-04-2018 12:35:41	Request
👁	Device1	Devices	Standard	Cancelled	13-04-2018 08:27:55	Request
👁	Device1	Devices	Advanced	Cancelled	11-04-2018 13:01:44	Request
👁	Device1	Devices	Standard	Cancelled	11-04-2018 13:01:08	Request
👁	Device1	Devices	Advanced	Cancelled	11-04-2018 13:00:41	Request
👁	Device1	Devices	Standard	Cancelled	11-04-2018 13:00:19	Request
👁	Device1	Devices	Standard	Cancelled	11-04-2018 12:59:53	Request
👁	Device1	Devices	Standard	Cancelled	11-04-2018 12:59:18	Request
👁	DeviceInterno	Devices	Advanced	Cancelled	11-04-2018 12:38:29	Request
👁	DeviceInterno	Devices	Standard	Cancelled	11-04-2018 12:36:13	Request
👁	Tests_epkmain_2_3_0	Devices	Standard	Completed	03-04-2018 14:50:06	Request
👁	Tests_epkmain_2_3_0	Devices	Standard	Cancelled	03-04-2018 12:38:15	Key compromise
👁	TestingDevice1	Devices	Standard	User Pending	03-04-2018 10:46:45	Superseded
👁	TestingDevice1	Devices	Standard	Completed	03-04-2018 10:38:51	Request
👁	TestingDevice	Devices	Standard	Completed	02-04-2018 14:09:25	Request

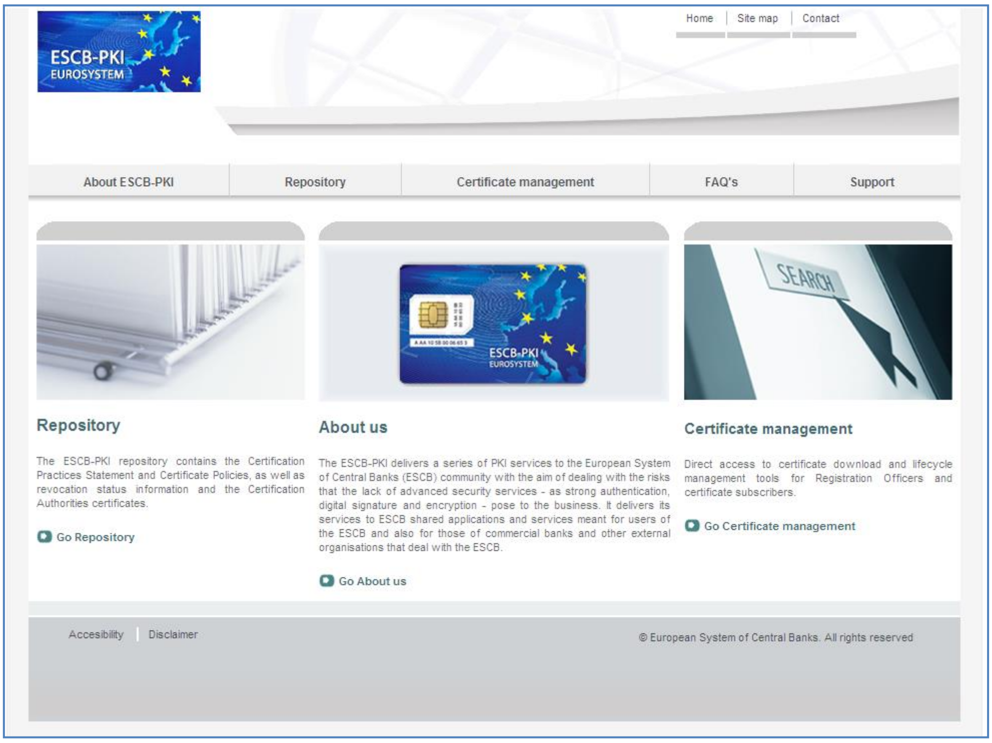
Figure 34 - Certificate requests list

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.

6. 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 35 - 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.