

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI PROJECT



SUBSCRIBER'S GUIDE

VERSION 3.1

TABLE OF CONTENTS

GLOSSARY AND ACRONYMS 6

1. Introduction..... 7

2. Personal certificates provided by the ESCB-PKI..... 8

 2.1. Software-based certificates 8

 2.2. Token-based certificates 9

3. End-user processes..... 10

 3.1. Request token-based certificates 10

 3.1.1. STEP 1: Preparation 11

 3.1.2. STEP 2: Request 11

 3.1.3. Notification..... 12

 3.1.4. STEP 3: Certificate acceptance/Download (face-to-face option) 12

 3.1.5. STEP 3: Certificate acceptance/Download (remote option) 14

 3.1.6. Notification..... 15

 3.1.7. Final recommendation: set your suspension code..... 15

 3.2. Request software-based certificates..... 16

 3.2.1. STEP 1: Preparation 17

 3.2.2. STEP 2: Request 17

 3.2.3. Notification..... 17

 3.2.4. STEP 3: Certificate acceptance/Download (face-to-face option) 18

 3.2.5. STEP 3: Certificate acceptance/Download (remote option) 19

 3.2.6. Notification..... 20

 3.2.7. STEP 4: Install your standard certificate..... 20

 3.2.8. Final recommendation: set your suspension code..... 21

 3.3. Certificate renewal (expired certificate) 22

 3.4. Certificate Suspension/reactivation (Key Compromise) 22

 3.5. Recover an old Encryption key..... 23

 3.6. Set your personal suspension code..... 23

4. ESCB-PKI Token Management 24

 4.1. Change your PIN..... 24

 4.2. Forgotten PIN 24

 4.3. Check your certificates..... 25

 4.4. Forgotten PIN and PUK 25

 4.5. Damaged token 25

 4.6. Lost / Stolen token 26

5. More information about ESCB-PKI..... 27

 5.1. Certificate management 28

TABLE OF ILLUSTRATIONS

Figure 1 - Token-based certificate request process.....	10
Figure 2 - Software-based certificate request process	16
Figure 3 - ESCB-PKI Website.....	27
Figure 4 - ESCB-PKI Website: Certificate management	28

Project name:	ESCB-PKI
Author:	ESCB-PKI Project team
File name:	ESCB-PKI - Subscriber's Procedures v.2.0.docx
Version:	3.1
Date of issue:	31.12.2023
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
0.1	Draft	07.10.2011	Initial version
0.2	Draft	15.10.2011	Several additions
0.10	Draft	20.10.2011	BdE Revision
0.11	Draft	05.11.2011	BdE Revision
0.12	Draft	14.11.2011	BdE Revision
0.16	Draft	28.11.2011	BdE Revision
1.0	Draft	24.01.2012	Version for SRM-WG revision
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	20.12.2022	Terms and Conditions acceptance procedure update
3.1	Final	31.12.2023	Updated http links to ESCB-PKI website to https

GLOSSARY AND ACRONYMS

Acronym	Definition
CB	ESCB Central Bank (ECB or NCB)
ECB	European Central Bank
ESCB-PKI	European System of Central Banks - Public Key Infrastructure
FAQ	Frequently Asked Questions
IAM	Identity and Access Management
NCB	National Central Bank
PIN	Personal Identification Number
PUK	Personal Unlock Number
PKI	Public Key Infrastructure
RO	Registration Officer
SSCD	Secure Signature Creation Device

1. INTRODUCTION

The present document aims at providing information on how to manage ESCB-PKI certificates from the end user's point of view.

This document has three main blocks:

- 1) The first part will depict the user processes from the perspective of the certificate lifecycle (Chapter 3)
- 2) The second block will explain the processes from the token lifecycle angle (Chapter 4)
- 3) Finally, the last chapter presents the ESCB-PKI Website (Chapter 5)

2. PERSONAL CERTIFICATES PROVIDED BY THE ESCB-PKI

The following certificates will be available for ESCB users:

Software-based

- 1) Standard certificates: used for authentication, signing and encryption.
- 2) Mobile device certificates: used within mobile devices for authentication and signature.
- 3) Secure e-mail gateway: to be installed in a secure e-mail gateway to sign and encrypt on behalf of the end user.

Token-based

- 1) Advanced certificates: used for authentication, signing and encryption.
- 2) Administrator certificates: used for users that have got a second account that they use for administrator tasks. They are mainly valid for authentication although they can also be used for signature.
- 3) Provisional certificates: used temporarily when a user with token-based certificates (either advanced or administrator) has forgotten his smartcard or token. They have limited lifetime.

The difference between standard and advanced certificates relies on where the digital certificate is kept: while for token-based certificates the private keys are stored inside a physical token (i.e. smart card, USB token, etc.), for software-based certificates the private keys are stored in a software container such as a file or a keystore.

This simple difference has further implications regarding the level of trust that can be achieved. The usage of token-based certificates provides a higher level of trust.

2.1. SOFTWARE-BASED CERTIFICATES

According to the *ESCB Identity and Access Management Policy* software-based certificates can be used to authenticate against applications with a criticality assessment up to Medium.

ESCB-PKI provides the following types of software-based certificates:

- Standard certificates: general purpose software-based certificate valid for authentication, signature and encryption
- Mobile device certificates: typically used in a mobile device for authentication and signature. This certificate can be complemented with a copy of the encryption private key that is part of an advanced certificate package and that has been recovered in software format.
- Secure e-mail gateway certificates: certificate valid for encryption and signature to be installed in a secure e-mail gateway to implement secure e-mail.

2.2. TOKEN-BASED CERTIFICATES

According to the *ESCB Identity and Access Management Policy*, token-based certificates can be used to authenticate against applications which have a criticality assessment Medium, High or Very High.

ESCB-PKI provides the following types of token-based certificates:

- **Advanced certificates:** this is a package of three different certificates: i) authentication, ii) signature and iii) encryption. Depending on what your Central Bank has decided, there could be two different types of advanced certificate packages:
 - **Advanced certificate package with encryption key recovery.**
 - The authentication and signature private keys are generated inside the cryptographic token, so that there is not any other copy. Therefore, these certificates are considered “advanced”
 - The encryption private key is generated by the Certification Authority and stored i) in the token and ii) in the Key Archive. In the future you will be able to recover a copy of the encryption private key from the Key Archive in software or token-based formats when i) your smartcard card has been replaced and you need to decrypt old information or ii) you need a software-based copy of your encryption private key to be stored in a mobile device. Since the private key can be recovered in software-based format, this certificate is considered “standard”
 - **Advanced certificate package without encryption key recovery.**
 - The authentication, signature and encryption private keys are generated inside the cryptographic token, so that there is not any other copy. Therefore, the three certificates are considered “advanced”. You have to take into account and, if your smartcard is replaced, you will not be able to decrypt old information that was encrypted for you.
- **Administrator certificates:** this is a single certificate mainly valid for authentication, although you can also use it for signature. This certificate is used in case that you have got an account that is linked to the authentication certificate included in the advanced certificate package, and a second account used for administrator tasks and that is linked to this certificate. The private key is generated inside the token.
- **Provisional certificates:** this is a certificate with a limited lifetime that is stored in a provisional token in case that you have forgotten your smartcard or token with advanced or administrator certificates. The certificate is valid for authentication and signature. The certificate will expire at the end of the date of the issuance. Optionally, your Registration Officer can request a longer certificate with the maximum lifetime defined by your Central Bank’s Security Officer.

3. END-USER PROCESSES

3.1. REQUEST TOKEN-BASED CERTIFICATES

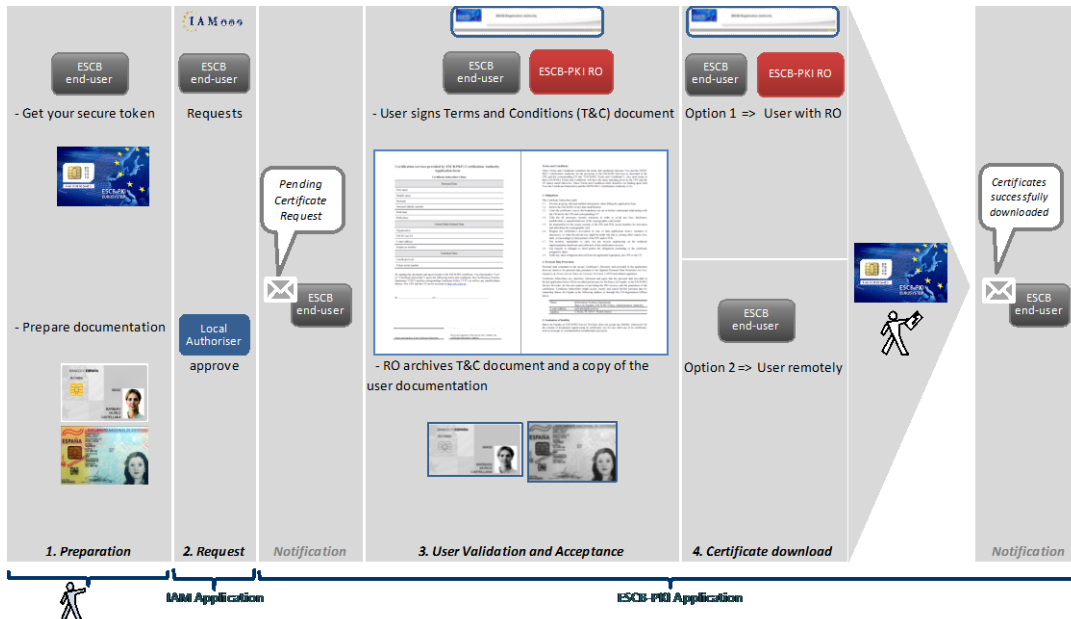


Figure 1 - Token-based certificate request process

The process, which will be described in greater detail in the following sections, can be summarized as follows:

- 1) The user must obtain a secure token and prepare all the documentation needed.
- 2) The user must request an ESCB-PKI advanced or administrator certificate using IAM interfaces. Provisional certificates can only be requested by a Registration Officer via ESCB-PKI interface for administrators.

When the request is approved the user will receive an email stating *“certificate request process initiated”*.

- 3) The user must accept and sign the ESCB-PKI Terms and Conditions online using the button *“Terms and Conditions”* located in the certificate request page at the ESCB-PKI Website.

According to the ESCB-PKI CPS an evidence of the signed Terms and Conditions document will be kept for 15 years.

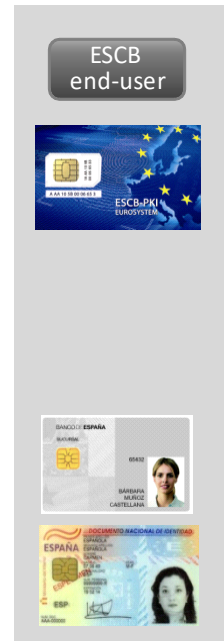
- 4) The user may then download the certificates into their secure token.

The user will receive an email stating: *“process completed”*


3.1.1. STEP 1: PREPARATION

- 1) Obtain your personal secure token.
 - This token may be an ESCB-PKI token or any other ESCB-PKI certified secure token. You can check the list of certified tokens at the ESCB-PKI website.
 - Set your personal PIN.
 - Please remind that you have to keep both your personal PIN and personal PUK (code used to reset the PIN of the secure device in case you forget it) secrets.

- 2) Prepare the documentation needed. To request your certificate you must present to your Registration Officer either:
 - A legal document accepted by the legislation applicable to the Central Bank acting as Registration Authority to dully identify an individual. Examples of valid documents are your National ID Card and your Passport.
 - Your Employee ID Card if you are an employee of the Central Bank acting as Registration Authority



3.1.2. STEP 2: REQUEST

- 1) Enter to the end-user IAM interface. Select the option **Request an ESCB certificate.**
 - Select the type of certificate to be requested: **“TOKEN”** (meaning “advanced”) or **“ADMINISTRATOR”**.
 - Select your preference for the certificate delivery:
 - **“FACE-TO-FACE”** with the RO support.
 - **“REMOTE”** without the RO support.
 - Select the reason for the request: **“NEW CERTIFICATE”**.
 - Enter the serial number of your personal secure token. If you are using an ESCB-PKI secure token, the serial number is printed on the card. 

- 2) The request must be approved.



NOTE. - Possible reasons for the request:


- **NEW CERTIFICATE** New certificate requested.
- **CERTIFICATE EXPIRATION** Old certificate is next to expiring.
- **LOST CERTIFICATE** Old certificates have been compromised (i.e. token lost or stolen).
- **REPLACED TOKEN/UNRECOVERABLE CERTIFICATE** Old certificates not available (i.e. token damaged or forgotten PIN and PUK).

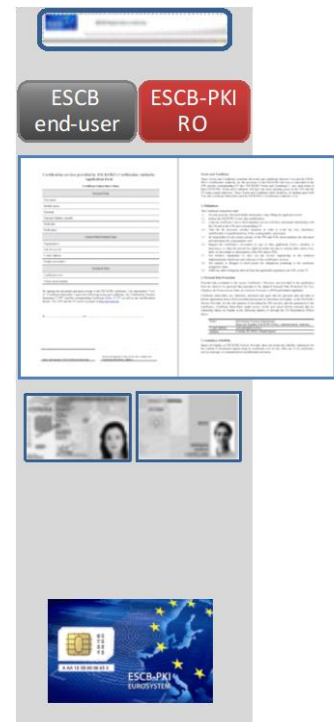
3.1.3. NOTIFICATION

When the request is approved, if you entered the token serial number you will receive an email of confirmation and you can then proceed to the next step. If you did not enter the token serial number, your Registration Officers will receive a notification to enter the token serial number before proceeding with the next step, and you will receive an email confirmation afterwards.



3.1.4. STEP 3: CERTIFICATE ACCEPTANCE/DOWNLOAD (FACE-TO-FACE OPTION)

- 1) Come before your Registration Officer (RO), holding your personal secure token and your personal documentation.
 - The RO validates the correctness of the information included in the request (validates it against the user documentation).
- 2) Read, accept and sign the Terms and Conditions document online at the ESCB-PKI Website. To do so you may complete the following steps:
 - a) At the ESCB-PKI Website click the "**Certificate delivery for remote users**" option. You must authenticate using your IAM user-id/password. You may also use the "**Personal Certificate management**" option. For this option to work you must first authenticate using a CAF compliant advanced certificate.
 - b) Select the adequate certificate request by clicking in the  button - the request details will be displayed. Then click the **Terms and Conditions** button.
 - c) The Terms and Conditions page will be opened where you can accept and sign them.



The RO will start the certificate download:


- 3) Insert your secure token in the reader and enter your personal PIN.
 - The key-pair will be generated into your personal secure token. Take into account that the process will take some time because, in the case of the advanced certificate package, three key-pairs will be generated (authentication, encryption and signing).

- The three certificates will be stored in your personal secure token.
- 4) According to the ESCB-PKI CPS an evidence of the signed Terms and Conditions document will be kept for 15 years.

3.1.5. STEP 3: CERTIFICATE ACCEPTANCE/DOWNLOAD (REMOTE OPTION)

1) At the ESCB-PKI Website click the "**Certificate delivery for remote users**" option. You must authenticate using your IAM user-id/password. You may also use the "**Personal Certificate management**" option. For this option to work you must first authenticate using a CAF compliant advanced certificate.


- All requests currently associated with your user-id will be displayed.

2) Select the **RO-pending** request by clicking in the  button - the request details will be displayed. Then click the **Terms and Conditions** button.

- The Terms and Conditions page will be opened where you can accept and sign them.
- Send a copy of your personal documentation to your RO¹.

If everything is correct the RO will allow the remote download. Then you will receive an email with the link to the ESCB-PKI application.

3) Click again on the "**Certificate delivery for remote users**" option. All requests currently associated to your user-id will be displayed.

4) Select the **User-Pending** request clicking in the  button, the details of the request will be shown.

5) Insert your token in the reader and click on the **Download** button. If the serial number of the token is not the one indicated in the request an error will be displayed.

6) The system will display the list of certificates that will be generated.

- Click on the **Accept** button.
- The system will prompt you to enter your personal PIN. The key-pair will be generated into your personal secure token. Take into account that the process will take some time because, in the case of the advanced certificate package, three key-pairs will be generated (authentication, encryption and signing)
- The 3 certificates will be stored in the secure token.



¹ If you have been identified by means of your Central Bank employee id card there is no need to send a copy of this documentation

3.1.6. NOTIFICATION

When the certificates are downloaded an email will be sent to the user.



3.1.7. FINAL RECOMENDATION: SET YOUR SUSPENSION CODE

The suspension code is used to request the suspension of your certificates. This code is the only way to prove you were the actual owner of your certificates in case your personal secure token is lost or stolen.

If you have not done it before, set now your ESCB-PKI suspension code using the "**Personal Certificate management**" option in the ESCB-PKI webpage.

3.2. REQUEST SOFTWARE-BASED CERTIFICATES

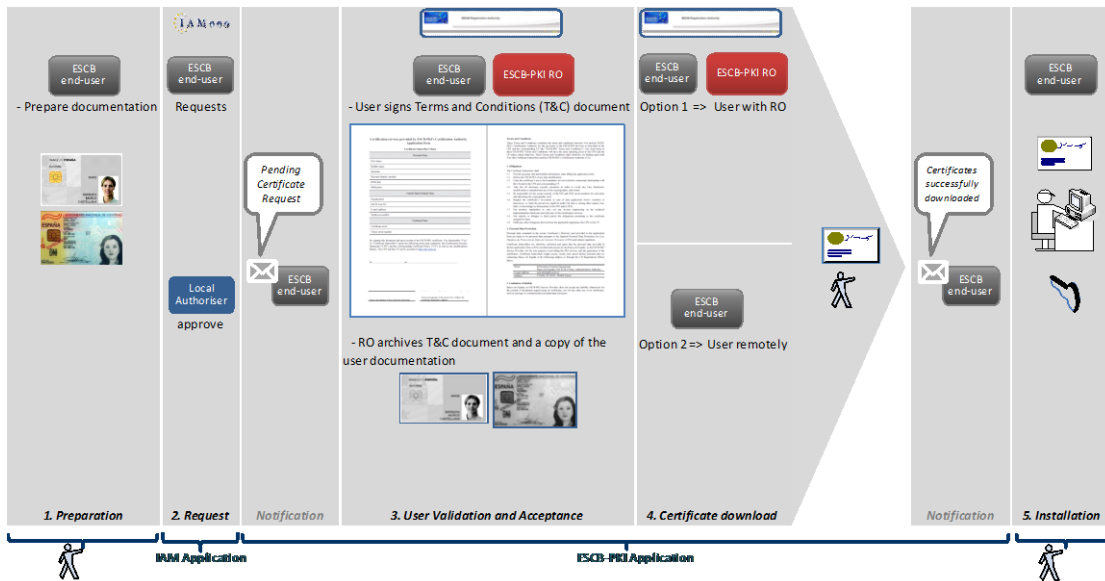


Figure 2 - Software-based certificate request process

The process, which will be described in greater detail in the following sections, can be summarized as follows:

- 1) The user must prepare all the documentation needed.
- 2) The user must request an ESCB-PKI software-based certificate (i.e. standard, mobile device or secure e-mail gateway) using IAM interfaces.

When the request has been approved the user will receive an email stating the following: *"certificate request process initiated"*

- 3) The user must accept and sign the ESCB-PKI Terms and Conditions online using the button "Terms and Conditions" located in the certificate request page at the ESCB-PKI Website.

According to the ESCB-PKI CPS an evidence of the signed Terms and Conditions document will be kept for 15 years.

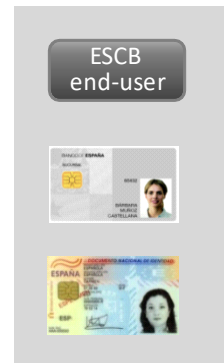
- 4) The user may then download the certificate.

The user will receive an email stating *"process completed"*.

- 5) The user installs the certificate in the PC, mobile device or secure e-mail gateway.

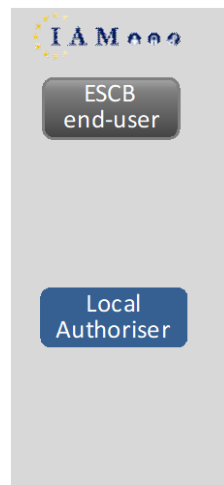
3.2.1. STEP 1: PREPARATION

- 1) Prepare the documentation needed. To request your certificate you must deliver to your Registration Officer either:
 - A legal document accepted by the legislation applicable to the Central Bank acting as Registration Authority to dully identify an individual. Examples of valid documents are your National ID Card and your Passport.
 - Your Employee ID Card if you are an employee of the Central Bank acting as Registration Authority



3.2.2. STEP 2: REQUEST

- 1) Enter to the end-user IAM interface. Select the option **Request an ESCB certificate**.
 - Select the type of certificate to be requested: **“SOFTWARE”**(meaning “standard”), **“MOBILE DEVICE”** or **“SECURE E-MAIL GATEWAY”**.
 - Select your preference for the certificate delivery:
 - **“FACE-TO-FACE”** with the RO support.
 - **“REMOTE”** without the RO support.
 - Select the reason for the request: **“NEW CERTIFICATE”**.
- 2) The request must be approved.



NOTE. - Possible reasons for the request:


- **NEW CERTIFICATE** New certificate requested.
- **CERTIFICATE EXPIRATION** Old certificate is next to expiring.
- **LOST CERTIFICATE** Old certificate has been compromised (i.e. PIN compromise, stolen PC).
- **REPLACED TOKEN/UNRECOVERABLE CERTIFICATE** Old certificate not available (i.e. file damaged or forgotten PIN).

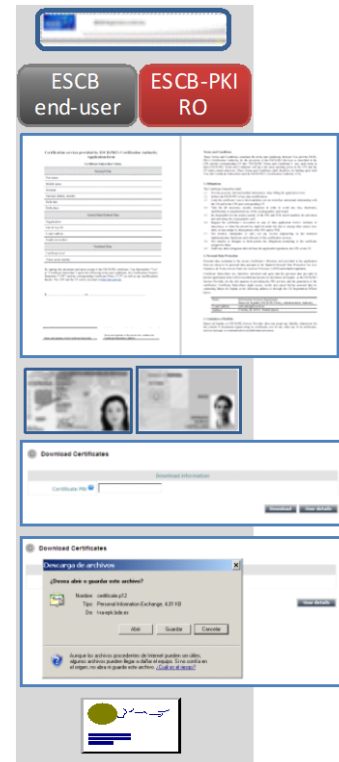
3.2.3. NOTIFICATION

When the request is approved you will receive an email; you can then proceed to the next step.



3.2.4. STEP 3: CERTIFICATE ACCEPTANCE/DOWNLOAD (FACE-TO-FACE OPTION)

- 1) Come before your Registration Officer (RO) with your personal documentation.
 - The RO validates the correctness of the information included in the request).
- 2) Read, accept and sign the Terms and Conditions document online at the ESCB-PKI Website. To do so you may complete the following steps:
 - a) At the ESCB-PKI Website click the "**Certificate delivery for remote users**" option. You must authenticate using your IAM user-id/password. You may also use the "**Personal Certificate management**" option. For this option to work you must first authenticate using a CAF compliant advanced certificate.
 - b) Select the adequate certificate request by clicking in the  button - the request details will be displayed. Then click the **Terms and Conditions** button.
 - c) The Terms and Conditions page will be opened where you can accept and sign them.




The RO will start the certificate download:

- 3) You will be requested to set a PIN code to protect the certificate and the keys generated.
 - Type your PIN and click on the **Download** button.
- 4) The RO will download the keys into a file protected by your PIN.
 - The certificate will be downloaded to the local system, protected by the PIN, to ensure that only you and no one else has access to the private key.
- 5) According to the ESCB-PKI CPS an evidence of the signed Terms and Conditions document will be kept for 15 years.


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

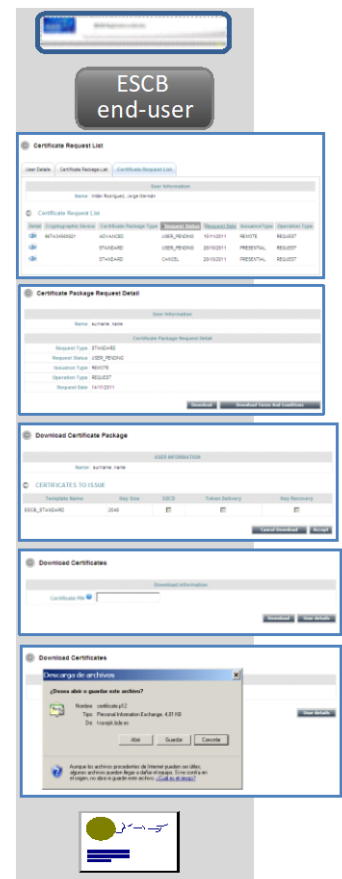
3.2.5. STEP 3: CERTIFICATE ACCEPTANCE/DOWNLOAD (REMOTE OPTION)

- 1) In the ESCB-PKI Website select the "**Certificate delivery for remote users**" option. You have to authenticate using your IAM user-id / password. You may also use the "**Personal certificate management**" option. In that case you must authenticate using a CAF compliant certificate.
 - All requests currently associated to your user-id will be displayed.
- 2) Select the **RO-Pending** request clicking on the  button, the details of the request will be shown. Then click on the **Terms and conditions** button.
 - The Terms and Conditions page will be opened where you can accept and sign them.
 - Send a copy of your personal documentation to your RO.



If everything is correct the RO will allow the remote download. Then you will receive an email with the link to the ESCB-PKI application.

- 3) Select again the "**Certificate delivery for remote users**" option. All requests currently associated to your user-id will be displayed.
- 4) Select the **User-Pending** request clicking on the  button and the details of the request will be presented.
- 5) Click on the **download** button.
- 6) The details of the certificate are shown. Click on the **Accept** button.
- 7) The system will request you to type a PIN to protect the certificate and keys generated. Type your PIN and click on the **Download** button.
- 8) The keys and the certificate will be generated and a File Download dialog box will pop up asking "**Do you want to open or save this file?**"
 - Click **Save** to download the keys into a file protected by your PIN.



If you open the .p12 file, 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.

If you click on the **Cancel** button the process will be cancelled and you will not be able to download your certificates

The certificate will be downloaded to the local system, protected by the PIN; that will ensure that only you and no one else can access to the private key.

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

3.2.6. NOTIFICATION

When the certificates are downloaded an email will be sent to the user.



3.2.7. STEP 4: INSTALL YOUR STANDARD CERTIFICATE

The ESCB-PKI will deliver your standard certificate in a .P12 file. To install your certificate in your PC you must follow your Operating System and Web browser recommendations. Please contact your Local Help Desk if you need additional support.

This is an example of the process to be followed to install your certificate in a Windows environment with Internet Explorer.

- 1) Open the .P12 file and follow MS Wizard instructions to extract the keys and the certificate (click on the **Next** button).
- 2) You will be requested to type the PIN that protects your .P12 file.
 - Type your PIN.
 - Check the option “Enable strong private key protection” to protect the copy of the private key that is going to be installed in the MS Windows account.
 - Check the option “Mark this key as exportable” if you want that the copy of the private key that is going to be installed in the MS Windows account is ready to be exported again in the future.
- 3) Select the “Personal” certificate store to install the certificate and corresponding private key (click on the **Next** button until the process ends).



- 4) MS Windows will immediately start a new Wizard to install the certificate into the Internet Explorer container.
 - To protect your certificate, change the security level to **HIGH**.
 - Type the password to protect your private key once installed into your Windows account. You will be asked for this password whenever you use the private key (e.g. while authenticating in an application). Do not mistake this password with the one of the password-protected file, although both can be the same if you wish.
 - Then click on the **Accept** button.

- 5) Your certificate will be installed in the Internet Explorer certificate container.

NOTE: Detailed information available the ESCB-PKI "*User guide: importing and exporting standard certificates*" which is also available in the ESCB-PKI Website.

3.2.8. FINAL RECOMENDATION: SET YOUR SUSPENSION CODE

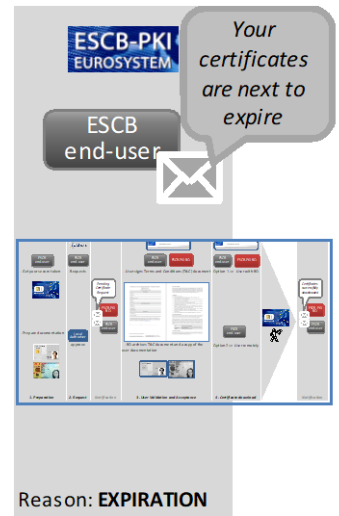
The suspension code is the only way to identify you in case your certificate is compromised (lost).

If you haven't done it before, set your ESCB-PKI suspension code. You will use this code to request the suspension of your certificate.

3.3. CERTIFICATE RENEWAL (EXPIRED CERTIFICATE)

When your certificate is next to expiring you will receive a message to remind you that you have to renew your certificates. In fact you will receive several messages, a first message 100 days before the expiration date, a second message 45 days before the expiration date and a third message 15 days before the expiration date.

- 1) The process you must follow to renew your certificates is the one described in previous sections of this chapter to request new certificates
 - The reason for the request (step 2) would be **CERTIFICATE EXPIRATION**

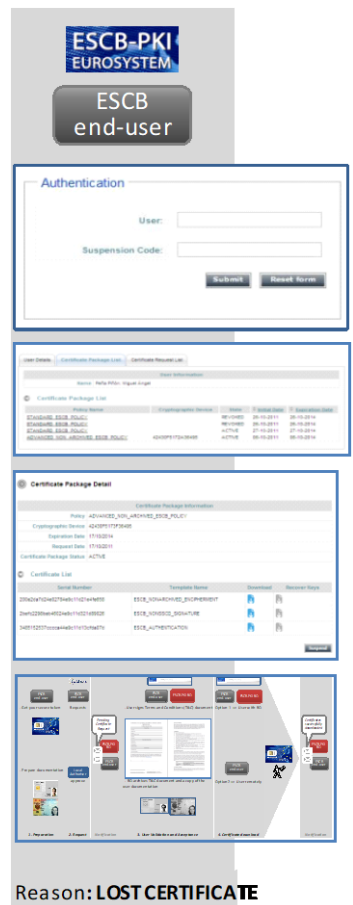


3.4. CERTIFICATE SUSPENSION/REACTIVATION (KEY COMPROMISE)

If you suspect that your keys have been comprised, you must perform the following actions:

- 1) First of all, suspend your compromised certificates to avoid that anyone could use them anymore
 - In the ESCB-PKI Website select the "**Certificate suspension**" option. You must authenticate using your ESCB-PKI suspension code (See **NOTE** below)
- 2) In the **Certificate list** tab select the certificate you want to suspend
- 3) Click on the **Suspend** button. Your certificates will be suspended

To reactivate your suspended certificates, in case you discover that no compromise do exist, you must send a request to your registration officer
- 4) Request new certificates (see previous sections in this chapter)
 - The reason for the request (step 2) would be **LOST CERTIFICATE**. This process will revoke your old compromised certificates



NOTE. - You could also use the "**Personal Certificate management**" option. In that case you must authenticate using a CAF compliant certificate.

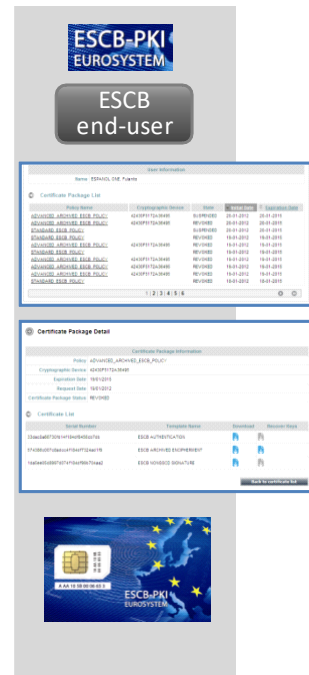
3.5. RECOVER AN OLD ENCRYPTION KEY

To recover an old encryption key² you must follow the steps described below:

- 1) At the ESCB-PKI Website click on the "**Personal Certificate management**" option. You must authenticate using a CAF compliant certificate.
- 2) In the left side menu of the application select the **Certificates** option and click on the certificate package you want to recover.
- 3) Insert your personal secure token in the reader and click on the



- 4) To store the keys and the certificate in your personal secure token the system will prompt you to type your personal PIN.

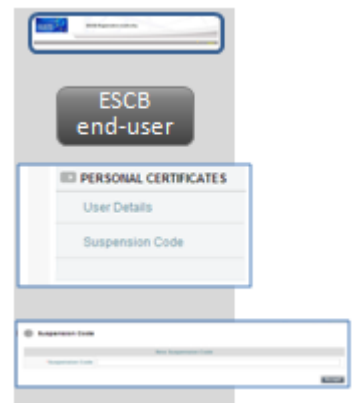


3.6. SET YOUR PERSONAL SUSPENSION CODE

The suspension code is used to request the suspension of your certificates. This code is the only way to prove you were the actual owner of your certificates in case your software certificate is lost or stolen.

To set your ESCB-PKI suspension code:

- 1) In the ESCB-PKI Website select the "**Personal certificate management**" option. You must authenticate using your ESCB-PKI certificate.
- 2) Select the **Suspension code** link from the left frame menu
 - Set your suspension code.



² For example, if your personal secure token was damaged and you have a new token, you may need to recover your old encryption key to decrypt old messages or documents.

4. ESCB-PKI TOKEN MANAGEMENT

The ESCB-PKI token is a secure device certified against the standard FIPS 140-2 Level 3.

You will receive your ESCB-PKI token along with a **closed BLIND ENVELOPE**. Inside this envelope you will find a document containing the PUK, the initial PIN and also the serial number of your token (this serial number is also printed in the secure token).

The PUK must be kept in a safe place. You will use this code to unlock your token in case it gets locked (e.g. this will happen after 5 wrong attempts to enter the PIN)

To manage your ESCB-PKI token you will need to install the token driver software in your computer. The driver is available in the ESCB-PKI Website (support tab).

Please contact to your Local Help Desk for assistance to install it on your PC.

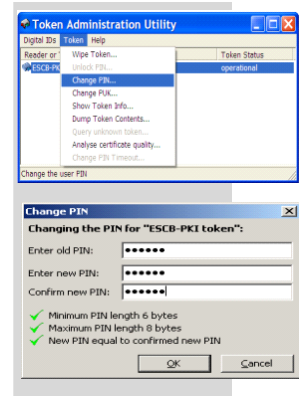


4.1. CHANGE YOUR PIN

You may change the initial PIN for a new one easier for you to remember:

- 1) Execute the token management tool.
- 2) Select the **Token** → **Change PIN** option.
- 3) Type your old PIN and the new PIN (twice). Press OK.

NOTE. – Do not use special characters for your PIN code.



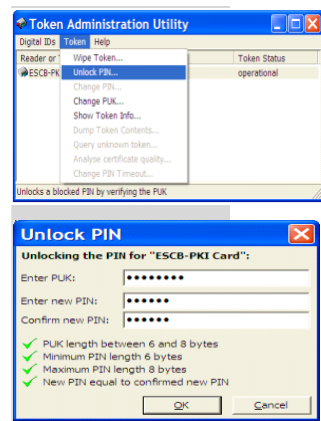
4.2. FORGOTTEN PIN

If you forget your PIN code or your token gets blocked, you have to set a new PIN. To do this, you must use your PUK.

The process can be summarized as follows:

- 1) Execute the token management tool.
- 2) Select the **Token** → **Reset PIN** option.
- 3) Type your **PUK** and the new PIN (twice). Press OK.

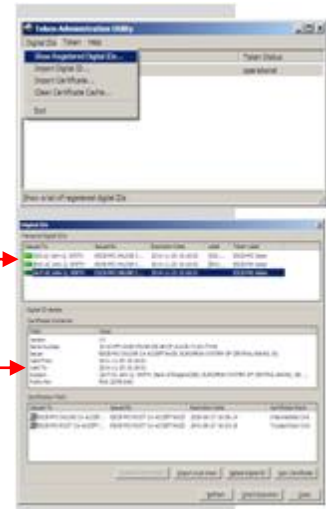
NOTE. – Do not use special characters for your PIN code.



4.3. CHECK YOUR CERTIFICATES

With the token management tool you can also check the certificates stored in your secure token:

- 1) Execute the token management tool.
- 2) Select the **Digital ids** → **Show registered digital ids** option.
- 3) The tool will show in the upper window all the certificates currently stored in your token.
- 4) Clicking on any certificate, the detailed information will be shown in the lower window.



4.4. FORGOTTEN PIN AND PUK

If you are not able to remember neither your PIN code nor your PUK it will be impossible to recover the certificates contained in your token and the token will remain unusable. In that situation you must:

- 1) Request a new secure token.
- 2) Request new advanced certificates (see chapter 3.1).
 - The reason for the request (step 2) will be **REPLACED TOKEN**.



4.5. DAMAGED TOKEN

If your token gets damaged, the process will be similar to the previous one:

- 1) Request a new secure token.
- 2) Request new advanced certificates (see chapter 3.1).
 - The reason for the request (step 2) will be **REPLACED TOKEN**.

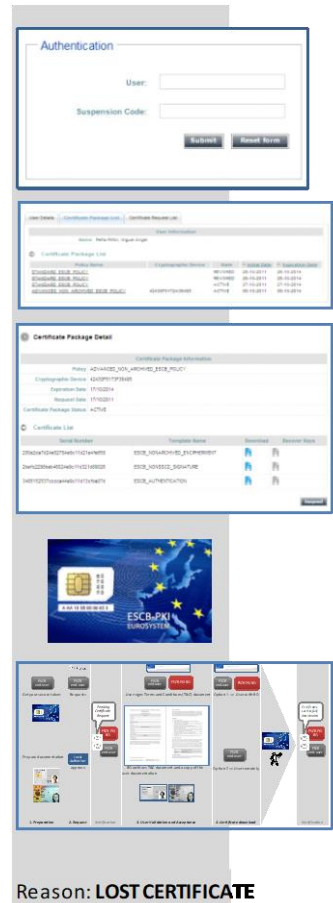


4.6. LOST / STOLEN TOKEN

If your secure token has been stolen or gets lost, your private keys could be compromised. The process you must follow is:

- 1) First of all, suspend your compromised certificates to avoid that anyone could use them anymore. In the ESCB-PKI Website select the "**Certificate suspension**" option. You must authenticate using your ESCB-PKI suspension code.
- 2) In the **Certificate list** select the certificate you want to suspend.
- 3) Click on the **Suspend** button. Your certificates will be suspended.
- 4) Request a new secure token.
- 5) Request new advanced certificates (see chapter 3.1).
 - The reason for the request (step 2) will be **LOST CERTIFICATE**.

NOTE.- In case you recover your token before having requested a new secure token and can assure that no compromise has taken place, in order to reactivate your suspended certificates you must request your Registration Officer to re-activate your suspended certificates for you.



5. 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.

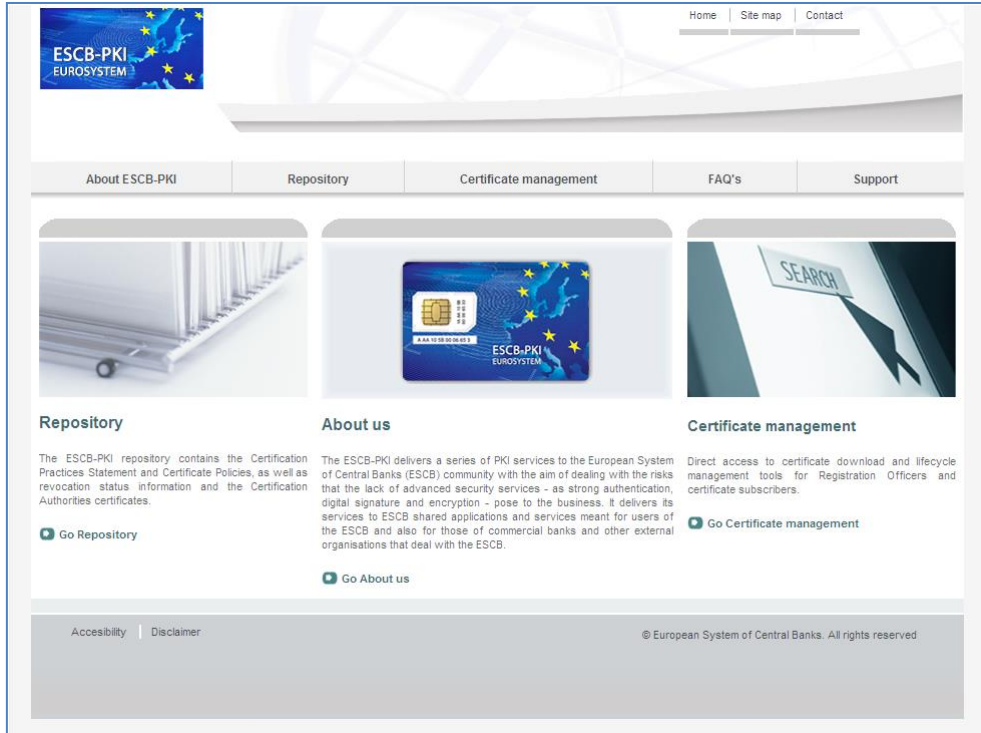


Figure 3 - ESCB-PKI Website

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.

5.1. CERTIFICATE MANAGEMENT

To enter to the RA application you must go into to the Certificate management tab in the ESCB-PKI Website

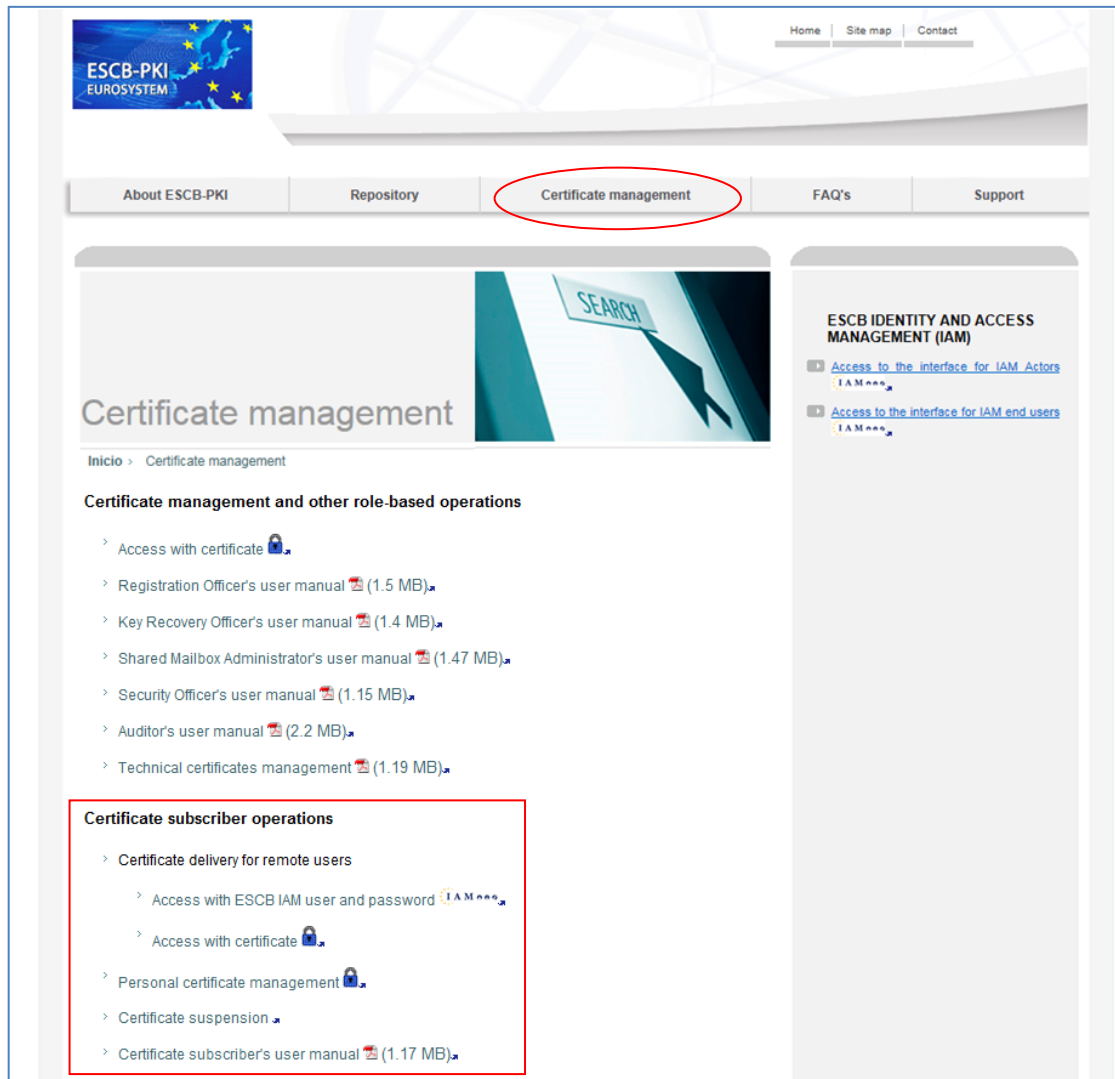


Figure 4 - ESCB-PKI Website: Certificate management

This web page contains the list of the ESCB-PKI services available to subscribers, namely:

- Certificate delivery for remote users
- Personal Certificate management
- Certificate suspension