KDPW | The Central Securities Depository of Poland

Remote Renewal of SWI Certificates

User’s Manual

Version 2.1

Table of Contents

Introduction

The User's Manual assists users in remote renewal of certificates used in the Information Exchange System (SWI).

The remote certificate renewal system available at https://cert.kdpw.pl allows users to renew certificates from their work stations without having to visit KDPW S.A. To be renewed, certificates must still be valid and cannot be revoked.

Remote renewal is available for certificates provided as PKCS#12 files.

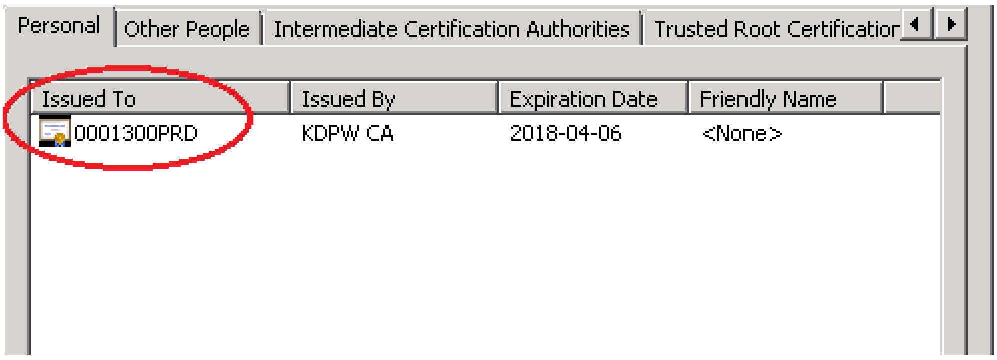
Accessing the system

Before renewing an Information Exchange System certificate, users must follow the steps below:

1. Check the system requirements described in the section "System requirements".

2. Prepare the certificate and the security password.

   The purpose of certificates is coded in the ending of the certificate name shown in the field "Issued to". Certificates issued by KDPW have the following codes in the field "Issued by": KDPW CA or KDPW CA RCT.


Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification

Issued To	Issued By	Expiration Date	Friendly Name
0001300PRD	KDPW CA	2018-04-06	<None>

The ending codes are:

PRD	– ESDI/WEB system production certificate;
TST	– ESDI/WEB system test certificate;
SDKP	– ESDK system production certificate;
SDKT	– ESDK system test certificate.

System requirements

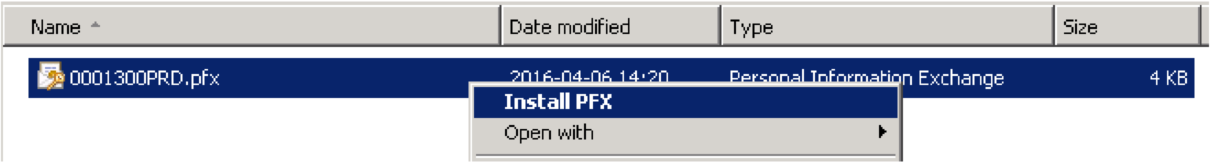
1. Operating system
    - Microsoft Windows 10
    - Java version 8

2. Web browser
    - Internet Explorer 11, Firefox, Chrome

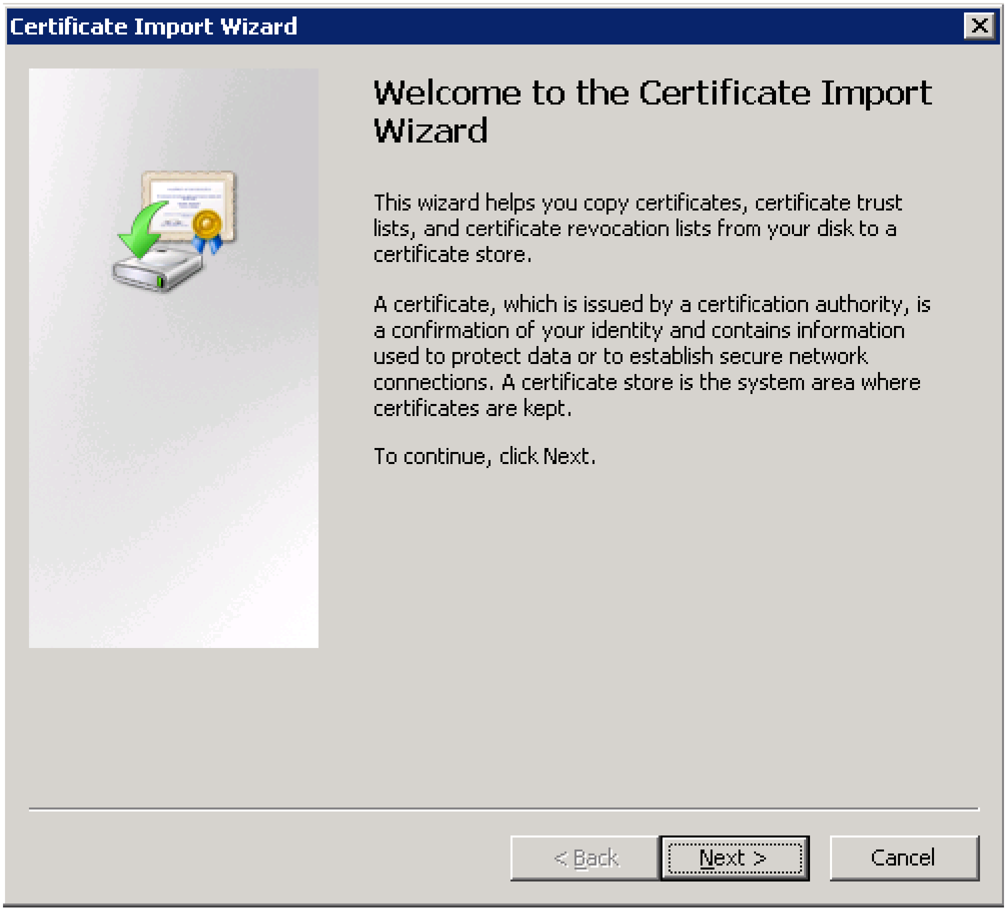
Installing a user certificate

To install a certificate in a *.p12 or *.pfx file, follow the steps below:

1. Log in the account of the user who is to use the certificate.
2. Right-click the certificate file and select the option “Install PFX” from the context menu.



3. The Certificate Import Wizard will open. Click “Next”.



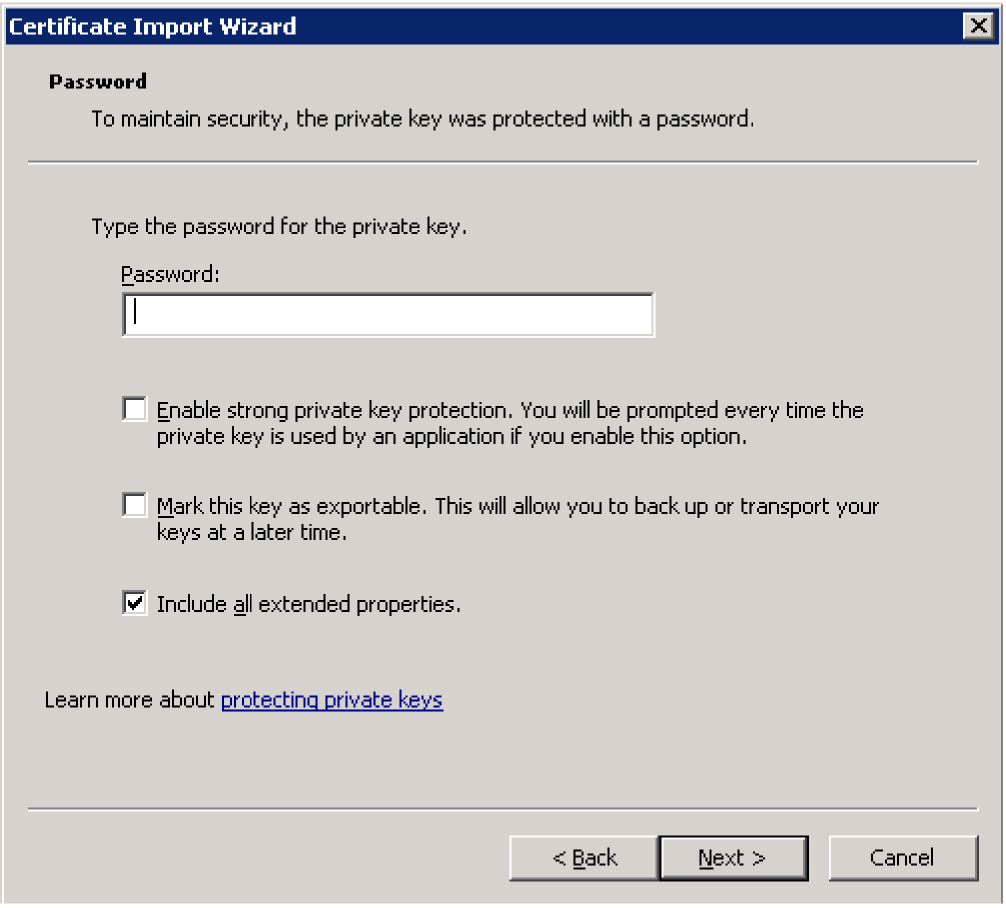
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

4. In the next window, enter the security password of the certificate file and confirm by clicking “Next”.



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

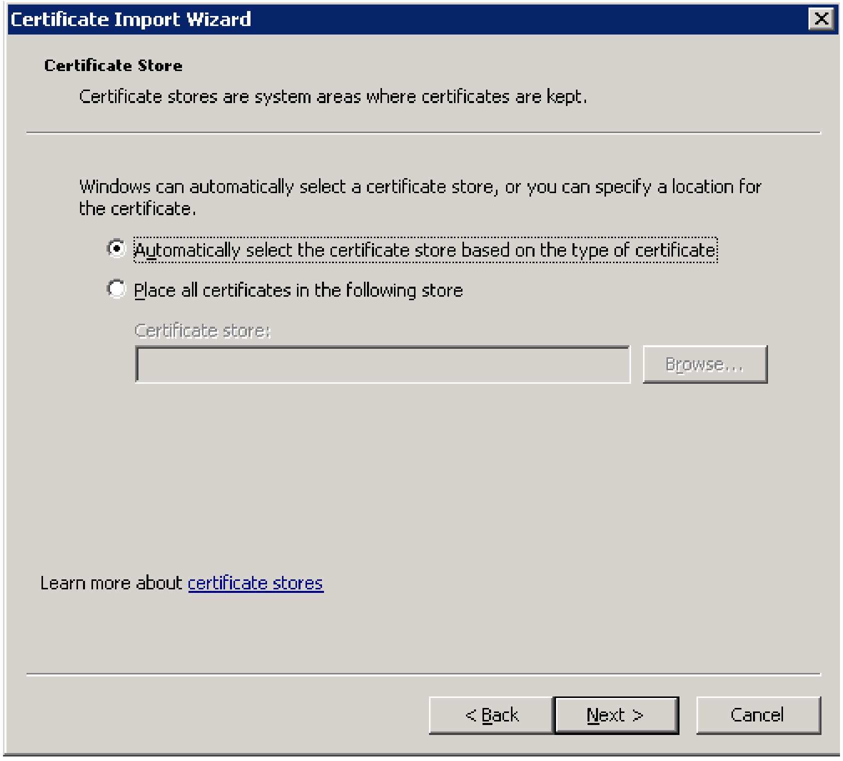
□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

Learn more about protecting private keys

We recommend to check the option “Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option”. If you enable this option, the certificate security password will be required at each time to use the certificate.

5. In the next window, make sure that the option “Automatically select the certificate store based on the type of certificate” is enabled.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

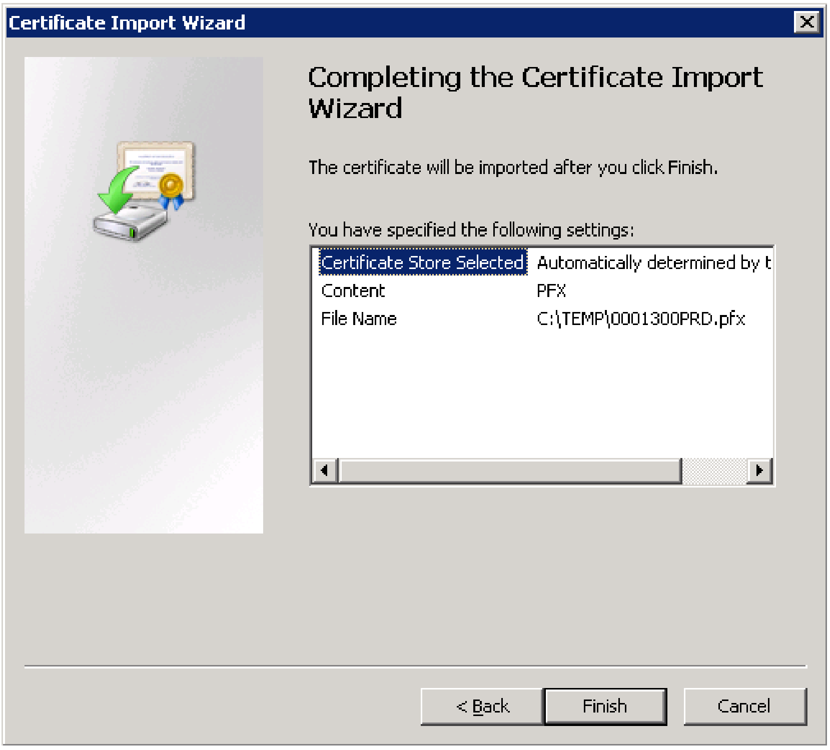
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

Learn more about certificate stores

6. In the next window, click “Finish”.



Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

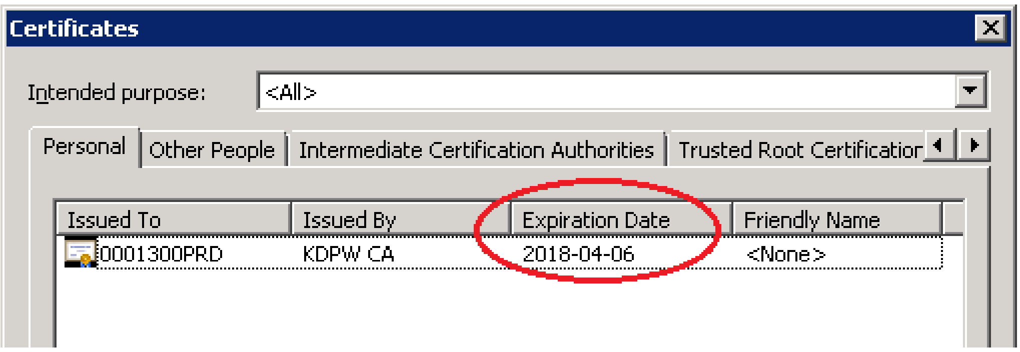
You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PFX
File Name	C:\TEMP\0001300PRD.pfx

Checking the certificate validity period

To check the certificate validity period, follow the steps below:

1. You must have an installed certificate; if you don’t, install a certificate according to the steps in the section “Installing a user certificate”.
2. Launch the web browser.
3. In the menu, select “Tools” → “Internet options” → “Content” → “Certificates”.
4. Go to the “Personal” tab.
5. In the certificate list window, the column “Expiration date” shows the expiration date of the certificate.


Certificates
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certificatior

Intended purpose: <All>

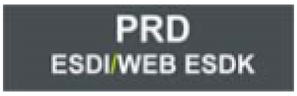
Issued To	Issued By	Expiration Date	Friendly Name
0001300PRD	KDPW CA	2018-04-06	<None>

Remote renewal of an ESDI/WEB user certificate

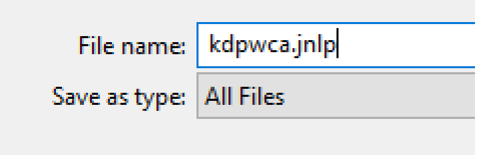
To renew a user’s certificate, follow the steps below:

1. Launch the web browser and go to https://cert.kdpw.pl.
2. In the menu, select the option “SWI – Production certificates” or “SWI – Test certificates”.
3. Depending on the version of the web browser used, there are different methods of downloading the program for remote renewal.

3.1 If you’re using Internet Explorer, right click on the image



and select “Save Target As”. In the “Save As” window, select directory where the file will be saved and save it under any name with the extension ".jnlp", e.g.:

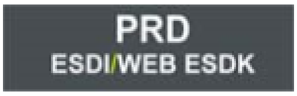


File name: kdpwca.jnlp

Save as type: All Files

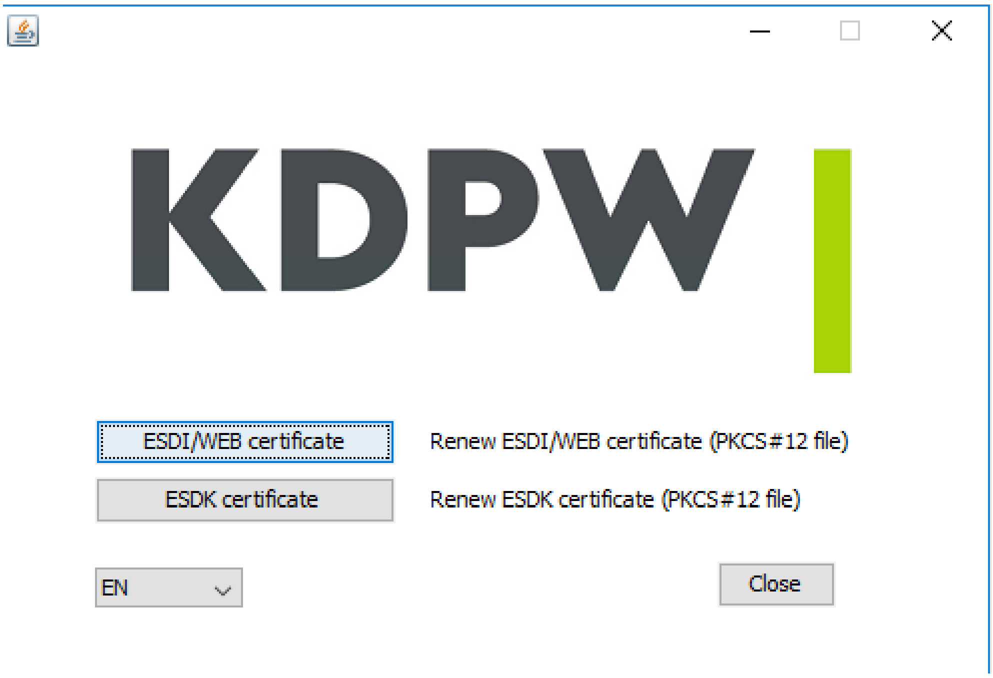
After saving the file, open it.

3.2 If you’re using Firefox or Chrome, click on the image



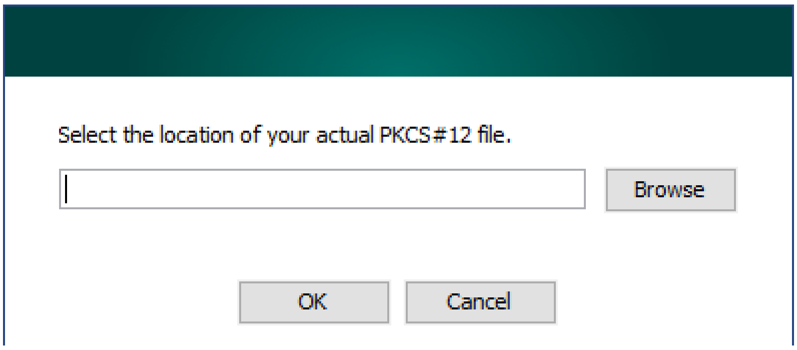
and run the file with jnlp extension, which will be downloaded.

4. The program will start


KDPW
ESDI/WEB certificate
Renew ESDI/WEB certificate (PKCS#12 file)
ESDK certificate
Renew ESDK certificate (PKCS#12 file)
EN
Close

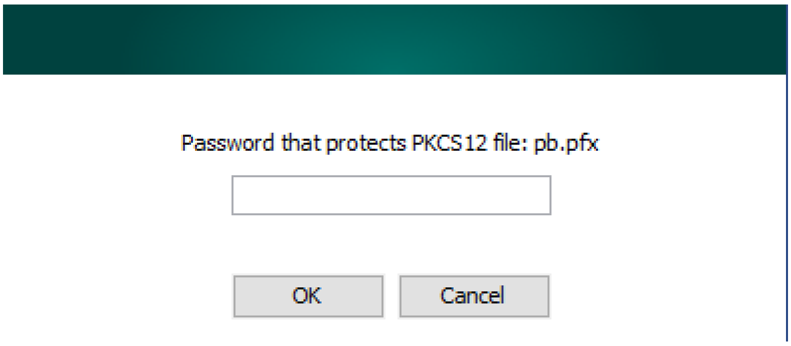
5. Select option “ESDI/WEB certificate”

6. In the window


Select the location of your actual PKCS#12 file.

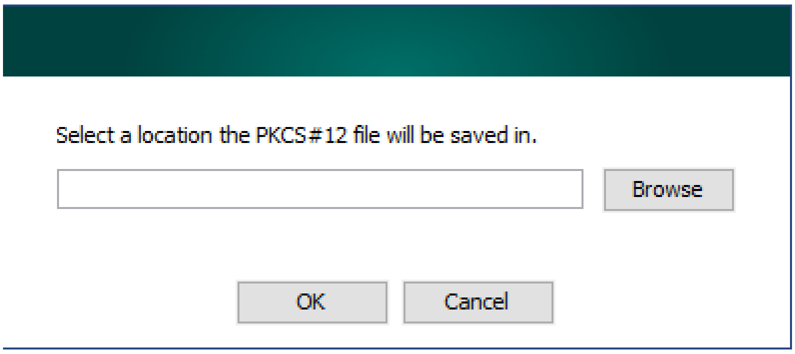
select the key file, that will be renewed.

7. In the window


Password that protects PKCS12 file: pb.pfx

enter the security password of the file, and then click “OK”.

8. In the window



Select a location the PKCS#12 file will be saved in.

select the target location to save the file and click “OK” The password of the new file will be the same as the password of the original file.

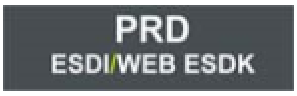
Note! Installation of new certificate is required.

Remote renewal of an ESDK user certificate

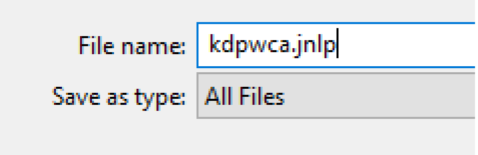
To renew a user’s certificate, follow the steps below:

1. Launch the web browser and go to https://cert.kdpw.pl.
2. In the menu, select the option “SWI – Production certificates” or “SWI – Test certificates”.
3. Depending on the version of the web browser used, there are different methods of downloading the program for remote renewal.

3.1 If you’re using Internet Explorer, right click on the image



and select “Save Target As”. In the “Save As” window, select directory where the file will be saved and save it under any name with the extension ".jnlp", e.g.:

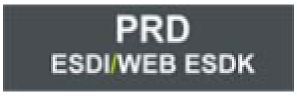


File name: kdpwca.jnlp

Save as type: All Files

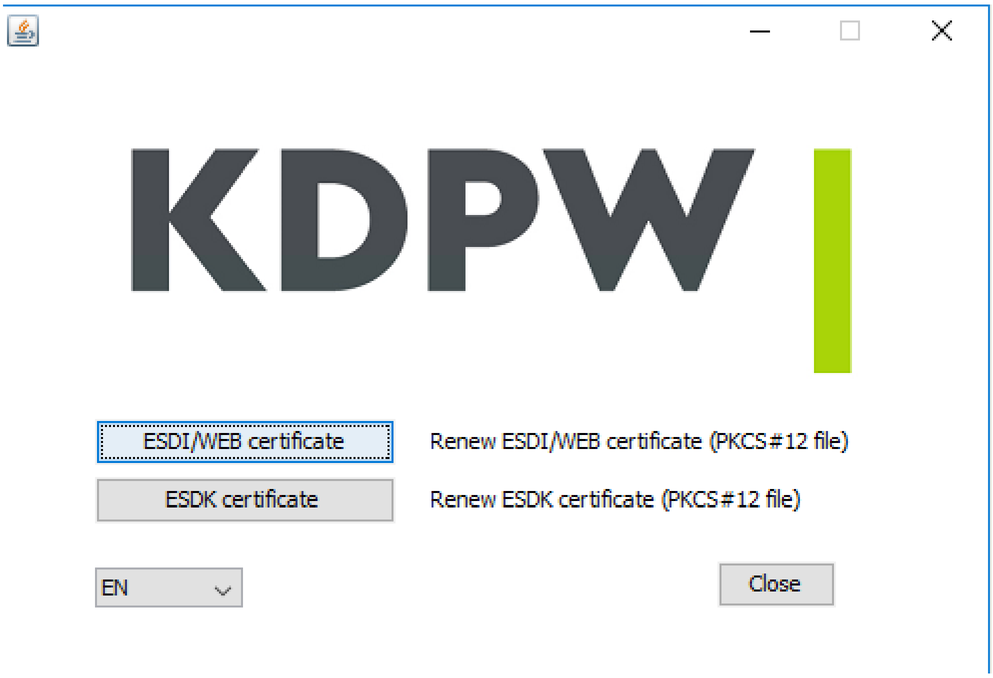
After saving the file, open it.

3.2 If you’re using Firefox or Chrome, click on the image



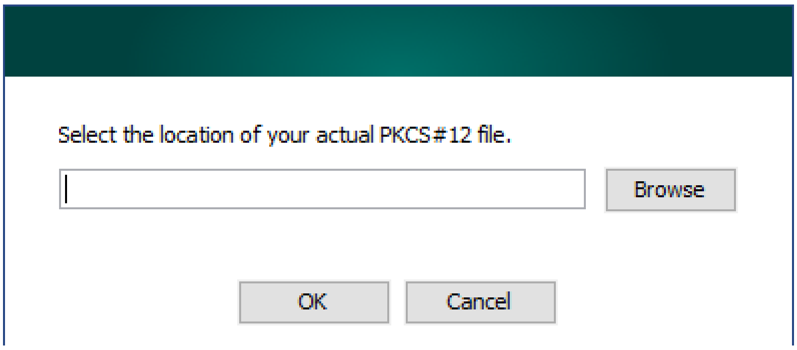
and run the file with jnlp extension, which will be downloaded.

4. The program will start


KDPW
ESDI/WEB certificate
Renew ESDI/WEB certificate (PKCS#12 file)
ESDK certificate
Renew ESDK certificate (PKCS#12 file)
EN
Close

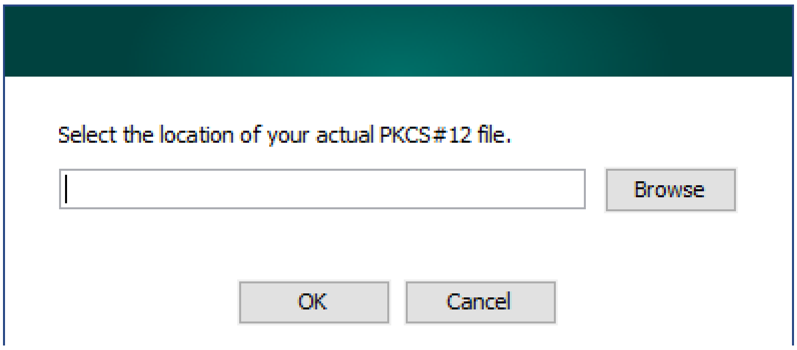
5. Select option “ESDK certificate”

6. In the window


Select the location of your actual PKCS#12 file.

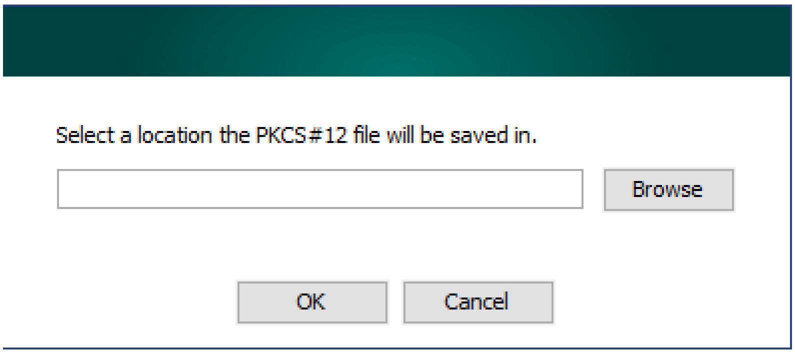
select the key file, that will be renewed.

7. In the window


Select the location of your actual PKCS#12 file.

enter the security password of the file, and then click “OK”.

8. In the window



Select a location the PKCS#12 file will be saved in.

select the target location to save the file and click “OK” The password of the new file will be the same as the password of the original file.

Note! Installation of new certificate is required.