Krajowy Depozyt Papierów Wartościowych

# Remote Renewal of SWI Certificates

## User's Manual

Version 1.1

# Table of Contents

Introduction ..... 3
Accessing the system ..... 4
System requirements ..... 5
Installing a user certificate ..... 8
Checking the certificate validity period ..... 11
Remote renewal of an ESDI/WEB user certificate in a card ..... 12
Remote renewal of an ESDI/WEB user certificate in a file ..... 14
Remote renewal of an ESDK user certificate ..... 16
Remote renewal of a VPN connection certificate ..... 18
Java applet trouble-shooting ..... 20

# 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.

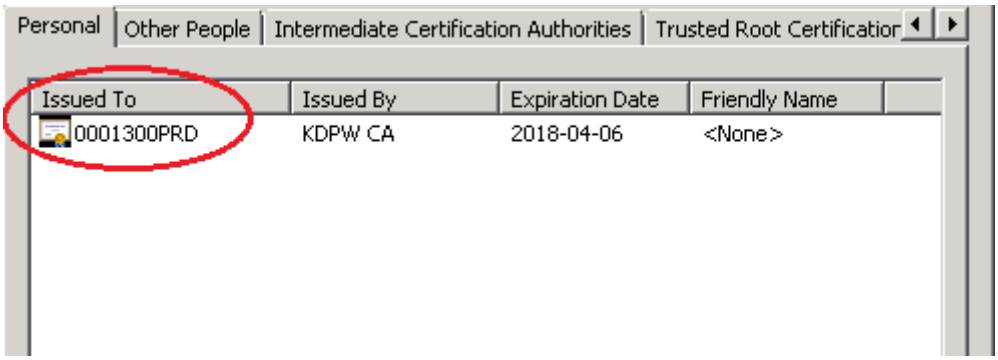
Remote renewal is available for certificates provided as cryptographic cards or PKCS#12 files.

# 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 PIN/password.
   Certificates may be provided as cryptographic cards or PKCS#12 files.
   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, KDPW CA RCT or KDPW CA VPN.




   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;
   VPN – VPN connection certificate.

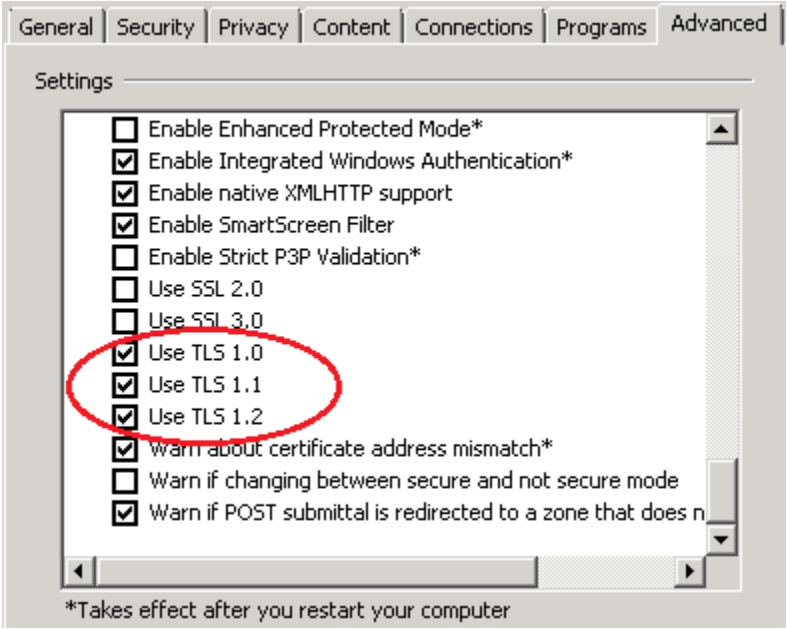
# System requirements

1. Operating system
   - Microsoft Windows 7, 8, 8.1, 10.
   - Java version 8 (32-bit).
   - SafeSign version 2.2 or a cryptographic card reader (only where the certificate to be renewed is provided as a card).

2. Web browser
   - Microsoft Internet Explorer version 11.
   - TLS protocol enabled.
   - The website https://cert.kdpw.pl added to the “Trusted sites” list.

The TLS protocol can be enabled in the web browser by following the steps below:

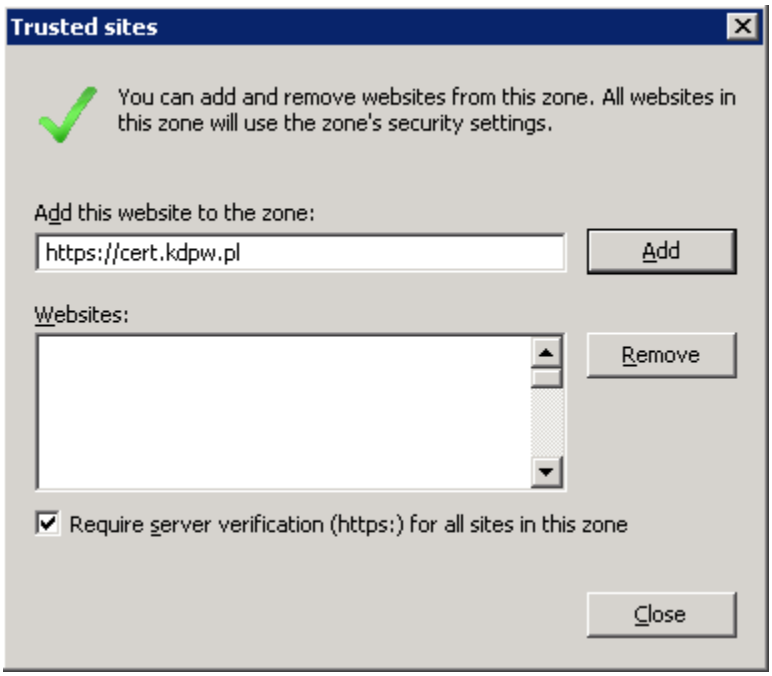
1. Log in the account of the user who is renewing the certificate.
2. Launch the Internet Explorer.
3. Select the menu “Tools” → “Internet options”.
4. Select the tab “Advanced”.
   *The tab “Advanced” may not be visible if the user’s access rights are limited in the system. To get access, please contact the local administrator of your computer.*
5. Make sure that at least one TLS protocol version is checked in the window “Advanced”. The following protocols are supported: TLS 1.0, TLS 1.1 and TLS 1.2.




6. Click “OK” to confirm the changes.

To add the site https://cert.kdpw.pl to the trusted sites, follow the steps below:

1. Launch the Internet Explorer.
2. Select the menu “Tools” → “Internet options”.
3. Select the tab “Security”.
   *The tab “Security” may not be visible if the user’s access rights are limited in the system. To get access, please contact the local administrator of your computer.*
4. Select the “Trusted sites” and click “Sites”.
5. Enter the address https://cert.kdpw.pl in the window and check the option “Require server verification (https:) for all sites in this zone”.

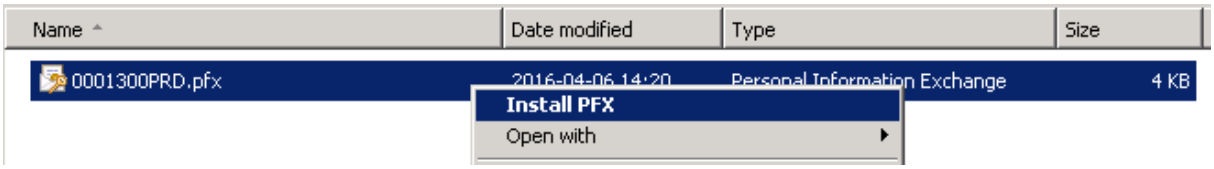



6. Click “Add”; the website should appear on the list.
7. Make sure that the added website is on the list and click “Close”.

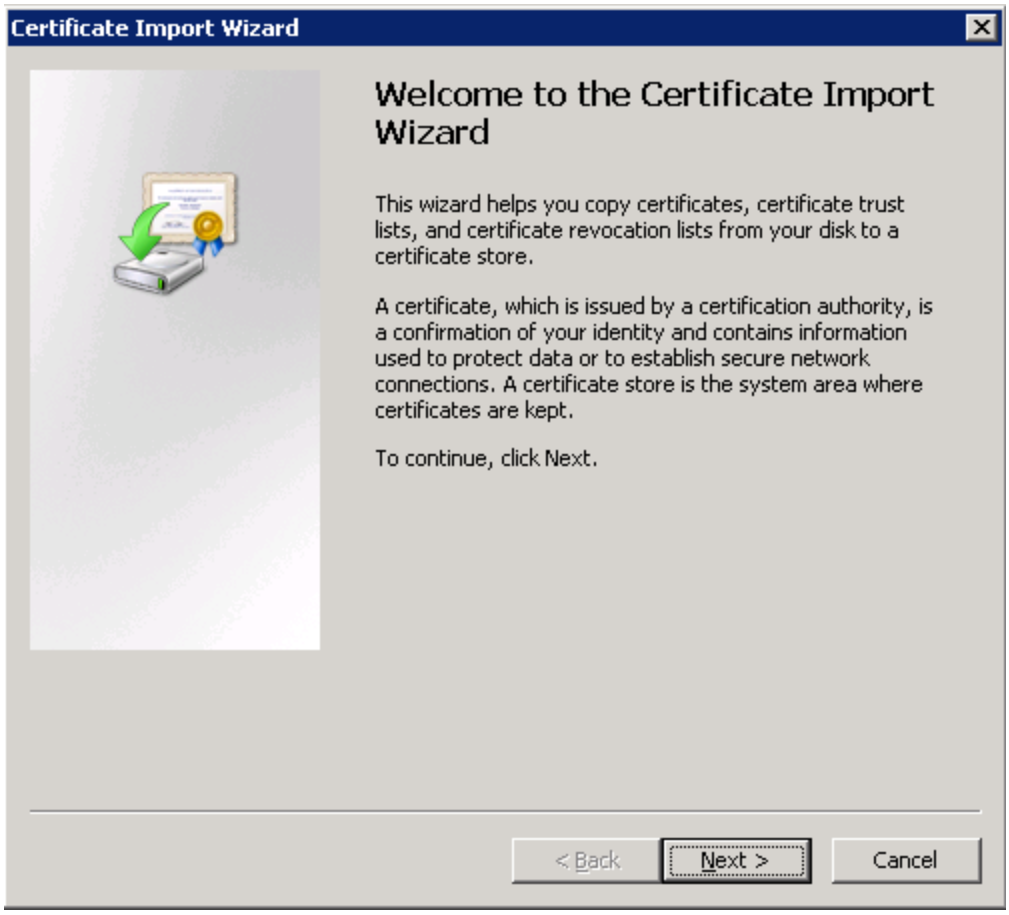
# Installing a user certificate

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

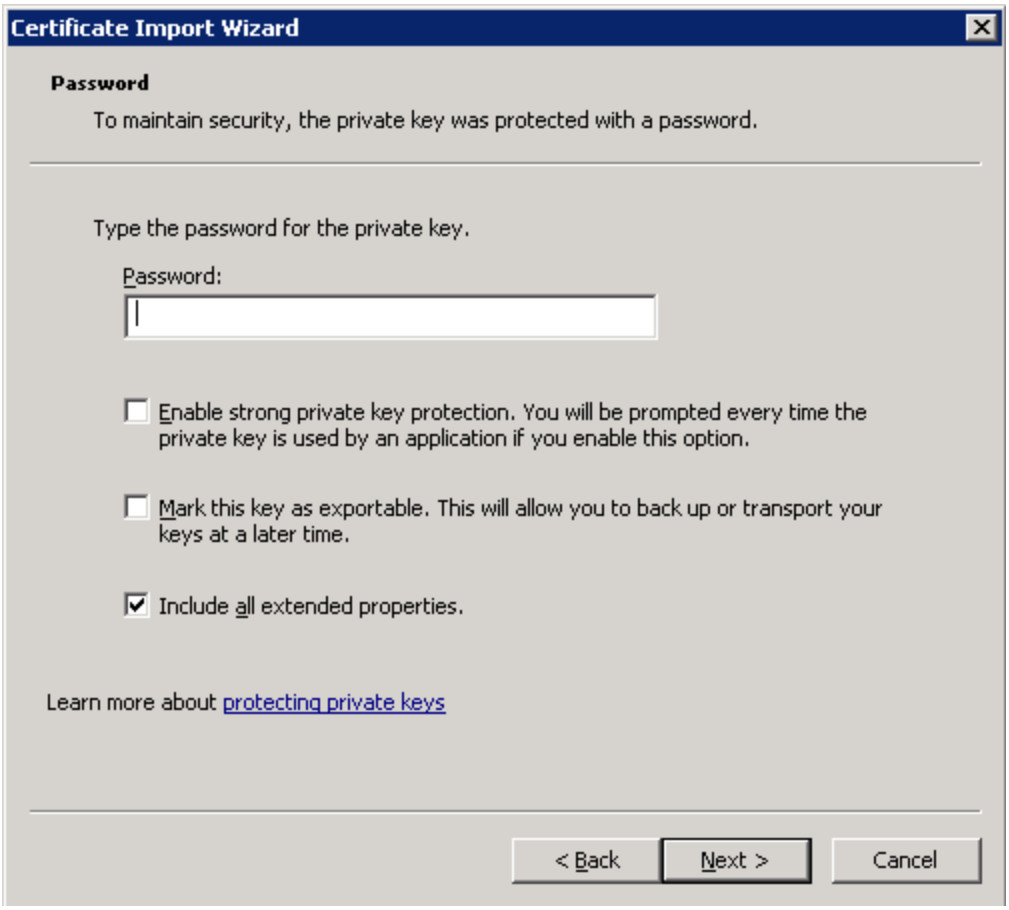
1. Log in the account of the user who is to use the certificate.
2. Right-click the certificate file and select the option “Install PFX” from the context menu.




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

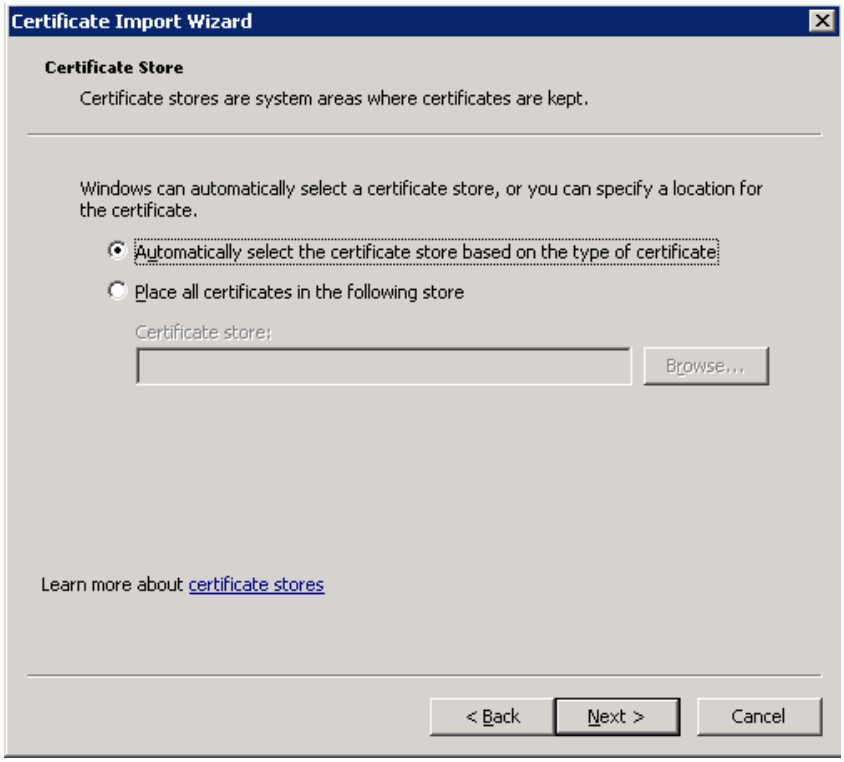



4. In the next window, enter the security password of the certificate file and confirm by clicking “Next”.

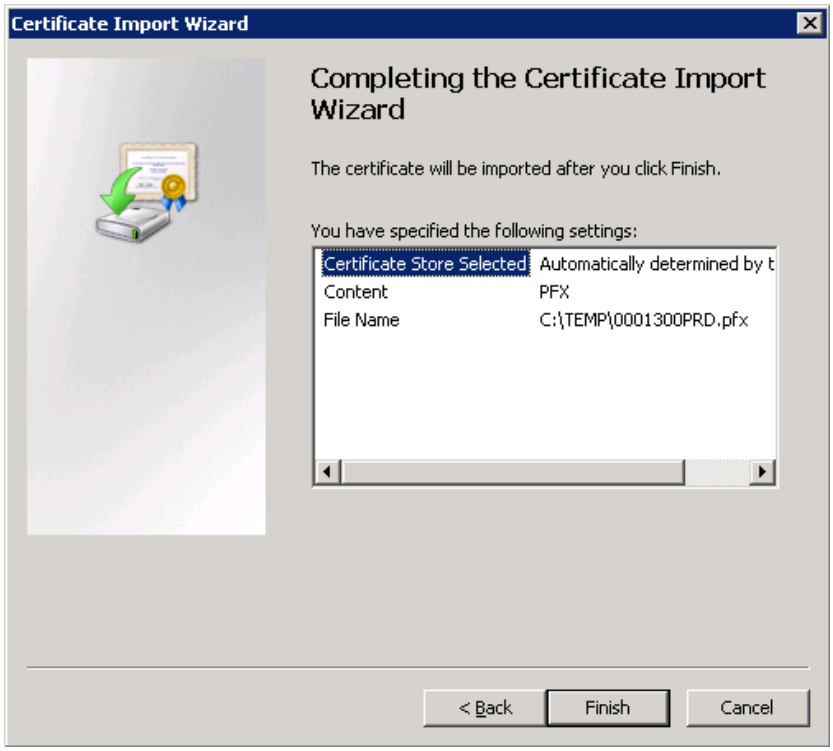



We recommend to check the option “Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option”. If you enable this option, the certificate security password will be required at each time to use the certificate.

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



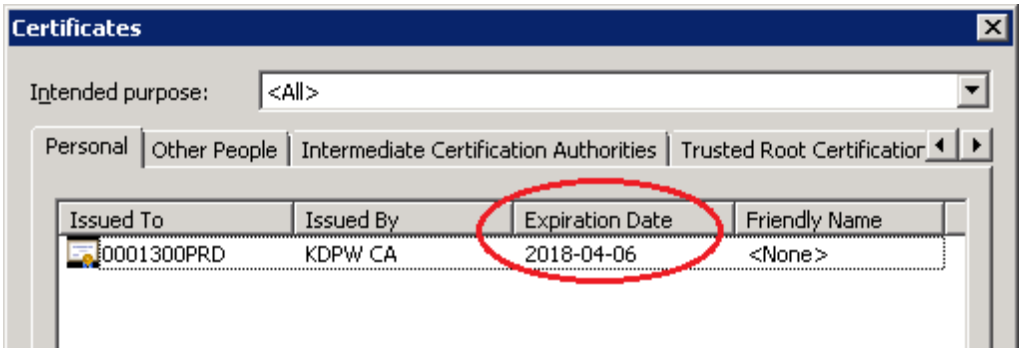

6. In the next window, click “Finish”.



# Checking the certificate validity period

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

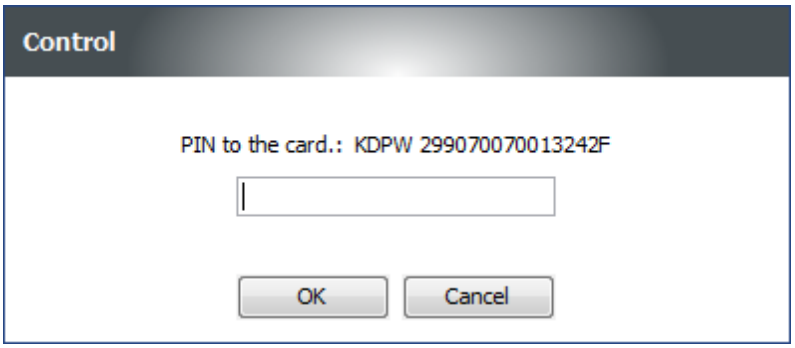
1. You must have an installed certificate; if you don't, install a certificate according to the steps in the section "Installing a user certificate".
2. Launch the web browser.
3. In the menu, select "Tools" → "Internet options" → "Content" → "Certificates".
4. Go to the "Personal" tab.
5. In the certificate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



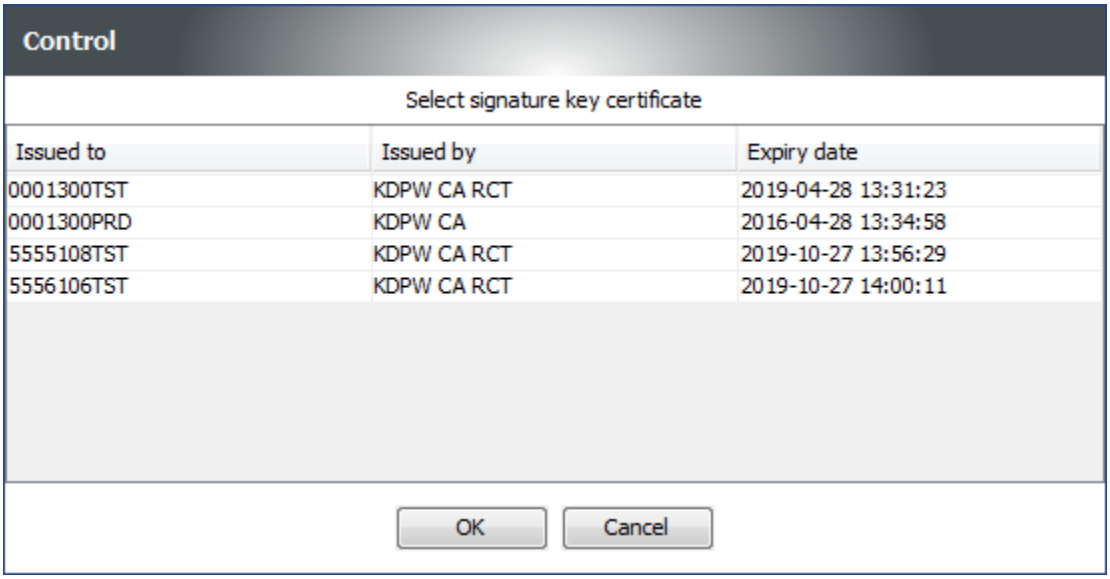
# Remote renewal of an ESDI/WEB user certificate in a card

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

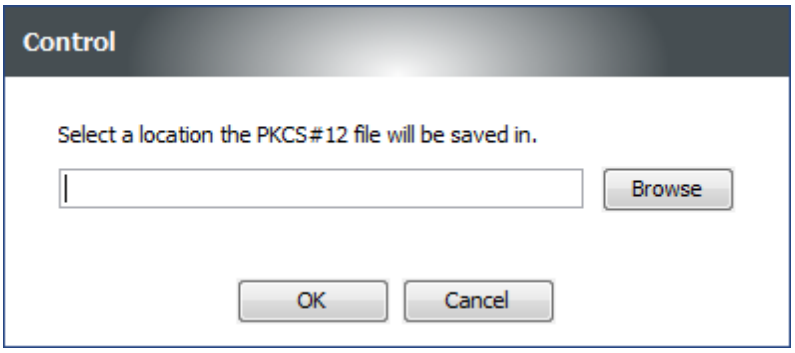
1. Insert the card in the cryptographic card reader.
2. Launch the Internet Explorer and go to https://cert.kdpw.pl.
3. In the menu, select the option "SWI – Production certificates" or "SWI – Test certificates".
4. Wait approximately 15 seconds for the Java applet to load and the option "ESDI/WEB certificate (card)" to become active.
5. Click the option "ESDI/WEB certificate (card)".
6. In the "Control" window, enter the card PIN and click "OK".



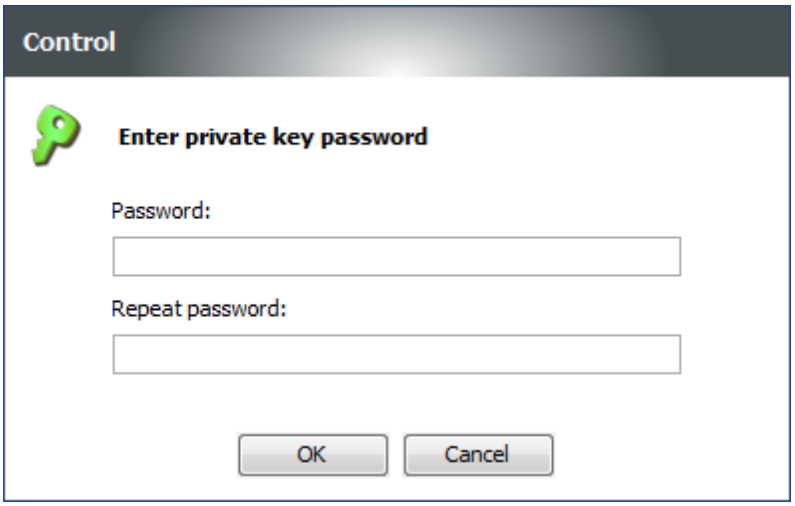

7. In the next window, select the certificate to be renewed. Certificates with the PRD ending are for the production environment, those with the TST ending are for the test environment.



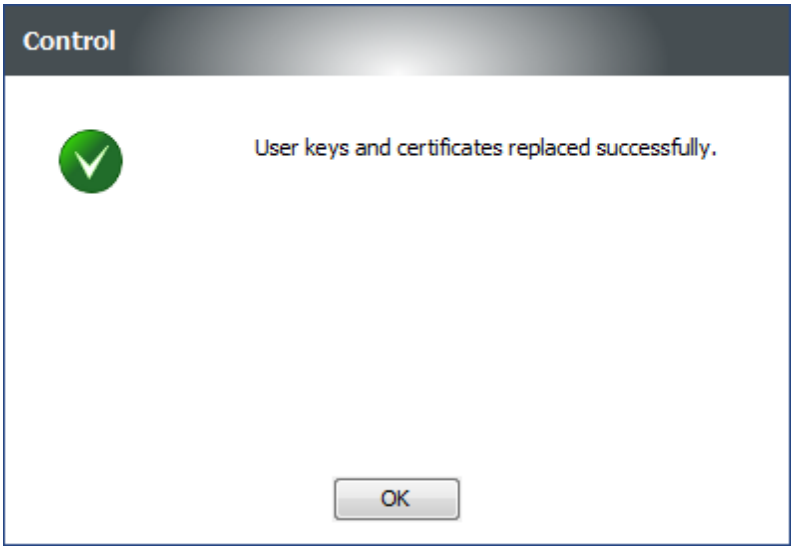

8. In the next window, select the target location to save the certificate and click "OK".




9. In the next window, enter the new password for the certificate file and click “OK”.
   Note: The remote renewal process saves the certificate in a file but not on the card.



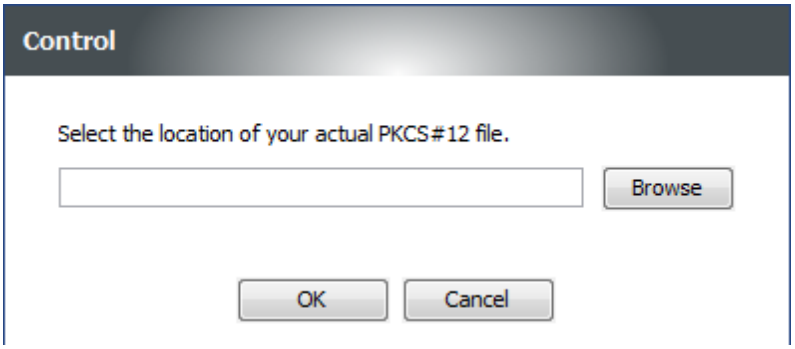

10. A message will be displayed if the renewal is successful.



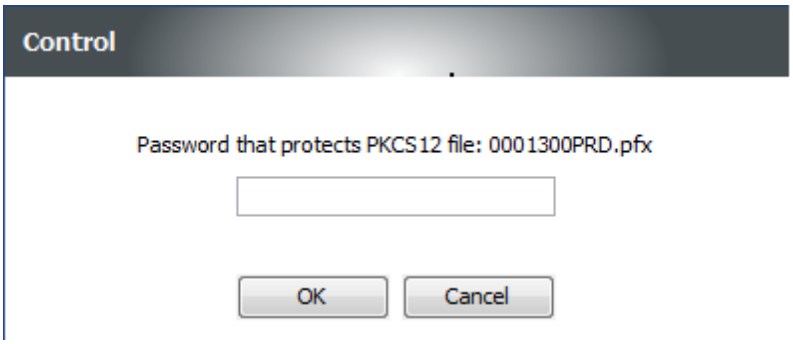
# Remote renewal of an ESDI/WEB user certificate in a file

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

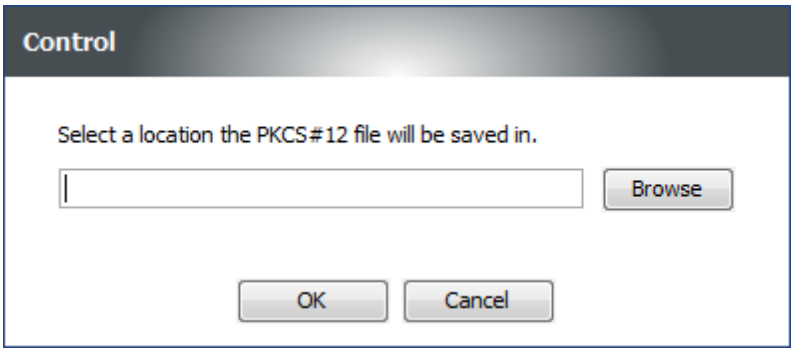
1. Launch the Internet Explorer and go to https://cert.kdpw.pl.
2. In the menu, select the option "SWI – Production certificates" or "SWI – Test certificates".
3. Wait approximately 15 seconds for the Java applet to load and the option "ESDI/WEB certificate (PKCS#12 file)" to become active.
4. Click the option "ESDI/WEB certificate (PKCS#12 file)".
5. In the next window, select the location of the certificate file.



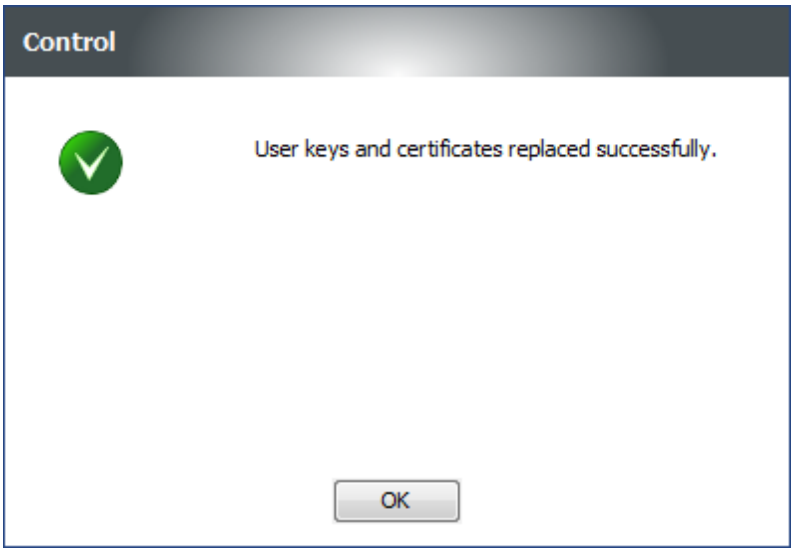

6. In the next window, enter the security password of the file. The password has been provided by the Chief Guarantor on a CD. The password of the new file will be the same as the password of the original file.




7. In the next window, select the target location to save the certificate and click "OK".




8. A message will be displayed if the renewal is successful.

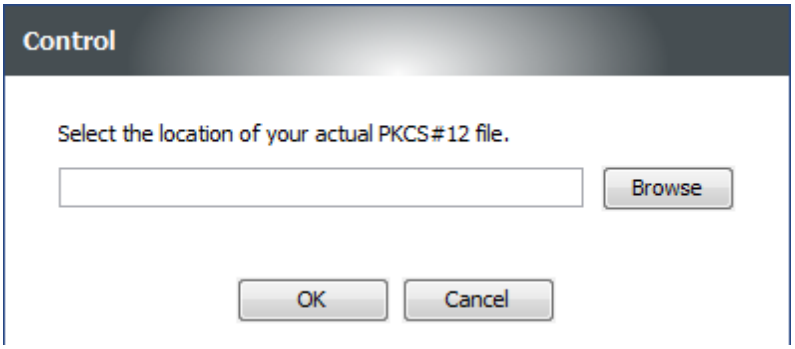



9. After renewing the certificate, the user must contact the user's IT Department to add the certificate to the application used to exchange messages in A2A mode via ESDI/WEB.

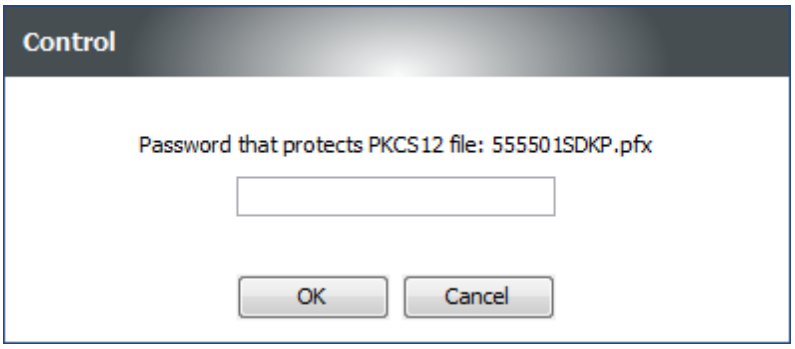
# Remote renewal of an ESDK user certificate

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

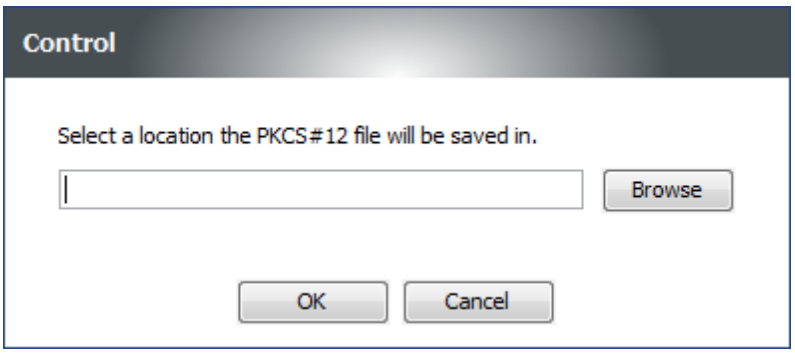
1. Launch the Internet Explorer and go to https://cert.kdpw.pl.
2. In the menu, select the option "SWI – Production certificates" or "SWI – Test certificates".
3. Wait approximately 15 seconds for the Java applet to load and the option "ESDK certificate (PKCS#12 file)" to become active.
4. Click the option "ESDK certificate (PKCS#12 file)".
5. In the next window, select the location of the certificate file.



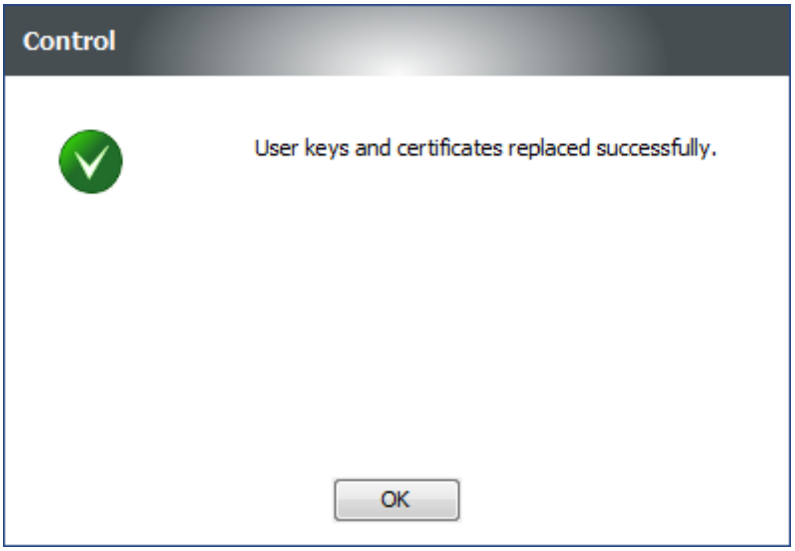

6. In the next window, enter the security password of the file. The password has been provided by the Chief Guarantor on a CD. The password of the new file will be the same as the password of the original file.




7. In the next window, select the target location to save the certificate and click "OK".



8. A message will be displayed if the renewal is successful.

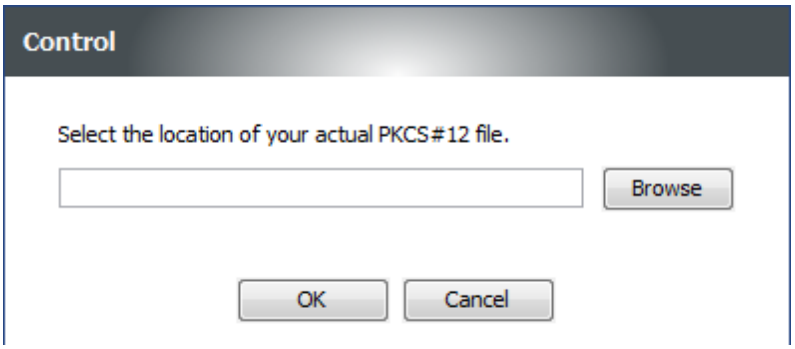



9. After renewing the certificate, the user must contact the user's IT Department to add the certificate to the application used to exchange messages via ESDK.

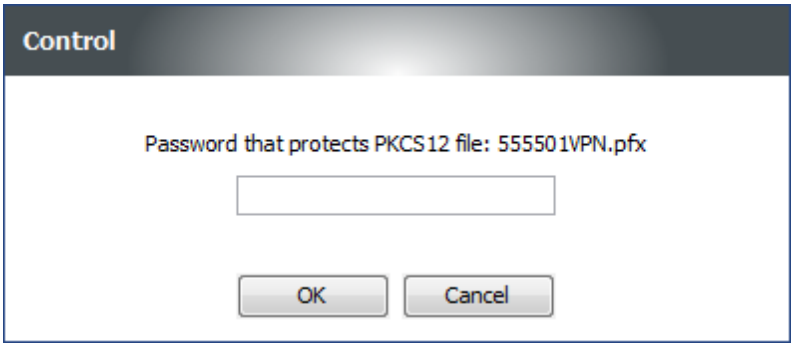
# Remote renewal of a VPN connection certificate

To renew a VPN connection certificate, follow the steps below:

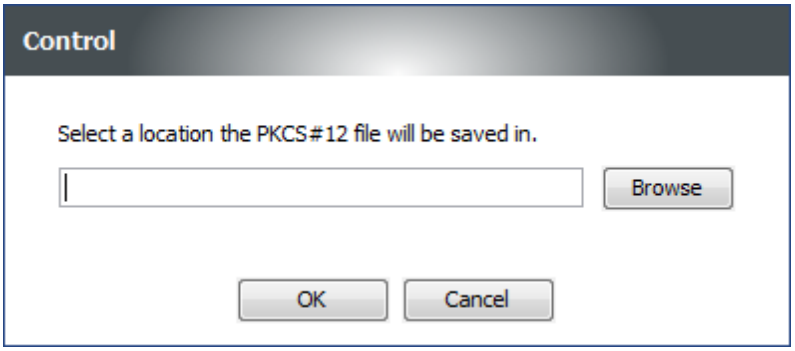
1. Launch the Internet Explorer and go to https://cert.kdpw.pl
2. In the menu, select the option “SWI – VPN certificates”.
3. Wait approximately 15 seconds for the Java applet to load and the option “VPN certificate (PKCS#12 file)” to become active.
4. Select the option “VPN certificate (PKCS#12 file)”.
5. In the next window, select the location of the certificate file.



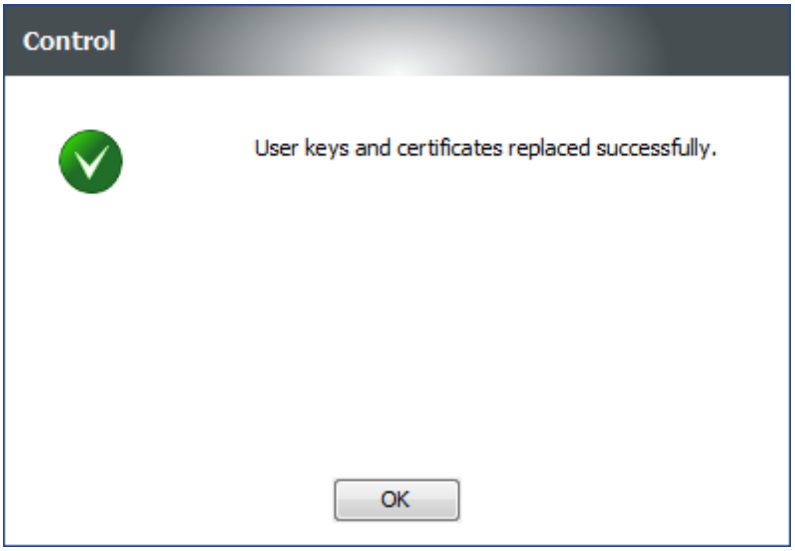

6. In the next window, enter the security password of the file. The password has been provided by the Chief Guarantor on a CD. The password of the new file will be the same as the password of the original file.




7. In the next window, select the target location to save the new certificate and click “OK”.



8. A message will be displayed if the renewal is successful.




9. After renewing the certificate, the user must contact the user's IT Department to add the certificate to the application/router connected to KDPW.

# Java applet trouble-shooting

In case of any trouble starting the Java applet, use the Java console. Follow the steps below:

1. In the Windows menu, select “Control panel” → “Programs and features” → “Java (32 bit)”.
2. In the “Java Control Panel” window, select the “Advanced” tab and enable the following options:
    a. Debugging
        i. Enable tracing
        ii. Enable logging
        iii. Show applet lifecycle exceptions
    b. Java console
        i. Show console
3. During the certificate renewal process, the Java console will pop up and trace all operations of the Java applet. The console will provide information on potential problems. If the console displays no message, Java has not started; please contact your local administrator to get access.