kdpw_
Trade Repository

"Procedure of Handling Certificates for KDPW_TR (A2A)"

Version 1.0

Table of Contents

Access to the KDPW_TR Trade Repository in A2A Mode 3

System Requirements 4

Certification Request 5

Certification Request Status 9

Installing the CA Certificate (only for Windows Vista and Windows 7) 11

Installing User Certificate (A2A) 15

Backup of A2A User Certificate 16

Revocation Of Certificate 21

ACCESS TO THE KDPW_TR TRADE REPOSITORY IN A2A MODE

Before using the KDPW_TR Trade Repository in A2A mode, users must do the following:

1. Check the minimum system requirements specified in the section “System Requirements”.

2. File a certification request. For details, see the section “Certification Request”.

3. Send to KDPW the original declaration to the certification request which confirms that the certification request has been filed. For details, see the section “Confirming the Certification Request”.

4. Install the certificate according to the section “Installing User Certificate”.

5. Make a backup copy of the security certificate. For details, see the section “Backup of User Certificate”.

SYSTEM REQUIREMENTS

11. Operating system:

- Windows XP, Windows Vista or Windows 7 plus the latest Service Pack
- Permissions to write in the Windows certificate store
- Installed controller xenroll.dll for Windows XP (default installation during system installation in the folder C:\windows\system32) or certenroll.dll for Windows Vista and Windows 7

2. Web browser:

- Microsoft Internet Explorer version 6.0 or higher
- Cookies enabled
- Permissions to enable Microsoft ActiveX controls

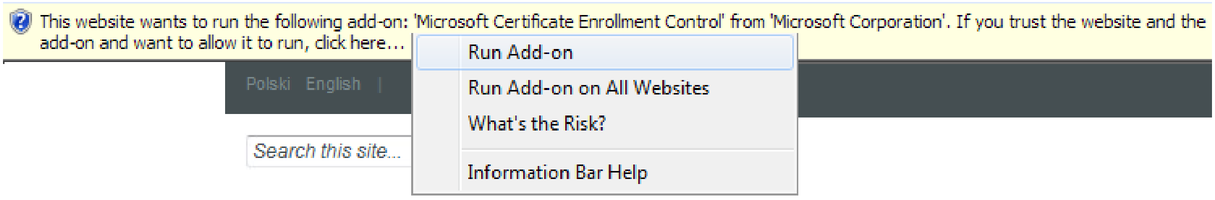
CERTIFICATION REQUEST

In order to issue a certificate, file a certification request by means of completing a relevant form available on the KDPW website under Business → Trade Repository EMIR → Application → A2A Certification Form.

When the page opens, the system may display a message which requests the user to enable the Microsoft Certificate Enrollment Control add-on for Windows XP or the Certificate Services Client for Windows Vista and Windows 7. Click the highlighted bar (see Fig. 1) and select the option "Enable Add-on" for Windows XP or "Enable ActiveX Control" for Windows Vista and Windows 7 (see Fig. 2).

Windows Vista and Windows 7 users should additionally change the security level for the selected internet zone. Open the browser preferences by clicking the menu Tools → Internet Options and select the tab Security. Select the zone "Internet" and click "Custom Level". Under the option "Initialise and script ActiveX controls not marked as safe" select "Prompt". Accept the settings by clicking the button "OK".

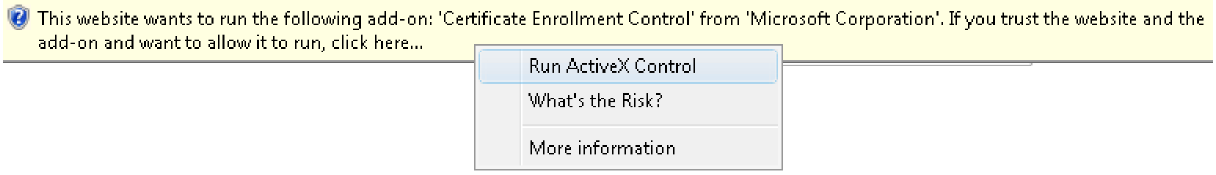
for Windows XP



This website wants to run the following add-on: 'Microsoft Certificate Enrollment Control' from 'Microsoft Corporation'. If you trust the website and the add-on and want to allow it to run, click here...

FIG. 1

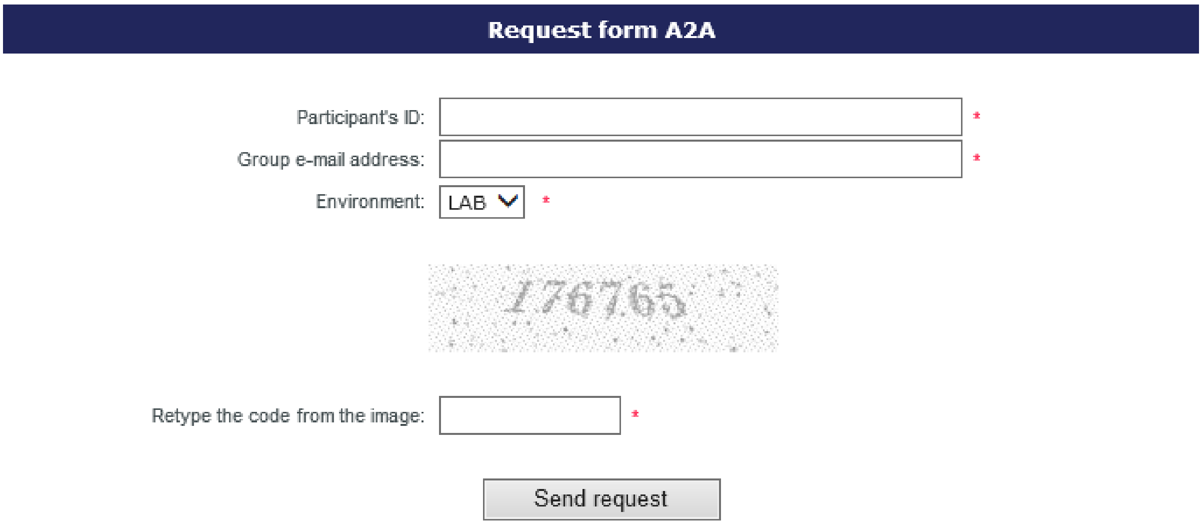
for Windows Vista and Windows 7



This website wants to run the following add-on: 'Certificate Enrollment Control' from 'Microsoft Corporation'. If you trust the website and the add-on and want to allow it to run, click here...

FIG. 2

The form (see Fig. 3) is available on the website. Enter all data necessary to send the certification request. The fields marked with an asterisk are mandatory. If the participant data are correct, select the option "Send request".



Request form A2A

Participant's ID: *

Group e-mail address: *

Environment: LAB *

176765

Retype the code from the image: *

FIG. 3

All fields in the form are mandatory.

Description of the form:

Participant's ID - Enter the participant's identifier: for ZUR and GUR - RT Reporting entity ID; for PUR - RT Counterparty ID.

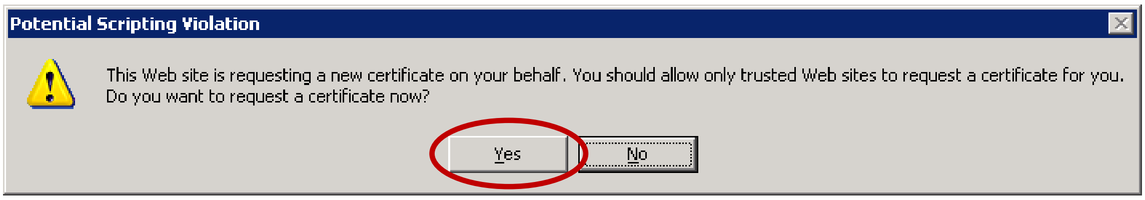
Group e-mail address - Enter the e-mail address to which messages are to be sent. For A2A mode, a group e-mail address is recommended.

Environment - Select the environment to have access to.

A confirmation that the request has been received and a status report of the certification request will be sent to the entered e-mail address.

Once the data are accepted by the application, another message will be displayed (see Fig. 4). Confirm by clicking "Yes".

For Windows XP

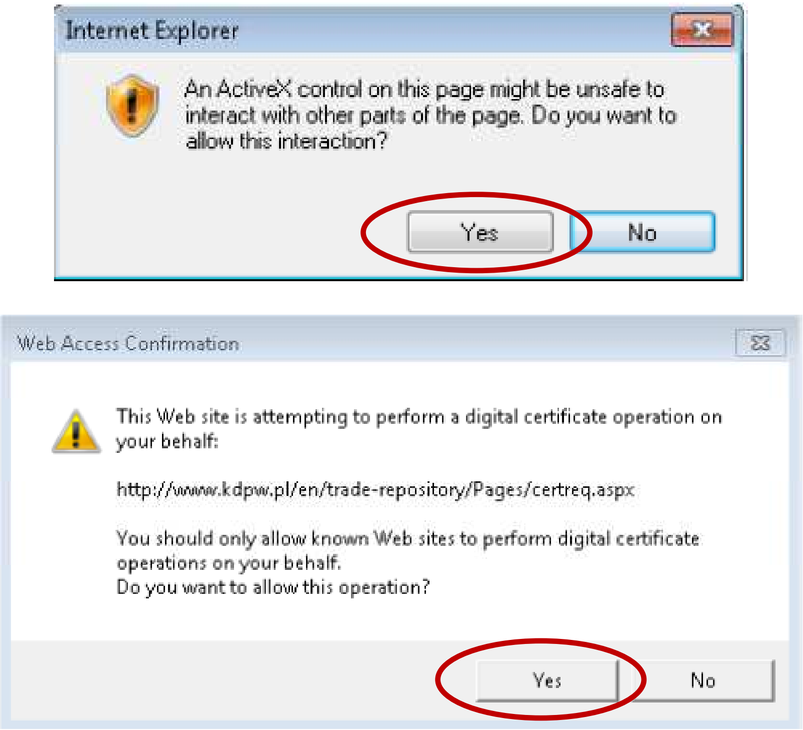


Potential Scripting Violation

This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?

For Windows Vista and Windows 7

Confirm both messages by clicking “Yes”.



Internet Explorer

An ActiveX control on this page might be unsafe to interact with other parts of the page. Do you want to allow this interaction?

Web Access Confirmation

This Web site is attempting to perform a digital certificate operation on your behalf:

http://www.kdpw.pl/en/trade-repository/Pages/certreq.aspx

You should only allow known Web sites to perform digital certificate operations on your behalf.
Do you want to allow this operation?

FIG. 4

If the entered data are incorrect or mandatory fields are left void, an error reason message will be displayed under the form.

If the form is completed correctly, after the user clicks “Send request”, the following message will be displayed:

Certification request No. **Number** for user **Participant identifier** (A2A) has been accepted for execution on YYYY-MM-DD at HH24:MM:SS.

The declaration to be sent to KDPW and the activation code below will be sent to the e-mail address entered in the request.

Your activation code

fe970a5d429fd2e76f2f415c90966a28

FIG. 5

A message confirming that the certification request has been accepted will be sent to the e-mail address entered in the form, together with the Declaration for the Certification Request, which should be signed by the authorised representatives and delivered to KDPW in the original.

Message topic:
KDPW_TR Trade Repository (A2A) – acceptance of certification request No. XXXX.

Message content:
Certification request No. XXXX for organisation Organisation name has been accepted for execution on YYYY-MM-DD at HH24:MM:SS.

KDPW_TR ID: XXXXXXXXXXXX
Sender ID: XXXX
KDPW_TR environment: XXX

To confirm the application, the attached declaration for the certification request must be signed by the authorised representatives and delivered to KDPW in the original together with the following activation code:

Your activation code
fe970a5d429fd2e76f2f415c90966a28

The declaration for the certification request is attached to this message.

FIG. 6

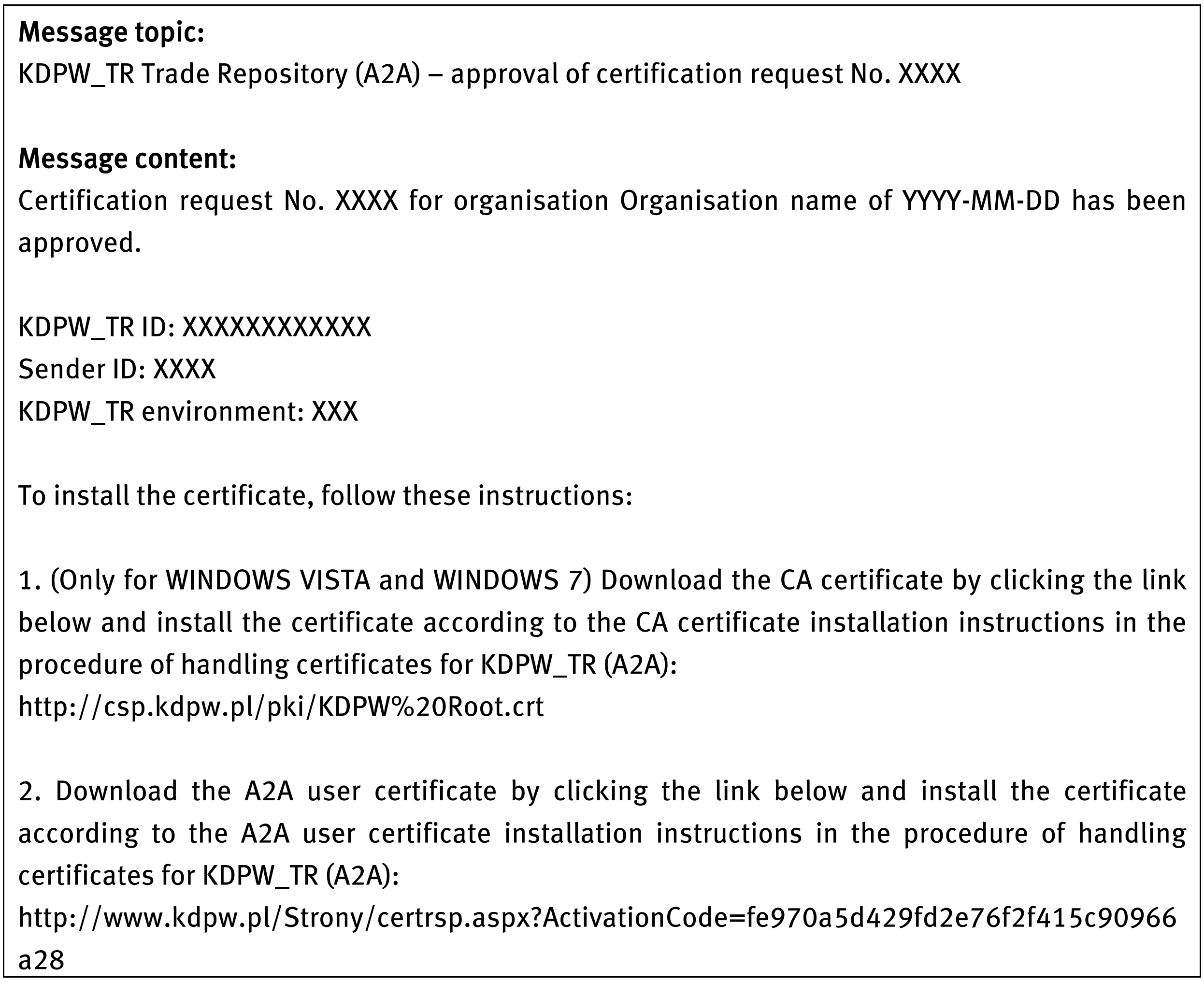
The Declaration for the Certification Request is generated automatically on the basis of the data entered in the registration form and the fields selected in the form.

Note !!!
A certification request and a private key are saved in the user's system profile of the computer from which the request was sent. If the user is deleted from the system or information of the generated request is lost (lack of access to the computer from which the request was sent), the form has to be completed once again and the certification request has to be re-sent. The list of registered requests can be viewed under the Certificates tab available in the Microsoft Management Console (MMC) or by entering the command "certmgr.msc" in the Run window.

Certification Request Status

Upon receipt of the declaration for the certification application and a check of signatures in the declaration, KDPW decides whether to approve the filed certification application. If the data delivered match the data entered in the application and the signatures match the signatures in the card of specimen signatures delivered to KDPW, the certification application will be approved. Otherwise, the application will be rejected.

The approval or rejection of the request is notified to the user in an e-mail message sent to the e-mail address entered in the request.
If the request is approved, the user receives the message shown in Fig. 7 and can download the certificate and install it in the user profile.



Message topic:
KDPW_TR Trade Repository (A2A) – approval of certification request No. XXXX

Message content:
Certification request No. XXXX for organisation Organisation name of YYYY-MM-DD has been approved.

KDPW_TR ID: XXXXXXXXXXXX
Sender ID: XXXX
KDPW_TR environment: XXX

To install the certificate, follow these instructions:

1. (Only for WINDOWS VISTA and WINDOWS 7) Download the CA certificate by clicking the link below and install the certificate according to the CA certificate installation instructions in the procedure of handling certificates for KDPW_TR (A2A):
http://csp.kdpw.pl/pki/KDPW%20Root.crt

2. Download the A2A user certificate by clicking the link below and install the certificate according to the A2A user certificate installation instructions in the procedure of handling certificates for KDPW_TR (A2A):
http://www.kdpw.pl/Strony/certrsp.aspx?ActivationCode=fe970a5d429fd2e76f2f415c90966a28

FIG. 7

If the request is rejected, the user receives the message shown in Fig. 8.

Message topic:
KDPW_TR Trade Repository (A2A) – rejection of certification request No. XXXX.

Message content:
Certification request No. XXXX for organisation Organisation name of YYYY-MM-DD has been rejected.

KDPW_TR ID: XXXXXXXXXXXX
Sender ID: XXXX
KDPW_TR environment: XXX

Rejection reason:
Content depending on rejection reason

To issue a certificate, complete the certification form again and send a new declaration for the certification request.

FIG. 8

Installing the CA Certificate (only for Windows Vista and Windows 7)

For Windows XP, ignore this section.

Before installing the CA certificate, make sure that the system requirements specified in the section "System Requirements" are fulfilled.

The certificate should be installed only in Windows Vista and Windows 7 in the user's system account from which the certification request was sent.

Upon receipt of an e-mail message confirming that the certification request has been approved, the CA certificate may be installed by means of clicking the link in point 1. Please follow these installation instructions:

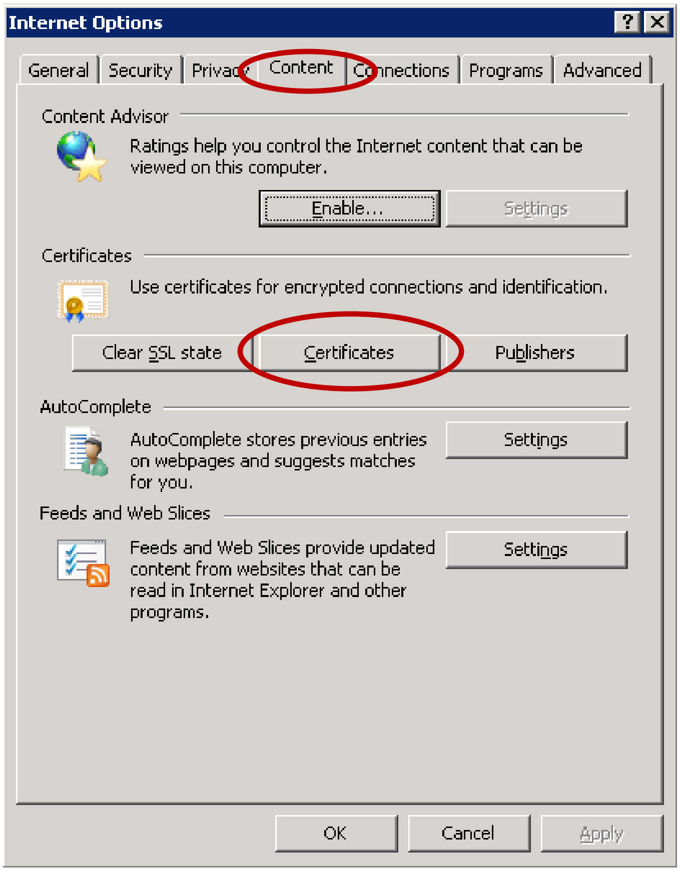
1. Click the link in point 1 provided in the e-mail message and save the file, for instance on the user desktop. The file name is "KDPW Root.crt".

2. Launch the Internet Explorer.

3. In the browser menu, select the option Tools → Internet Options.

4. Select the tab "Content".
The tab "Content" may not be visible if the user's access to the certificate store is restricted in the system. To get access, contact the local administrator of your computer.

5. Click the button "Certificates".



Ratings help you control the Internet content that can be viewed on this computer.

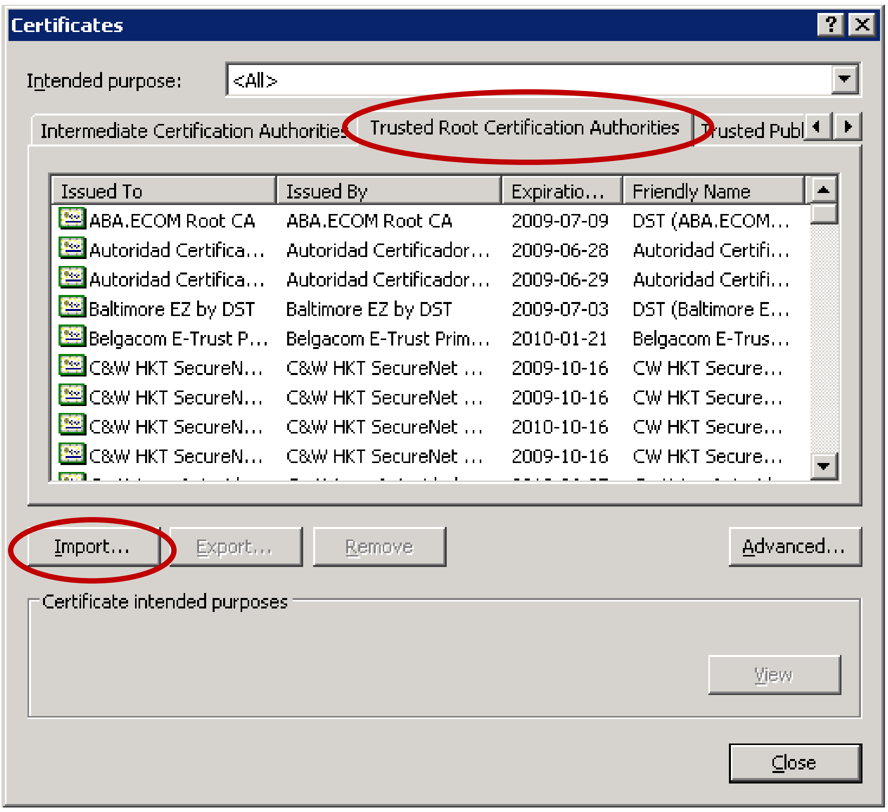
Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

FIG. 9

6. Select the tab “Trusted Root Certification Authorities” and click “Import”.


Certificates
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

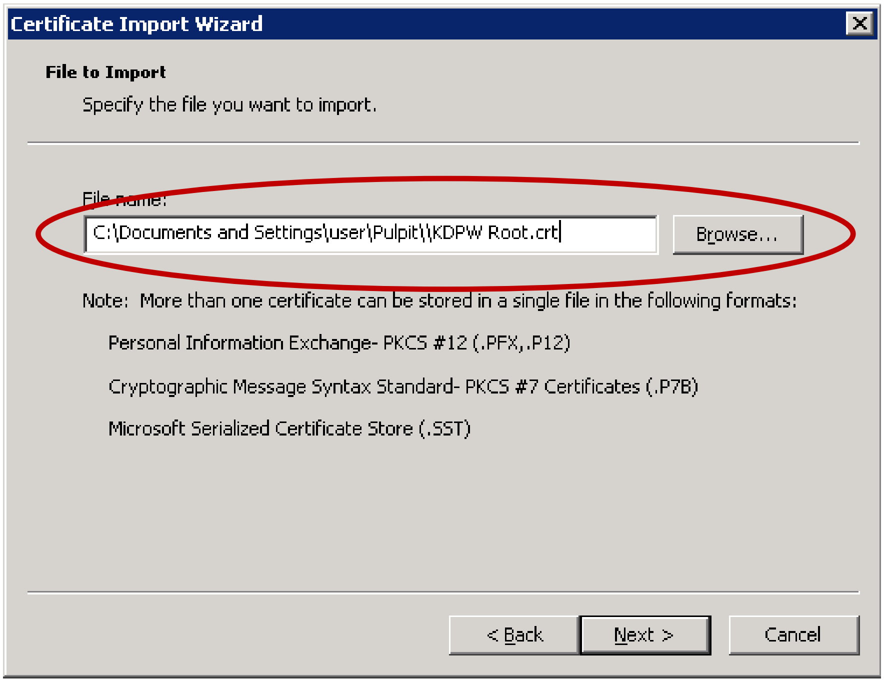
Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
ABA.ECOM Root CA	ABA.ECOM Root CA	2009-07-09	DST (ABA.ECOM...
Autoridad Certifica...	Autoridad Certificador...	2009-06-28	Autoridad Certifi...
Autoridad Certifica...	Autoridad Certificador...	2009-06-29	Autoridad Certifi...
Baltimore EZ by DST	Baltimore EZ by DST	2009-07-03	DST (Baltimore E...
Belgacom E-Trust P...	Belgacom E-Trust Prim...	2010-01-21	Belgacom E-Trus...
C&W HKT SecureN...	C&W HKT SecureNet ...	2009-10-16	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	2009-10-16	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	2010-10-16	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	2009-10-16	CW HKT Secure...

FIG. 10

7. In the pop-up window, click “Next”.

8. In the next window, click “Browse” and select the certificate file saved in point 1.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Documents and Settings\user\Pulpit\\KDPW Root.crt

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

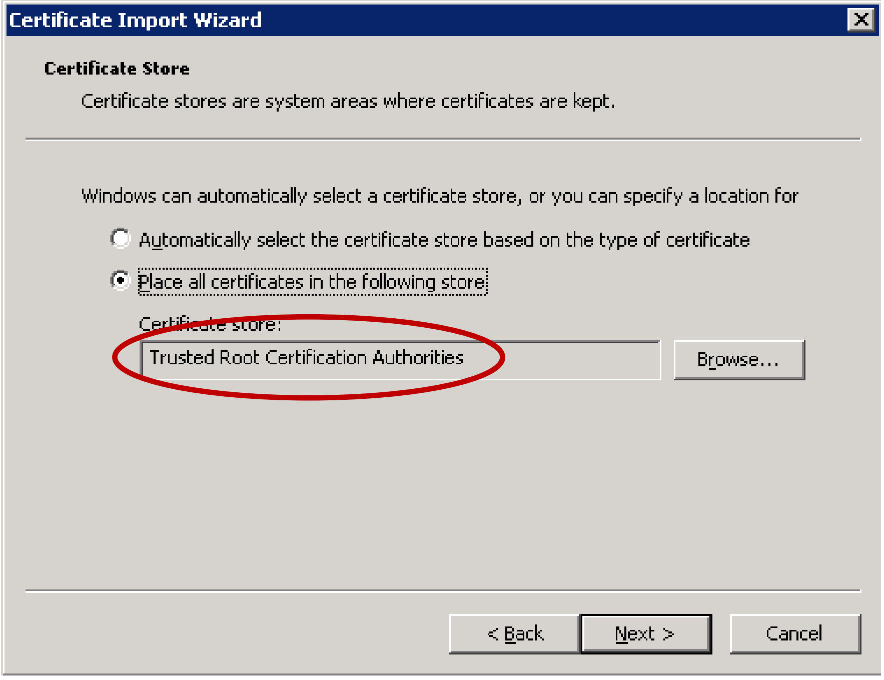
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

FIG. 11

9. Click “Next”.

10. Check whether “Trusted Root Certification Authorities” is displayed under the “Certificate Store”. In the next window, click “Next”.



Certificate Import Wizard

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

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

● Place all certificates in the following store

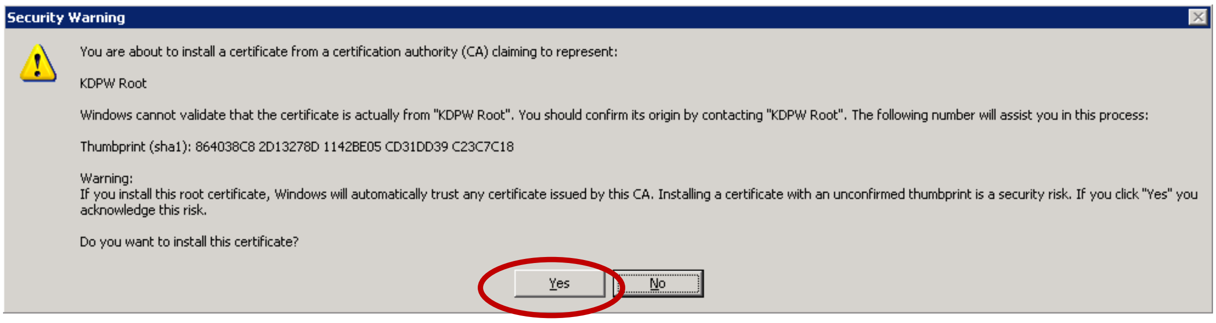
Certificate store:

Trusted Root Certification Authorities

FIG. 12

11. To end, click “Finish”.

12. In the new window, confirm installation of the CA certificate by clicking “Yes”.



You are about to install a certificate from a certification authority (CA) claiming to represent:

KDPW Root

Windows cannot validate that the certificate is actually from "KDPW Root". You should confirm its origin by contacting "KDPW Root". The following number will assist you in this process:

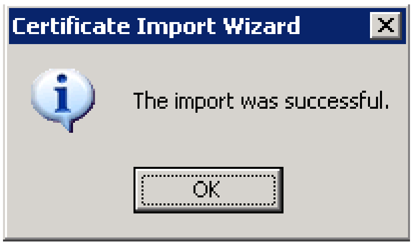
Thumbprint (sha1): 864038C8 2D13278D 1142BE05 CD31DD39 C23C7C18

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

FIG. 13

13. A window should be displayed.



The import was successful.

FIG. 14

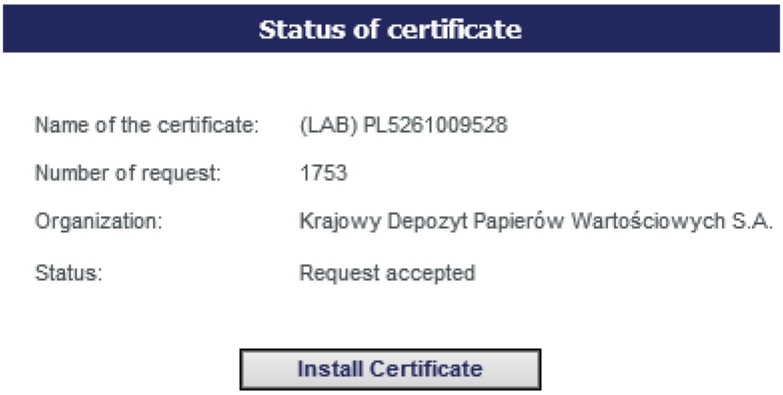
INSTALLING USER CERTIFICATE (A2A)

Before installing the A2A user certificate, make sure that the system requirements specified in the section “System Requirements” are fulfilled.

The certificate should be installed in the user’s system account from which the certification request was sent.

Upon receipt of an e-mail message confirming that the certification request has been approved, the certificate may be installed by clicking the link in point 2.

A window will be displayed with certificate details and an installation option (see Fig. 15). For Windows Vista and Windows 7, an additional message concerning ActiveX control interaction will also be displayed (see Fig. 16); accept it by clicking “Yes”.

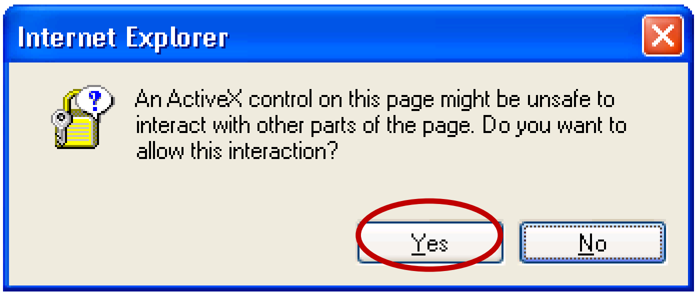


Status of certificate

Name of the certificate:	(LAB) PL5261009528
Number of request:	1753
Organization:	Krajowy Depozyt Papierów Wartościowych S.A.
Status:	Request accepted

FIG. 15

For Windows Vista and Windows 7



An ActiveX control on this page might be unsafe to interact with other parts of the page. Do you want to allow this interaction?

FIG. 16

Click “Install Certificate” and accept all messages until the installation complete message is displayed.

Backup of A2A User Certificate

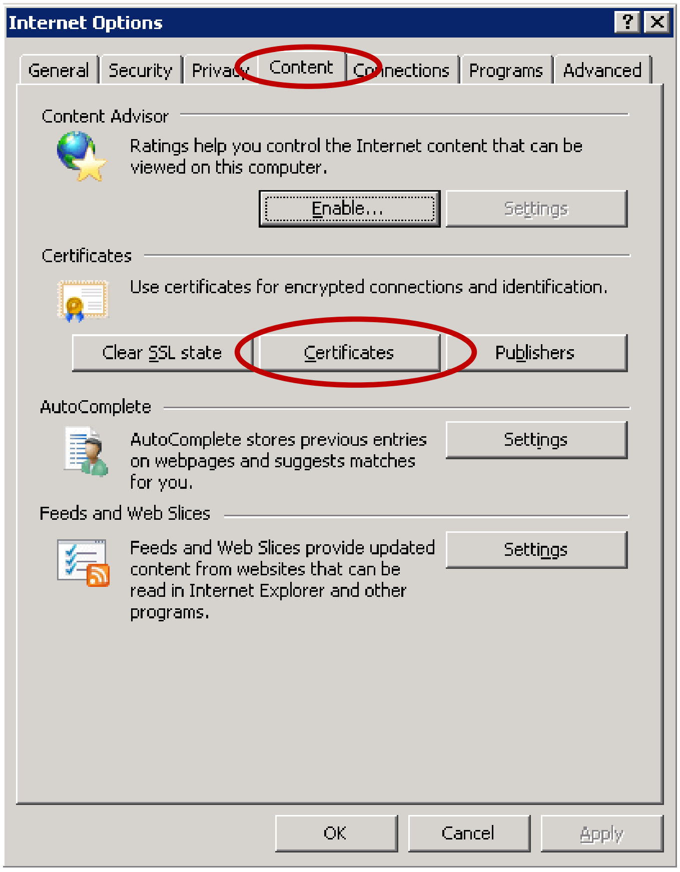
It is recommended to make a back-up copy immediately after the first installation of the certificate in the operating system. In case of any failure or re-installation, the user can promptly recover the certificate without having to re-send the certification application. To make back-up copies, please follow these instructions:

1. Launch the Internet Explorer.

2. In the browser menu, select the option Tools → Internet Options.

3. Select the tab "Content".
The tab "Content" may not be visible if the user's access to the certificate store is restricted in the system. To get access, contact the local administrator of your computer.

4. Click the button "Certificates".



Ratings help you control the Internet content that can be viewed on this computer.

Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

FIG. 17

5. Click the tab "Personal".

6. Select the certificate to backup and click "Export".

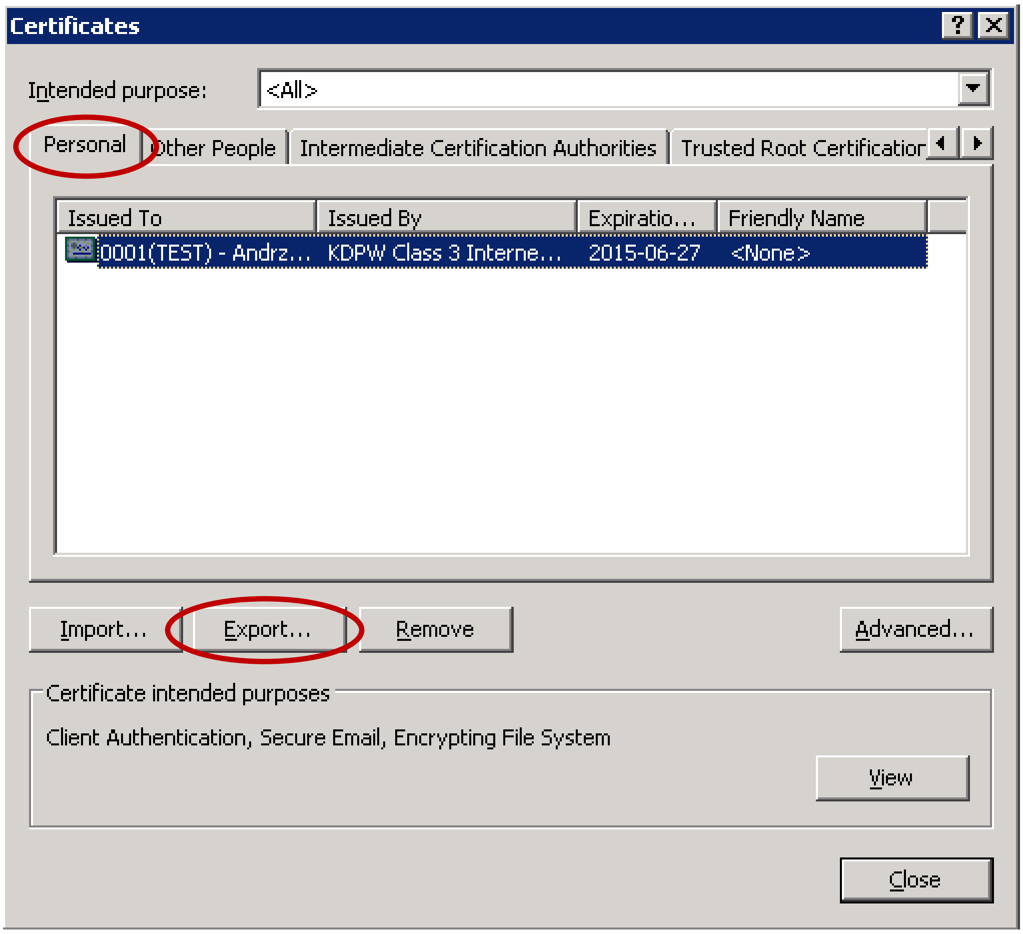
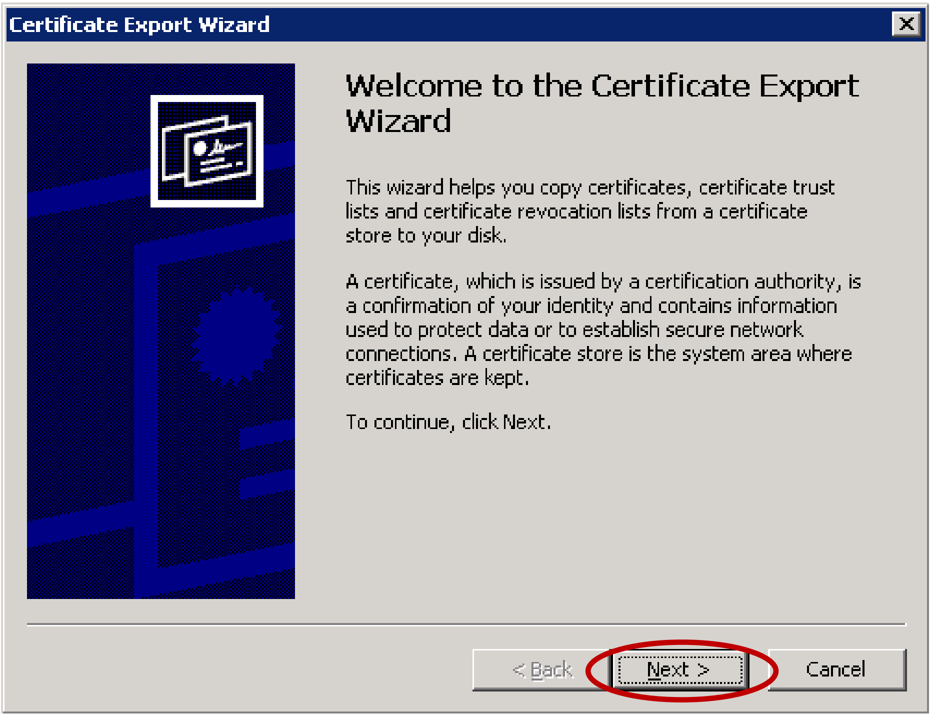


FIG. 18

7. In the export wizard window, click “Next”.



Certificate Export Wizard

Welcome to the Certificate Export Wizard

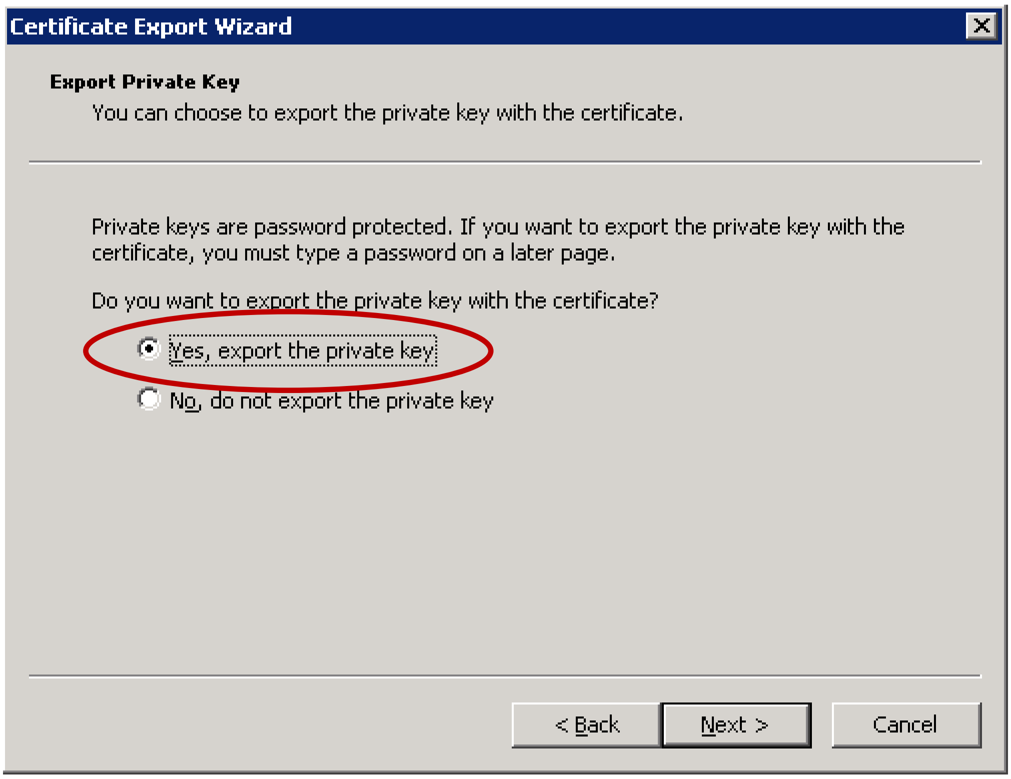
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

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.

FIG. 19

8. In the next window, select the option “Yes, export the private key”.



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

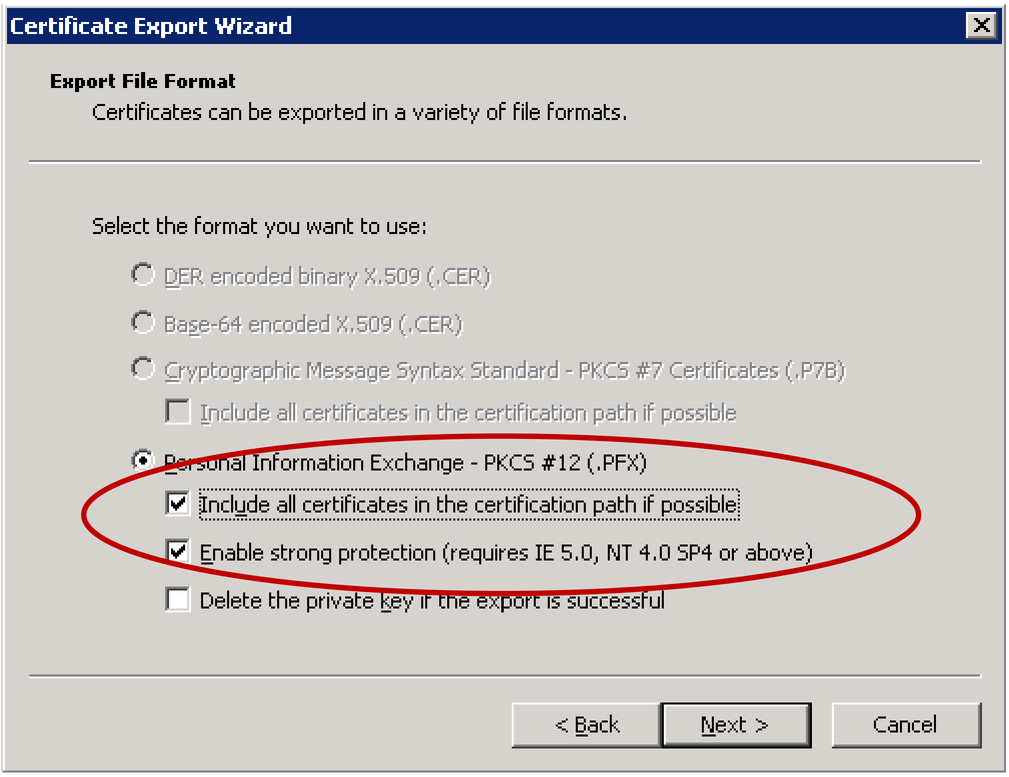
Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

FIG. 20

9. Select the options as in the Figure below and click “Next”.



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

☑ Include all certificates in the certification path if possible

☑ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

□ Delete the private key if the export is successful

FIG. 21

10. Enter a certificate file password and click “Next”.

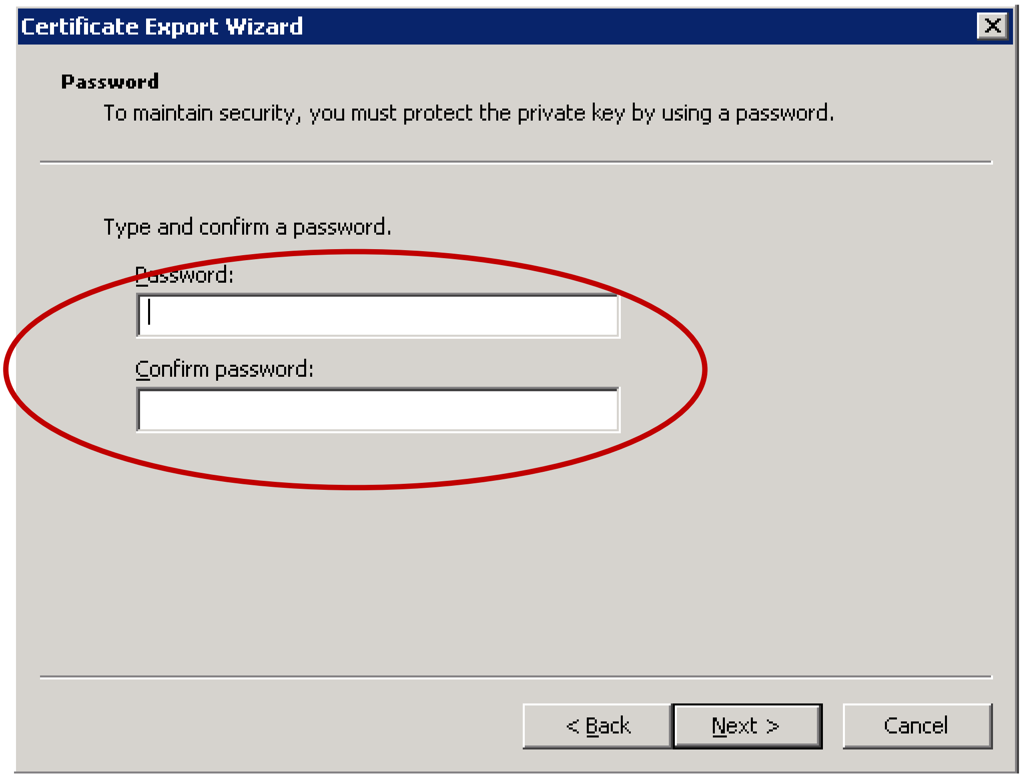
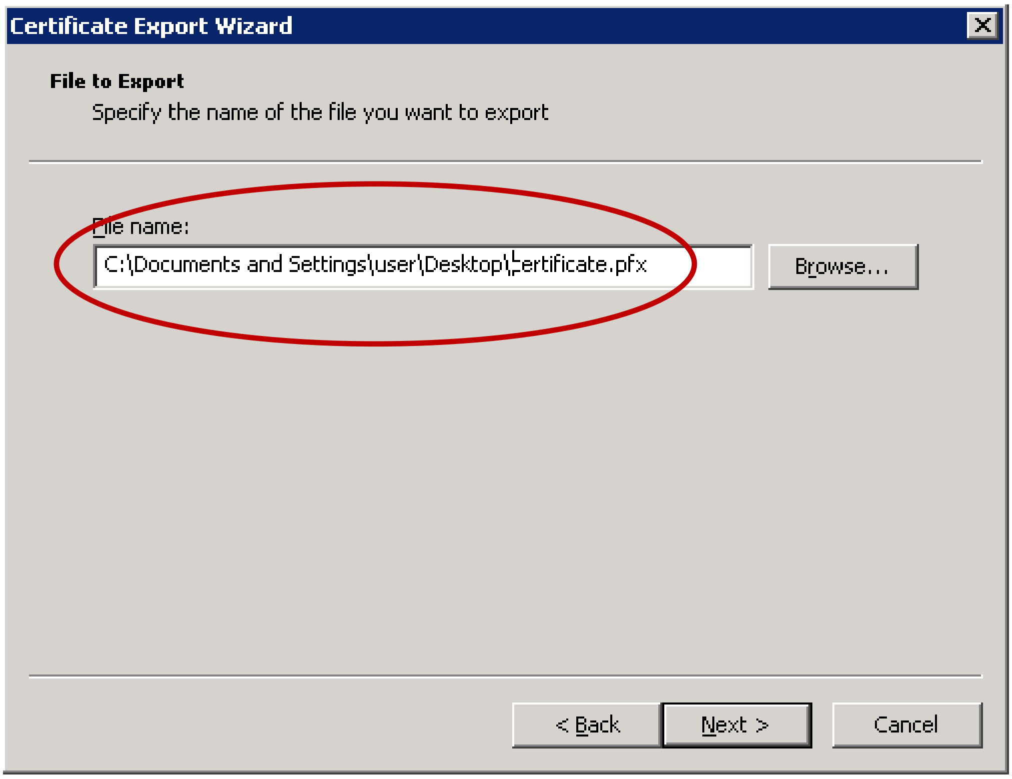

Certificate Export Wizard
Password
To maintain security, you must protect the private key by using a password.
Type and confirm a password.
Password:
Confirm password:
< Back
Next >
Cancel

FIG. 22

11. In the next window, enter the certificate file name and click “Next”.

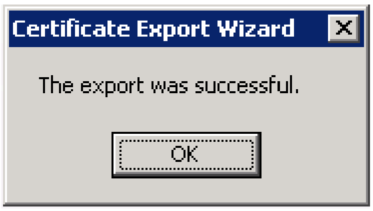

Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
Browse...
< Back
Next >
Cancel

File name: C:\Documents and Settings\user\Desktop\certificate.pfx

FIG. 23

12. Confirm by clicking “Finish”.

13. A window should be displayed.


Certificate Export Wizard

The export was successful.

FIG. 24

The export creates a pfx file on the hard drive. It can be saved on any data device. As certificates are issued for a term of three years, it is recommended to save the file on a CD or DVD.

REVOCATION OF CERTIFICATE

It is possible to revoke an A2A user certificate and thus deny user access to the KDPW_TR Trade Repository.

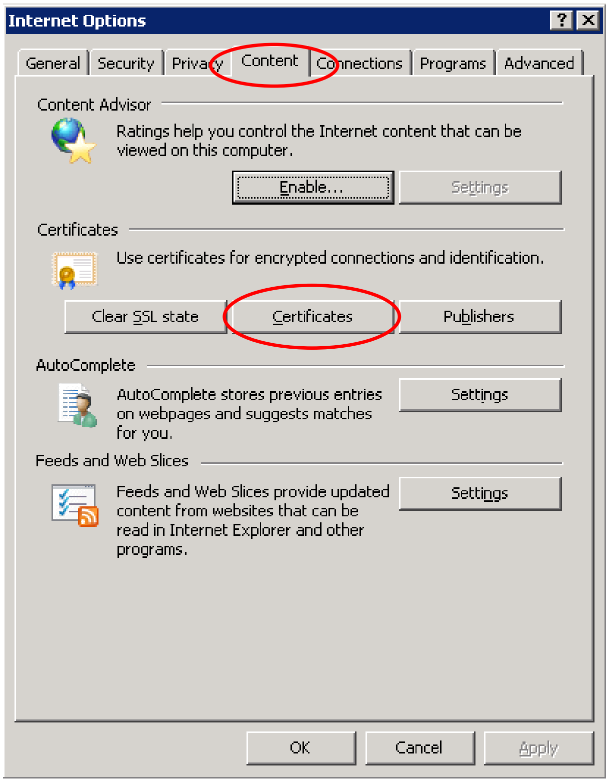
In order to revoke a certificate, send to KDPW the original "Application for revocation of certificate for KDPW_TR Trade Repository (A2A)" available on the website www.kdpw.pl, then click the link *Business → Trade Repository EMIR* and select "*Application*" in the right-hand menu. If the selected organisation holds more than one certificate, enter the identifier of the certificate to be revoked. Otherwise, all of the organisation's certificates will be revoked. The user certificate identifier is the certificate serial number or the activation code or the certification request number. The activation code and the certification request number are sent in the user certification process in an e-mail message to the e-mail address entered in the certification form.

The certificate serial number can be found as follows:

1. Launch the Internet Explorer.
2. In the browser menu, select the option Tools → Internet Options.
3. Select the tab "Content".

The tab "Content" may not be visible if the user's access to the certificate store is restricted in the system. To get access, contact the local administrator of your computer.

4. Click the button "Certificates".



Ratings help you control the Internet content that can be viewed on this computer.

Use certificates for encrypted connections and identification.

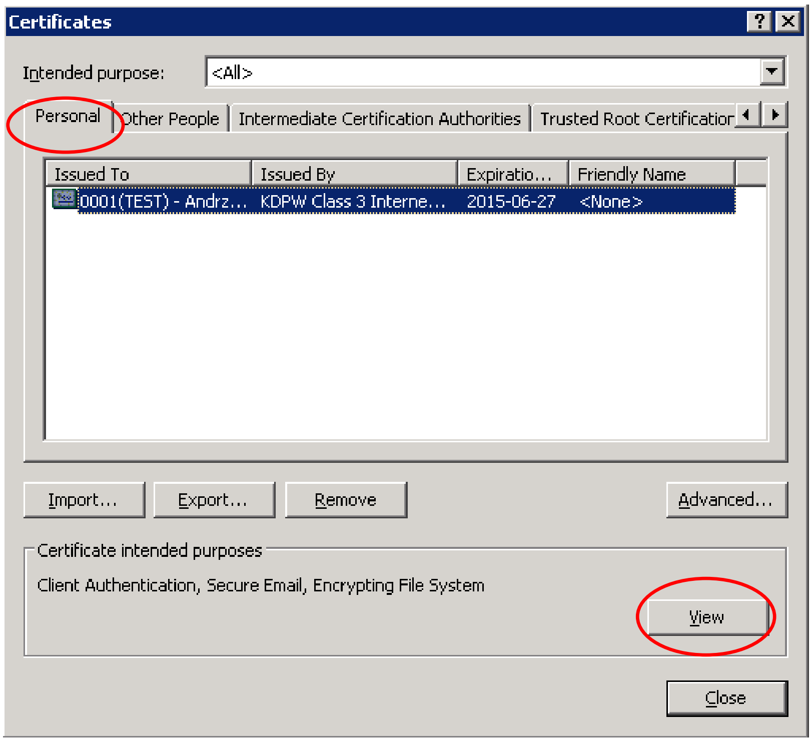
AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

FIG. 25

5. Click the tab “Personal”.

6. Select the certificate to be revoked and click “View”.


Certificates
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

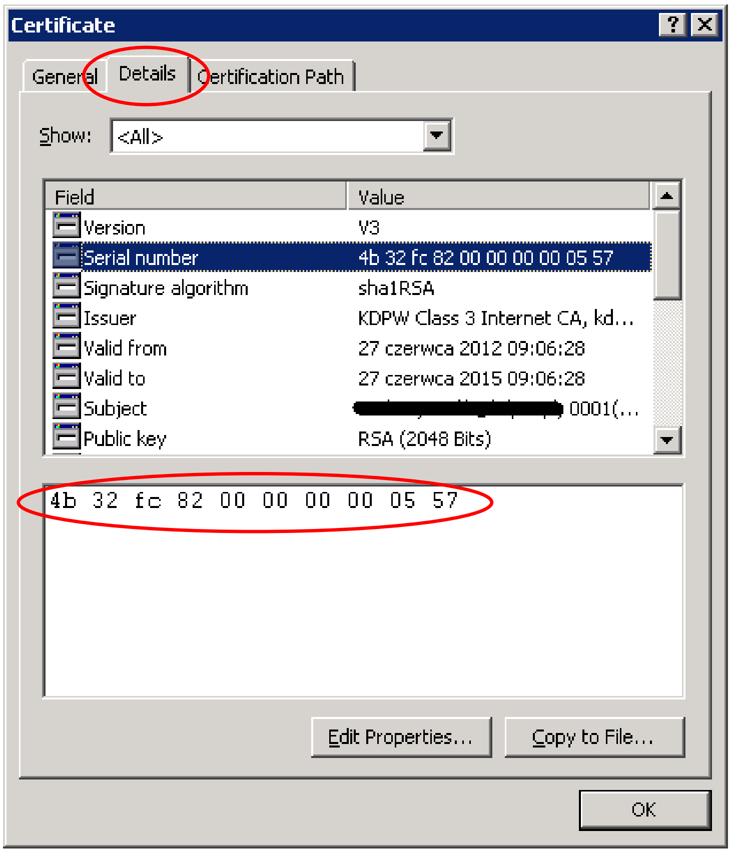
Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
0001(TEST) - Andrz...	KDPW Class 3 Interne...	2015-06-27	<None>

Certificate intended purposes: Client Authentication, Secure Email, Encrypting File System

FIG. 26

7. Click the tab “Details” and read the “Serial number”.



Show: <All>

Field	Value
Version	V3
Serial number	4b 32 fc 82 00 00 00 00 05 57
Signature algorithm	sha1RSA
Issuer	KDPW Class 3 Internet CA, kd...
Valid from	27 czerwca 2012 09:06:28
Valid to	27 czerwca 2015 09:06:28
Subject	[redacted] 0001(...
Public key	RSA (2048 Bits)

```
4b 32 fc 82 00 00 00 00 05 57
```

FIG. 27

Upon a check of the application for certificate revocation in KDPW and revocation of the certificate, the user receives an e-mail message with a confirmation:

Message topic:
KDPW_TR Trade Repository (A2A) – revocation of certificate for certification request No. XXXX

Message content:
The certificate for certification request No. XXXX issued to organisation Organisation name has been revoked on YYYY-MM-DD.

KDPW_TR ID: XXXXXXXXXXXX
Sender ID: XXXX
KDPW_TR environment: XXX

Revocation reason:
Certificate revoked by request of the Participant.

FIG. 28