KDPW

Procedura obsługi certyfikatów KDPW_TR (A2A)

Spis treści

I Dostęp do Repozytorium transakcji KDPW_TR w trybie A2A

Przed przystąpieniem do pracy z „Repozytorium Transakcji KDPW" w trybie A2A należy wykonać następujące kroki:

1. Weryfikacja minimalnych wymagań systemowych podanych w punkcie „Wymagania systemowe".

2. Złożenie wniosku certyfikacyjnego. Szczegóły podano w punkcie „Wniosek certyfikacyjny".

3. Przesłanie do KDPW oryginału oświadczenia do wniosku certyfikacyjnego potwierdzającego złożenie wniosku certyfikacyjnego. Szczegóły podano w punkcie „Potwierdzenie wniosku certyfikacyjnego".

4. Instalacja certyfikatu zgodnie z punktem „Instalacja certyfikatu użytkownika".

5. Wykonanie kopii bezpieczeństwa certyfikatu. Szczegóły podano w punkcie „Kopia bezpieczeństwa certyfikatu użytkownika".

II Wymagania systemowe

1. System operacyjny:

- Windows XP, Windows Vista lub Windows 7 plus najnowszy Service Pack.
- Uprawnienia pozwalające na zapis do magazynu certyfikatów Windows.
- Zainstalowana kontrolka xenroll.dll dla Windows XP (domyślnie instalowana jest podczas instalacji systemu w katalogu C:\windows\system32) lub certenroll.dll dla Windows Vista i Windows 7.

2. Przeglądarka:

- Microsoft Internet Explorer w wersji 6.0 lub nowszej.
- Włączona obsługa "cookie"..
- Uprawnienia pozwalające na uruchomienie kontrolek ActiveX firmy Microsoft.

III Wniosek certyfikacyjny

W celu uzyskania certyfikatu należy złożyć wniosek certyfikacyjny – wypełnić odpowiedni formularz znajdujący się na stronie internetowej KDPW w sekcji Usługi → Repozytorium transakcji wersja EMIR → Aplikacja → Formularz certyfikacyjny A2A.

Podczas uruchamiania strony system może wyświetlić komunikat informujący o konieczności uruchomienia dodatku „Microsoft Certificate Enrollment Control" dla Windows XP lub „Klient rejestrowania Usług certyfikatów…" dla Windows Vista i Windows 7. należy wtedy kliknąć na podświetlonym pasku (patrz rys.1) i wybrać opcję „Uruchom dodatek" dla Windows XP lub „Uruchom formant ActiveX" dla Windows Vista i Windows 7 (patrz rys.2).

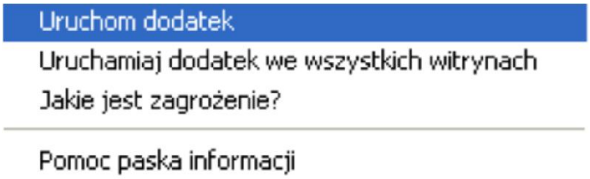
W przypadku pracy w systemie Windows Vista i Windows 7. należy dodatkowo zmienić poziom zabezpieczeń dla wybranej strefy internetowej. W tym celu trzeba uruchomić ustawienia przeglądarki poprzez wybranie opcji z menu Narzędzia → Opcje internetowe i wybrać zakładkę Zabezpieczenia. Następnie należy zaznaczyć strefę „Internet" i naciśnąć przycisk „Poziom niestandardowy". W opcji „Inicjowanie i wykonywanie skryptów formantów ActiveX niezaznaczonych jako bezpieczne do wykonywania" zaznacz pole „Monitoruj". Zaakceptuj zmiany potwierdzając przyciskiem „OK".

dla Windows XP

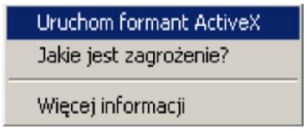
dla Windows Vista i Windows 7

Rys. 1

dla Windows XP

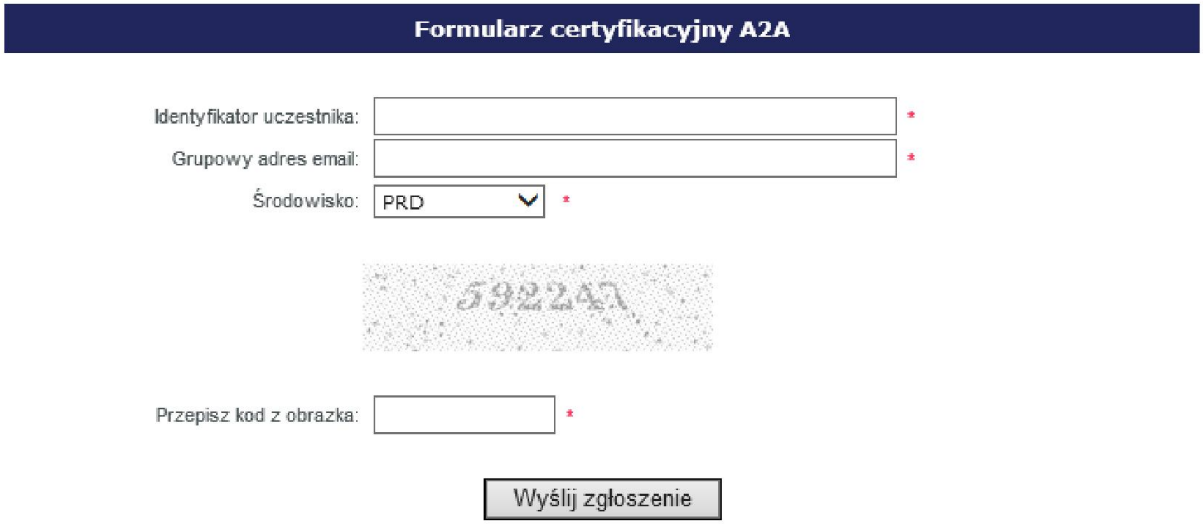


dla Windows Vista i Windows 7



Rys. 2

Na stronie znajduje się formularz (patrz rys. 3), w którym kolejno należy wprowadzać swoje dane niezbędne do wysłania zgłoszenia certyfikacyjnego. Pola oznaczone gwiazdką są wymagane.
W przypadku poprawności danych o uczestniku należy wybrać opcję „Wyślij zgłoszenie".



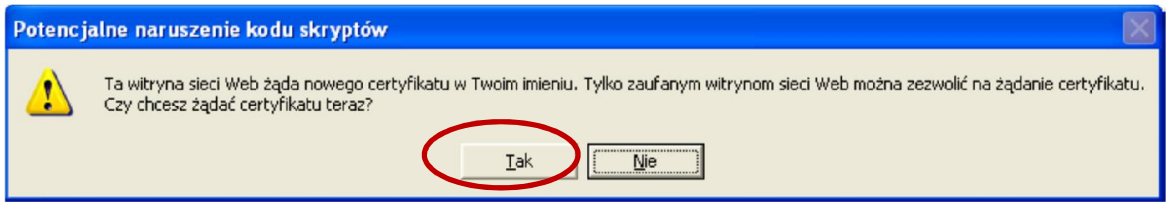
Rys. 3

Wypełnienie wszystkich pól w formularzu jest wymagane.

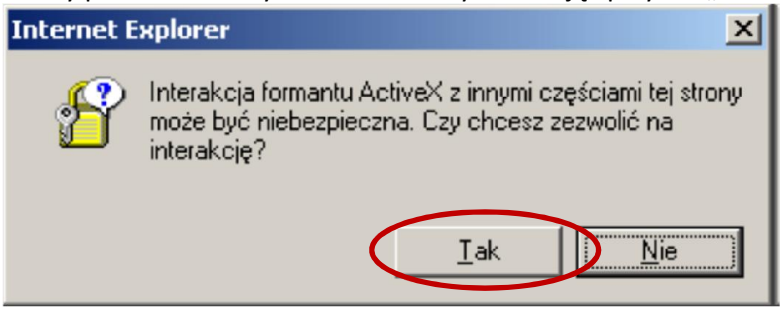
Opis formularza:
Identyfikator uczestnika - w polu należy podać kod LEI uczestnika
Grupowy adres e-mail - w polu należy wprowadzić adres e-mail, na który będą wysyłane powiadomienia. Ze względu na tryb A2A zalecany jest grupowy adres e-mail.
Środowisko - w polu tym należy wybrać do jakiego środowiska ma być nadany dostęp.

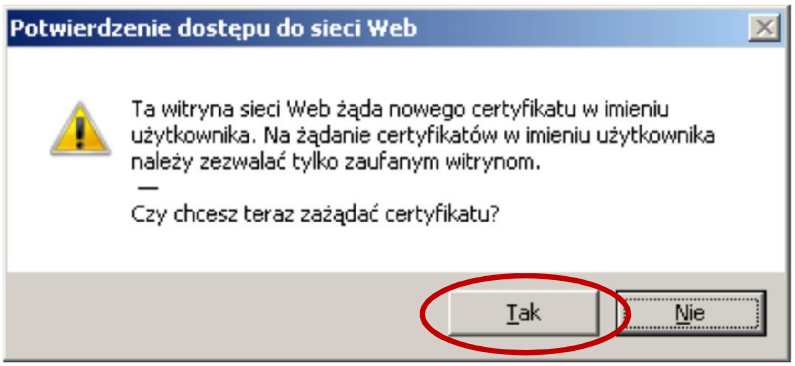
Na wskazany adres e-mail zostanie wysłana informacja o przyjęciu wniosku oraz informacja zawierająca status zgłoszenia certyfikacyjnego.
Po zaakceptowaniu danych przez aplikację pojawi się kolejny komunikat (patrz rys. 4), który należy potwierdzić naciskając przycisk „Tak".

Dla Windows XP



Dla Windows Vista i Windows 7
Należy potwierdzić obydwa komunikaty naciskając przycisk „TAK"





Rys. 4

W przypadku wprowadzenia błędnych danych lub nie wypełnienia wszystkich wymaganych pól, na ekranie pod formularzem, wyświetlany jest komunikat informujący o przyczynie błędu.
Po prawidłowym wypełnieniu formularza i naciśnięciu przycisku *Wyślij zgłoszenie* na ekranie użytkownika zostanie wyświetlony komunikat:

Zgłoszenie certyfikacyjne nr **Numer** dla użytkownika **Identyfikator uczestnika** (A2A) zostało przyjęte do realizacji w dniu RRRR-MM-DD o godzinie HH24:MM:SS .

Treść oświadczenia do wysłania do KDPW wraz z niżej podanym kodem aktywacyjnym zostanie przesłana na adres email podany w zgłoszeniu.

Twój kod aktywacyjny

fe970a5d429fd2e76f2f415c90966a28

Rys. 5

Na wskazany w formularzu adres email zostanie wysłana wiadomość potwierdzająca przyjęcie wniosku o wydanie certyfikatu wraz z *Oświadczeniem do wniosku certyfikacyjnego*, który po podpisaniu przez reprezentację należy dostarczyć do KDPW w formie oryginału.

Temat wiadomości:
Repozytorium Transakcji KDPW_TR (A2A) – przyjęcie zgłoszenia certyfikacyjnego nr XXXX

Treść wiadomości:
Zgłoszenie certyfikacyjne nr XXXX dla organizacji Nazwa organizacji zostało przyjęte do realizacji w dniu RRRR-MM-DD o godzinie HH24:MM:SS.

Kod KDPW_TR: XXXXXXXXXXXX
Sender ID: XXXX
Środowisko KDPW_TR: XXX

W celu potwierdzenia zgłoszenia należy dostarczyć do KDPW przesłany w załączeniu i podpisany zgodnie z reprezentacją podmiotu oryginał oświadczenia do wniosku certyfikacyjnego, wraz z niżej podanym kodem aktywacyjnym:

Twój kod aktywacyjny
fe970a5d429fd2e76f2f415c90966a28

Do tej wiadomości zostało załączone oświadczenie do wniosku certyfikacyjnego.

Rys. 6

Oświadczenie do wniosku certyfikacyjnego generowane jest automatycznie na podstawie danych wpisanych w formularzu rejestracyjnym oraz wybranych w nim pól.

Uwaga !!!
Zgłoszenie certyfikacyjne wraz z kluczem prywatnym jest zapisywane w profilu systemowym użytkownika, na komputerze z którego wysłano zgłoszenie. Usunięcie użytkownika z systemu lub utrata informacji o wygenerowanym zgłoszeniu (brak dostępu do komputera, z którego wysłano zgłoszenie certyfikacyjne) wiąże się z koniecznością ponownego wypełnienia formularza i wysłania zgłoszenia certyfikacyjnego. Listę zarejestrowanych zgłoszeń można przeglądać poprzez zakładkę „Certyfikaty" dostępną poprzez „Microsoft Management Console"(MMC) lub wpisując komendę „certmgr.msc" w oknie „Uruchom".

IV Status zgłoszenia certyfikacyjnego

Po otrzymaniu oświadczenia do wniosku certyfikacyjnego oraz po weryfikacji podpisów złożonych na nim, KDPW podejmuje decyzję odnośnie akceptacji złożonego wniosku certyfikacyjnego. W przypadku zgodności przesłanych danych z danymi podanymi we wniosku oraz poprawnej weryfikacji podpisów z kartą wzorów podpisów przekazaną do KDPW, złożony wniosek certyfikacyjny zostaje zaakceptowany. W przeciwnym wypadku wniosek zostaje odrzucony.

O akceptacji bądź odrzuceniu wniosku użytkownik zostanie poinformowany wiadomością e-mail przesłaną na wskazany we wniosku adres poczty elektronicznej.
W przypadku akceptacji wniosku użytkownik otrzyma wiadomość o treści jak na rys. 7 i będzie miał możliwość pobrania certyfikatu i zainstalowania go w swoim profilu użytkownika.

Temat wiadomości:
Repozytorium transakcji KDPW_TR (A2A) – akceptacja zgłoszenia certyfikacyjnego nr XXXX

Treść wiadomości:
Zgłoszenie certyfikacyjne nr XXXX dla organizacji Nazwa organizacji z dnia RRRR-MM-DD zostało zaakceptowane.

Kod KDPW_TR: XXXXXXXXXXXX
Sender ID: XXXX
Środowisko KDPW_TR: XXX

W celu zainstalowania certyfikatu wykonaj poniższe punkty

1. (Tylko dla systemu WINDOWS VISTA i WINDOWS 7) Pobierz certyfikat urzędu naciskając poniższy link i zainstaluj go zgodnie z instrukcją instalacji certyfikatu urzędu, zawartą w procedurze obsługi certyfikatów dla KDPW_TR (A2A):
http://csp.kdpw.pl/pki/KDPW%20Root.crt

2. Pobierz certyfikat użytkownika A2A naciskając poniższy link i zainstaluj go zgodnie z instrukcją instalacji certyfikatu użytkownika A2A, zawartą w procedurze obsługi certyfikatów dla KDPW_TR (A2A):
http://www.kdpw.pl/Strony/certrsp.aspx?ActivationCode=fe970a5d429fd2e76f2f415c90966a28

Rys. 7

W przypadku odrzucenia wniosku przysyłana jest wiadomość o następującej treści (rys. 8):

Temat wiadomości:
Repozytorium transakcji KDPW_TR (A2A) – odrzucenie zgłoszenia certyfikacyjnego nr XXXX.

Treść wiadomości:
Zgłoszenie certyfikacyjne nr XXXX dla organizacji Nazwa organizacji z dnia RRRR-MM-DD zostało odrzucone.

Kod KDPW_TR: XXXXXXXXXXXX
Sender ID: XXXX
Środowisko KDPW_TR: XXX

Powód odrzucenia:

Treść z przyczyną odrzucenia W celu wydania certyfikatu, proszę o ponowne wypełnienie formularza certyfikacyjnego i przesłanie nowego oświadczenia do wniosku certyfikacyjnego.

Rys. 8

V Instalacja certyfikatu urzędu (tylko dla systemu Windows Vista i Windows 7)

W przypadku systemu Windows XP punkt należy pominąć.

Przed dokonaniem instalacji certyfikatu urzędu należy upewnić się, czy spełnione są wymagania systemowe podane w punkcie „Wymagania systemowe".

Instalację certyfikatu należy przeprowadzić wyłącznie w systemie Windows Vista i Windows 7, na koncie systemowym użytkownika, z którego wysłane było zgłoszenie certyfikacyjne.

Po otrzymaniu wiadomości e-mail potwierdzającej akceptację zgłoszenia certyfikacyjnego, możliwe jest zainstalowanie certyfikatu urzędu poprzez wybranie linku podanego w punkcie 1.

Instalację należy przeprowadzić zgodnie z poniższą instrukcją:

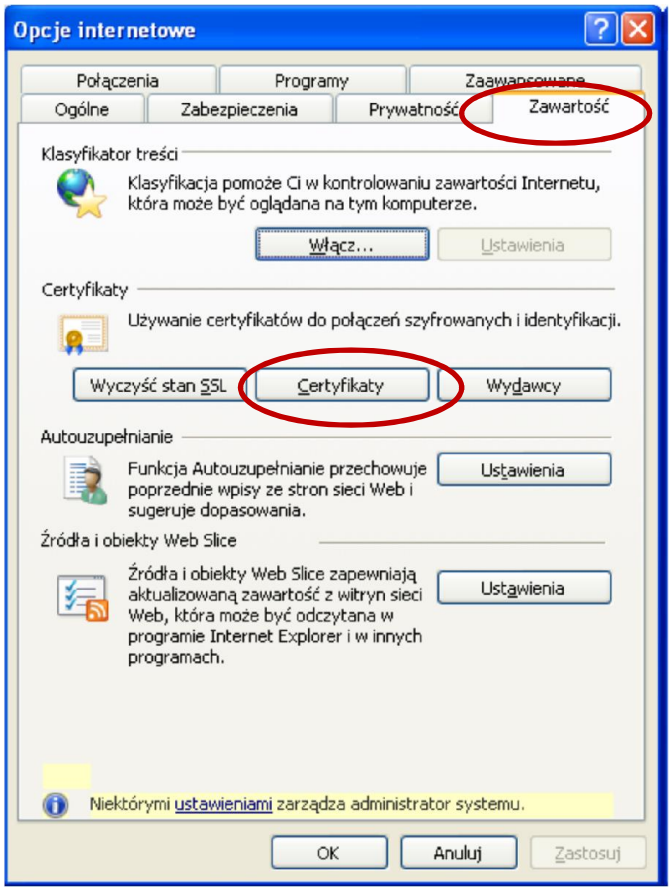
1. Kliknij na linku podanym w punkcie 1., w wiadomości pocztowej i zapisz plik np. na pulpicie użytkownika. Plik nosi nazwę „KDPW Root.crt".

2. Uruchom przeglądarkę Internet Explorer.

3. Z menu wybierz opcję „Narzędzia → Opcje internetowe".

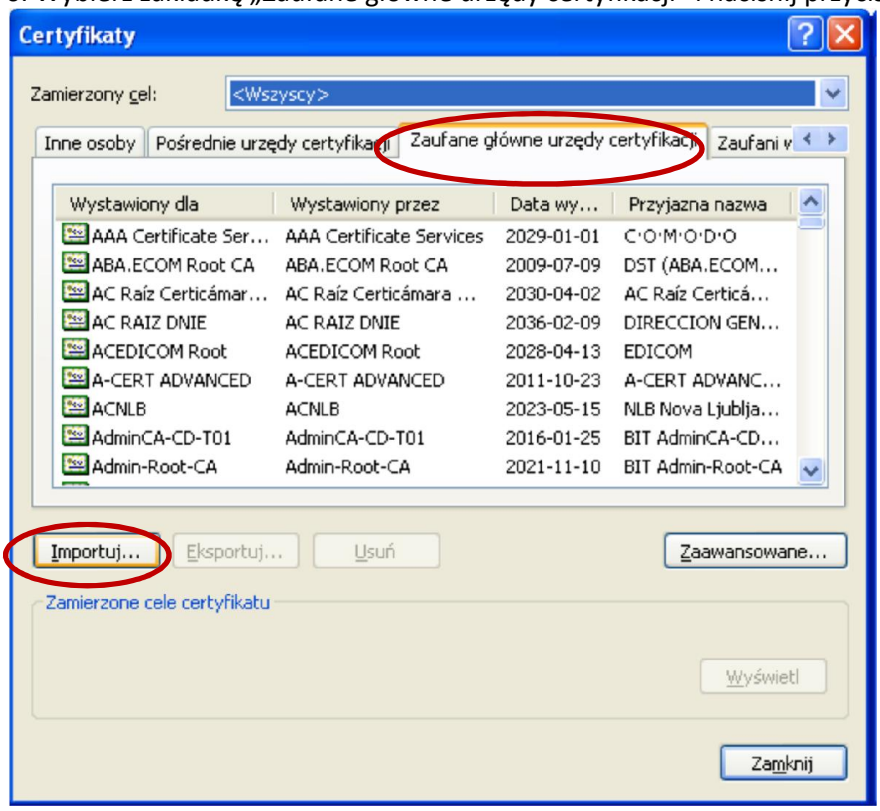
4. Przejdź do zakładki „Zawartość".
Zakładka „Zawartość" może być niewidoczna w przypadku systemowego ograniczenia uprawnień użytkownika do magazynów z certyfikatami. W celu uzyskania dostępu należy skontaktować się z lokalnym administratorem komputera.

5. Naciśnij przycisk „Certyfikaty".



Rys. 9

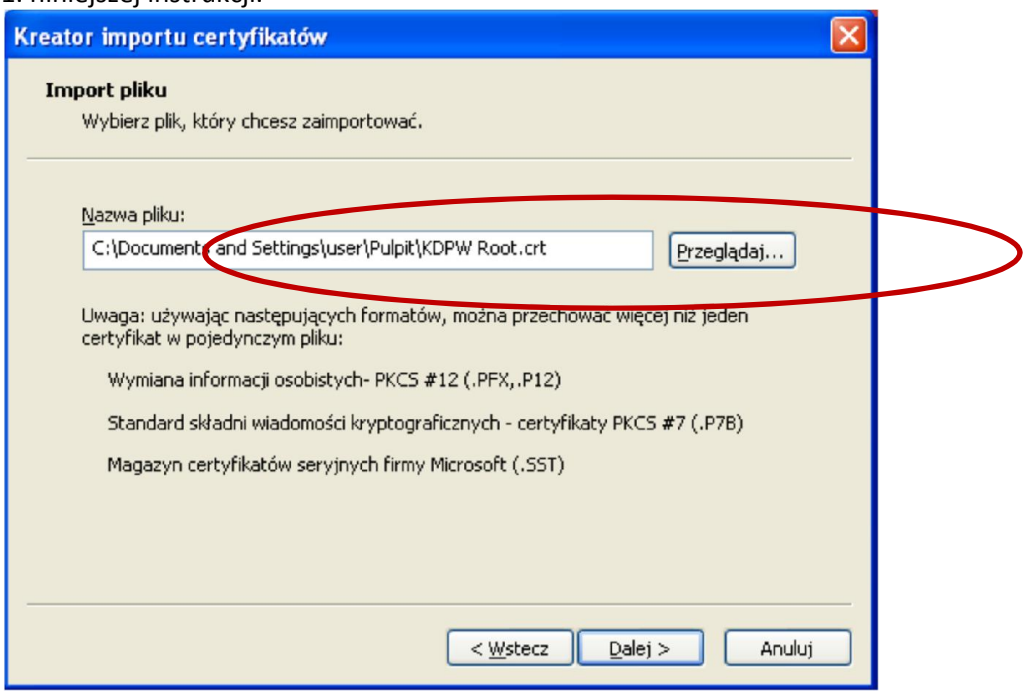
6. Wybierz zakładkę „Zaufane główne urzędy certyfikacji” i naciśnij przycisk „Importuj”.



Rys. 10

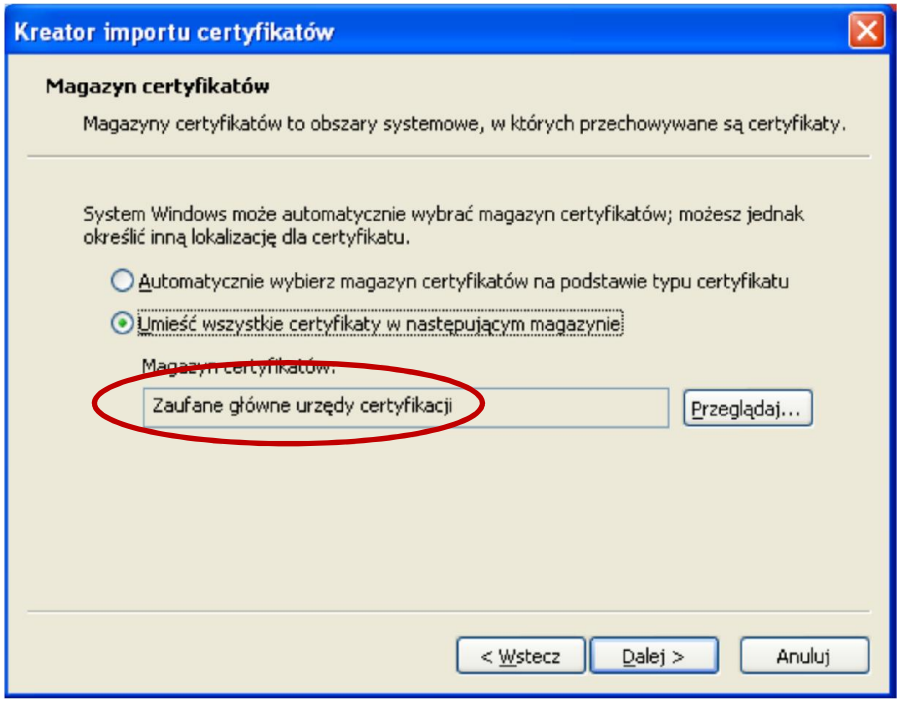
7. W pojawiającym się oknie naciśnij przycisk „Dalej”.

8. W następnym oknie naciśnij przycisk „Przeglądaj” i wskaż plik z certyfikatem zapisanym w punkcie 1. niniejszej instrukcji.



Rys. 11

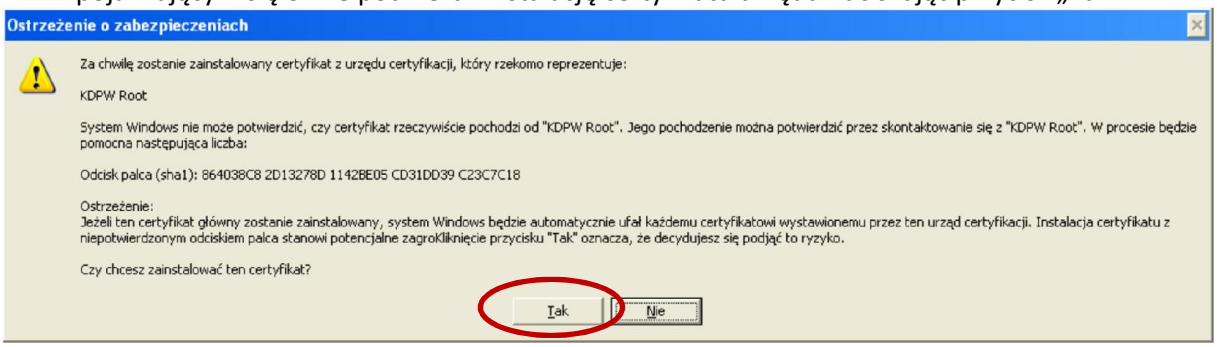
9. Naciśnij przycisk „Dalej”.
10. Zwróć uwagę czy w pozycji „Magazyn certyfikatów” podana jest wartość „Zaufane główne urzędy certyfikacji”. W kolejnym oknie naciśnij przycisk „Dalej”.



Rys. 12

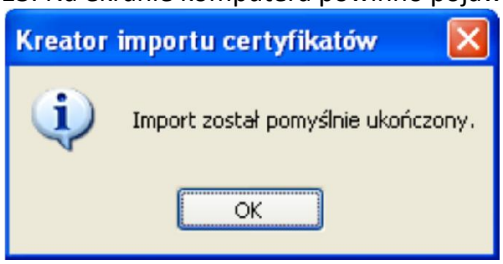
11. Naciśnij przycisk „Zakończ”.

12. W pojawiającym się oknie potwierdź instalację certyfikatu urzędu naciskając przycisk „Tak”.



Rys. 13

13. Na ekranie komputera powinno pojawić się okno.



Rys. 14

VI Instalacja certyfikatu użytkownika (A2A)

Przed dokonaniem instalacji certyfikatu użytkownika A2A, należy upewnić się, czy spełnione są wymagania systemowe podane w punkcie „Wymagania systemowe”.

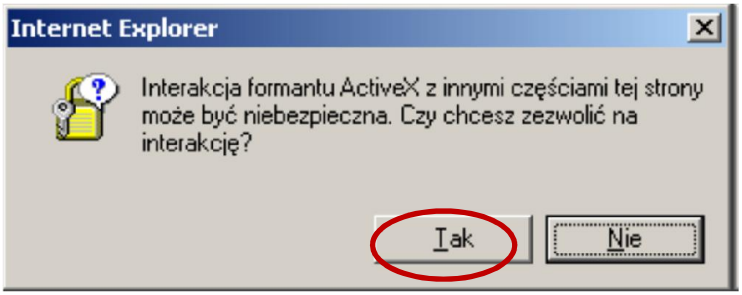
Instalację certyfikatu należy przeprowadzić na koncie systemowym użytkownika, z którego wysłane było zgłoszenie certyfikacyjne.

Po otrzymaniu wiadomości e-mail potwierdzającej akceptację zgłoszenia certyfikacyjnego możliwe jest zainstalowanie certyfikatu poprzez wybranie linku podanego w punkcie 2.

Na ekranie pojawi się okno zawierające szczegóły certyfikatu wraz z opcją pozwalającą na wykonanie instalacji (patrz. rys. 15). W przypadku systemu Windows Vista i Windows 7 pojawi się również dodatkowy komunikat informujący o interakcji formantu ActiveX (patrz rys. 16), który należy zaakceptować naciskając przycisk „TAK”.

Rys. 15

Dla Windows Vista i Windows 7



Rys. 16

Po naciśnięciu przycisku „Zainstaluj certyfikat”, należy kolejno akceptować wszystkie pojawiające się komunikaty do momentu pojawienia się informacji o prawidłowym zakończeniu instalacji.

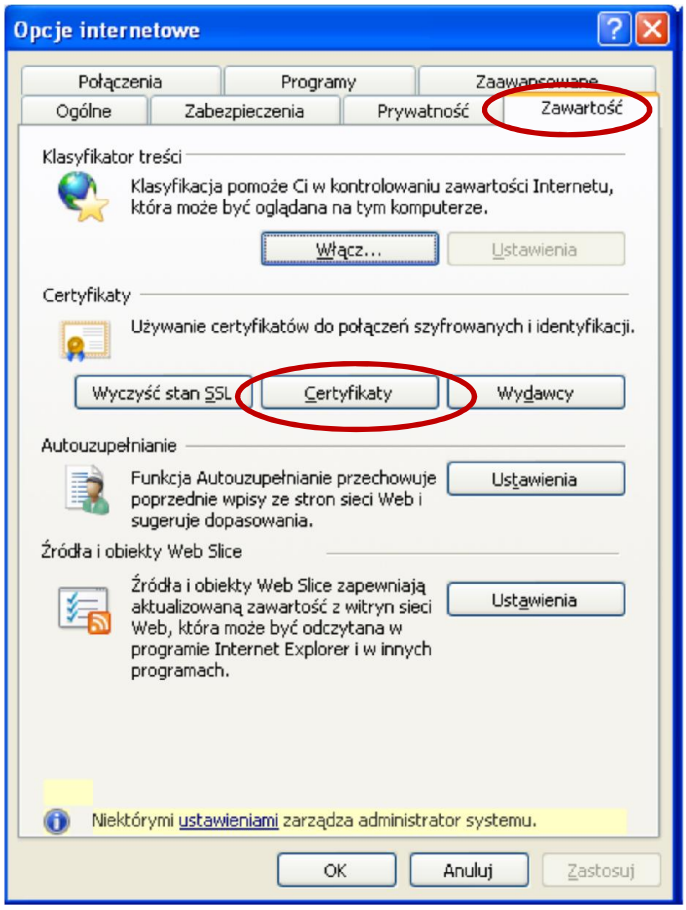
VII Kopia bezpieczeństwa certyfikatu użytkownika A2A

Zaleca się wykonanie kopii bezpieczeństwa od razu po pierwszym zainstalowaniu certyfikatu w systemie operacyjnym. W przypadku awarii lub konieczności ponownej instalacji, użytkownik jest w stanie szybko odtworzyć certyfikat bez konieczności ponownego wysyłania zgłoszenia certyfikacyjnego.
Kopie bezpieczeństwa należy wykonać zgodnie z poniższą instrukcją:
1. Uruchom przeglądarkę Internet Explorer.

2. Z menu wybierz opcję „Narzędzia → Opcje internetowe".

3. Przejdź do zakładki „Zawartość".
Zakładka „Zawartość" może być niewidoczna w przypadku systemowego ograniczenia uprawnień użytkownika do magazynów z certyfikatami. W celu uzyskania dostępu należy skontaktować się z lokalnym administratorem komputera.

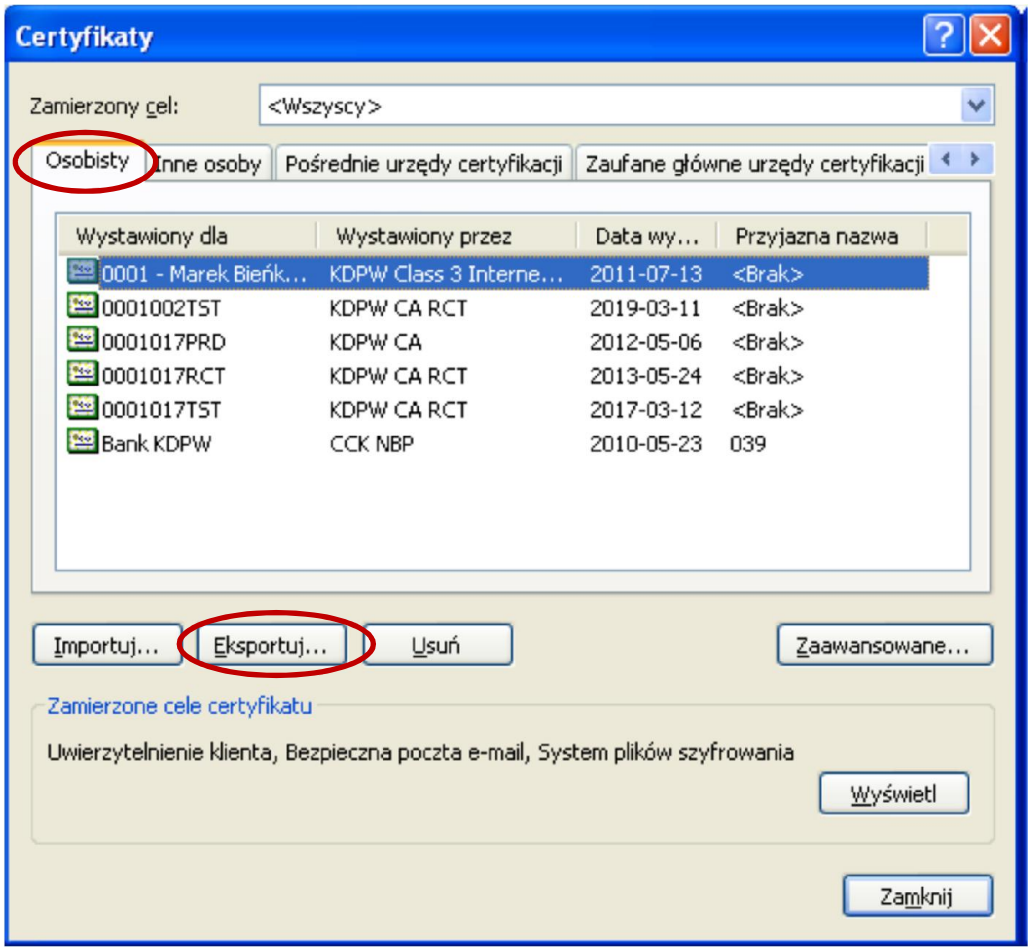
4. Naciśnij przycisk „Certyfikaty"



Rys. 17

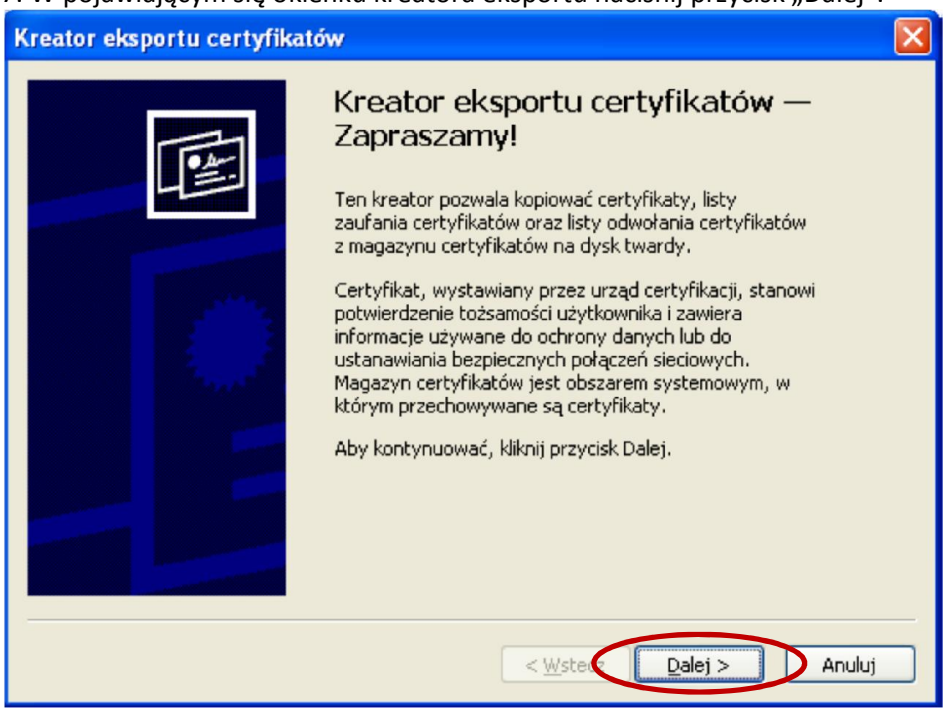
5. Przejdź do zakładki „Osobisty".

6. Zaznacz certyfikat przeznaczony do zarchiwizowania i naciśnij przycisk „Eksportuj".



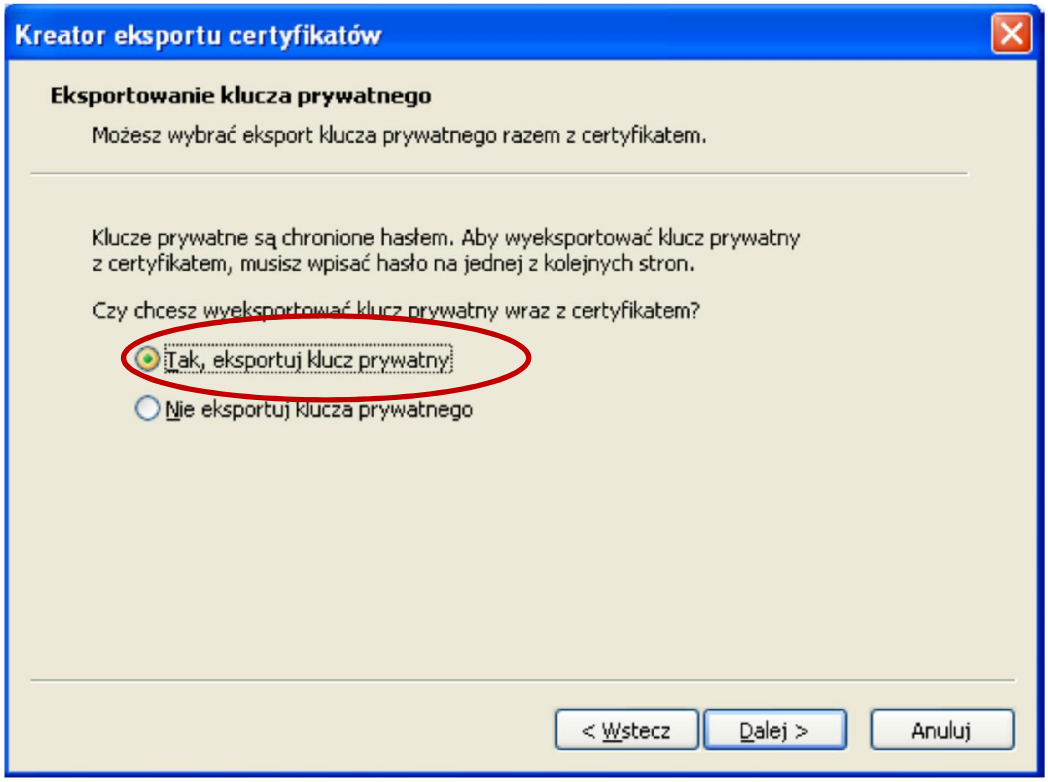
Rys. 18

7. W pojawiającym się okienku kreatora eksportu naciśnij przycisk „Dalej”.



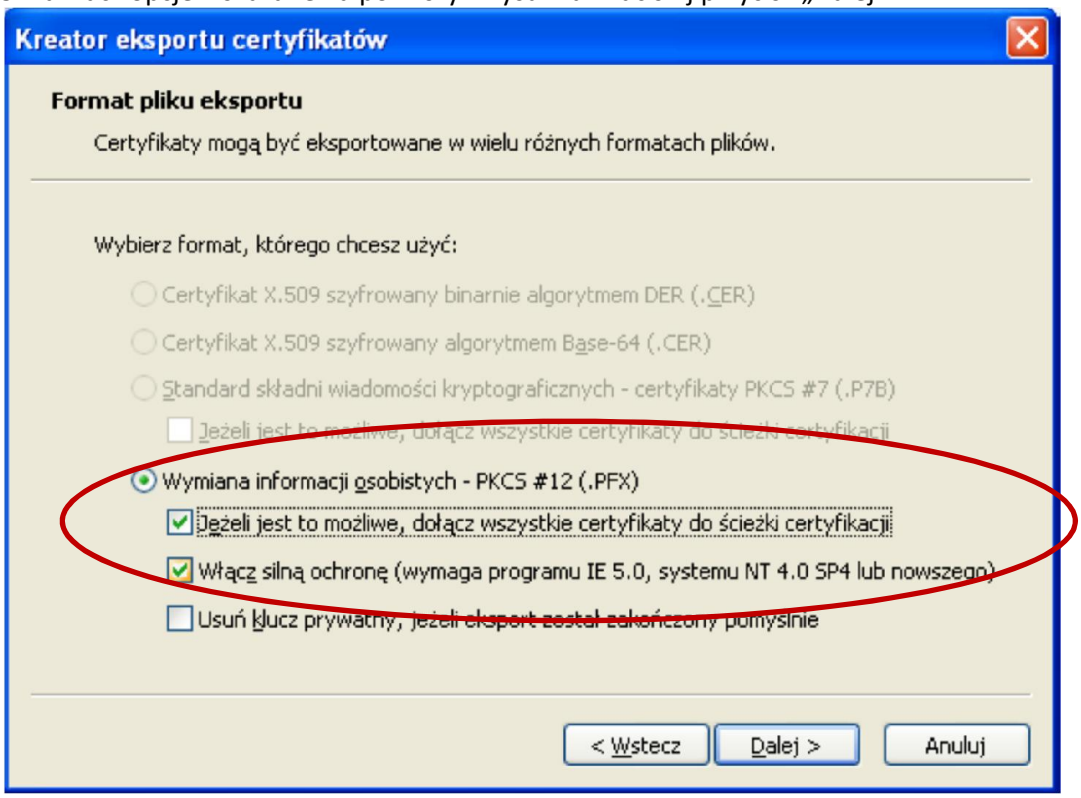
Rys. 19

8. W kolejnym oknie zaznacz opcję: „Tak, eksportuj klucz prywatny”.



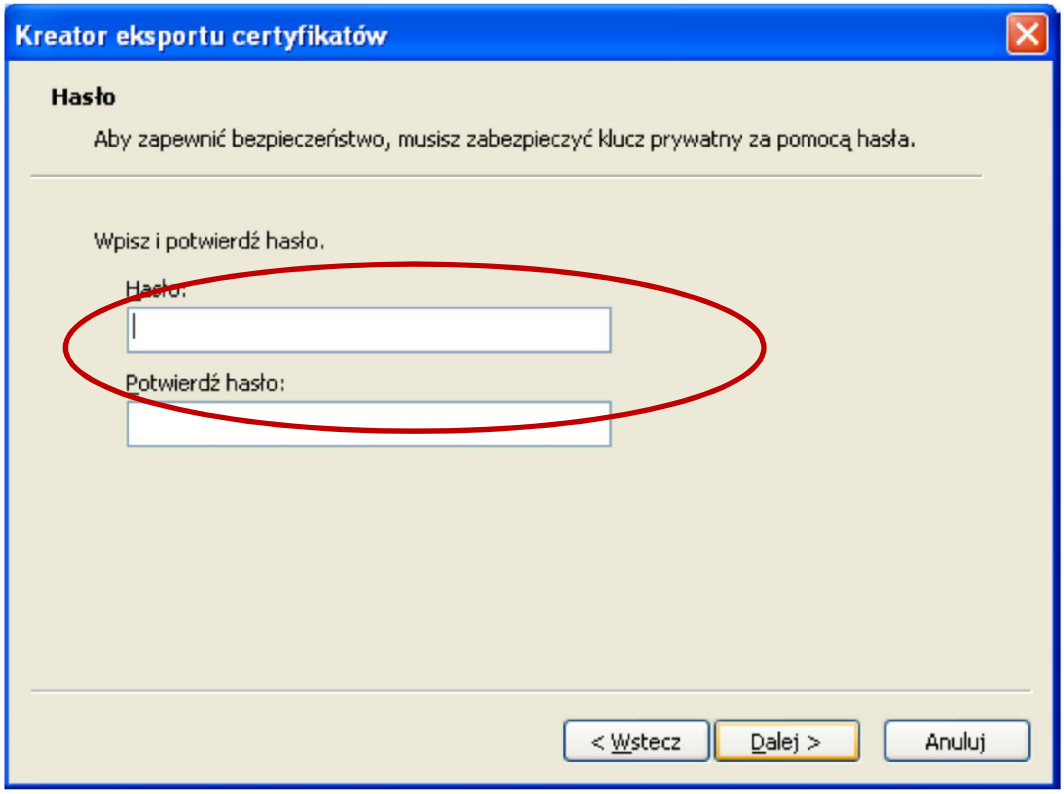
Rys. 20

9. Zaznacz opcje wskazane na poniższym rysunku i naciśnij przycisk „Dalej”



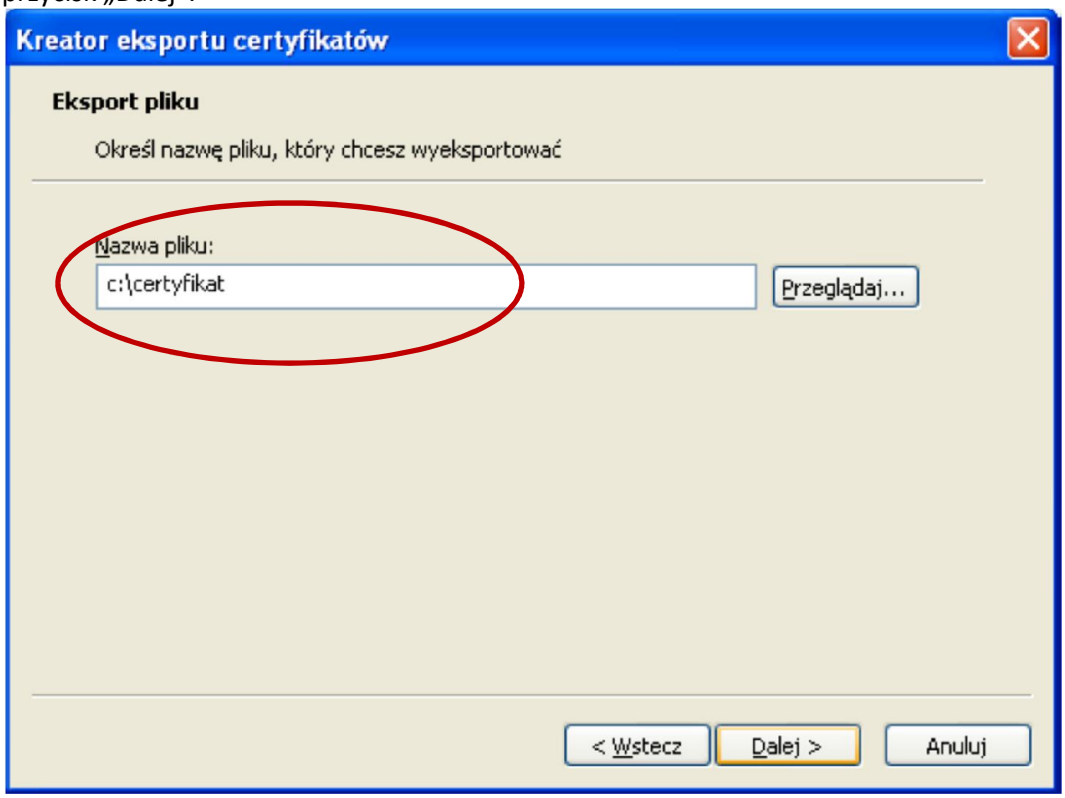
Rys. 21

10. Wprowadź hasło do pliku, w którym zostanie zapisany certyfikat i naciśnij przycisk „Dalej”.



Rys. 22

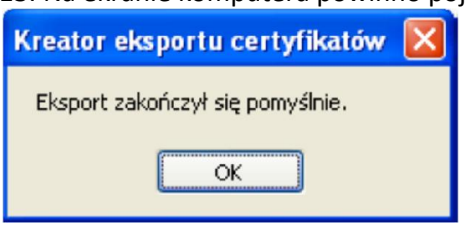
11. W następnym oknie wprowadź nazwę pliku, do którego zostanie zapisany certyfikat i naciśnij przycisk „Dalej”.



Rys. 23

12. Potwierdź naciskając przycisk „Zakończ”.

13. Na ekranie komputera powinno pojawić się okno.



Rys. 24

Po zakończeniu eksportu, na dysku utworzony został plik o rozszerzeniu pfx, który można zapisać na dowolnym nośniku danych. Z uwagi na to, że certyfikaty wydawane są na okres trzech lat, zaleca się zapisanie pliku na nośniku CD lub DVD.

VIII Unieważnienie certyfikatu

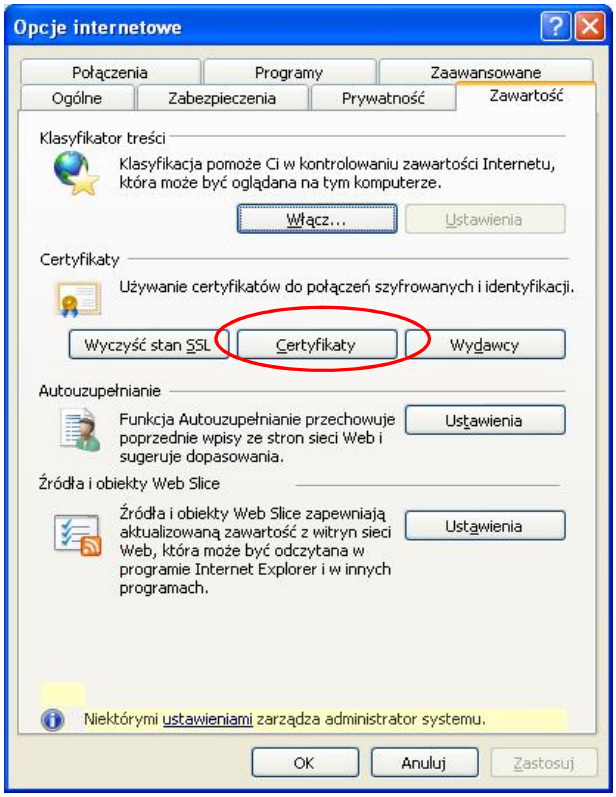
Istnieje możliwość unieważnienia certyfikatu użytkownika A2A, co skutkuje odebraniem dostępu do „Repozytorium transakcji KDPW_TR".
W celu unieważnienia certyfikatu należy wysłać do KDPW oryginał „Wniosku o unieważnienie certyfikatu", który jest do pobrania ze strony internetowej www.kdpw.pl, następnie kliknąć link *Usługi → Repozytorium transakcji wersja EMIR,* a następnie z menu po prawej stronie wybrać „Aplikacja". Jeżeli wybrana osoba posiada więcej niż jeden certyfikat, należy podać dane identyfikujące unieważniany certyfikat. W przypadku ich braku, unieważnione zostaną wszystkie certyfikaty dla podanego użytkownika. Na dane identyfikujące certyfikat użytkownika składają się: numer seryjny certyfikatu, lub kod aktywacyjny, lub numer zgłoszenia certyfikacyjnego. Kod aktywacyjny oraz numer zgłoszenia certyfikacyjnego są przekazywane podczas procesu uzyskiwania certyfikatu użytkownika za pomocą wiadomości na wskazany w formularzu certyfikacyjnym adres e-mail.
Informacje o numerze seryjnym certyfikatu należy odczytać zgodnie z poniższą instrukcją:

1. Uruchom przeglądarkę Internet Explorer.

2. Z menu wybierz opcję „Narzędzia → Opcje internetowe".

3. Przejdź do zakładki „Zawartość".
Zakładka „Zawartość" może być niewidoczna w przypadku systemowego ograniczenia uprawnień użytkownika do magazynów z certyfikatami. W celu uzyskania dostępu należy skontaktować się z lokalnym administratorem komputera.

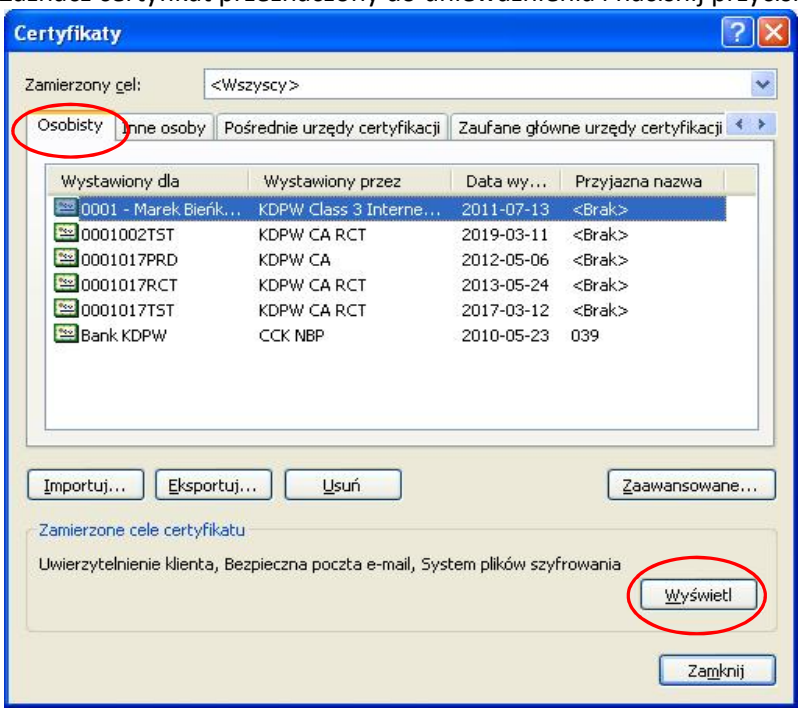
4. Naciśnij przycisk „Certyfikaty"



Rys. 25

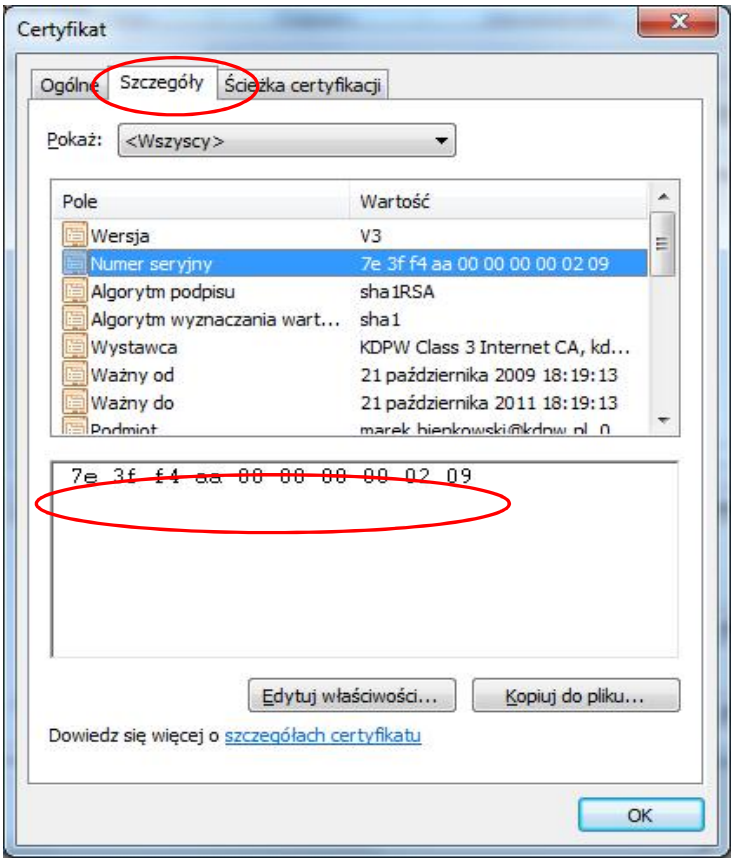
5. Przejdź do zakładki „Osobisty”.

6. Zaznacz certyfikat przeznaczony do unieważnienia i naciśnij przycisk „Wyświetl”.



Rys. 26

7. Przejdź do zakładki „Szczegóły” i odczytaj wartość z pozycji „Numer seryjny”.



Rys. 27

Po weryfikacji wniosku unieważnienia certyfikatu w KDPW i unieważnieniu certyfikatu, użytkownik otrzymuje email potwierdzający:

Temat wiadomości:
Repozytorium transakcji KDPW_TR (A2A) – unieważnienie certyfikatu dla zgłoszenia certyfikacyjnego nr XXXX

Treść wiadomości:
Certyfikat dla zgłoszenia certyfikacyjnego nr XXXX, wydany dla organizacji Nazwa organizacji został unieważniony w dniu RRRR-MM-DD.

Kod KDPW_TR: XXXXXXXXXXXX
Sender ID: XXXX
Środowisko KDPW_TR: XXX

Powód unieważnienia:
Certyfikat unieważniony na wniosek Uczestnika.

IX ZAŁĄCZNIK NR 1 Wniosek o unieważnienie certyfikatu

_____, dnia _____ r.

WNIOSEK O UNIEWAŻNIENIE CERTYFIKATU DO REPOZYTORIUM TRANSAKCJI KDPW_TR (A2A)

Niżej podpisani, działając w imieniu i na rzecz _____ z siedzibą w _____, przy ul. _____ („**Uczestnik**”) zwracamy się z prośbą o unieważnienie certyfikatu do Repozytorium transakcji KDPW_TR zawierającego następujące dane:

Sender ID: ☐☐☐☐

e-mail: _____

Dane identyfikujące certyfikat*: _____

*Numer seryjny lub kod aktywacyjny lub numer zgłoszenia certyfikacyjnego

W przypadku nie podania żadnych danych identyfikujących certyfikat, zostaną unieważnione wszystkie certyfikaty dla danego Uczestnika dla trybu A2A. Unieważnienie certyfikatu skutkuje odebraniem dostępu do Repozytorium transakcji KDPW_TR.

_____

data i podpisy osób uprawnionych do reprezentowania Uczestnika