

Procedura obsługi certyfikatów KDPW_TR (A2A)

Spis treści

Ι	DOSTĘP DO REPOZYTORIUM TRANSAKCJI KDPW_TR W TRYBIE A2A 2
II	WYMAGANIA SYSTEMOWE
111	WNIOSEK CERTYFIKACYJNY
IV	STATUS ZGŁOSZENIA CERTYFIKACYJNEGO7
V	INSTALACJA CERTYFIKATU URZĘDU (TYLKO DLA SYSTEMU WINDOWS VISTA I WINDOWS 7)9
VI	INSTALACJA CERTYFIKATU UŻYTKOWNIKA (A2A)13
VII	KOPIA BEZPIECZEŃSTWA CERTYFIKATU UŻYTKOWNIKA A2A14
VIII	UNIEWAŻNIENIE CERTYFIKATU 19
IX	ZAŁĄCZNIK NR 1 WNIOSEK O UNIEWAŻNIENIE CERTYFIKATU

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 \rightarrow Repozytorium transakcji wersja EMIR \rightarrow Aplikacja \rightarrow 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

dodatek: "Microsoft Certificate Enrollment Control" z "Microsoft Corporation"

dla Windows Vista i Windows 7

dodatek: "Klient rejestrowania Usług certyfikatów w usłudz..." z "Microsoft Corporation". J

Rys. 1

dla Windows XP

Uruchom dodatek

Uruchamiaj dodatek we wszystkich witrynach Jakie jest zagrożenie?

Pomoc paska informacji

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".



Formularz certyfikacyjny A2A

Identyfikator uczestnika:		
Grupowy adres email:		
Środowisko:	RD 💉 *	
	592247	
Przepisz kod z obrazka:	*	
	Wyćlij załoszenie	-

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 Vista i Windows 7

Należy potwierdzić obydwa komunikaty naciskając przycisk "TAK"

Internet E	xplorer	(
£	Interakcja formantu ActiveX z innymi częściami tej strony może być niebezpieczna. Czy chcesz zezwolić na interakcję?	
	<u>I</u> ak <u>Nie</u>	



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".

Połączen	ia	Progra	my	Zaa	wapcowape
Ogólne	Zabe	zpieczenia	Pryw	atność	Zawartoś
lasvfikator t	reści —				
Kla kt	asyfikacja óra może	pomoże Ci w ł być oglądana i	kontrolowa na tym kom	niu zawarto Iputerze,	ości Internetu,
		W	łącz		stawienia
ertyfikaty -					
	ywanie c	ertyfikatów do	połączeń s	szyfrowany	ch i identyfika
Wyczys	ść stan <u>S</u> S	iL <u>C</u> erl	tyfikaty		Vy <u>d</u> awcy
utouzupełnia	anie				
Fu po su	inkcja Aul przednie geruje do	touzupełnianie wpisy ze stron pasowania.	przechowu i sieci Web	ije U	stawienia
ródła i obiek	ty Web Sl	ice –			
źr ak w pr pr pr	ódła i obie tualizowa eb, która ogramie I ogramach	ekty Web Slice ną zawartość : może być odc: nternet Explor).	zapewniaj; z witryn sie zytana w er i w innyc	a U ci U	st <u>a</u> wienia
) Niektór	ymi <u>ustav</u>	vieniami zarząd	lza administ	trator syste	emu.
					_
			11		

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

rtyfikaty				?
amierzony <u>c</u> el:	:yscy>			
Inne osoby Pośrednie urzę	dy certyfika (i Zaufane g	łówne urzędy	certyfikacji Zaufani (4
Wystawiony dla	Wystawiony przez	Data wy	Przyjazna nazwa	^
🔛 AAA Certificate Ser	AAA Certificate Services	2029-01-01	CIOIMIOIDIO	-
🔤 ABA.ECOM Root CA	ABA.ECOM Root CA	2009-07-09	DST (ABA.ECOM	
🔛 AC Raíz Certicámar	AC Raíz Certicámara	2030-04-02	AC Raíz Certicá	
🔛 AC RAIZ DNIE	AC RAIZ DNIE	2036-02-09	DIRECCION GEN	
🔛 ACEDICOM Root	ACEDICOM Root	2028-04-13	EDICOM	
🔤 A-CERT ADVANCED	A-CERT ADVANCED	2011-10-23	A-CERT ADVANC	
🔛 ACNLB	ACNLB	2023-05-15	NLB Nova Ljublja	
🔛 AdminCA-CD-T01	AdminCA-CD-T01	2016-01-25	BIT AdminCA-CD	
Admin-Root-CA	Admin-Root-CA	2021-11-10	BIT Admin-Root-CA	V
Importuj Eksportuj	. Usuń		Zaawansowa	ne.
Zamierzone cele certufikatu				
zamerzone cele certymota				
			₩yświe	tl
			Zam	knij

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.

Kreator importu certyfikatów	
Import pliku	
Wybierz plik, który chcesz zaimportówac.	
Nazwa pliku:	
C:\Document_and Settings\user\Pulpit\KDPW Root.crt Przeglądaj	>
Uwaga: używając następujących formatów, można przechowac więcej niż jeden certyfikat w pojedynczym pliku:	
Wymiana informacji osobistych- PKCS #12 (.PFX,.P12)	
Standard składni wiadomości kryptograficznych - certyfikaty PKCS #7 (.P7B)	
Magazyn certyfikatów seryjnych firmy Microsoft (.SST)	
< <u>W</u> stecz <u>Dalej</u> Anuluj	



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".

Kreator importu certyfikatów
Magazyn certyfikatów
Magazyny certyfikatów to obszary systemowe, w których przechowywane są certyfikaty.
System Windows może automatycznie wybrać magazyn certyfikatów; możesz jednak określić inną lokalizację dla certyfikatu. O Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu O Umieść wszystkie certyfikaty w następującym magazynie
Magazyn certyfikatów.
Zaufane główne urzędy certyfikacji Przeglądaj
<u>W</u> stecz <u>D</u> alej > Anuluj





11. Naciśnij przycisk "Zakończ".

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



13. Na ekranie komputera powinno pojawić się okno.

Kreator	importu certyfikatów 💦 🔀
٩	Import został pomyślnie ukończony.
	ОК
Rvs. 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".

		Status certyfikatu
Ν	lazwa certyfikatu:	(PRD) PL5261009528
Ν	lumer żądania:	3979
С)rganizacja:	Krajowy Depozyt Papierów Wartościowych S.A.
S	status:	Żądanie zaakceptowane

Zainstaluj certyfikat

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 \rightarrow 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"

je intern	etowe				
Połączer	nia	Progra	my	Zaawa	ancowane
Ogólne	Zabe	zpieczenia	Prywat	ność 🤇	Zawartoś
asyfikator I Q K ki	:reści lasyfikacja tóra może l	pomoże Ci w I być oglądana <u>W</u>	kontrolowaniu na tym kompu łącz	u zawartośc uterze. Usta	i Internetu, awienia
ertyfikaty -					
, U	żywanie ce	ertyfikatów do	połączeń szy	/frowanych	i identyfikad
Wyczy	ść stan <u>S</u> SI	L <u>C</u> er	tyfikaty	Wy Wy	dawcy
utouzupełni P sv ródła i obieł	ianie unkcja Auto oprzednie (ugeruje do sty Web Sli	ouzupełnianie wpisy ze stron pasowania, ce –	przechowuje sieci Web i	Us <u>t</u> a	awienia
ź a w p p	ródła i obie ktualizowar /eb, która i rogramie Ir rogramach	kty Web Slice ną zawartość może być odc; nternet Explor	zapewniają z witryn sieci zytana w er i w innych	Usta	awienia
		ieniami zarzad	za administra	tor system	и.
) Niektó	rymi <u>ustaw</u>				

Rys. 17

- 5. Przejdź do zakładki "Osobisty".
- 6. Zaznacz certyfikat przeznaczony do zarchiwizowania i naciśnij przycisk "Eksportuj".

Certyfikaty				? 🗙			
Zamierzony <u>c</u> el:	<wszyscy></wszyscy>			~			
Osobisty Inne osoby	Pośrednie urzędy certyfikacji	Zaufane głów	ine urzędy certyfikacji	< >			
Wystawiony dla	Wystawiony przez	Data wy	Przyjazna nazwa				
🔤 0001 - Marek Bier	ńk KDPW Class 3 Interne	2011-07-13	<brak></brak>				
0001002TST	KDPW CA RCT	2019-03-11	<brak></brak>				
50001017PRD	KDPW CA	2012-05-06	<brak></brak>				
20001017RCT	KDPW CA RCT	2013-05-24	<brak></brak>				
🔤 0001017TST	KDPW CA RCT	2017-03-12	<brak></brak>				
🔛 Bank KDPW	CCK NBP	2010-05-23	039				
Importuj Eksportuj Usuń Zaawansowane Zamierzone cele certyfikatu							
Uwierzytelnienie klienta, Bezpieczna poczta e-mail, System plików szyfrowania							
			Zamk	nij			

Rys. 18

7. W pojawiającym się okienku kreatora eksportu naciśnij przycisk "Dalej".

Kreator eksportu certyfikato	św.	×
	Kreator eksportu certyfikatów — Zapraszamy! Ten kreator pozwala kopiować certyfikaty, listy zaufania certyfikatów oraz listy odwołania certyfikatów z magazynu certyfikatów na dysk twardy. Certyfikat, wystawiany przez urząd certyfikacji, stanowi potwierdzenie tożsamości użytkownika i zawiera informacje używane do ochrony danych lub do ustanawiania bezpiecznych połączeń sieciowych. Magazyn certyfikatów jest obszarem systemowym, w którym przechowywane są certyfikaty. Aby kontynuować, kliknij przycisk Dalej.	
	< Wstere Dalej > Anuluj	

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".

eator eksportu certyfikatów	
Hasło Aby zapewnić bezpieczeństwo, musisz zabezpieczyć klucz prywatny za pomocą hasła.	
Wpisz i potwierdź hasło.	
Haeto.	
Potwierdź hasło:	
< Wstecz Dalej > Anuluj	
	_

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

Kreator eksportu certyfikatów	<
Eksport pliku Określ nazwę pliku, który chcesz wyeksportować Vazwa pliku: C:\certyfikat C:\certyfikat Przeglądaj	
< <u>W</u> stecz <u>D</u> alej > Anuluj)

Rys. 23



- 12. Potwierdź naciskając przycisk "Zakończ".
- 13. Na ekranie komputera powinno pojawić się okno.

Kreator eksportu certyfikatów	×
Eksport zakończył się pomyślnie.	
ОК	
kys. 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 email.

Informacje o numerze seryjnym certyfikatu należy odczytać zgodnie z poniższą instrukcją:

- 1. Uruchom przeglądarkę Internet Explorer.
- 2. Z menu wybierz opcję "Narzędzia \rightarrow 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"





- 5. Przejdź do zakładki "Osobisty".
- 6. Zaznacz certyfikat przeznaczony do unieważnienia i naciśnij przycisk "Wyświetl".

bisty Inne osoby	Pośrednie urzędy certyfikacji	Zaufane głów	ine urzędy certyfikac
Wystawiony dla	Wystawiony przez	Data wy	Przyjazna nazwa
🗏 0001 - Marek Bieńk.	KDPW Class 3 Interne	2011-07-13	<brak></brak>
0001002TST	KDPW CA RCT	2019-03-11	<brak></brak>
0001017PRD	KDPW CA	2012-05-06	<brak></brak>
0001017RCT	KDPW CA RCT	2013-05-24	<brak></brak>
0001017TST	KDPW CA RCT	2017-03-12	<brak></brak>
Bank KDPW	CCK NBP	2010-05-23	039
portuj Eksport nierzone cele certyfika	uj Usuń utu Bezpieczna poczta e-mail, Sys	tem plików szyf	Zaawansow

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

Pole	Wartość
Wersja	V3
Numer seryjny	7e 3f f4 aa 00 00 00 00 02 09
🗐 Algorytm podpisu	sha 1RSA
Algorytm wyznaczania wart	sha1
Wystawca	KDPW Class 3 Internet CA, kd
Ważny od	21 października 2009 18:19:13
Ważny do	21 października 2011 18:19:13
Podmiot	marek hienkowski@kdnw.nl. 0



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 tra dane:	nsakcji KDPW_TR zawierającego następujące

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