BANK OCHRONY ŚRODOWISKA S.A. ul. Żelazna 32 / 00-832 Warszawa tel.: (+48 22) 850 87 35 faks: (+48 22) 850 88 91 e-mail: bos@bosbank.pl

Instrukcja Użytkownika systemu bankowości internetowej dla firm

Instrukcja instalacji i konfiguracji podpisu kwalifikowanego dla systemu bankowości elektronicznej

BOŚBank24 iBOSS

infolinia 0 801 355 455 | www.bosbank.pl

Sąd Rejonowy dla m.st. Warszawy XII Wydział Gospodarczy Krajowego Rejestru Sądowego I KRS 0000015525 | NIP 527 020 33 13 Kapitał zakładowy: 228 732 450 zł wpłacony w całości.



- 1. Instalacja czytnika kart, dołączonego oprogramowania i certyfikatu.
- 2. Instalacja obsługi technologii Java[™] w przeglądarce internetowej.
- 3. Instalacja aplikacji do autoryzacji SafeDevice[™] jX (pobranie automatyczne.
- 4. Logowanie.

Do poprawnej pracy aplikacji BOŚBank24 iBOSS z wykorzystaniem podpisu kwalifikowanego niezbędne są:

- 1. Zainstalowanie oprogramowania CryptoCard Suite (dostarczone z KIR).
- 2. Zainstalowany certyfikat w systemie.
- 3. Przeglądarka internetowa z obsługą Java™ (Sun) (do pobrania z Internetu).
- 4. Zainstalowane oprogramowanie SafeDevice[™] jX (pobierany automatycznie).

1. Instalacja czytnika kart, dołączonego oprogramowania i certyfikatu.

Zestaw otrzymany z Krajowej Izby Rozliczeniowej S.A. powinien zawierać:

- Kartę z podpisem kwalifikowanym.
- Czytnik kart.
- Płytę Cd z oprogramowaniem.
- Instrukcje instalacji oprogramowania i aktywacji karty.

Instalację czytnika oraz oprogramowania CryptoCard Suite prosimy przeprowadzić zgodnie z instrukcją otrzymaną z KIR S.A.

Wszelkie pytania dotyczące procesu instalacji i aktywacji karty prosimy kierować do pracowników KIR S.A. pod numerem telefonu 801 500 207 lub 22 545 55 55.

Instalacja certyfikatu w systemie

Po instalacji należy zarejestrować certyfikat w systemie. W tym celu należy uruchomić oprogramowanie CryptoCard Suite, wybrać zakładkę Narzędzia, w sekcji Dodatkowe narzędzia wcisnąć przycisk "Uruchom". W oknie CryptoCard Suite: Dodatkowe narzędzia, należy zaznaczyć Rejestracja certyfikatu w systemie (Rys. 1) i kliknąć Dalej



Rys.1

Następnie należy wybrać dostępną kartę elektroniczną klikając na SetEID... (Rys. 2)

Wybierz dostępną kartę elektroniczną	K
Wybierz kartę elektroniczną	
 SCM Microsystems Inc. SCR33x USB Smart Card Reader 0 CryptoCard PKI Token 1(PIN1), 04019149 CryptoCard PKI Token 2(PIN2), 04019149 CryptoCard PKI Token 3(PIN3), 04019149 SetEID, 04019149 	
<wstecz dalei=""> Anulu</wstecz>	i Pomoc

Rys. 2

Następnie wybrać certyfikat w celu importu w systemie operacyjnym (Rys. 3) i kliknąć Dalej.

CryptoCard Su	iite: Dodatkowe na	rzędzia		×
Import certyfil Ten asyster operacyjnyr	katu nt pozwala ci zarejestro n.	ować certyfikat X.509 v	w systemie	KR
Wybrany certyfi	kat			
Wydany dla	Wydany przez	Ważny od	Ważny do	
Anna	Kwalifikowany UZK	2006.01.02 12:00.0	0 2008.01.02.12	.00.00
				Więcej
	< Wstecz	Dalej >	Anuluj	Pomoc

Rys. 3

W kolejnym oknie podajemy nazwę dla importowanego certyfikatu i klikamy Zakończ (Rys. 4). Pojawi się komunikat **"Certyfikat został poprawnie zainstalowany"**.

Import certyfikatu Ten asystent pozwa	ala ci zarejestrować certyfikat X.509 w systemie	4
operacyjnym.		
🗹 Zarejestruj certyfikat	w systemie operacyjnym	
Przyjazna nazv	va Anna	_
Magazyn certyfikató	iw: Osobisty	-



Po instalacji należy się upewnić, czy certyfikat jest poprawnie zainstalowany w systemie. W tym celu należy w oprogramowaniu CryptoCard Suite, wybrać zakładkę Narzędzia, sekcji Menadżer certyfikatów wcisnąć Uruchom. Zakładka "Osobisty" zawiera listę certyfikatów, na której powinien znajdować się właściwy opis (Rys. 5)

CryptoCard Suit	e		X Cer	tyfikat y				? X
Certyfikat o Ogólne	do logowania Karty elektroniczne	Konfiguracja Narzędzia	l za	imierzony gel: Osobisty Inne oso	<wszyscy>oby Pośrednie urzędy ce</wszyscy>	rtyfikacji Zaufane gl	ówne urzędy certyfika	
Pozwa opera funkcj	ala skontrolować czy wszystkie cyjnego i oprogramowania Cryp jonują poprawnie.	e składniki systemu otoCard Suite Uruchom		Wystawiony dla Maciej	Wystawiony pr Kwalifikowany C	zez Data wyg, DZK 2008-01-0	 Przyjazna nazwa test 	
Menadžer certyfi Służy operat	katów do zerządzania cestyfikatami w cyjnym.	v systemie						
Dodatkowe natz Pozwa zainst elektro	ędzia alają na stworzenie wniosku o alowanie otrzymanego certyfik onicznej i w systemie operacyjn	certyfikat oraz atu na karcie işm. Uruchom		Importuj [] Zamierzone cele ce <wszyscy></wszyscy>	isportuj <u>U</u> suń rtyfikatu		Zaawansov 	vane
	OK	Anuluj Pomoc					Za	mknij

Rys 5.

2. Instalacja obsługi technologii Java™ w przeglądarce internetowej

W pierwszym kroku należy upewnić się czy w systemie zainstalowane są komponenty umożliwiające obsługę aplikacji wykorzystujących środowisko Java[™]. W przypadku przeglądarek IE9 i wyższych można sprawdzić poprawność konfiguracji poprzez: Narzędzia > Opcje internetowe > Programy >

Zarządzaj dodatkami (Rys. 6)

	Opcje internetowe		8 23				
	Ogólne Zabe Połączenia	zpieczenia Prywatno Programy	ść Zawartość Zaawansowane				
	Domyślna przeglądark Program Int przeglądark	a sieci Web ernet Explorer jest domyślną ą sieci Web.	Ustaw jako domyślny				
	Powiedz przegląd	mi, jeśli Internet Explorer nie larką sieci Web.	jest domyślną				
	Zarządzanie dodatkam Włącz lub w zainstalowa	i vłącz dodatki przeglądarki ne w tym systemie.	Zarządzaj dodatkami				
Rys. 6	Edytowanie HTML Wybierz pro do edytowa Edytor HTML	Zarządzanie dodatkami Wyświetł dodatki do pr	ogramu Internet Explorer i z	arządzaj nimi			X
	Programy internetowe Wybierz pro używane dła	Rodzaje dodatków	Nazwa Groove GFS Browser H	Wydawca Âleper Microsoft Corporation	Stan Wyłączone	Czas ładow	Czas na 🔦
	internetowy e-mail.	Dostawcy wyszukiwania	Office Document Cacl Groove Folder Synchro Novell, Inc.	ne Handler Microsoft Corporation Dization Microsoft Corporation	Włączone Wyłączone	0,02 s	0,00 s
		Ochrona przed śledzeniem	IESSOObj Class Oracle America, Inc. — Java(tm) Plug-In SSV H	Novell, Inc. Helper Oracle America, Inc.	Włączone	0,11 s 0,03 s	0,00 s
		Pokaž: Załadowane dodatki	Java(tm) Plug-In 2 SSV	Helper Oracle America, Inc.	Włączone	0,03 s	0,07 s
Instrukcja użytkownika systemu ban	kowości interne	Wybierz dodatek, które etowej dla tirm	go stan chcesz zmodyfikov BOSBank24 iBO	vać lub o którym chcesz wyśv ISS	vietlić szczego Strc	ółowe inforr DNA 5	macje.

UWAGA !!!

Środowisko Java™ (JRE) musi pochodzić z firmy Sun Microsystems.

Odpowiednią aplikację można pobrać ze strony producenta: <u>http://java.sun.com</u>

Do poprawnej pracy wymagane jest środowisko uruchomieniowe J2SE Runtime Environment (JRE) w wersji co najmniej 1.7.

Po instalacji należy upewnić się, czy obsługa Java jest uruchomiona w przeglądarce (Rys. 6).

3. Instalacja aplikacji do autoryzacji SafeDevice[™] jX

Wykorzystanie bezpiecznego podpisu kwalifikowanego na stronach internetowych wymaga instalacji aplikacji SafeDevice™ jX.

Przy logowaniu się do serwisu BOŚBank24 iBOSS za pomocą podpisu kwalifikowanego następuje automatyczne pobranie i zapisanie się do pliku SafeDeviceDLL.dll na dysku lokalnym Klienta do katalogu aktualnie zalogowanego Użytkownika. Applet zabezpieczony jest certyfikatem, więc podczas pierwszego uruchomienia Użytkownik po zapoznaniu się z certyfikatem zabezpieczającym, musi zezwolić przeglądarce internetowej na uruchomienie apletu. Należy wówczas nacisnąć przycisk Yes lub zaznaczyć "Always trust content from this publisher" i nacisnąć przycisk Yes.

Instalacja trwa kilka sekund i za wyjątkiem ww. okna certyifkatu jest niezauważalna dla Użytkownika.

Wymagania systemowe:

System operacyjny:

• NT SP6a/2000/XP/Vista/Windows7/Windows8

Przeglądarka:

- IE9 I wyższe,
- Mozilla 1.5 i wyższe
- Chrome 35 i wyższe,
- Opera 9.0 l wyższe.

Java Runtime Environment 1.7 lub nowsze.

4. Logowanie

W celu skorzystania z usługi BOŚBank24 iBOSS, należy w przeglądarce internetowej wpisać adres: <u>https://bosbank24.pl/iboss</u>

Aby zalogować się przy pomocy podpisu niekwalifikowanego, należy wybrać z listy "Podpis kwalifikowany". W kolejnym kroku zostanie wyświetlona strona z listą certyfikatów. Należy wybrać z listy certyfikatów właściwy, ale aby certyfikaty się pojawiły na liście musi zostać uruchomiony

program obsługi procesu automatyzacji przez strony internetowe (SafeDevice[™] jX- opis instalacji w punkcie 3). Uruchomienie przebiega automatycznie.





Podczas pierwszego otwarcia strony zostanie wyświetlony komunikat z prośba o zezwolenie na uruchomienie aplikacji. Aby komunikat nie pojawiał się powtórnie, należy oznaczyć checkbox przy komunikacie: **"Do not show this again for apps from the publisher and lacation above"** (Rys. 8)

	Name:	com.asseco.def3000.cardapplet.CardApplet
	Publisher:	ASSECO POLAND SA
-	Location:	https://bosbank24.pl//card-applet-distr-32bit.jar
This applica risk. Run th	ition will run with unrestri his application only if you	icted access which may put your computer and personal information at trust the publisher.
This applicants for the second s	ition will run with unrestri is application only if you show this again for apps	icted access which may put your computer and personal information at trust the publisher. from the publisher and location above

Rys. 8

Następnie należy potwierdzić chęć kontynuowania sesji (Rys. 9) potwierdzając zaufanie połączenia.

Do y The co	ou want to Continue? onnection to this website is untrusted.
	Website: https://javadl-esd-secure.oracle.com:9090
Note:	The certificate is not valid and cannot be used to verify the identity of this website. More Information
	Continue Cancel



Następnie po wybraniu właściwego certyfikatu, należy kliknąć przycisk Zaloguj.

Po chwili pojawi się okno zawierające informacje wykorzystywane do podpisu (Rys. 10).





Ostatnim etapem jest właściwe użycie podpisu poprzez wpisane kodu PIN oraz wciśnięcie przycisku OK. (Rys. 11)

to Caro	ditional
Lul	
	mercu
xplorer\IEXPLORE	.EXE
CM Microsystems I	nc. SCR33x USB Smar
SetEID	
e18a862ab4b9b39	cdf1c58f6dae09c0
4019144	•
-4	-
	xplorer\IEXPLORE CM Microsystems I ietEID e18a862ab4b9b39 4019144

Rys. 11