Kdpw\_ Krajowy Depozyt Papierów Wartościowych

Instrukcja instalacji, konfiguracji oraz użytkowania oprogramowania Cisco VPN Client, wykorzystywanego w ramach systemu ESDK.

1.	Wstęp	3
2.	Instrukcja instalacji oprogramowania Cisco VPN Client	4
3.	Instrukcja importu certyfikatów	9
4.	Instrukcja konfiguracji oprogramowania Cisco VPN Client	13
5.	Instrukcja użytkowania oprogramowania Cisco VPN Client	17

\_\_\_\_\_

## 1. Wstęp

Niniejsza instrukcja przedstawia sposób instalacji, konfiguracji oraz użytkowania programu Cisco VPN Client, dla potrzeb komunikacji z Krajowym Depozytem Papierów Wartościowych S.A. w ramach systemu ESDK.

Oprogramowanie Cisco VPN Client dostarczane jest użytkownikom ESDK przez KDPW na podstawie warunków licencyjnych Cisco, dopuszczających możliwość przekazywania oprogramowania VPN Client podmiotom trzecim, pod warunkiem wykorzystywania go tylko i wyłącznie do zestawiania połączeń pomiędzy systemem klienta a koncentratorem VPN Cisco, użytkowanym w KDPW.

## 2. Instrukcja instalacji oprogramowania Cisco VPN Client.

Oprogramowanie Cisco VPN Client dostarczane jest użytkownikowi na płycie CD. Dopuszczalne jest zainstalowane tego oprogramowania na dowolnej ilości stacji klienckich ESDK, z których zestawiane jest połączenie VPN z węzłem VPN w sieci KDPW S.A.

Przed rozpoczęciem instalacji oprogramowania VPN Client, należy zalogować się do stacji roboczej profilem z uprawnieniami administratora lokalnego stacji. Zalecane jest także zakończenie działania wszystkich innych aplikacji.

Dla prawidłowego działania oprogramowania Cisco VPN Client, niezbędne jest zapewnienie komunikacji pomiędzy stacją kliencką a węzłem VPN pracującym w KDPW S.A. . W tym celu należy zmodyfikować konfigurację urządzeń sieciowych klienta (routery, firewall'e itp.) w taki sposób, aby zezwolić na ruch sieciowy pomiędzy stacją kliencką a węzłem VPN w KDPW S.A. dostępnym w sieci internet (Informacje na temat adresu IP oraz portu węzła VPN, dostępne są w załączniku nr 1 do instrukcji instalacji i konfiguracji oprogramowania Cisco VPN Client).

W przypadku gdy stacja kliencka wyposażona jest w oprogramowanie typu personal firewall, niezbędna może okazać się jego rekonfiguracja lub wyłączenie. Reguły tego oprogramowania powinny zezwalać na komunikację stacji klienckiej z węzłem VPN pracującym w KDPW S.A..

UWAGA:

W przypadku instalacji oprogramowania Cisco VPN Client na stacji z systemem Windows XP SP2 z uaktywnioną zaporą sieciową, należy w konfiguracji zapory wprowadzić następujące wyjątki dla ruchu przychodzącego:

udp 500 tcp 55005 tcp 62514 udp 62514 tcp 62515 udp 62515 2.1. W celu rozpoczęcia procesu instalacji należy uruchomić program *"vpnclient\_setup.exe"* z katalogu instalacyjnego na CD-ROM:

P:\vpn client\vpn 4.8.02.00	)10-k9		
Plik Edycja Widok Ulubione Narzędzia	a Pomoc		
Ġ Wstecz 🔹 🕥 🕤 🏂 🔎 Wyszuk	aj 🝺 Foldery	B 🕑 🗙 🍤	· · · ·
Adres 🛅 P:\vpn client\vpn 4.8.02.0010-k9			💌 🛃 Przejdź
<ul> <li>DelayInst.exe</li> <li>installservice.exe</li> <li>instmsi.exe</li> <li>instmsiw.exe</li> <li>sig.dat</li> <li>vpnclient_fc.mst</li> <li>vpnclient_jp.mst</li> <li>vpnclient_setup.exe</li> <li>vpnclient_setup.ini</li> <li>vpnclient_setup.msi</li> <li>vpnclient_setup.pdf</li> <li>vpnclient_setup.sms</li> </ul>			
Obiektów: 12	11,6 MB	🧐 Lokalny intranet	.::

2.2. W oknie



należy wybrać język, w którym będzie przeprowadzony proces instalacji oprogramowania, a następnie nacisnąć przycisk "*OK*."

#### 2.3. W oknie



należy nacisnąć przycisk "Next »"

#### 2.4. W oknie

🛱 Cisco Systems VPN	Client 4.8.02.0010 Setup	
License Agreement You must agree with the lin	cense agreement below to proceed.	Ø
Client Software License Agr THE SOFTWARE TO WHICH Y SYSTEMS. THE USE OF THIS OF THE GREEMENT SET FOF INDICATE THAT YOU AGREE CONDITIONS OF THAT AGRE CONDITIONS CAREFULLY BE TERMS AND CONDITIONS OF CASE YOU WILL BE DENIED Ownership of the Software 1. The software contained in are requesting access, is ow	eement of Cisco Systems YOU ARE REQUESTING ACCESS IS THE PROPERTY OF C SOFTWARE IS GOVERNED BY THE TERMS AND CONDIT RTH BELOW. BY CLICKING "YES" ON THIS SCREEN, YOU TO BE BOUND BY THE TERMS AND EMENT. THEREFORE, PLEASE READ THE TERMS AND FORE CLICKING ON "YES". IF YOU DO NOT AGREE TO T T THE AGREEMENT, CLICK "NO" ON THIS SCREEN, IN WI ACCESS TO THE SOFTWARE.	TISCO TIONS THE HICH h you e
_	<ul> <li>I accept the license agreement</li> <li>I do not accept the license agreement</li> </ul>	
	Reset  Kext Next	Cancel

należy zaakceptować warunki licencji zaznaczając opcję *"I accept the license agreement*", a następnie nacisnąć przycisk *"Next >*"

### 2.5. W oknie

🕏 Cisco Systems VPN Client 4.8.02.0010 Setup
Destination Folder       Select a folder where the application will be installed.
The Wise Installation Wizard will install the files for Cisco Systems VPN Client 4.8.02.0010 in the following folder. To install into a different folder, click the Browse button, and select another folder. You can choose not to install Cisco Systems VPN Client 4.8.02.0010 by clicking Cancel to exit the Wise Installation Wizard.
C:\Program Files\Cisco Systems\VPN Client\ Browse
< Back Next > Cancel

należy wskazać folder, w którym zostanie zainstalowane oprogramowanie, a następnie nacisnąć przycisk "*Next >*"

#### 2.6. W oknie

🕏 Cisco Systems VPN	Client 4.8.02	2.0010 Setup		
Ready to Install the Appl Click Next to begin instal	ication lation.			Ø
Click the Back button to the wizard.	o reenter the installatio	on information or clic	k Cancel to exit	
		< Back	Next >	Cancel

należy nacisnąć przycisk "Next >"

Rozpoczęty właśnie proces kopiowania plików, może potrwać kilka minut.



należy nacisnąć przycisk "Finish", kończący proces instalacji.

#### 2.8. W oknie



należy nacisnąć przycisk "YES", akceptując tym samym ponowne uruchomienie systemu operacyjnego.

2.9. Po wykonaniu powyższych czynności proces instalacji oprogramowania Cisco VPN Client został zakończony.

# 3. Instrukcja importu certyfikatów.

- 3.1. W celu dokonania importu certyfikatów, należy uruchomić program Cisco VPN Client. Start > Programy > Cisco System VPN Client > VPN Client
- 3.2. Import certyfikatu Centrum Autoryzacji KDPW.

Korzystając z uruchomionego graficznego interfejsu użytkownika, należy zaimportować certyfikat centrum autoryzacji, poprzez wybranie opcji "*Import...*" z menu "*Certificates*".

Status: Disconne	ected   VPN Client - Vers	ion 4.8.02.0010	
Connection Entries Status	Certificates Log Options Help		
🦾 🖶	View		ahaha
Connect New I	Import		CISCO
Connection Entries Certificate	Export		
Connection Entry	Enroll	Transport	
	Verify		
	Delete		
	Change Certificate Password		
	Retrieve Approved Certificate		
	Show CA/RA Certificates		
<u> </u>			
Not connected.			

W oknie importu certyfikatu należy zaznaczyć opcję *"Import from File"*, a następnie korzystając z przycisku *"Browse"* odszukać plik zawierający certyfikat. W polu *"Import Password:"* należy wprowadzić hasło certyfikatu, a na zakończenie nacisnąć przycisk *"Import"*.

Ø VPN Client   Import Certificate	X						
Import from File							
Import Path: P:\KDPW CA VPN root.cer	Browse						
Import Password:							
C Import from Microsoft Certificate store Import Certificate: Entering a new password may be required. It is recommended to password protect							
New Password:							
Confirm Password:							
Import	Cancel						

Poprawny import certyfikatu zakończony jest pojawieniem się następującego okna informacyjnego:

VPN Client
Certificate successfully imported.
ОК

3.3. Import certyfikatu użytkownika.

Korzystając z uruchomionego graficznego interfejsu użytkownika, należy zaimportować certyfikat użytkownika, poprzez wybranie opcji *"Import…"* z menu *"Certificates"*.

Krajowy Depozyt Papierów Wartościowych S.A.

status: Disconne	cted   VPN Client - Versi	ion 4.8.02.0010	
Connection Entries Status	Certificates Log Options Help		
🦾 💼 🚦	View		ahaha
Connect New Ir	Import		CISCO
Connection Entries Certificate	Export		
Connection Entry	Enroll	Transport	
	Verify		
	Delete		
	Change Certificate Password		
	Retrieve Approved Certificate		
	✓ Show CA/RA Certificates		
		·	
<u> </u>			
Not connected.			

W oknie importu certyfikatu należy zaznaczyć opcję *"Import from File*", a następnie korzystając z przycisku *"Browse*" odszukać plik zawierający certyfikat. W polu *"Import Password:*" należy wprowadzić hasło certyfikatu, a na zakończenie nacisnąć przycisk *"Import*".

VPN Client   Import Certificate							
<ul> <li>Import from File</li> </ul>							
Import Path: P:\999101VPN.p12	Browse						
Import Password:							
Import from Microsoft Certificate store     Import Certificate:     Entering a new password may be required. It is recommended to password protect     identificates							
New Password:							
Confirm Password:							
Import	Cancel						

Poprawny import certyfikatu zakończony jest pojawieniem się następującego okna informacyjnego:



3.4. Weryfikacja poprawności importu certyfikatów.

Po zaimportowaniu certyfikatu Centrum Autoryzacji KDPW oraz certyfikatu użytkownika, należy zweryfikować poprawność wykonania w/w czynności (ważność certyfikatu).

Korzystając z graficznego interfejsu użytkownika, należy uaktywnić zakładkę *"Certificates"*, następnie wybrać uprzednio zaimportowany certyfikat użytkownika poprzez kliknięcie na nim prawym przyciskiem myszy. Z menu kontekstowego należy wybrać opcję *"Verify"*.

Status: Dis	connecte	d   VPN C	lien	t - \	/ersion	4.8.02.00	010	
Connection Entries	: Status Certi	ficates Log C	ptions	Help				
View Impo	ort Export	Enroll	<b>Verify</b>	,	XX Delete			cisco
Number	Certificate	-09		Store		Keu Size	Validitu	
1	999101VPN			Piece	_	1024	until sty 29, 2009 11:50:	06
		View						
		Export						
		Verify						
		Delete				1		
	-	Change Ce	rtificat	e Pass	word	1		
		Retrieve Ap	oprove	d Cert	ificate			
<u> </u>			_	_				
Not connected.								

Ważność certyfikatu użytkownika, potwierdzona jest pojawieniem się następującego okna informacyjnego:



# 4. Instrukcja konfiguracji oprogramowania Cisco VPN Client

- 4.1. W celu dokonania konfiguracji należy uruchomić program Cisco VPN Client. Start > Programy > Cisco System VPN Client > VPN Client
- 4.2. Korzystając z uruchomionego graficznego interfejsu użytkownika, należy stworzyć nowe połączenie wybrać opcję "*New*…" z menu "*Connection Entries*"

Status: Disconne	ected   VPN	l Client - Versio	n 4.8.02.0010	
Connection Entries Status	Certificates Log	Options Help		
Connect to	Ctrl+O			مليمان
Disconnect	Ctrl+D	Delete		CISCO
Create Shortcut				
Modify		Host	Transport	
Delete				
Duplicate				
Erase Saved User Pass	word			
Set as Default Connect	ion Entry			
New				
Import				
. Exit VPN Client	Ctrl+Q			
Not connected.				

4.3. W oknie nowego połączenia należy wprowadzić kolejno:

•	W polu: <i>"Connection Entry:"</i>	ESDK (Dowolna nazwa identyfikująca połączenie).
•	W polu: <i>"Description:"</i>	Połączenie z systemem ESDK w KDPW S.A. (Dowolny opis określający połączenie).
•	W polu: <i>"Host:"</i>	Adres IP węzła VPN w KDPW S.A. (Informacje na temat adresu IP węzła VPN, dostępne są w załączniku nr.1 do instrukcji instalacji i konfiguracji oprogramowania Cisco VPN Client).

Krajowy Depozyt Papierów Wartościowych S.A.

VPN Client   Create New VPN Co	onnec 🔀				
Connection Entry: ESDK					
Description: Połączenie z systemem ESDK	CISCO				
Host: xxx.xxx.xxx					
Authentication Transport Backup Servers Dial-Up					
<u>Group Authentication</u> <u>Mutual Group</u>	up Authentication				
Name:					
Password:					
Confirm Password:					
C Certificate Authentication          Name:       Image: Image					
	Cancel				
Erase User Hassword	Lancel				

- 4.4. W oknie nowego połączenia, w zakładce "Authentication" należy:
  - Zaznaczyć opcję "Certificate Authentication".
  - W polu "*Name:*" wybrać uprzednio zaimportowany certyfikat.

VPN Client   Create New VPN Co	onnec 🔀				
Connection Entry: ESDK					
Description: Połączenie z systemem ESDK	CISCO				
Host xxx.xxx.xxx					
Authentication Transport Backup Servers Dial-Up					
C <u>G</u> roup Authentication C <u>M</u> utual Gro	up Authentication				
Name:					
Password:					
C <u>o</u> nfirm Password:					
<ul> <li>Certificate Authentication</li> <li><u>N</u>ame: 1 - 999101VPN (Cisco)</li> <li>Send CA Certificate Chain</li> </ul>					
Erase User Password	Cancel				

- 4.5. W oknie nowego połączenia, w zakładce "*Transport*" należy:
  - Zaznaczyć opcję "Enable Transparent Tunneling"
  - Wybrać opcję "IPSec over TCP"
  - W polu *"TCP Port:"* wprowadzić numer portu TCP. Informacje na temat portu TCP węzła VPN, dostępne są w załączniku nr.1 do instrukcji instalacji i konfiguracji oprogramowania Cisco VPN Client.

VPN Client   Create New VPN Co	onnec 🔀
Connection Entry: ESDK	
Description: Połączenie z systemem ESDK	cisco
Host XXX XXX XXX	
Authentication Transport Backup Servers Dial-Up	
<ul> <li>✓ Enable Transparent Tunneling</li> <li>○ IPSec over UDP (NAT / PAT )</li> <li>○ IPSec over ICP TCP Port: yyyyy</li> </ul>	
Allow Local LAN Access Peer response timeout (seconds): 90	
Erase <u>U</u> ser Password <u>S</u> ave	Cancel

4.6. Zakładkę "*Backup Servers*" w oknie nowego połączenia należy pozostawić bez zmian.

VPN Client   Create New VPN Co	onnec 🔀
Connection Entry: ESDK Description: Połączenie z systemem ESDK Host: xxx.xxx.xxx	cisco
Authentication Transport Backup Servers Dial-Up	
Enable Backup Servers	
	Add
	<u>R</u> emove
	+
	+
Erase <u>U</u> ser Password <u>S</u> ave	Cancel

4.7. Zakładkę "*Dial-Up*" w oknie nowego połączenia należy pozostawić bez zmian.

VPN Client   Create New VPN Co	onnec 🔀
Connection Entry: ESDK	սիսիս
Host: XXX XXX XXX XXX	cisco
Authentication Transport Backup Servers Dial-Up	
Connect to Internet via dial-up  Microsoft Dial-Up Networking Phonebook Entry:  Third party dial-up application Application:	<b>▼</b> <u>B</u> rowse
Erase <u>U</u> ser Password <u>S</u> ave	Cancel

4.8. Po wykonaniu powyższych czynności należy zapisać konfigurację naciskając przycisk *"Save"*.

### 5. Instrukcja użytkowania oprogramowania Cisco VPN Client.

5.1. Nawiązywanie połączenia VPN z KDPW S.A.

W celu rozpoczęcia działania połączenia VPN z KDPW S.A. należy:

- uruchomić oprogramowanie Cisco VPN Client.
   Start > Programy > Cisco System VPN Client > VPN Client
- W oknie graficznego interfejsu użytkownika oprogramowania "Cisco VPN Client" uruchomić uprzednio skonfigurowane połączenie z KDPW S.A. poprzez dwukrotne przyciśnięcie lewego przycisku myszy.

Status: Disconnected	VPN Clie	nt - Version 4.8.02	.0010	
Connection Entries Status Certifica	tes Log Optior	ns Help		
Connect New Import	Modify Del	<b>S</b> ete		uluilu cisco
Connection Entries Certificates Log				
Connection Entry		Host	Transport	
ESDK			IPSec/TCP	
Not connected				
Not connected.				

• W oknie dialogowym

VPN Client   User Authentication f X
Enter Username and Password.
uluulu Username:
CISCO Password:
OK Cancel

należy wprowadzić nazwę użytkownika oraz hasło użytkownika a następnie nacisnąć przycisk "*OK*".

 Poprawne zestawienie tunelu VPN, zasygnalizowane jest pojawieniem się odpowiedniej ikony w obszarze powiadomień (obok zegara systemowego). 5.2. Zakończenie połączenia VPN z KDPW S.A.

W celu zakończenia działania połączenia VPN z KDPW S.A. należy:

- uruchomić interfejs graficzny oprogramowania Cisco VPN Client.
   Start > Programy > Cisco System VPN Client > VPN Client
- następnie kliknąć prawym przyciskiem myszy na aktywnym połączeniu i z menu kontekstowego wybrać opcję "*Disconnect*".

Status: Connected   VPN Client	nt - Version 4.8.02.00	)10	
Connection Entries Status Certificates Log Op	tions Help		
Disconnect New Import Modify	Delete		ili.ili. cisco
Connection Entries Certificates Log		1	
Connection Entry	Host	Transport	
SDK ESDK		Connect	
		Disconnect	
		Duplicate	
	_	Delete	
		Create Shortcut	
		Modify	
		Erase Saved User Password	
		Set as Default Connection En	try
Connected to "ESDK".	Ca	nnected Time: 0 day(s), 00:00.34	•

 Zakończenie działania tunelu VPN, zasygnalizowane jest pojawieniem się odpowiedniej ikony w obszarze powiadomień (obok zegara systemowego).