

CEPiK 2 – dostęp VPN

v.1.7

Metryka dokumentu

Tytuł	CEPiK 2 – dostęp VPN		
Autor	Centralny Ośrodek Informatyki		
Zatwierdzający			
Historia zmian	Wersja	Data	Opis zmian
	1.0	30.10.2015 r.	Utworzenie dokumentu
	1.1	23.11.2015 r.	Aktualizacja
	1.2	01.03.2016 r.	Windows 10
	1.3	23.03.2016 r.	Aktualizacja / zalecenia
	1.4	24.03.2016 r.	Aktualizacja
	1.5	24.03.2016 r.	Aktualizacja
	1.6	16.05.2016	Aktualizacja – klient AnyConnect
	1.7	18.10.2016	Aktualizacja L2L

Spis treści

Metryka dokumentu.....	2
1. Wstęp	4
2. Zalecenia.....	4
3. Zestawienie połączenia VPN.....	4
3.1. Połączenie typu Remote Access – Cisco VPN Client.....	4
4. Instalacja oprogramowania „Cisco VPN Client” w systemie MS Windows 10	9
5. Instalacja oprogramowania „Cisco AnyConnect Secure Mobility”	12

1. Wstęp

W dokumencie opisano realizację połączeń VPN do systemu CEPiK 2.

2. Zalecenia

Ze względu na łatwość implementacji oraz wsparcie producenta zaleca się używanie klienta VPN instalowanego na stacji klienckiej. Aktualnie istnieje możliwość realizacji połączenia VPN z wykorzystaniem klienta „Cisco VPN Client” oraz klienta „Cisco AnyConnect”. Usługa VPN jest realizowana w trybie Remote Access, client – server.

CEPiK 2 będzie wspierał połączenia typu Remote Access. Zestawiając takie połączenie z CEPiK 2 system CEPiK 2 w ramach połączenia VPN Remote Access wymusi określoną politykę bezpieczeństwa sieci – w trakcie zestawionego połączenia VPN nie będzie dostępu do innych niż CEPiK 2 treści w sieci publicznej Internet.

Połączenie LAN to LAN będzie realizowane wyłącznie dla dużych podmiotów w trybie oddzielnych ustaleń. Podmiot zamierzający wykorzystać taki sposób połączenia z CEPiK 2 realizuje to we własnym zakresie. Podmiot musi przede wszystkim zabezpieczyć połączenie VPN przed ingerencją osób nieuprawnionych oraz przed atakami z sieci publicznej Internet, np. poprzez wyłączenie dostępu do treści zawartych w sieci publicznej Internet w trakcie trwania połączenia VPN.

3. Zestawienie połączenia VPN

Do poprawnego zestawienia tunelu VPN wymagane jest posiadanie certyfikatu wydanego przez Centrum Certyfikacji dla CEPiK. Certyfikat jest dostarczony w postaci pliku w formacie PKCS#12 (.p12).

3.1. Połączenie typu Remote Access – Cisco VPN Client

Kanał VPN typu remote access ma na celu umożliwienie połączenia z CEPiK 2 jednej stacji roboczej z wykorzystaniem transmisji poprzez szyfrowany kanał VPN. Jest to połączenie oparte o architekturę klient – serwer i do zestawienia kanału szyfrowanego niezbędne jest oprogramowanie klienckie, które musi zostać zainstalowane na stacji roboczej. Do poprawnego skonfigurowania zdalnego dostępu należy pobrać i zainstalować oprogramowanie Cisco VPN Client.

Oprogramowanie „Cisco VPN Client” domyślnie instaluje się niepoprawnie w systemie Microsoft Windows 10. Instrukcja instalacji dla tego systemu jest opisana w rozdziale 4.

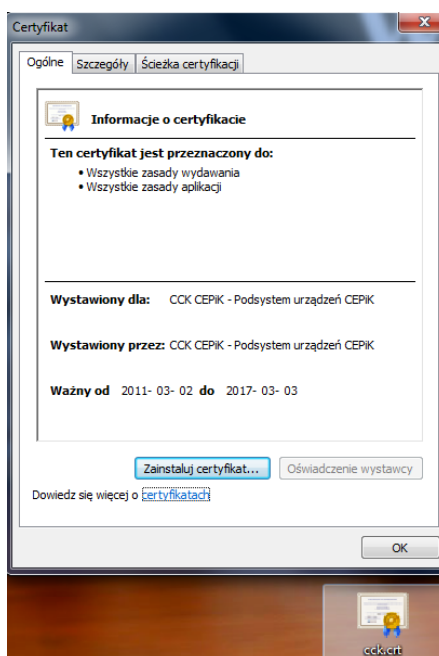
Obsługa zgłoszeń związanych z połączeniami VPN typu Remote Access z wykorzystaniem klientów Cisco VPN Client oraz Cisco AnyConnect będzie realizowana przez Service Desk CEPiK, w zakresie instalacji i konfiguracji oprogramowania.

Na początek

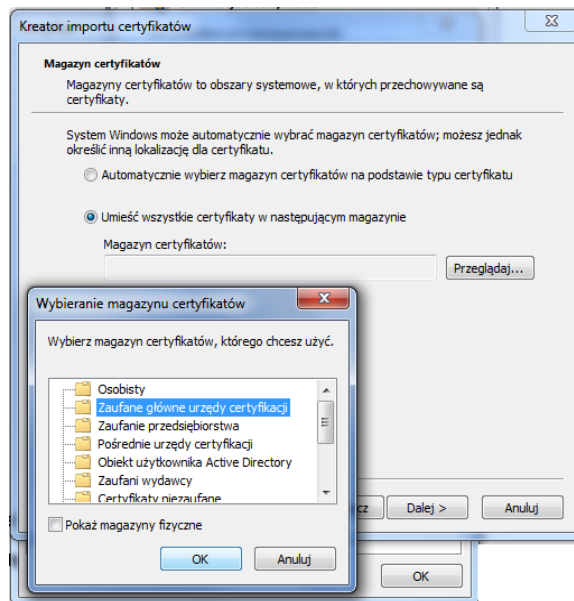
Zainstaluj oprogramowanie Cisco VPN Client. Po poprawnej instalacji Cisco VPN Client w systemie operacyjnym, przystępujemy do instalacji wymaganych certyfikatów.

Krok 1. Instalacja certyfikatu urzędu

W pierwszym kroku instalujemy otrzymany certyfikat urzędu **CA**. W tym celu dwukrotnie klikamy na certyfikat (w poniższym przykładzie jest to **cck.crt**):



Wybieramy „Zainstaluj certyfikat”, następnie klikamy „Dalej”, wybieramy „Umieść wszystkie certyfikaty w następującym miejscu” i klikamy w opcję „Przeglądaj”

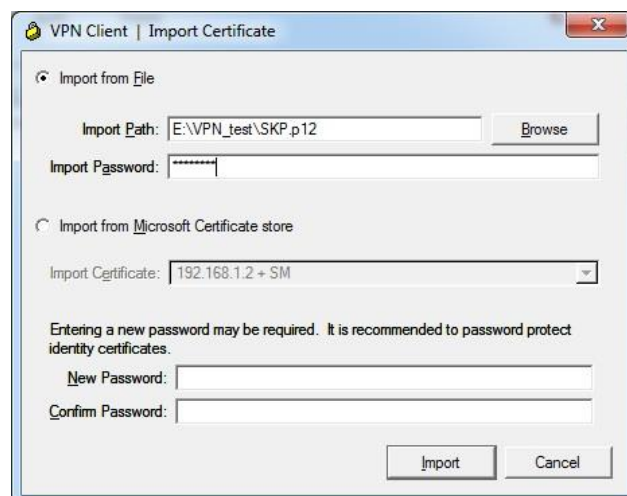


W okienku „**Wybieranie magazynu certyfikatów**” zaznaczamy „**Zaufane główne urzędy certyfikacji**” i klikamy „**OK**”. Następnie klikamy „**Dalej**”, w razie wystąpienia komunikatu z ostrzeżeniem o imporcie nieznanego klucza, wybieramy opcję zezwalającą na import i klucz został zaimportowany.

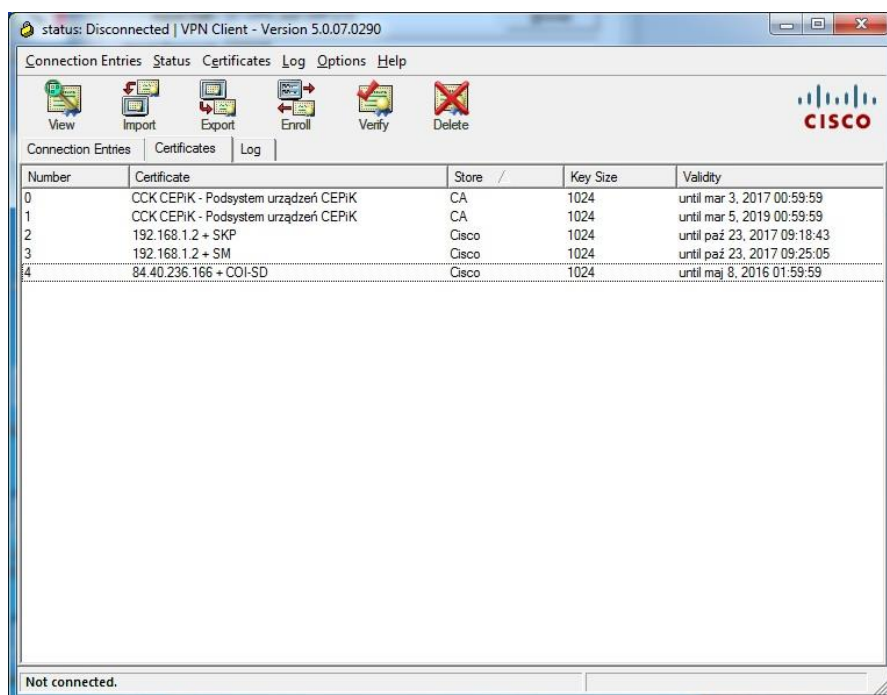
Krok 2. Instalacja certyfikatu użytkownika

W drugim kroku uruchamiamy program **Cisco VPN Client** i definiujemy połączenie VPN.

Instalujemy otrzymany certyfikat z pliku „**p.12**”. Z wybieramy zakładkę **Certificates** i opcję **Import Certificate**. Wskazujemy plik z certyfikatem (**Import Path**) i wpisujemy otrzymane hasło do pliku (**Import Password**), a następnie klikamy przycisk **Import**.



Certyfikat powinien się pojawić na liście (zakładka **Certificates**).

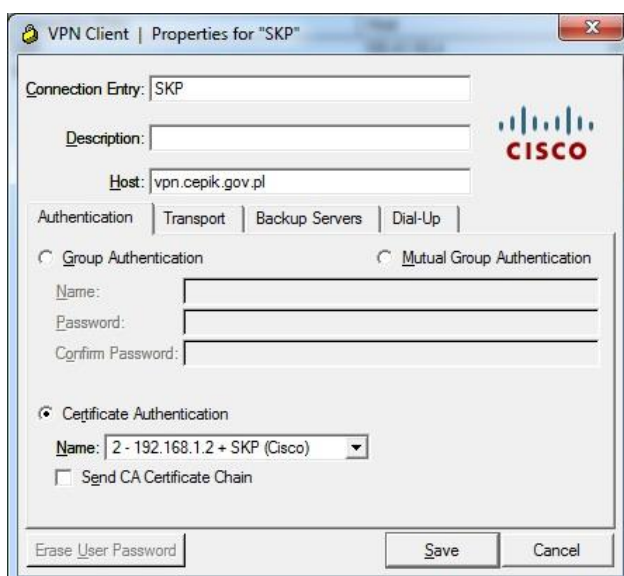


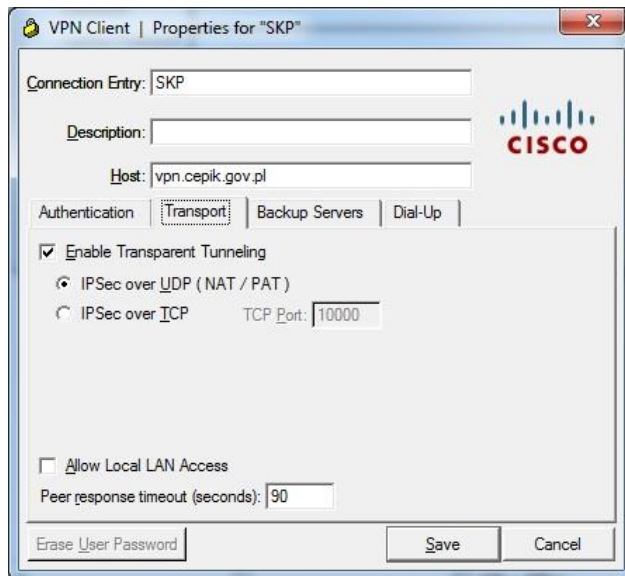
Krok 3. Zdefiniowanie połączenia VPN

W zakładce **Connection Entries** definiujemy nowe połączenie. Wybieramy opcję **New**. Wypełniamy lub wybieramy następujące pola:

Connection Entry

- **Host** – podajemy adres **vpn.cepik.gov.pl**;
- **Authentication** -> **Certificate Authentication** - wskazujemy zainstalowany przez nas certyfikat jako parametr uwierzytelniania;
- **Transport** -> **Enable Transparent Tunneling** – wybieramy opcję **IPSec over UDP**.

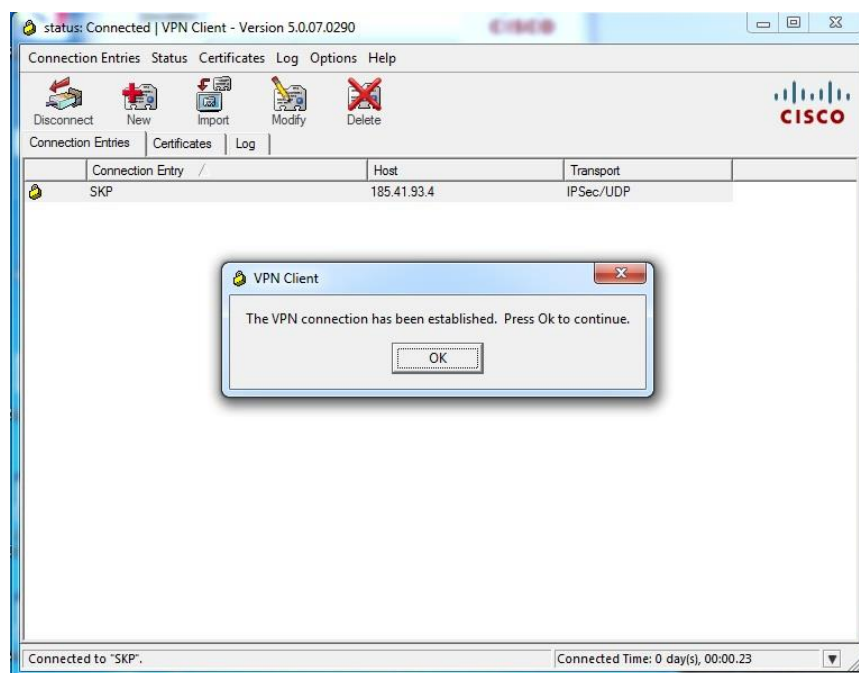




Pozostałe parametry pozostawiamy bez zmian i zapisujemy konfigurację przyciskiem **Save**.

Krok 4. Pierwsze połączenie VPN z CEPIK 2

W celu zestawienia połączenia należy wybrać zdefiniowany uprzednio profil i dwukrotnie kliknąć lub wybrać opcję **Connect** z paska narzędziowego. Poprawne zestawienie połączenia zostanie zasygnalizowane przez aplikację komunikatem i ikoną zamkniętej kłódki przy nazwie profilu.

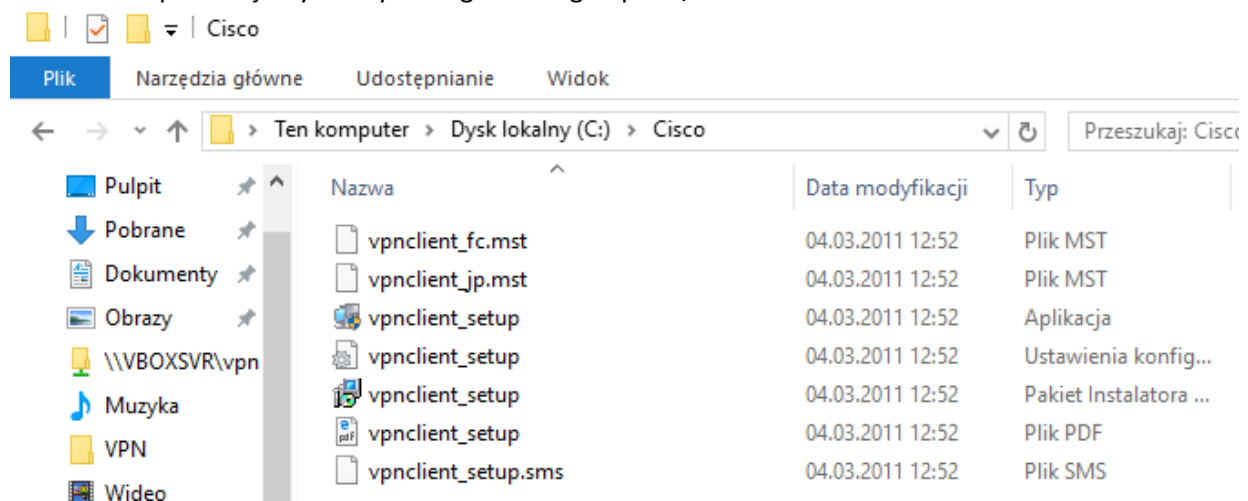


Po zakończeniu pracy rozłączamy połączenie VPN wybierając opcję **Disconnect**.

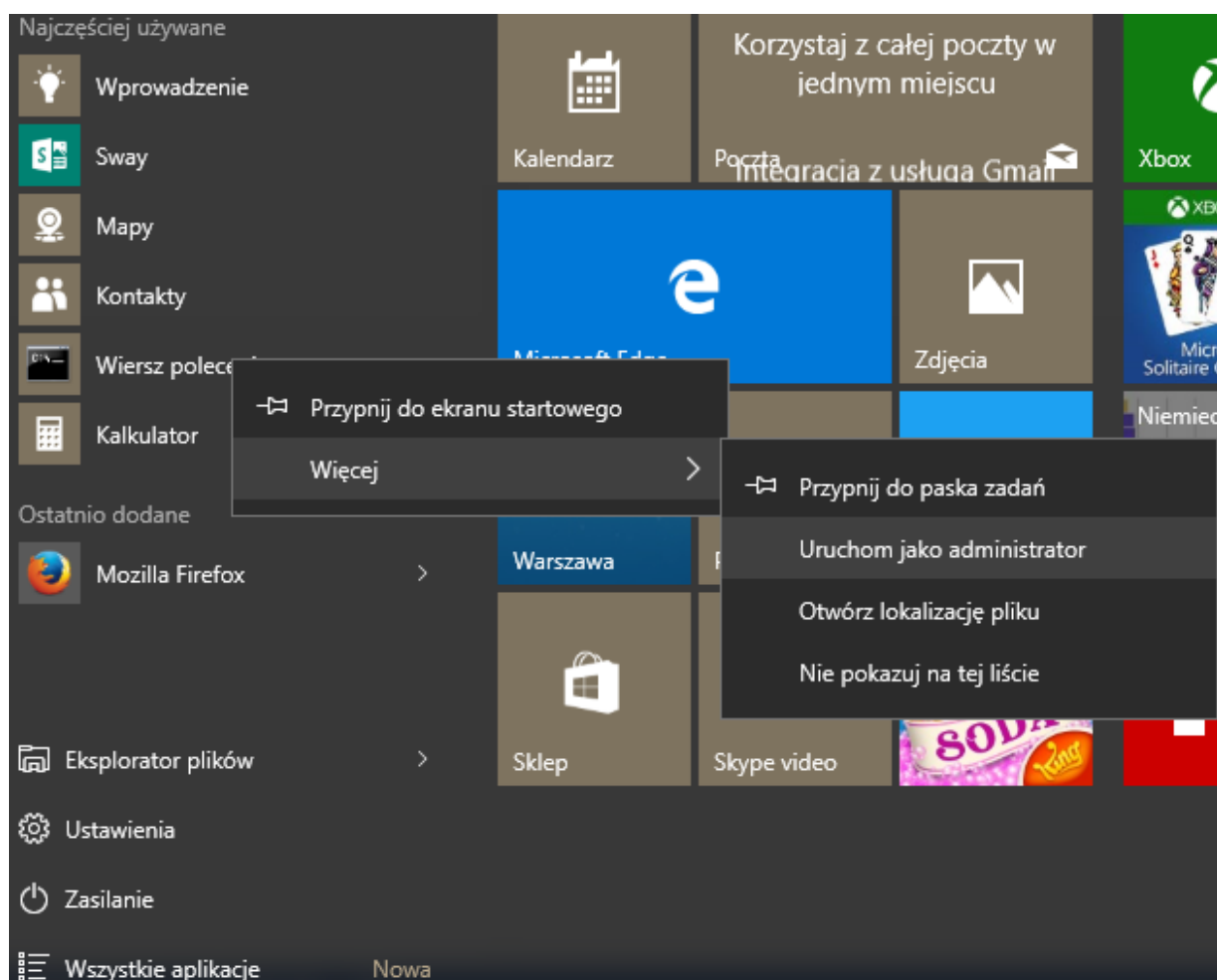
4. Instalacja oprogramowania „Cisco VPN Client” w systemie MS Windows 10

Instrukcja dotyczy instalacji klienta w wersji 5.0.07.0440

- **Instalacja sterownika DNE Update**
Pobieramy i instalujemy [ftp://ftpsupport.citrix.com/dneupdate64.msi](http://ftpsupport.citrix.com/dneupdate64.msi)
- **Instalacja oprogramowania „Cisco VPN Client”**
 - pobieramy oprogramowanie vpnclient-winx64-msi-5.0.07.0440
 - rozpakowujemy do wybranego katalogu np. C:\Cisco



- uruchamiamy „Wiersz poleceń” jako administrator



- instalujemy oprogramowanie poleceniem: „msiexec /i vpnclient_setup.msi”

```
Administrator: Wiersz polecenia
Microsoft Windows [Version 10.0.10586]
(c) 2016 Microsoft Corporation. Wszelkie prawa zastrzeżone.

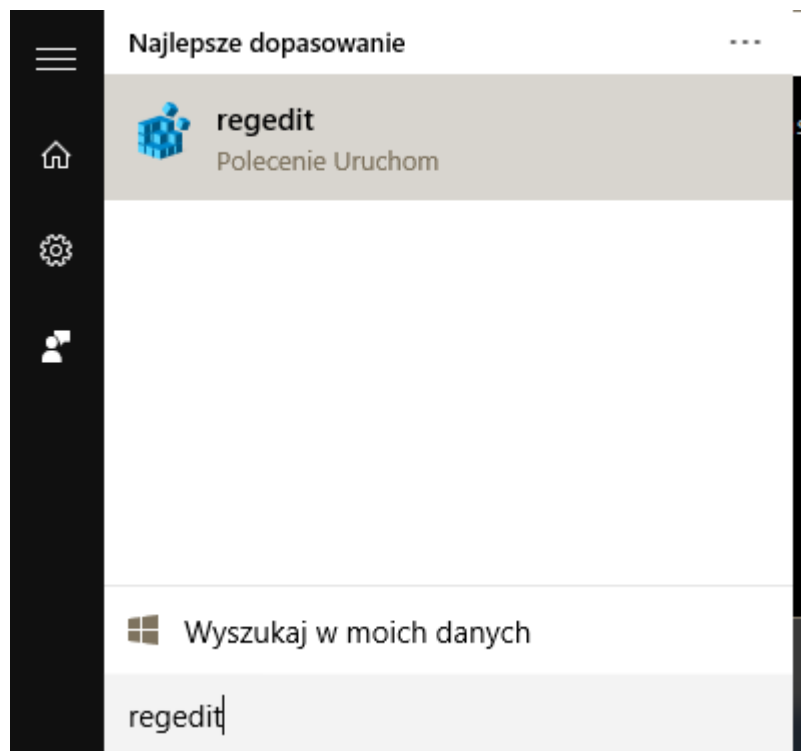
C:\Windows\system32>cd \Cisco

C:\Cisco>msiexec /i vpnclient_setup.msi
```

- **Poprawka rejestru.**

Wymagana jest drobna zmiana w rejestrze systemowym:

- uruchamiamy edytor rejestru

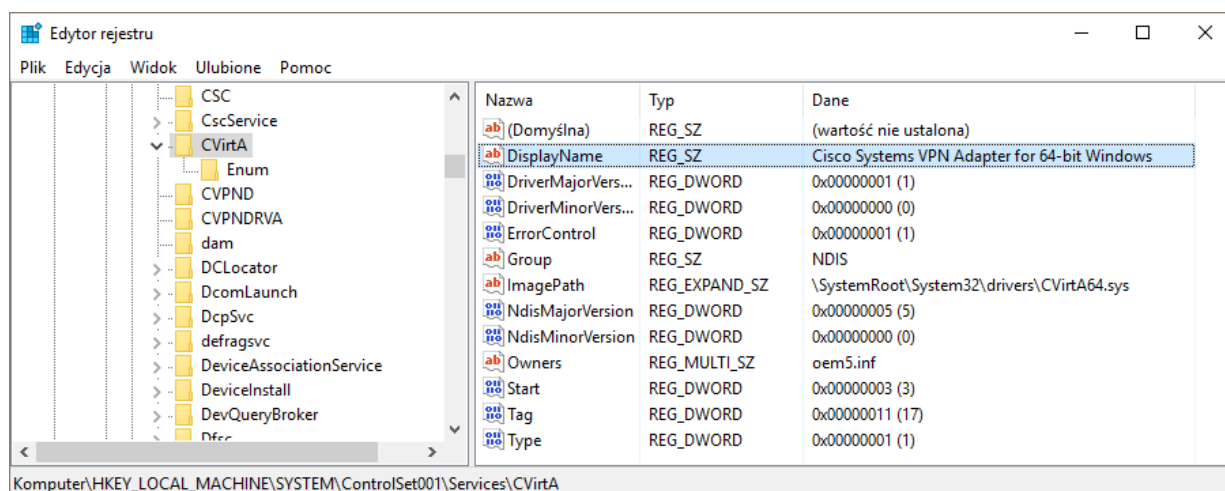


- szukamy klucza

HKLM\SYSTEM\ControlSet001\Services\CVirtA\DisplayName

i modyfikujemy jego wartość usuwając wszystko co jest przed „Cisco Systems ...”

(@oemX.inf,%CVirtA_Desc%;

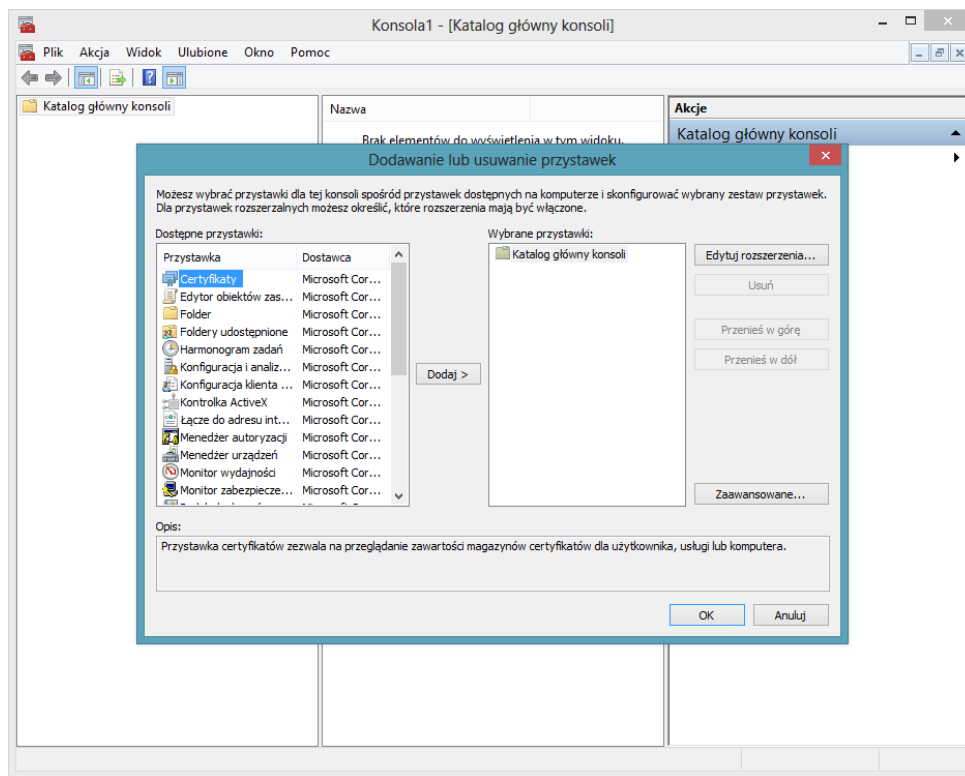


5. Instalacja oprogramowania „Cisco AnyConnect Secure Mobility”

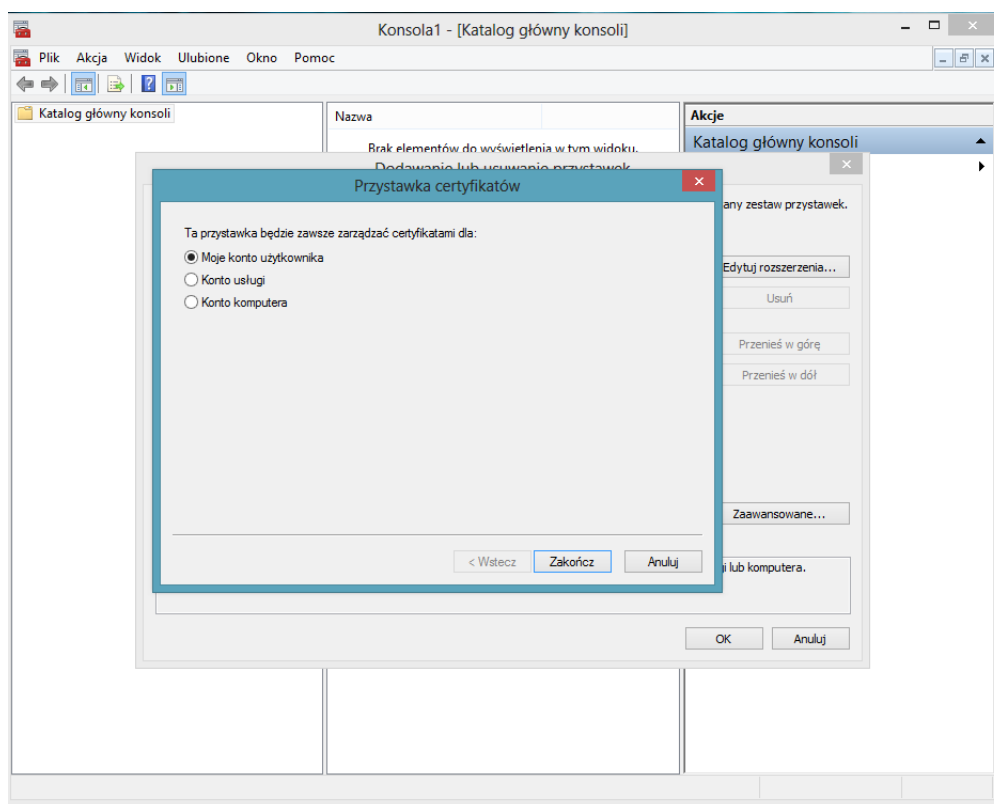
Do poprawnego skonfigurowania zdalnego dostępu należy pobrać i zainstalować oprogramowanie Cisco AnyConnect Secure Mobility Client ver. anyconnect-win-3.1.14018-pre-deploy-k9.msi ze strony <https://www.cepik.gov.pl/cepik20/pliki/anyconnect-win-3.1.14018-pre-deploy-k9.msi> lub skorzystać z innego alternatywnego rozwiązania wspierającego połączenia IKE2 lub SSL.

Przed przystąpieniem do instalacji Cisco AnyConnect Secure Mobility Client w systemie operacyjnym, przystępujemy do instalacji wymaganych certyfikatów w systemie Windows za pomocą konsoli MMC (Microsoft Management Console).

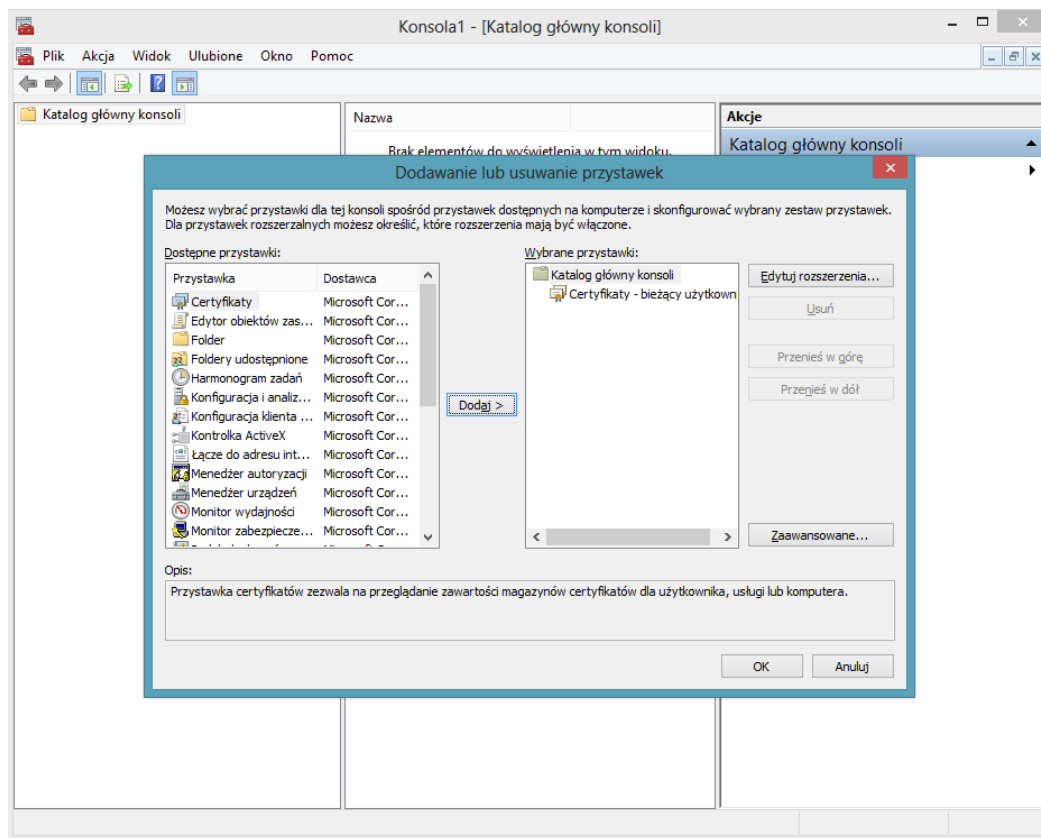
W pierwszym kroku instalujemy otrzymany certyfikat urzędu **CA**. W tym celu otwieramy konsolę MMC. Wybieramy z menu Plik –Dodaj/Usuń przystawkę. Wybieramy z lewej strony przystawkę „Certyfikaty.”



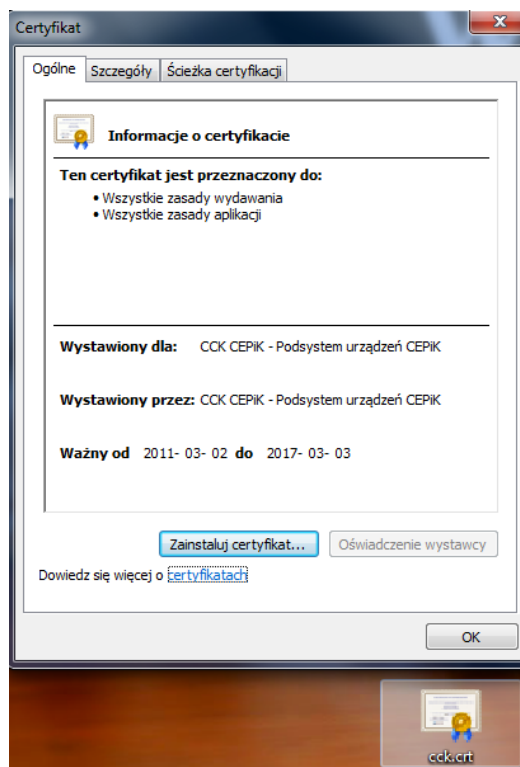
Następnie klikamy dodaj pozostawiając bez zmian ustawienia domyślne.

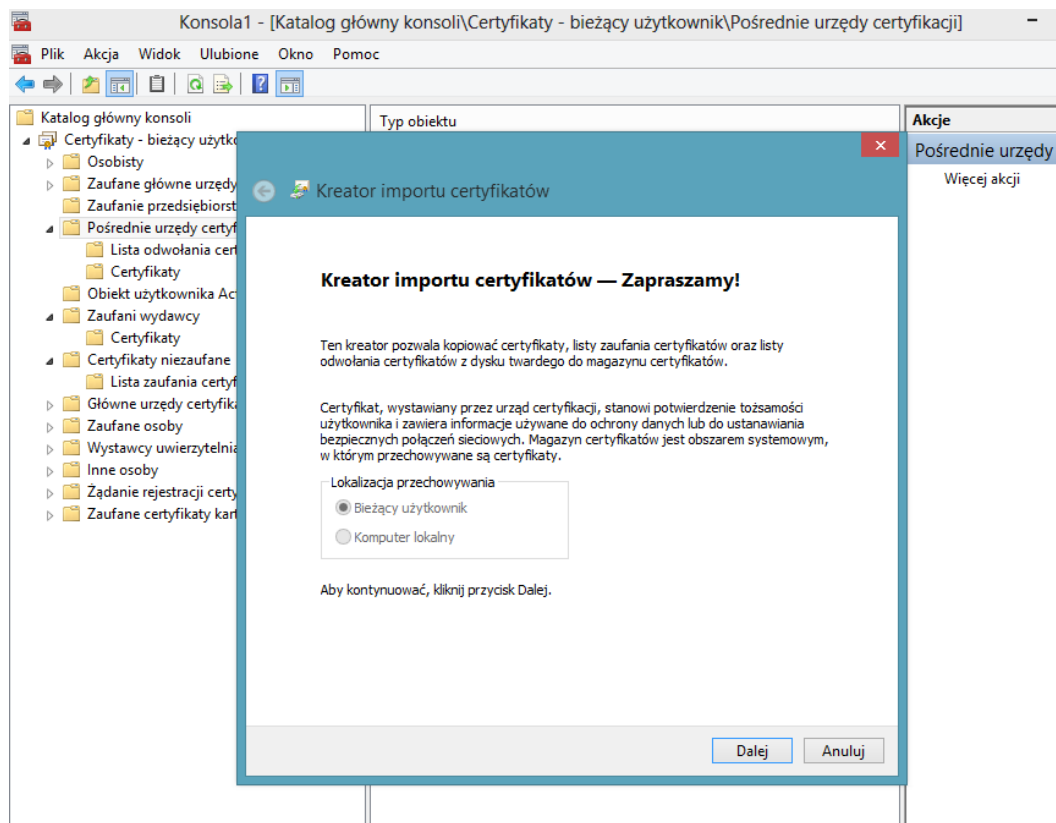
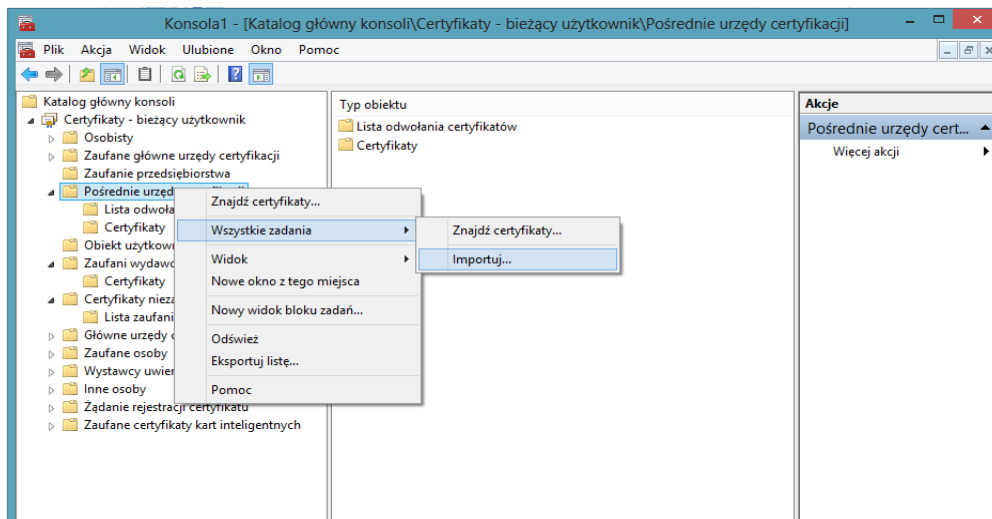


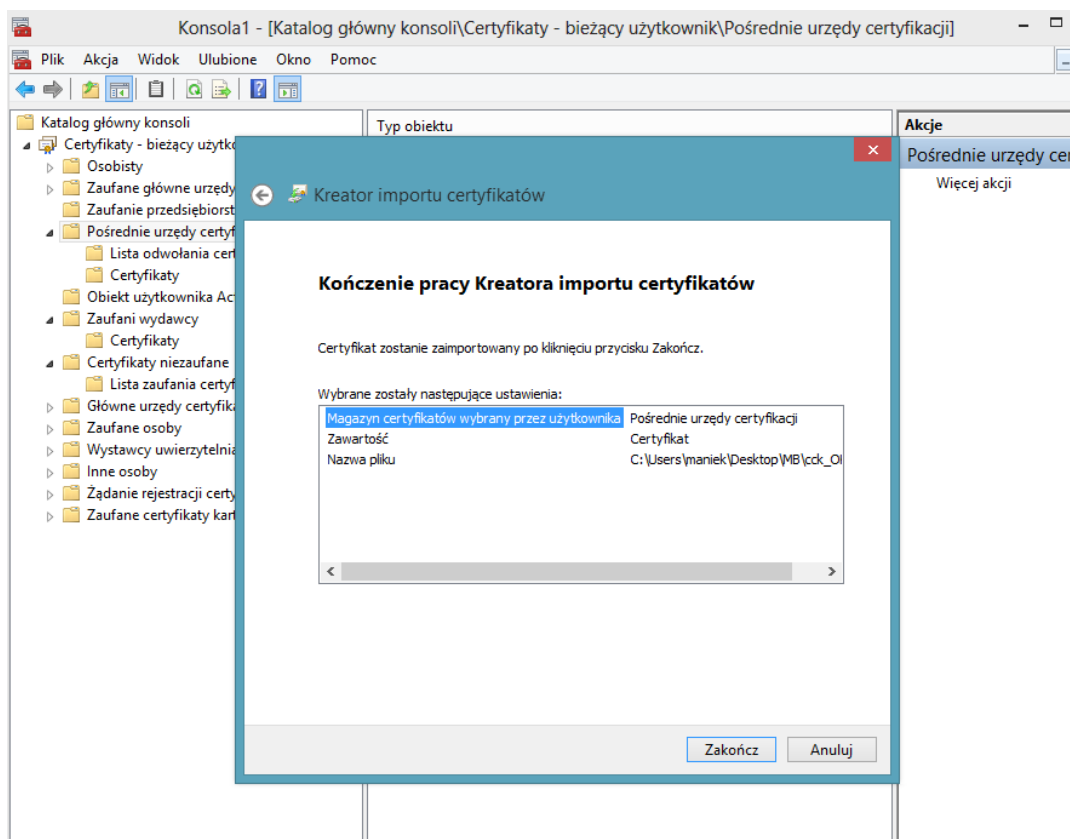
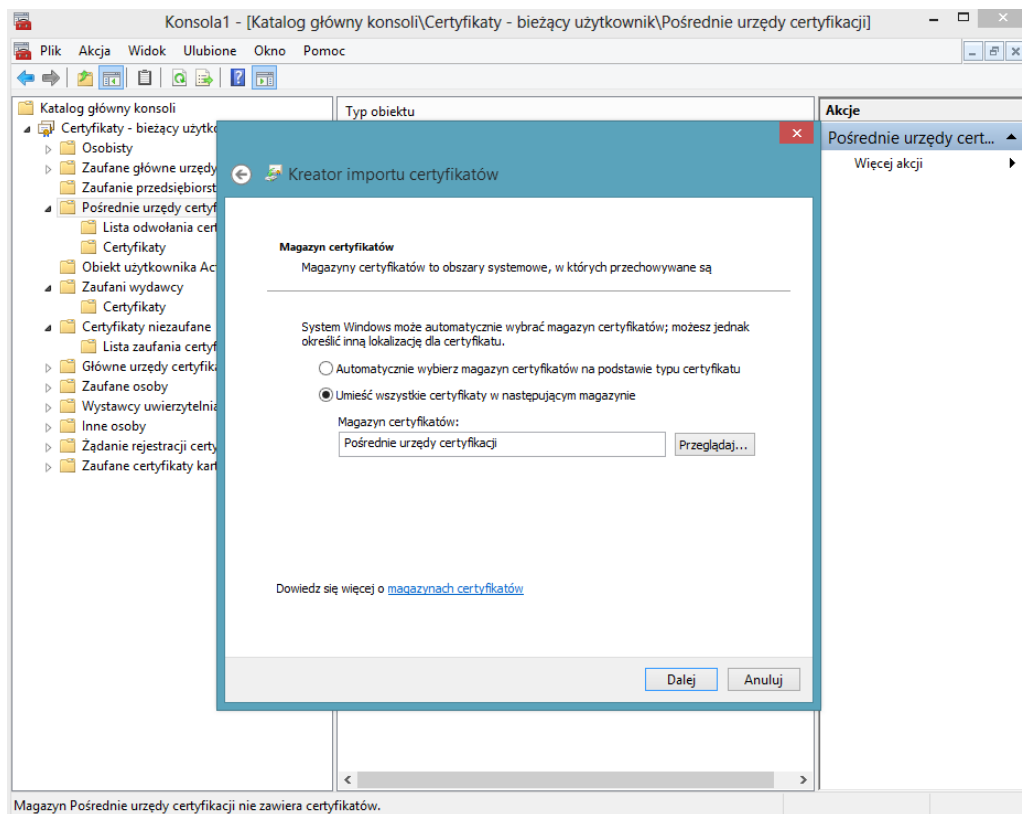
Wybieramy klawisz „Zakończ” i jak na zdjęciu poniżej możemy wybrać klawisz „OK”

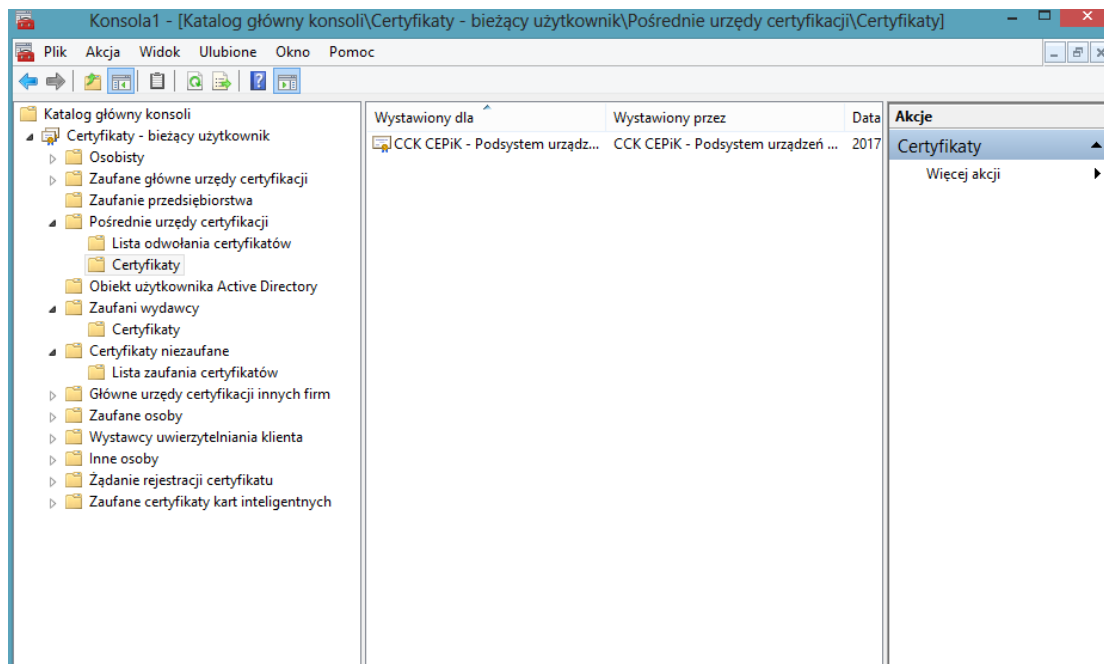


Mamy skonfigurowaną i uruchomioną konsolę **MMC**, następnie dodajemy certyfikat **CA** (w tym przypadku **cck.crt**):

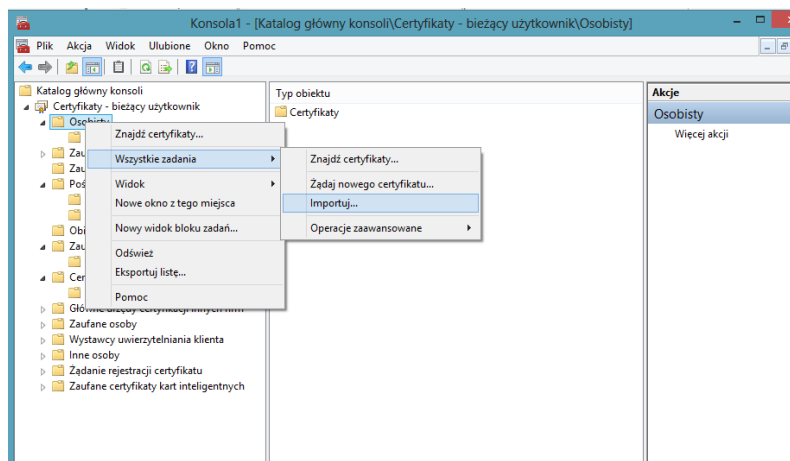


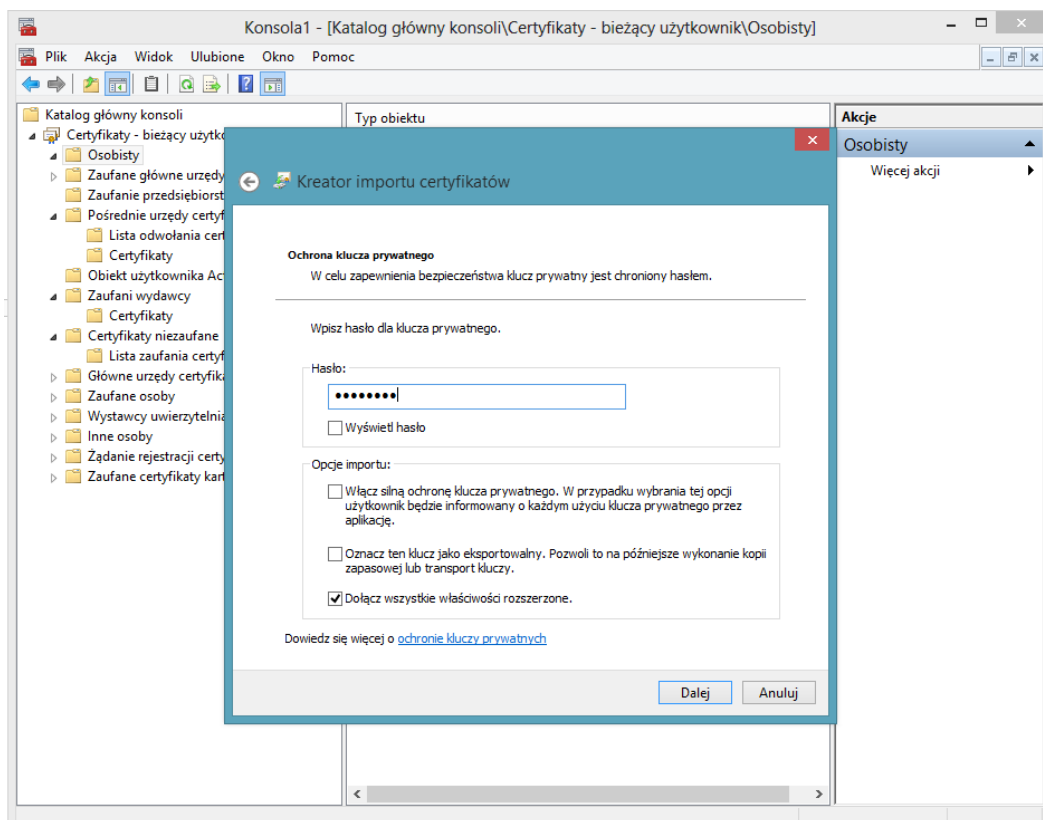
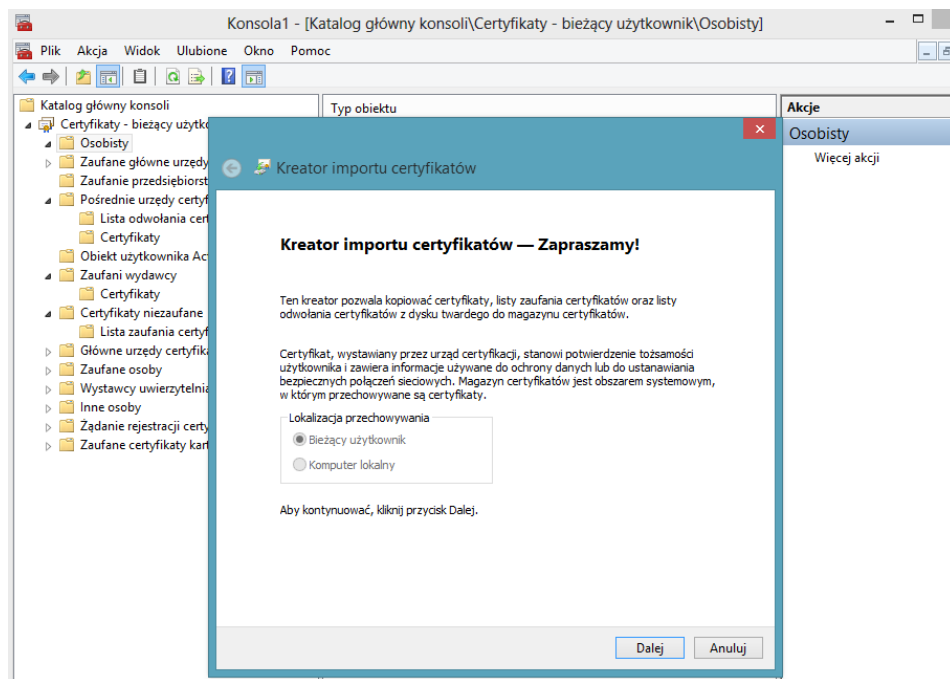


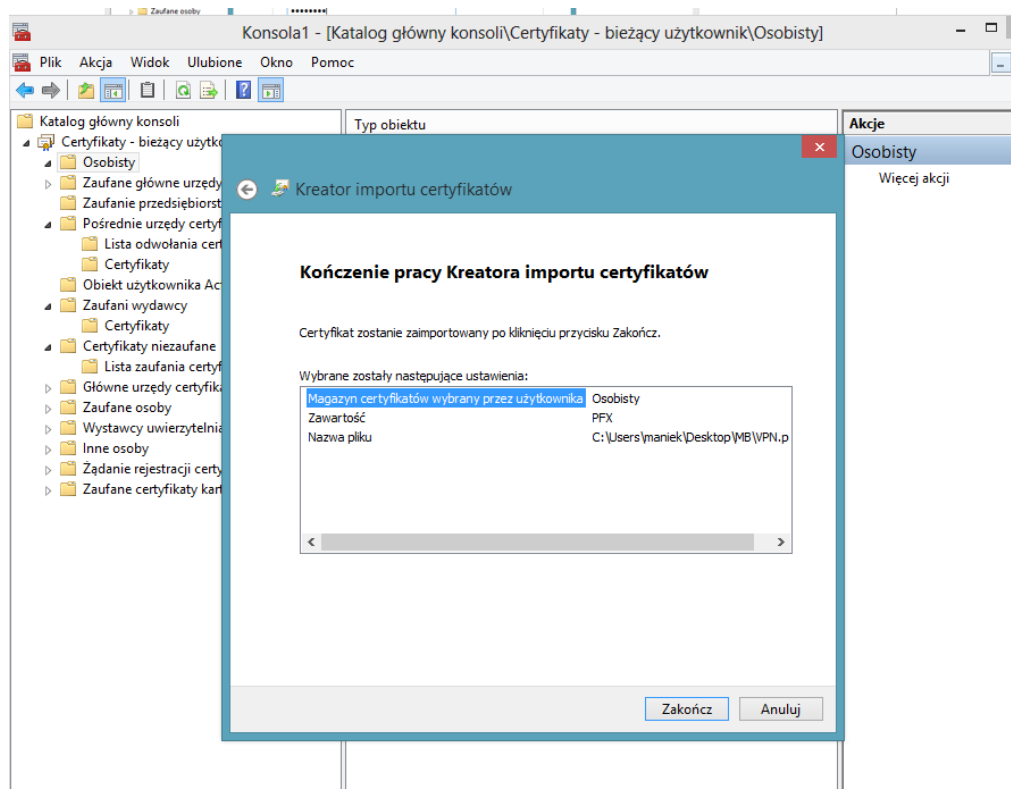
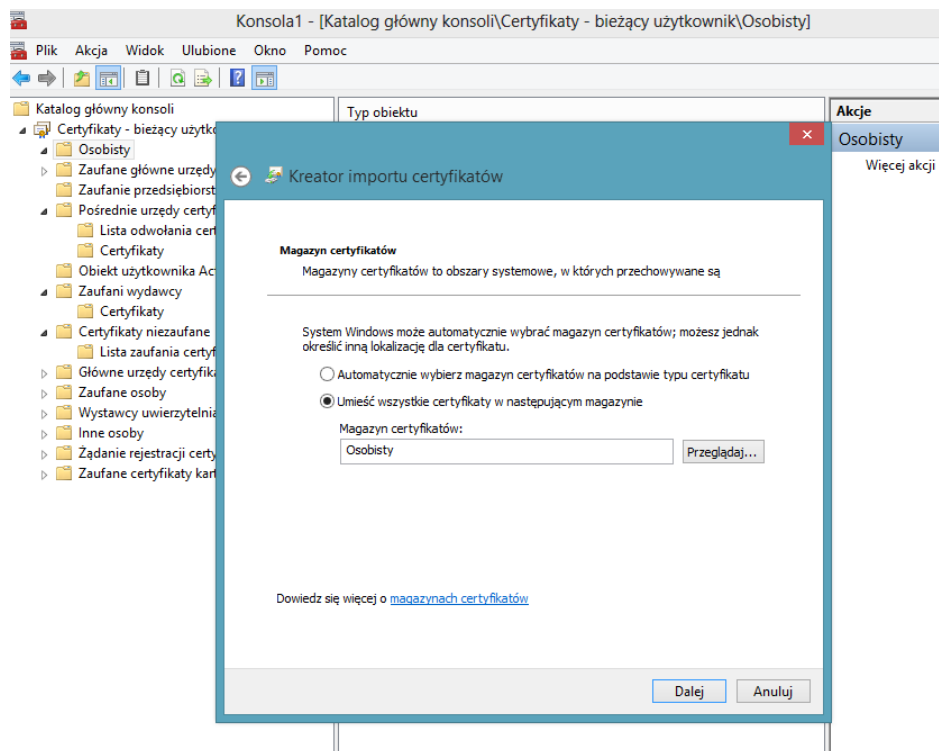


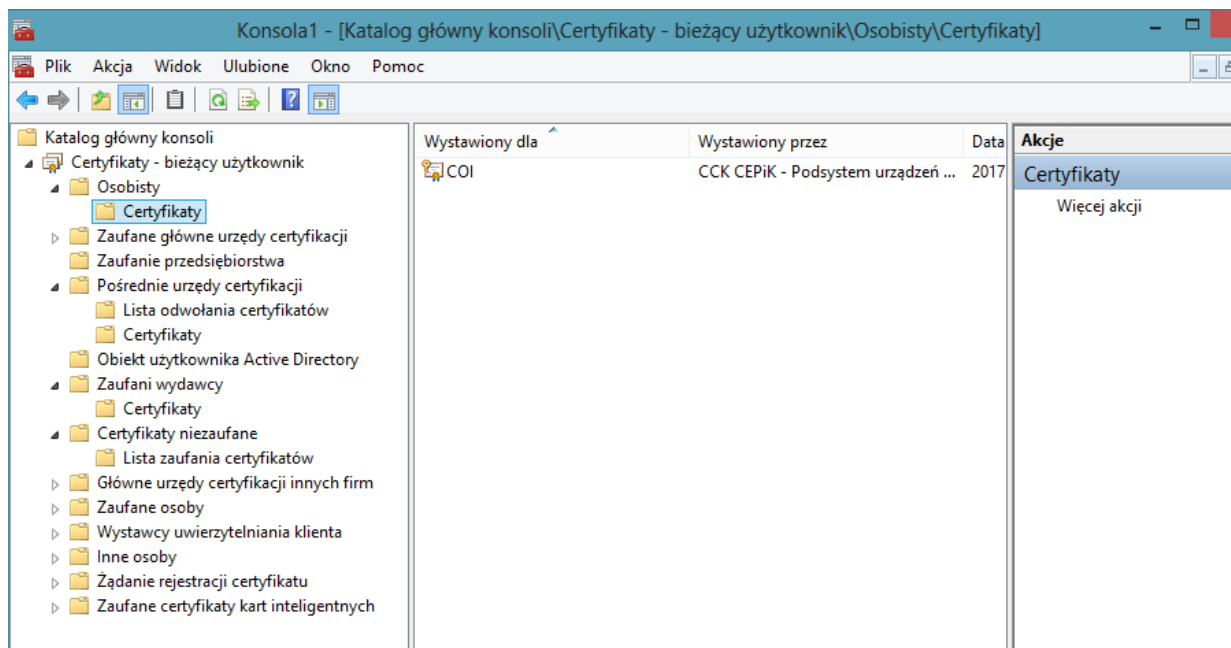


Kolejnym krokiem jest zainstalowanie certyfikatu klienta. Wykonujemy czynności zgodnie z podpowiedzią instalatora certyfikatów. W tym celu wybieramy z menu certyfikatów **Osobistych** polecenie „importuj”. W przypadku instalowania certyfikatu w formacie „p12” należy podać także hasło do certyfikatu..









Odpowiednie certyfikaty zostały zaimportowane i można przystąpić do instalacji klienta Cisco AnyConnect.

Klient do pobrania z portalu CEPiK , po autoryzacji certyfikatem:

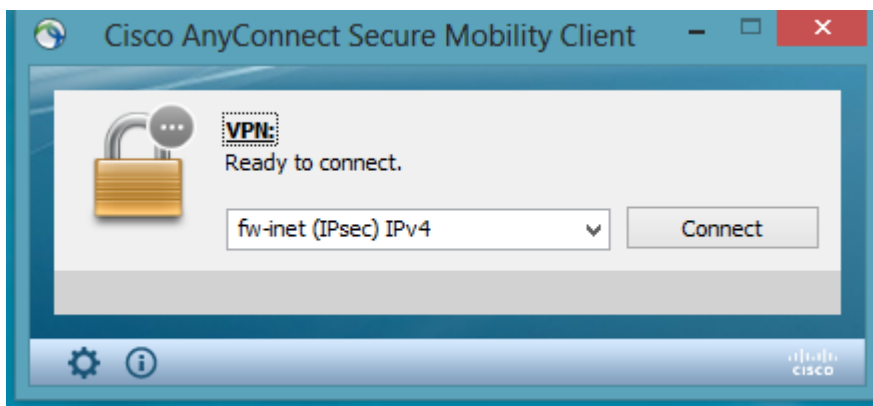
<https://www.cepik.gov.pl/cepik20/pliki/anyconnect-win-3.1.14018-pre-deploy-k9.msi>

lub po pobraniu ze strony producenta.

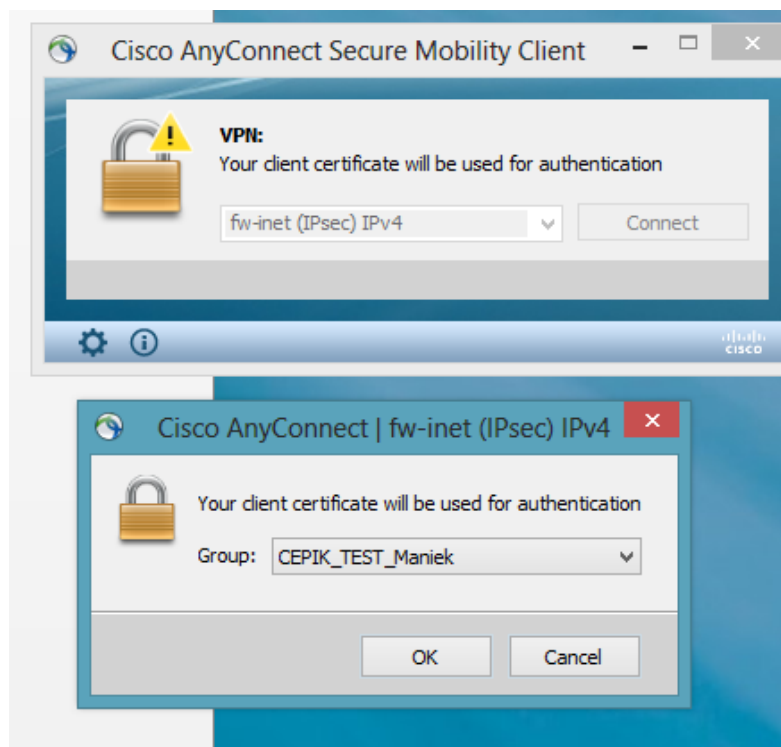
Wraz z certyfikatami Wystawca certyfikatu dostarczy odpowiednio skonfigurowany profil połączeniowy dla klienta Cisco Anyconnect. Instalujemy klienta Cisco AnyConnect i kolejnym krokiem wgrujemy dostarczony profil do następującego katalogu systemu Windows:

„C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile”

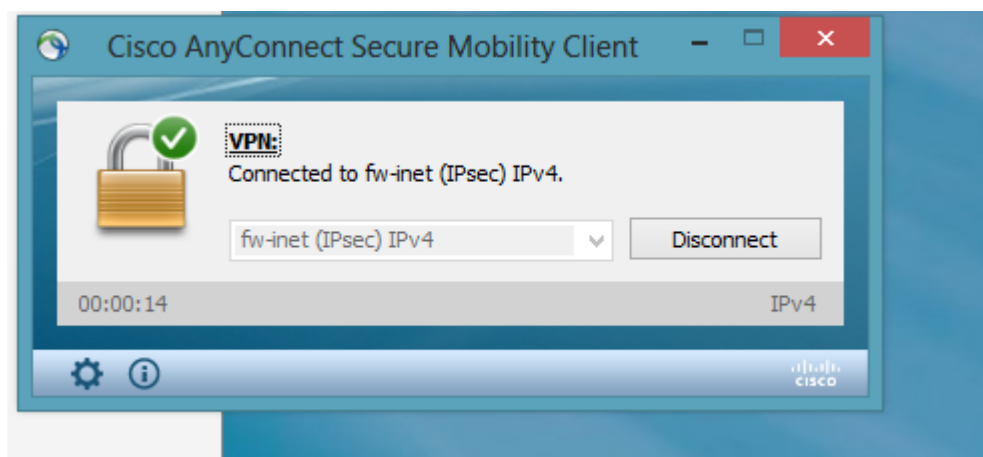
Uruchamiamy aplikację Cisco AnyConnect . Po prawidłowym wgraniu dostarczonego plik z „profilem” mamy wypełnione pole adresem IP lub nazwą domenową połączenia .



Klikamy „Connect”.



W szczególnym przypadku zależnym od konfiguracji po stronie Wykonawcy, może pojawić się pytanie o wybór grupy. Należy wybrać zgodnie z otrzymaną informacją przekazaną wraz z certyfikatami. W przypadku wątpliwości należy skontaktować się bezpośrednio z Wystawcą certyfikatów systemu w celu potwierdzenia którą grupę należy wybrać podczas uruchomienia.



Po zakończeniu pracy rozłączamy połączenie VPN wybierając opcję **Disconnect**.