centralny ośrodek informatyki

CEPiK 2 – dostęp VPN
v.1.5

ul. Suwak 3 | 02-676 Warszawa | tel.: +48 22 250 28 83 | fax: +48 22 250 29 87 | e-mail: coi@coi.gov.pl | www.coi.gov.pl

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

Spis treści

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". Od początku maja zostanie udostępniona możliwość użycia klienta „Cisco AnyConnect". Usługa VPN jest realizowana w trybie Remote Acces, 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 trakci 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" intaluje się niepoprawnie w systemie Microsoft Windows

10. Instrukcja instalacji dla tego systemu jest opisana w rozdziale 4.

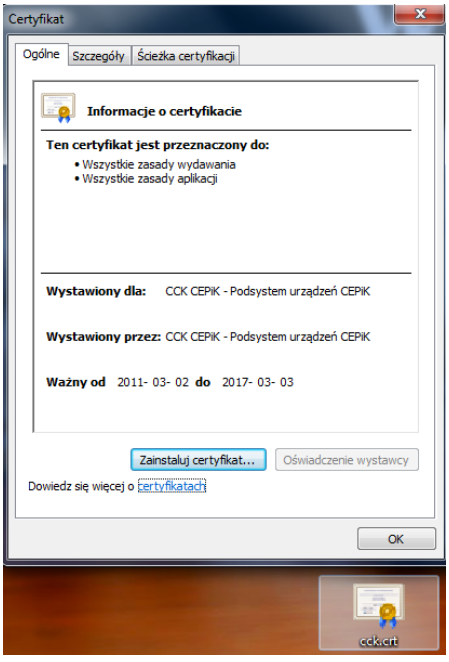
Obsługa zgłoszeń związanych z połączeniami VPN typu Remote Access z wykorzystaniem klientów Cisco VPN Client oraz Cisco AnyConnect będzie realizowana przez Service Desk CEPiK, w zakresie instalacji i konfiguracji oprogramowania.

Na początek

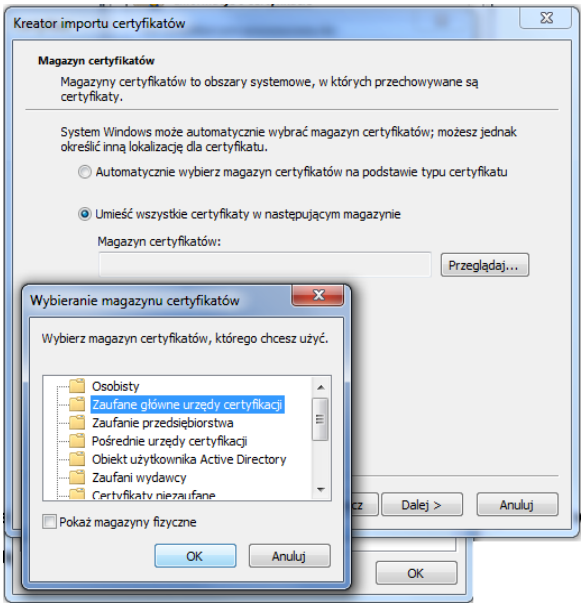
Zainstaluj oprogramowanie Cisco VPN Client. Po poprawnej instalacji Cisco VPN Client w systemie operacyjnym, przystępujemy do instalacji wymaganych certyfikatów.

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**”



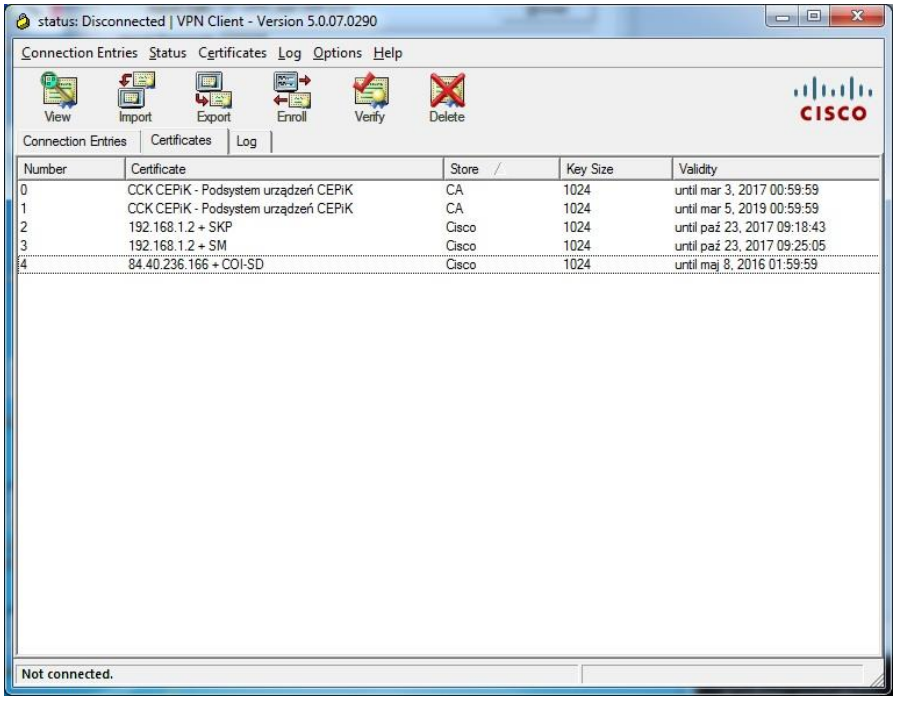
W okienku „**Wybieranie magazynu certyfikatów**” zaznaczamy „**Zaufane główne urzędy certyfikacji**” i klikamy „**OK**”. Następnie klikamy klikamy „**Dalej**”, w razie wystąpienia komunikatu z ostrzeżeniem o imporcie nieznanego klucza, wybieramy opcję zezwalającą na import i klucz został zaimportowany.

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**).

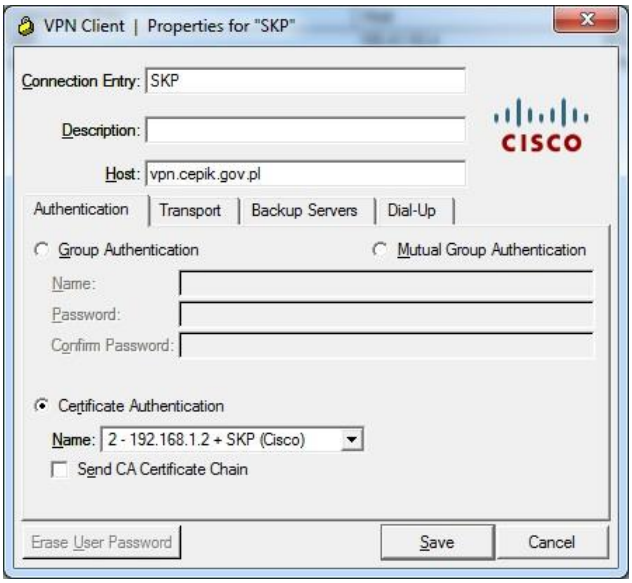


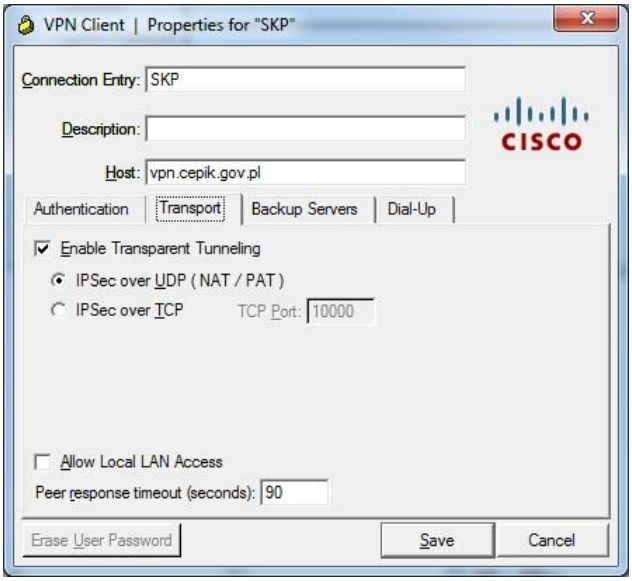
Krok 3. Zdefiniowanie połączenia VPN

W zakładce **Connection Entries** definiujemy nowe połaczenie. 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**.

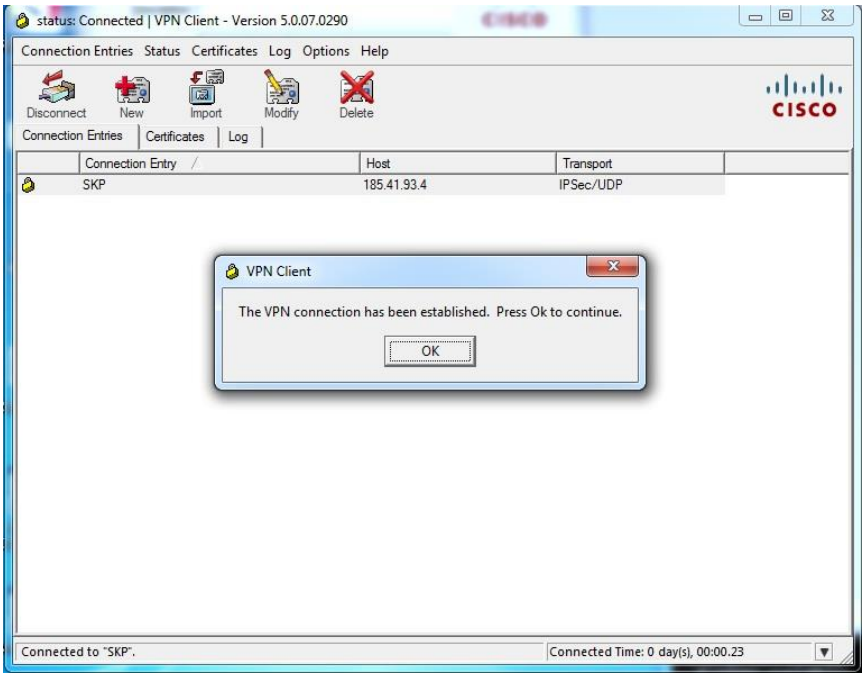




Pozostałe parametry pozostawiamy bez zmian i zapisujemy konfigurację przyciskiem **Save**.

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.

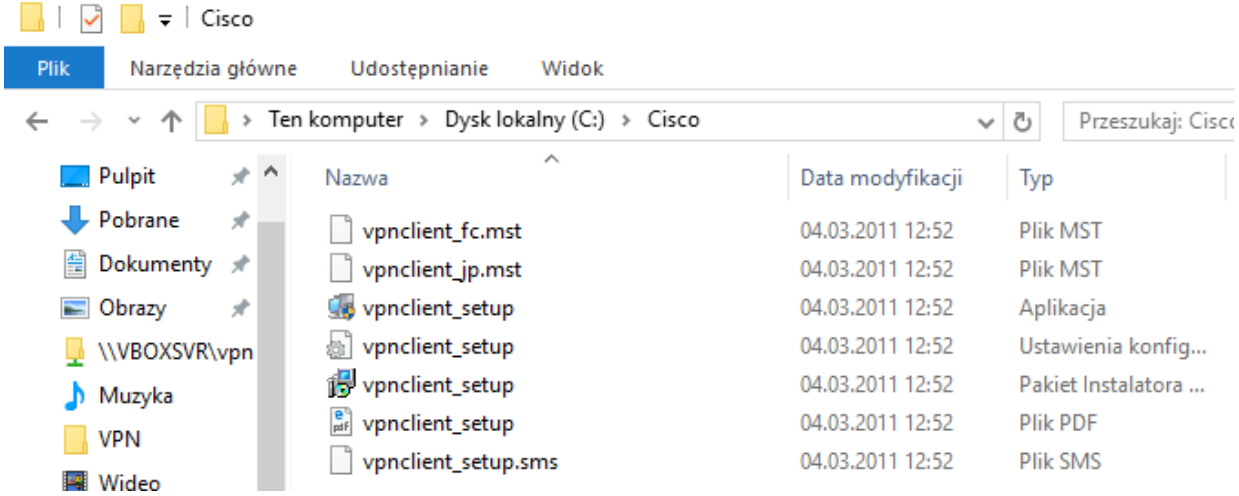


Po zakończeniu pracy rozłączamy połączenie VPN wybierając opcję **Disconect**.

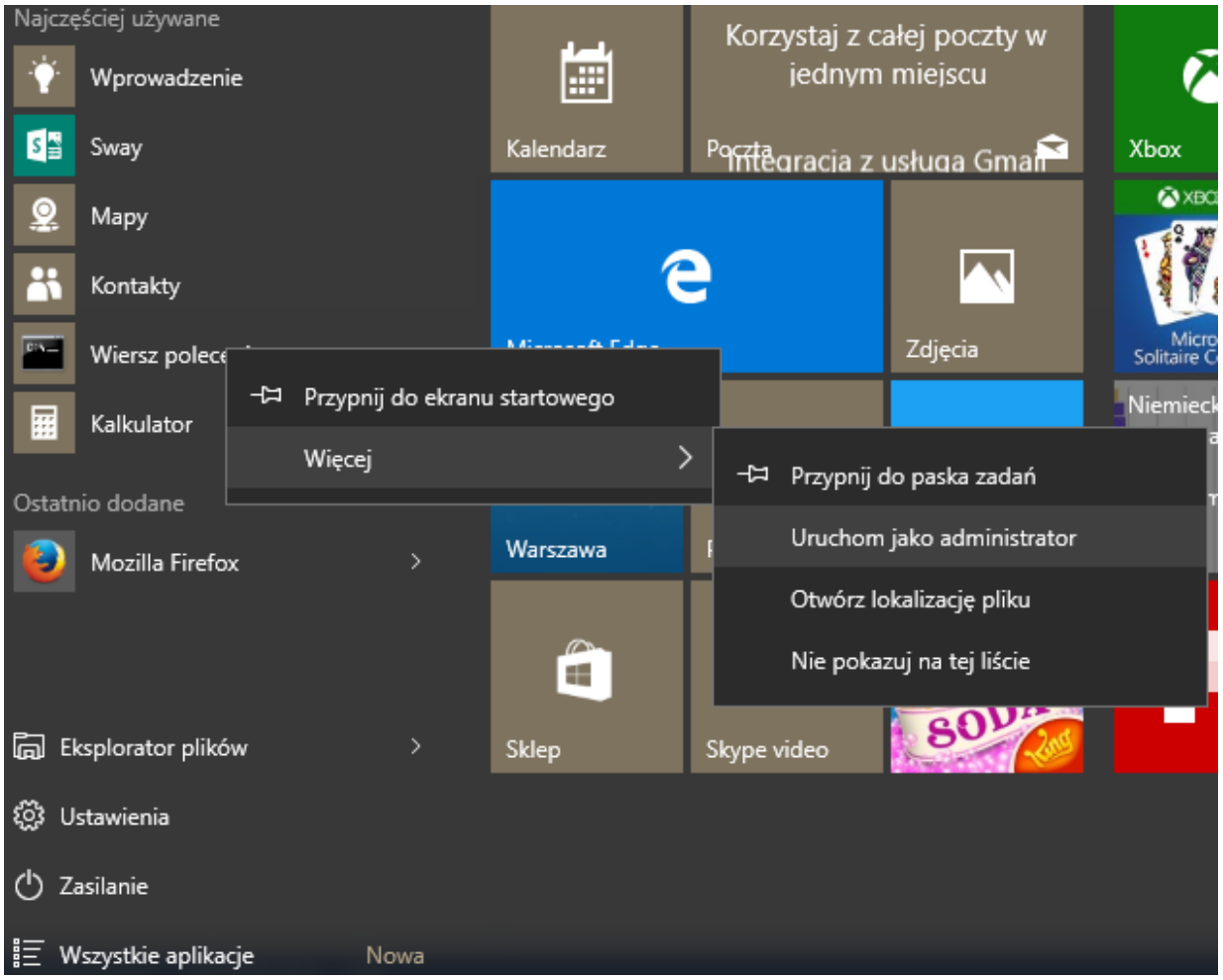
4. Instalacja oprogramowania „Cisco VPN Client" w systemie MS Windows 10

Instrukcja dotyczy instalacji klienta w wersji 5.0.07.0440

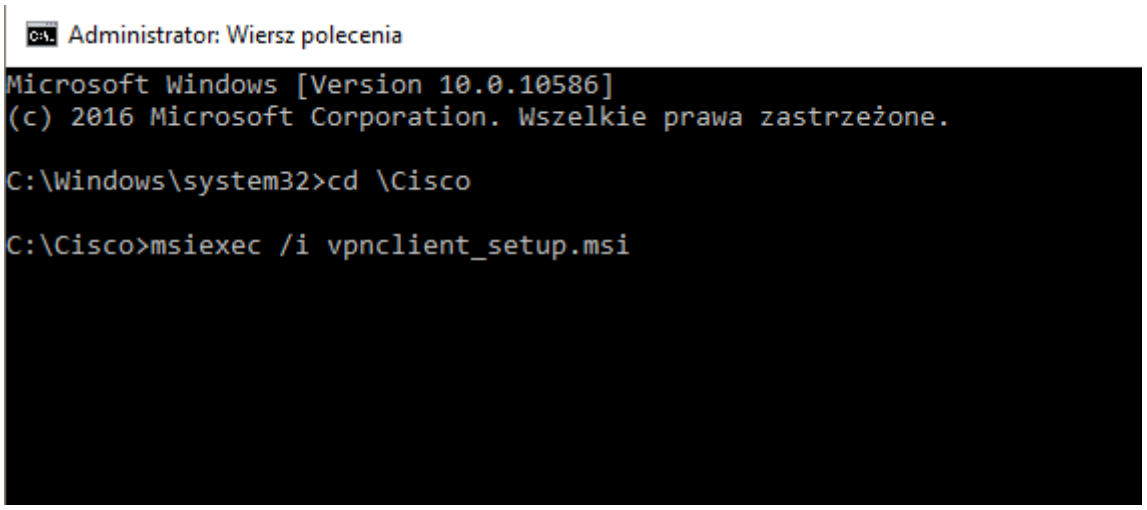
- **Instalacja sterownika DNE Update**
  Pobieramy i instalujemy ftp://ftpsupport.citrix.com/dneupdate64.msi
- **Instalacja oprogramowania „Cisco VPN Client"**
  - pobieramy oprogramowanie vpnclient-winx64-msi-5.0.07.0440
  - rozpakowujemy do wybranego katalogu np. C:\Cisco



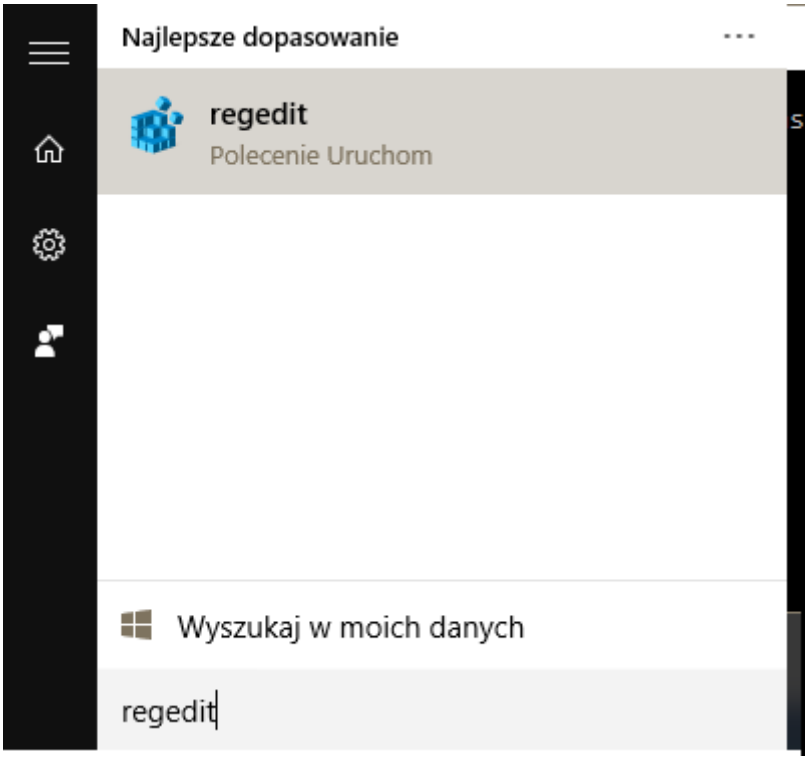
- uruchamiamy „Wiersz poleceń” jako administrator



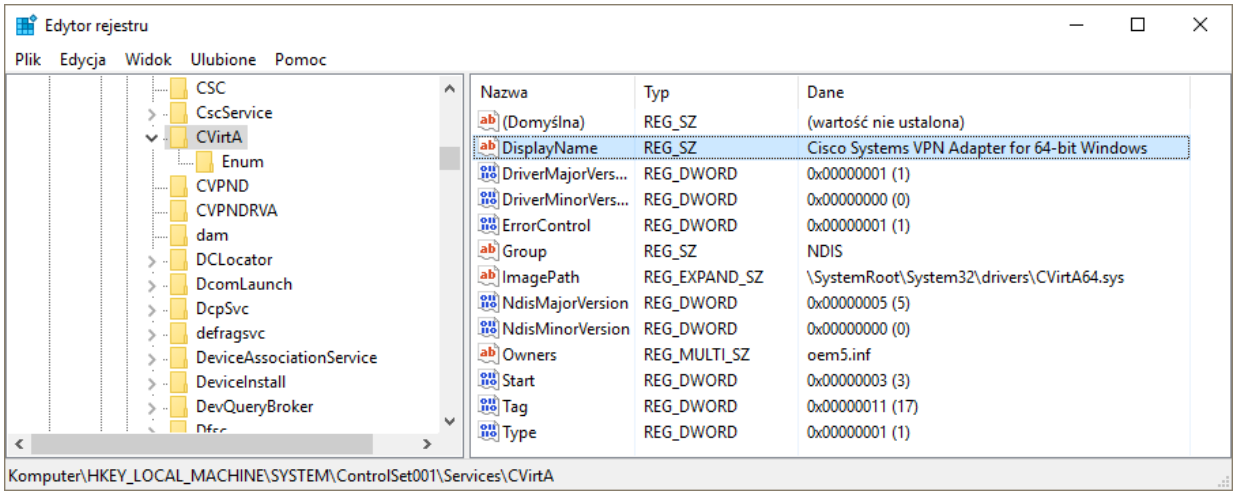
- instalujemy oprogramowanie poleceniem: „msiexec /i vpnclient_setup.msi”



- **Poprawka rejestru.**
  Wymagana jest drobna zmiana w rejestrze systemowym:
  - uruchamiamy edytor rejestru



- szukamy klucza
HKLM\SYSTEM\ControlSet001\Services\CVirtA\DisplayName
i modyfikujemy jego watość usuwając wszystko co jest przed „Cisco Systems …”
(@oemX.inf,%CVirtA_Desc%;)

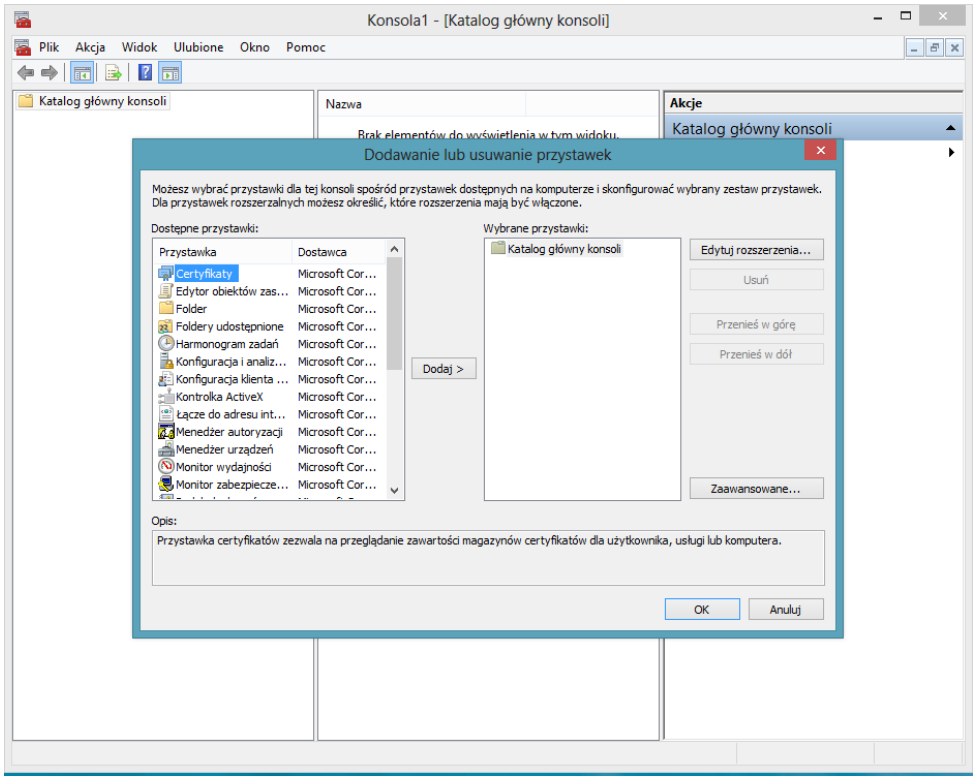


5. Instalacja oprogramowania „Cisco AnyConnect Secure Mobility”

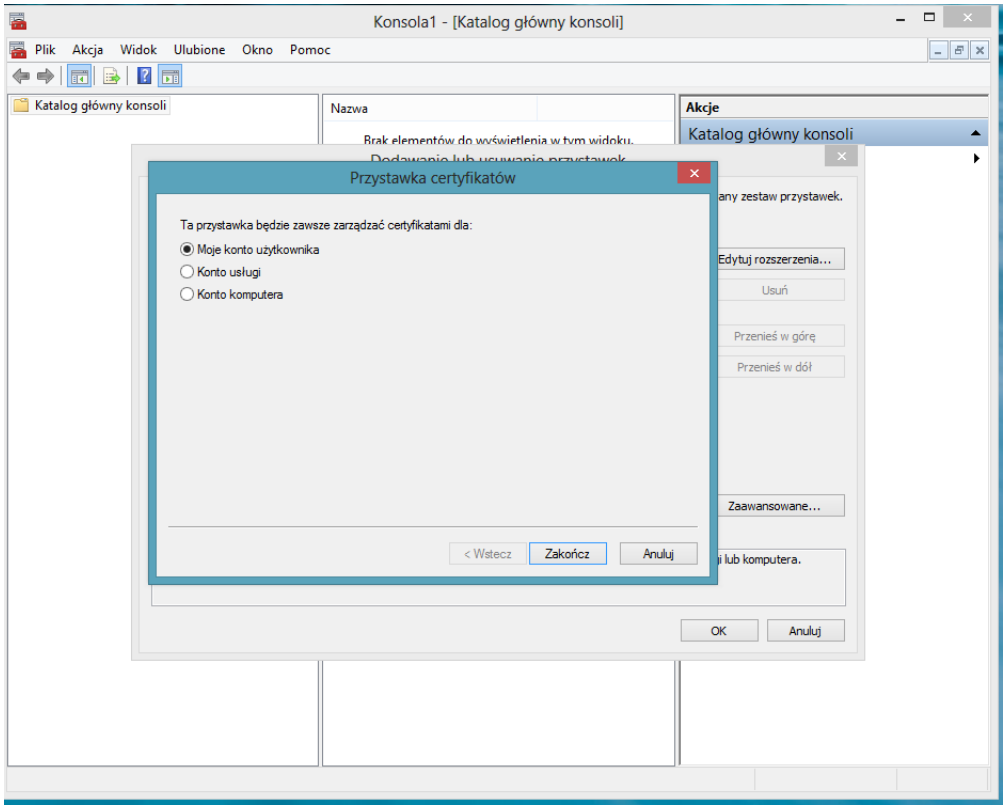
Do poprawnego skonfigurowania zdalnego dostępu należy pobrać i zainstalować oprogramowanie Cisco AnyConnect Secure Mobility Client ver. Min 4.2 lub skorzystać z innego alternatywnego rozwiązania wspierającego połączenia IKe2 lub SSl.

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)

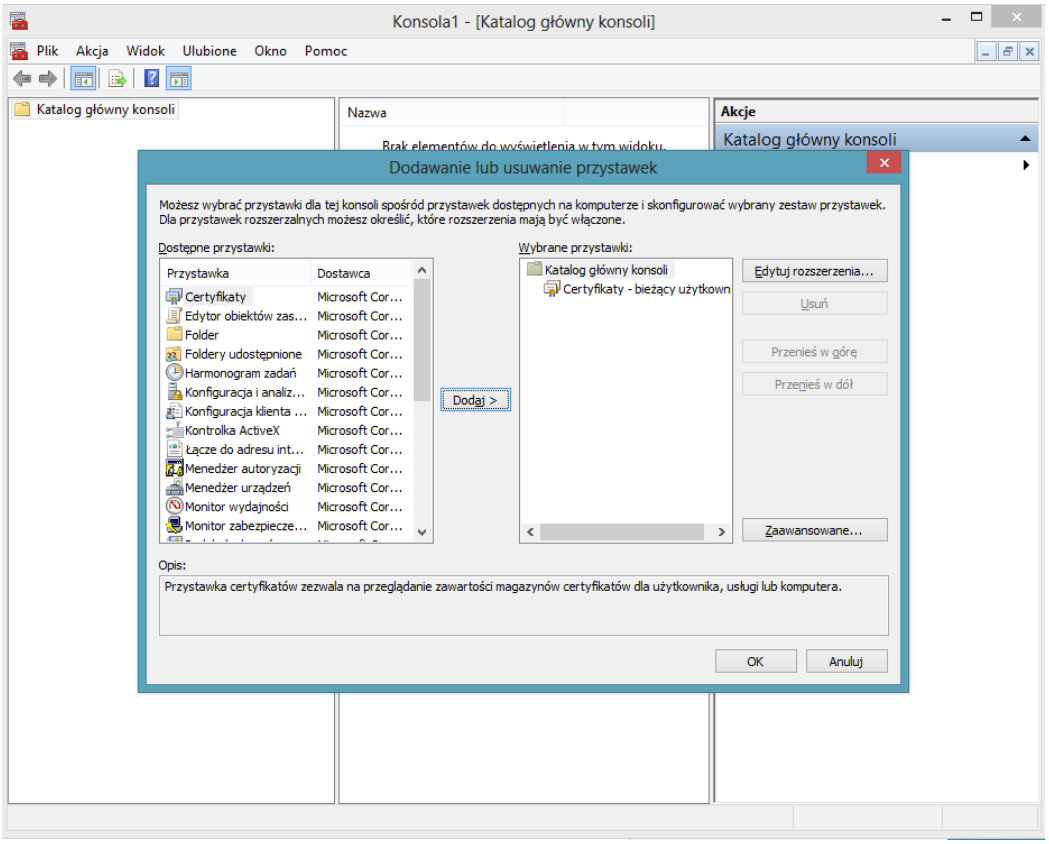
W pierwszym kroku instalujemy otrzymany certyfikat urzędu **CA**. W tym celu otwieramy konsole MMC. Wybieramy z menu Plik –Dodaj/Usuń przystawkę. Wybieramy z lewej strony przystawkę „Certyfikaty.”



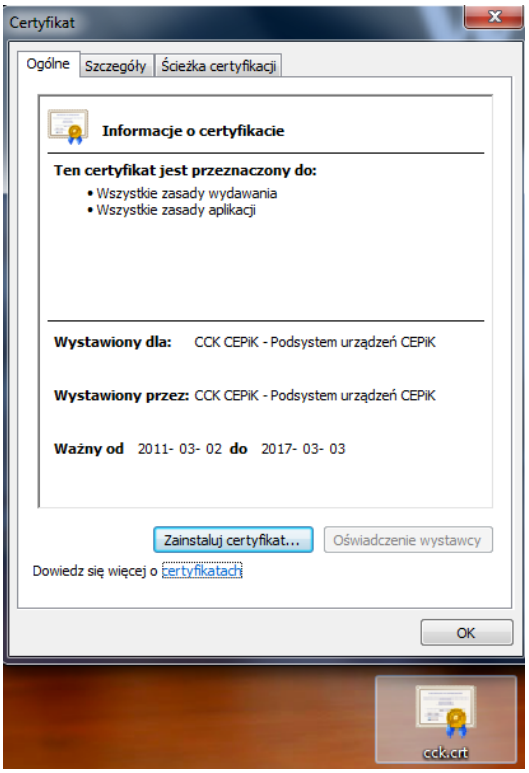
Następnie klikamy dodaj pozostawiając bez zmian ustawienia domyślne.

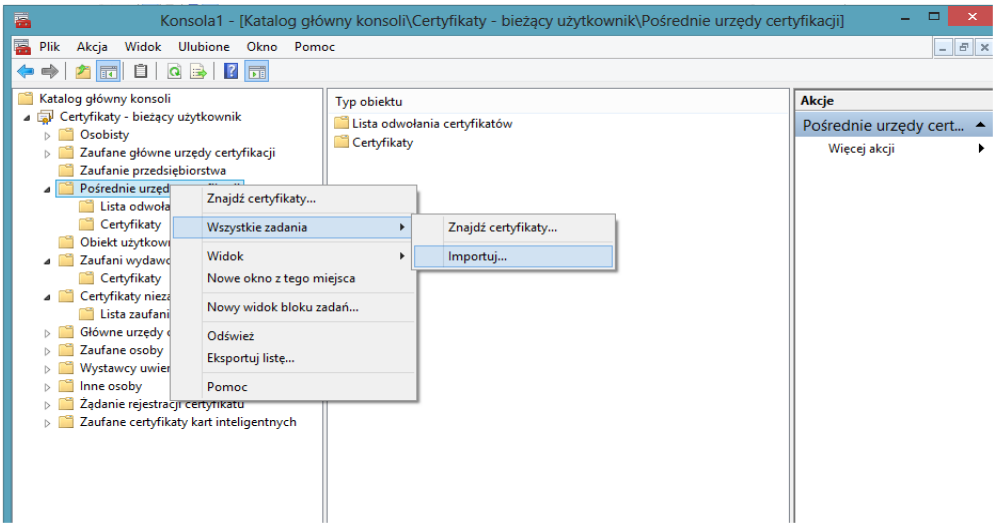


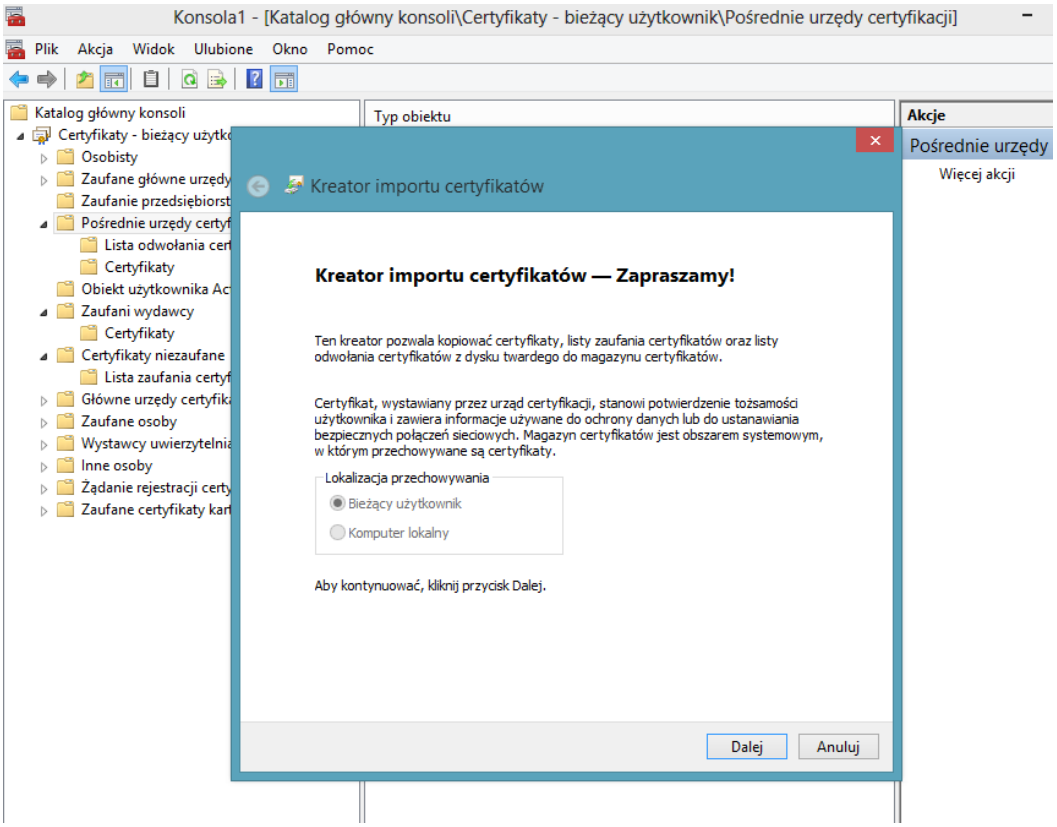
Wybieramy klawisz „Zakończ” i jak na zdjęciu poniżej możemy wybrać klawisz „OK”

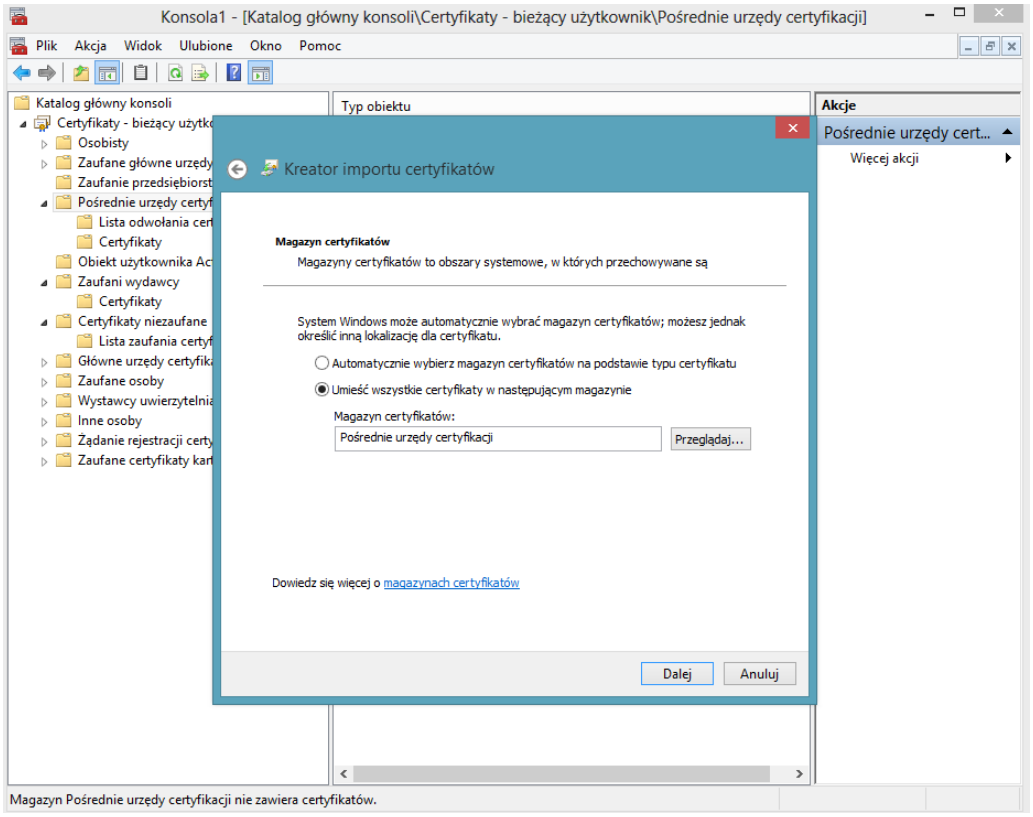


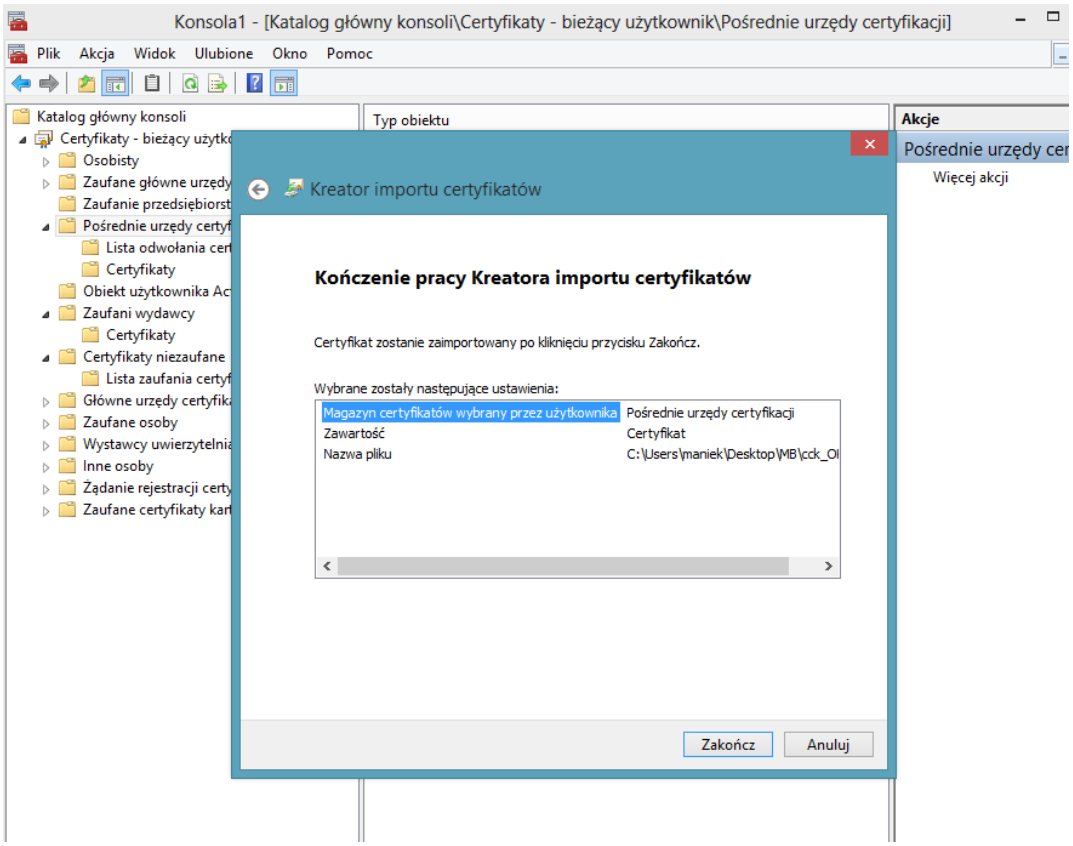
Mamy skonfigurowaną i uruchomioną konsolę **MMC**, następnie dodajemy certyfikat **CA** (w tym przypadku **cck.crt**):

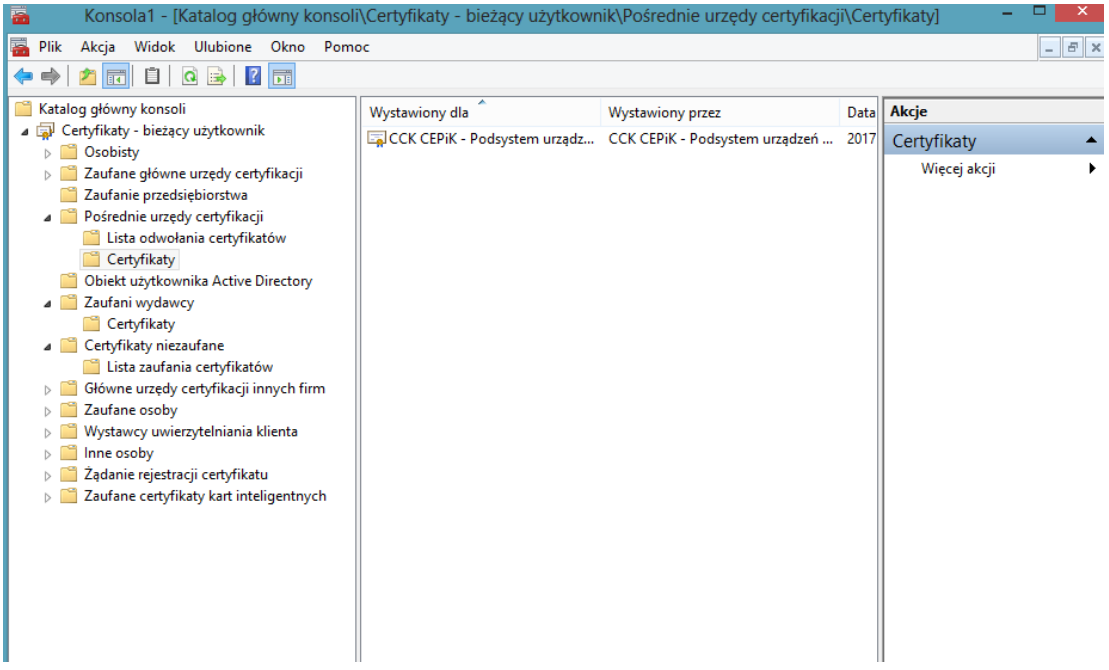

Certyfikat
Ogólne
Szczegóły
Ścieżka certyfikacji
Informacje o certyfikacie
Ten certyfikat jest przeznaczony do:
• Wszystkie zasady wydawania
• Wszystkie zasady aplikacji
Wystawiony dla: CCK CEPiK - Podsystem urządzeń CEPiK
Wystawiony przez: CCK CEPiK - Podsystem urządzeń CEPiK
Ważny od 2011- 03- 02 do 2017- 03- 03
Zainstaluj certyfikat...
Oświadczenie wystawcy
Dowiedz się więcej o certyfikatach
OK
cck.crt


Konsola1 - [Katalog główny konsoli\Certyfikaty - bieżący użytkownik\Pośrednie urzędy certyfikacji]
Plik Akcja Widok Ulubione Okno Pomoc
Katalog główny konsoli
Certyfikaty - bieżący użytkownik
Osobisty
Zaufane główne urzędy certyfikacji
Zaufanie przedsiębiorstwa
Pośrednie urzęd
Lista odwoła
Certyfikaty
Obiekt użytkow
Zaufani wydawc
Certyfikaty
Certyfikaty niez
Lista zaufani
Główne urzędy
Zaufane osoby
Wystawcy uwier
Inne osoby
Żądanie rejestracji certyfikatu
Zaufane certyfikaty kart inteligentnych
Typ obiektu
Lista odwołania certyfikatów
Certyfikaty
Akcje
Pośrednie urzędy cert...
Więcej akcji
Znajdź certyfikaty...
Wszystkie zadania
Widok
Nowe okno z tego miejsca
Nowy widok bloku zadań...
Odśwież
Eksportuj listę...
Pomoc
Znajdź certyfikaty...
Importuj...

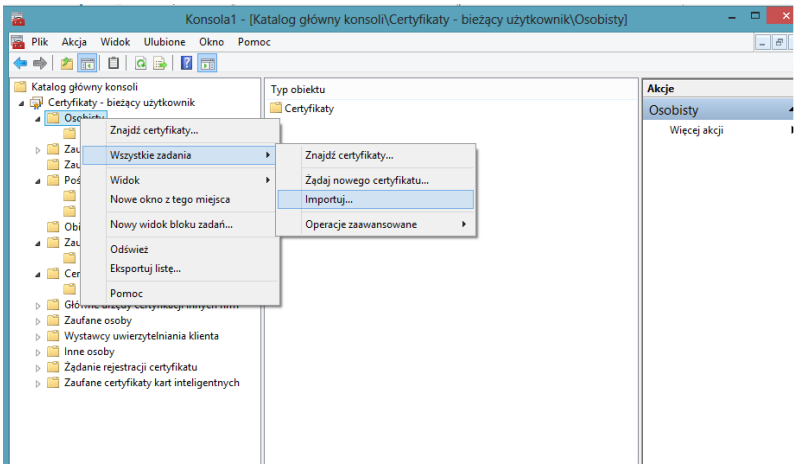

Konsola1 - [Katalog główny konsoli\Certyfikaty - bieżący użytkownik\Pośrednie urzędy certyfikacji]
Plik Akcja Widok Ulubione Okno Pomoc
Katalog główny konsoli
Typ obiektu
Akcje
Pośrednie urzędy
Więcej akcji
Kreator importu certyfikatów
Kreator importu certyfikatów — Zapraszamy!
Ten kreator pozwala kopiować certyfikaty, listy zaufania certyfikatów oraz listy odwołania certyfikatów z dysku twardego do magazynu certyfikatów.
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.
Lokalizacja przechowywania
Bieżący użytkownik
Komputer lokalny
Aby kontynuować, kliknij przycisk Dalej.
Dalej
Anuluj

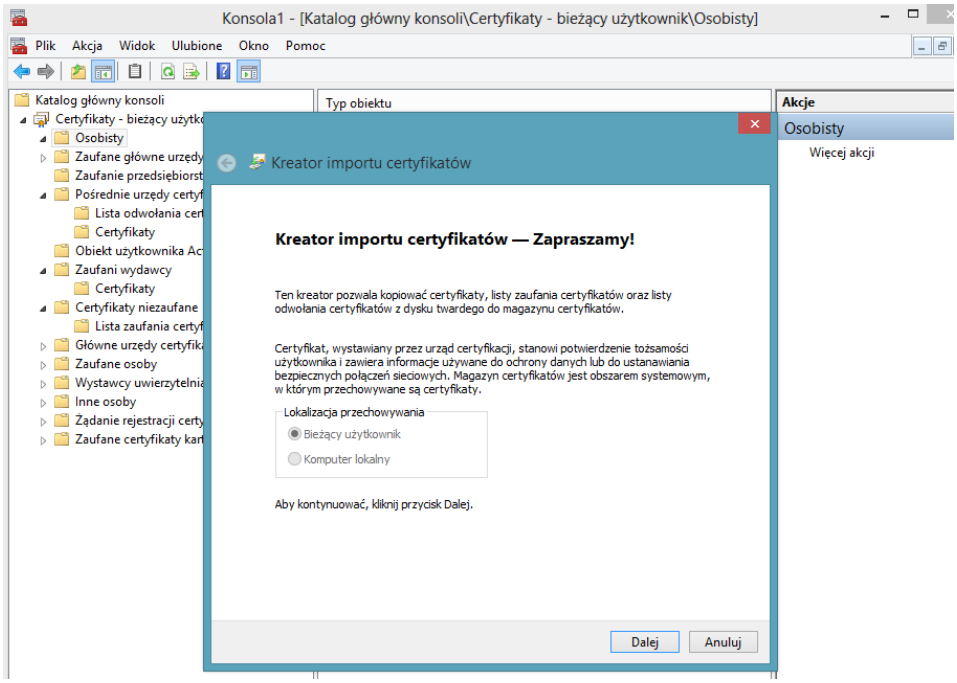

Konsola1 - [Katalog główny konsoli\Certyfikaty - bieżący użytkownik\Pośrednie urzędy certyfikacji]
Plik Akcja Widok Ulubione Okno Pomoc
Katalog główny konsoli
Typ obiektu
Akcje
Pośrednie urzędy cert...
Więcej akcji
Kreator importu certyfikatów
Magazyn certyfikatów
Magazyny certyfikatów to obszary systemowe, w których przechowywane są
System Windows może automatycznie wybrać magazyn certyfikatów; możesz jednak określić inną lokalizację dla certyfikatu.
Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu
Umieść wszystkie certyfikaty w następującym magazynie
Magazyn certyfikatów:
Pośrednie urzędy certyfikacji
Przeglądaj...
Dowiedz się więcej o magazynach certyfikatów
Dalej
Anuluj
Magazyn Pośrednie urzędy certyfikacji nie zawiera certyfikatów.

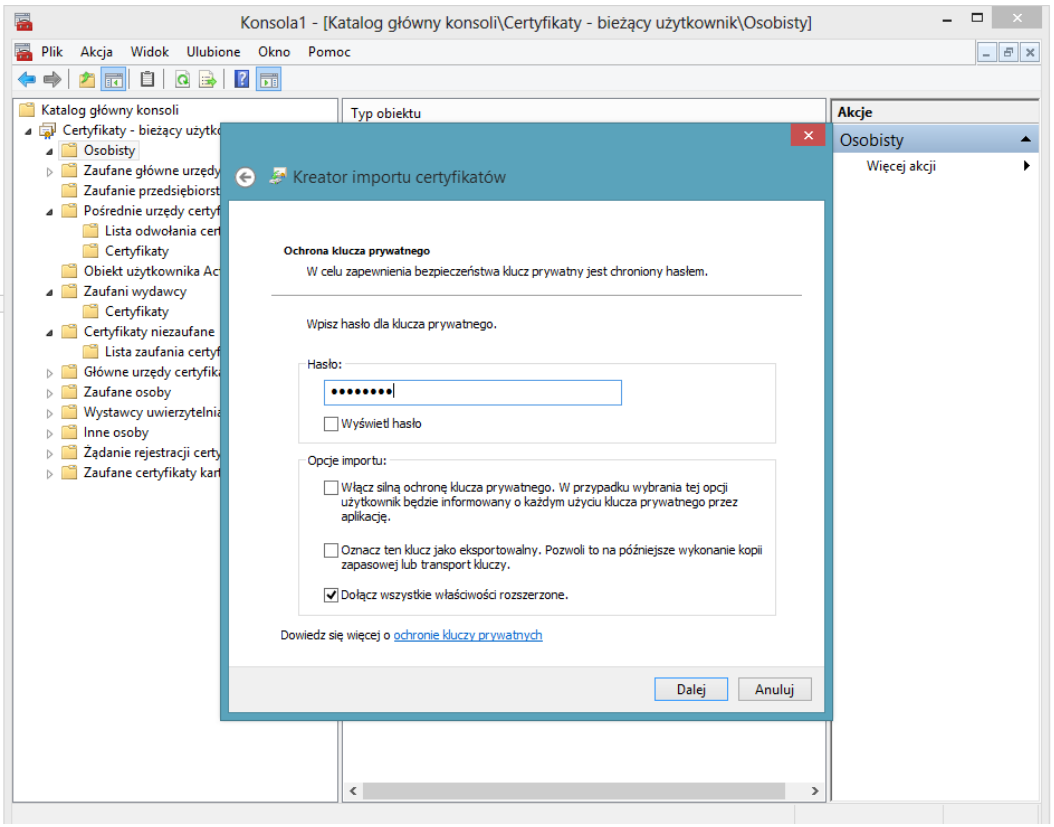


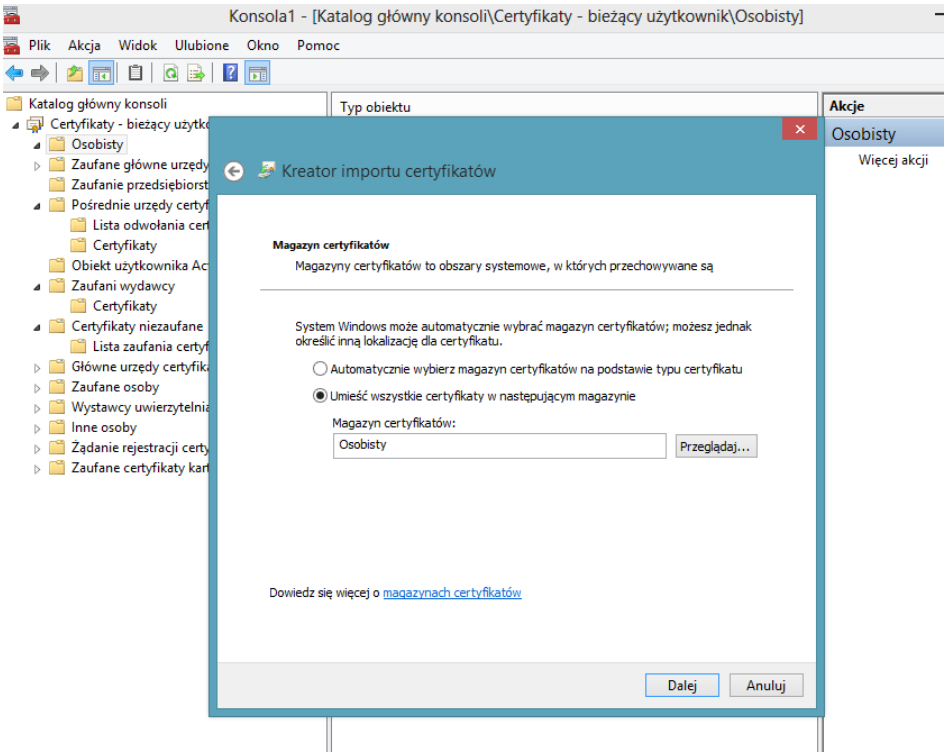


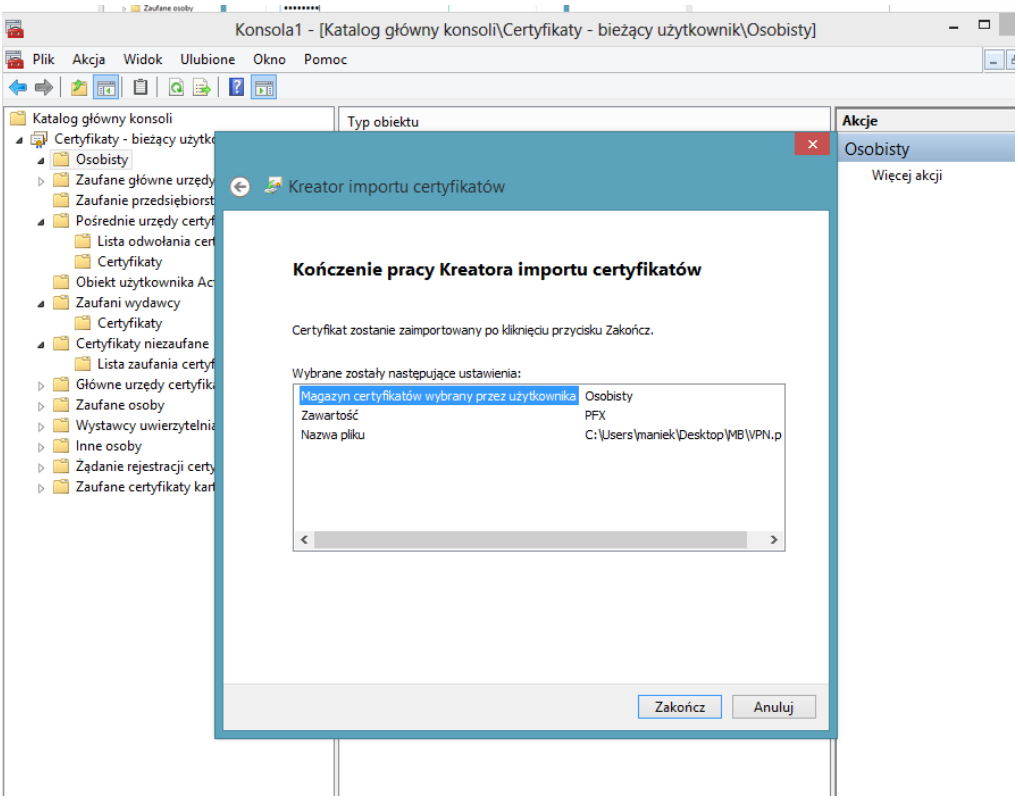
Kolejnym krokiem jest zainstalowanie certyfikatu klienta. Wykonujemy czynności zgodnie z podpowiedzią instalatora certyfikatów. W tym celu wybieramy z menu certyfikatów **Osobistych** polecenie **„importuj”**. W przypadku instalowania certyfikatu w formacie „**p12”** należy podać także hasło do certyfikatu..

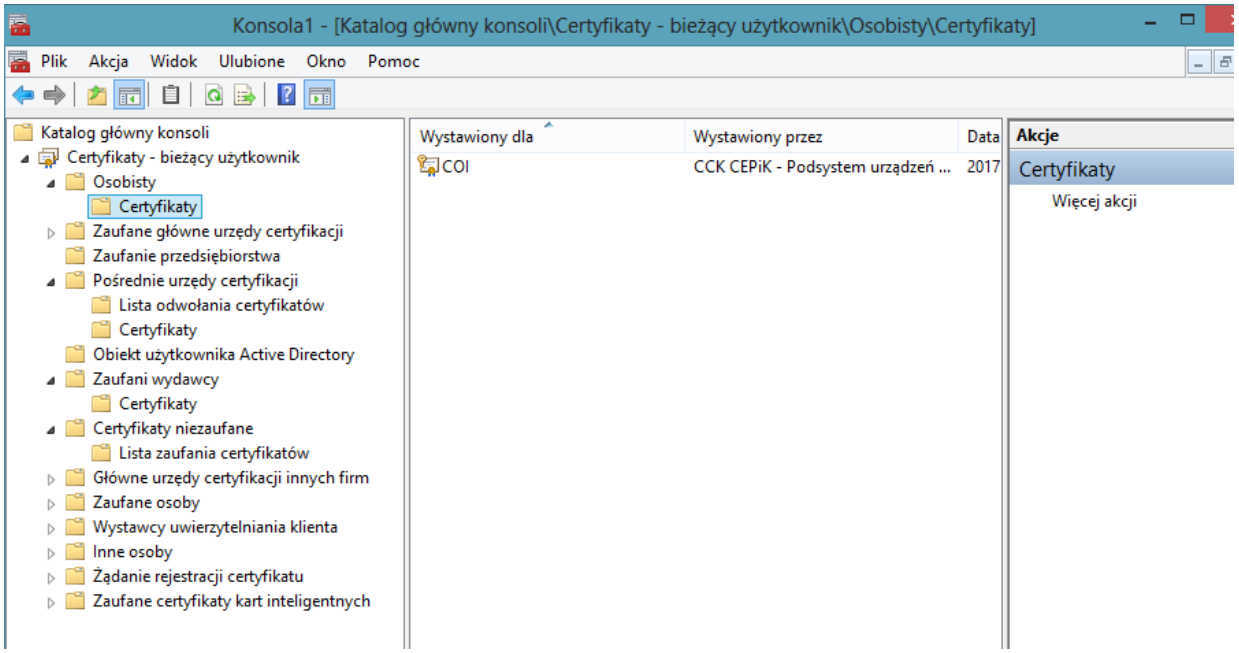

Konsola1 - [Katalog główny konsoli\Certyfikaty - bieżący użytkownik\Osobisty]
Plik Akcja Widok Ulubione Okno Pomoc
Katalog główny konsoli
Certyfikaty - bieżący użytkownik
Osobisty
Zaufane osoby
Wystawcy uwierzytelniania klienta
Inne osoby
Żądanie rejestracji certyfikatu
Zaufane certyfikaty kart inteligentnych
Typ obiektu
Certyfikaty
Akcje
Osobisty
Więcej akcji
Znajdź certyfikaty...
Wszystkie zadania
Widok
Nowe okno z tego miejsca
Nowy widok bloku zadań...
Odśwież
Eksportuj listę...
Pomoc
Znajdź certyfikaty...
Żądaj nowego certyfikatu...
Importuj...
Operacje zaawansowane


Konsola1 - [Katalog główny konsoli\Certyfikaty - bieżący użytkownik\Osobisty]
Plik Akcja Widok Ulubione Okno Pomoc
Katalog główny konsoli
Osobisty
Zaufane główne urzędy
Zaufanie przedsiębiorst
Pośrednie urzędy certyf
Lista odwołania cert
Certyfikaty
Obiekt użytkownika Ac
Zaufani wydawcy
Certyfikaty
Certyfikaty niezaufane
Lista zaufania certyf
Główne urzędy certyfik
Zaufane osoby
Wystawcy uwierzytelni
Inne osoby
Żądanie rejestracji certy
Zaufane certyfikaty kart
Typ obiektu
Akcje
Osobisty
Więcej akcji
Kreator importu certyfikatów
Kreator importu certyfikatów — Zapraszamy!
Ten kreator pozwala kopiować certyfikaty, listy zaufania certyfikatów oraz listy odwołania certyfikatów z dysku twardego do magazynu certyfikatów.
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.
Lokalizacja przechowywania
Bieżący użytkownik
Komputer lokalny
Aby kontynuować, kliknij przycisk Dalej.
Dalej
Anuluj


Konsola1 - [Katalog główny konsoli\Certyfikaty - bieżący użytkownik\Osobisty]
Plik Akcja Widok Ulubione Okno Pomoc
Katalog główny konsoli
Typ obiektu
Akcje
Osobisty
Więcej akcji
Kreator importu certyfikatów
Ochrona klucza prywatnego
W celu zapewnienia bezpieczeństwa klucz prywatny jest chroniony hasłem.
Wpisz hasło dla klucza prywatnego.
Hasło:
Wyświetl hasło
Opcje importu:
Włącz silną ochronę klucza prywatnego. W przypadku wybrania tej opcji użytkownik będzie informowany o każdym użyciu klucza prywatnego przez aplikację.
Oznacz ten klucz jako eksportowalny. Pozwoli to na późniejsze wykonanie kopii zapasowej lub transport kluczy.
Dołącz wszystkie właściwości rozszerzone.
Dowiedz się więcej o ochronie kluczy prywatnych
Dalej
Anuluj


Konsola1 - [Katalog główny konsoli\Certyfikaty - bieżący użytkownik\Osobisty]
Plik Akcja Widok Ulubione Okno Pomoc
Katalog główny konsoli
Typ obiektu
Akcje
Osobisty
Więcej akcji
Kreator importu certyfikatów
Magazyn certyfikatów
Magazyny certyfikatów to obszary systemowe, w których przechowywane są
System Windows może automatycznie wybrać magazyn certyfikatów; możesz jednak określić inną lokalizację dla certyfikatu.
Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu
Umieść wszystkie certyfikaty w następującym magazynie
Magazyn certyfikatów:
Osobisty
Przeglądaj...
Dowiedz się więcej o magazynach certyfikatów
Dalej
Anuluj





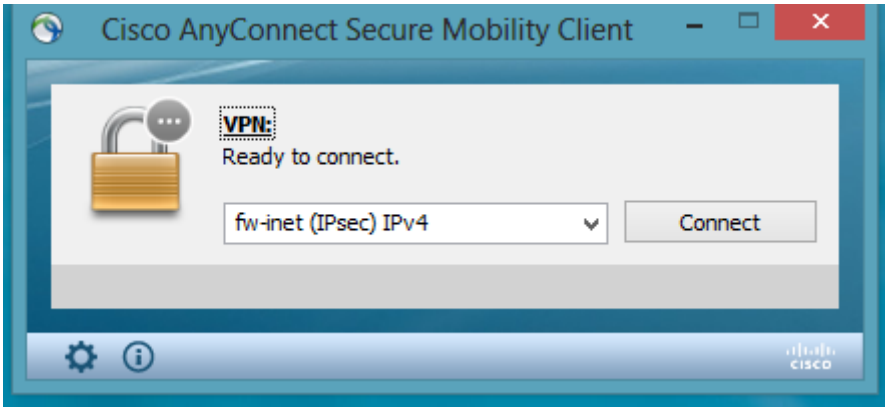
Odpowiednie certyfikaty zostały zaimportowane i można przystąpić do instalacji klienta Cisco AnyConnect.

anyconnect-win-4.2.03013-web-deploy-k9.exe

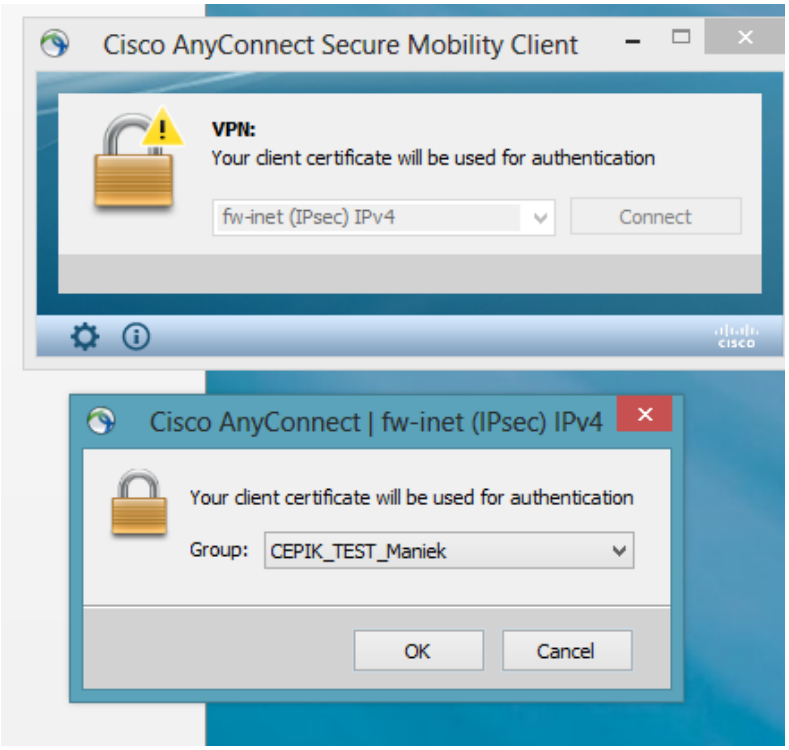
Wraz z certyfikatami Wystawca certyfikatu dostarczy odpowiednio skonfigurowany profil połączeniowy dla klienta Cisco Anyconnect. Instalujemy klienta Cisco AnnyConnect i kolejnym krokiem wgrywamy dostarczony profil do następującego katalogu systemu Windows:

„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 .

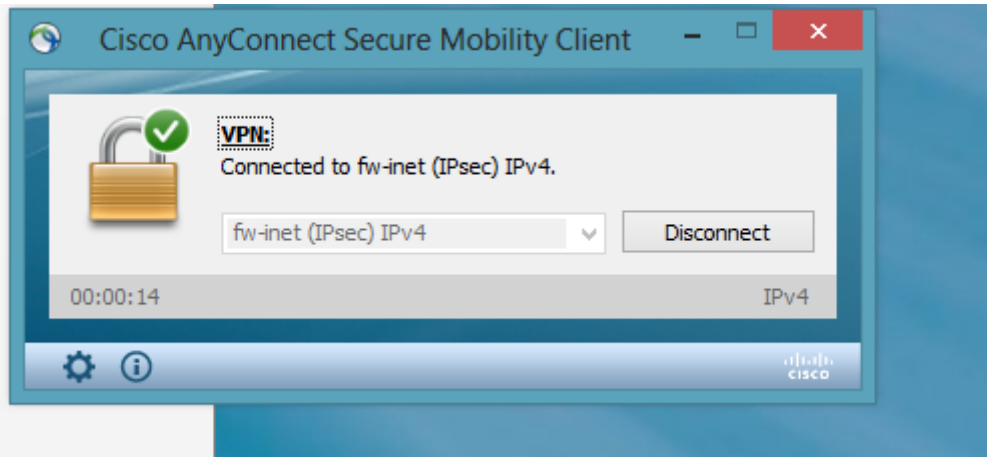


Klikamy **„Connect ”.**



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 sytemu w celu potwierdzenia którą grupę należy wybrać podczas uruchomienia.



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

6. Połączenie typu LAN-TO-LAN

W przypadku połączeń VPN typu LAN-to-LAN urządzenie sieciowe (np. router) należy odpowiednio skonfigurować, aby do połączenia VPN wykorzystywało otrzymany certyfikat wraz z kluczem prywatnym.

Parametry połączenia IPsec:

- ikev1 AES256 HMAC-SHA1,
- host: vpn.cepik.gov.pl lub 185.41.93.4

W celu weryfikacji, czy podmiot posiada zestawione połączenie VPN L2L należy skontaktować się z lokalnym administratorem sieci lub osobą odpowiedzialną w podmiocie za lokalne administrowanie systemem.

CEPiK 2 nie będzie wpierał rozwiązań VPN typu L2L, w związku z tym Service Desk CEPiK nie będzie przyjmował zgłoszeń związanych z połączeniami typu L2L. Takie połączenia są możliwe, ale za ich prawidłową konfigurację po stronie podmiotu odpowiada podmiot.

6.1. Parametry IPSEC

Faza 1

Authentication — Certyfikat

Encryption — AES-256 & SHA

SA Lifetime — 86400

Key Group — 5

Faza 2

ESP-AES-256-SHA