

Problemy z konfiguracją Cisco VPN Client

Poniższe czynności należy wykonać na koncie użytkownika posiadającego uprawnienia do konfiguracji Cisco VPN Client lub administratora.

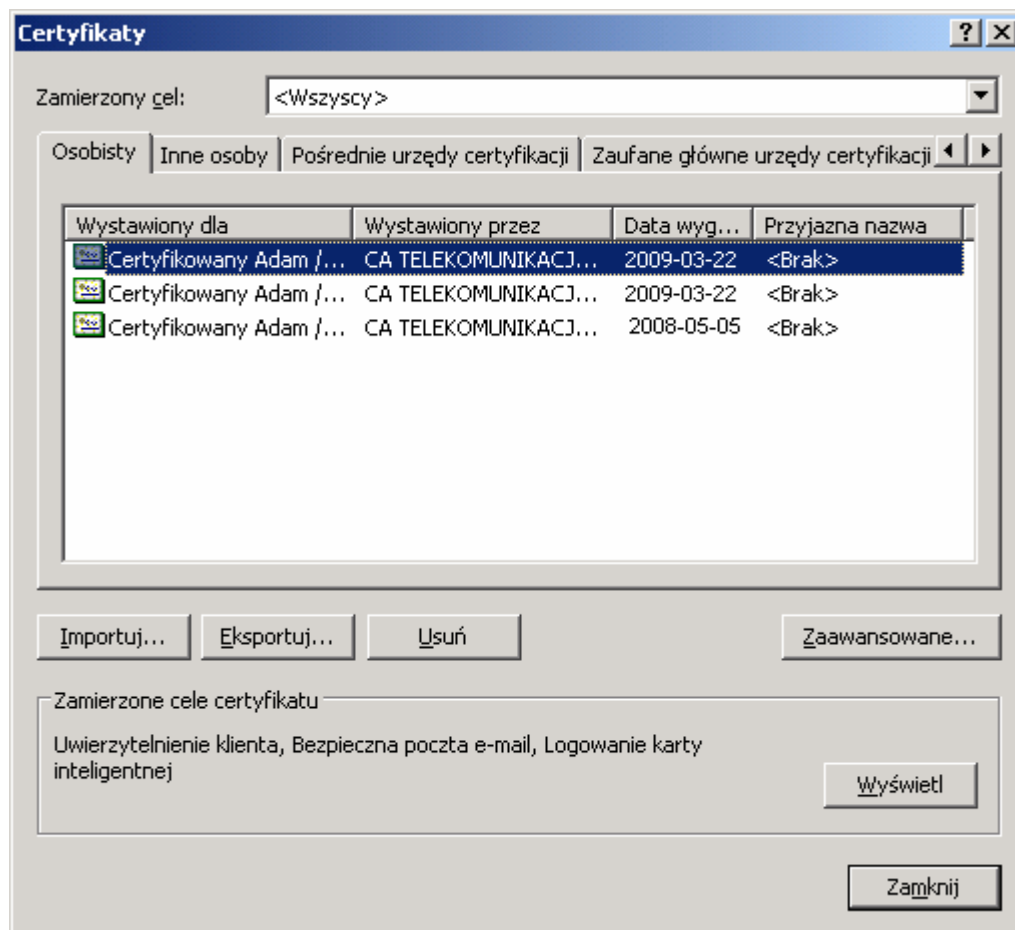
Aplikacja **Cisco VPN Client** nie posiada funkcjonalności umożliwiającej rozróżnienie certyfikatów oraz sprawdzenia ich ważności na podstawie listy CRL. Umożliwia jedynie wyświetlenie listy posiadanych w systemie certyfikatów oraz blokuje użycie certyfikatów wygasłych.

W przypadku posiadania więcej niż 2 certyfikatów (np. 2 ważne certyfikaty oraz unieważniony ale nie wygasły certyfikat do szyfrowania) może pojawić się problem ze wskazaniem ważnego certyfikatu do podpisu, używanego do uwierzytelnienia.

Poniższe rozwiązanie pozwoli na jednoznaczne wskazanie certyfikatu do podpisu w kliencie Cisco VPN.

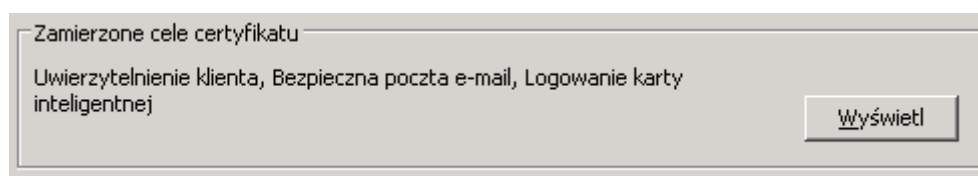
W aplikacji Cisco VPN Client, użycie opcji Delete w zakładce Certificate powoduje nieodwracalne usunięcie obiektów z tokenu lub karty!

1. Zamknąć wszystkie aplikacje, które korzystają z certyfikatów (**Internet Explorer, Outlook, Cisco VPN Client**)
2. W zależności od posiadanego typu urządzenia kryptograficznego:
 - *Aladdin*: Podłączyć token do komputera i odczekać kilka sekund aby certyfikaty zostały zainstalowane w systemie
 - *Gemplus*: Włożyć kartę do czytnika komputera i odczekać kilka sekund aby certyfikaty zostały zainstalowane w systemie (w pasku zadań na ikonie symbolizującej czytnik pojawia się migający czerwony punkt)
3. Otworzyć przeglądarkę **Microsoft Internet Explorer** a następnie z menu **Narzędzia** wybrać **Opcje internetowe**
4. Odnaleźć i wskazać zakładkę **Zawartość** a następnie nacisnąć przycisk **Certyfikaty**
5. W oknie **Certyfikaty** w zakładce **Osobisty** odszukać certyfikaty wystawione przez *CA Telekomunikacja Polska* – czyli używane w usłudze BPTP

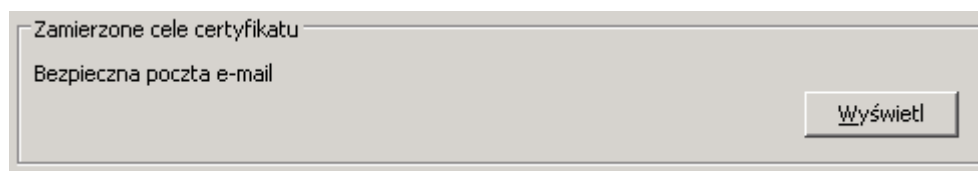


Certyfikaty rozróżniamy na podstawie informacji wyświetlanych w sekcji **Zamierzone cele certyfikatu**.

Dla certyfikatów do podpisu wyświetlana jest informacja:



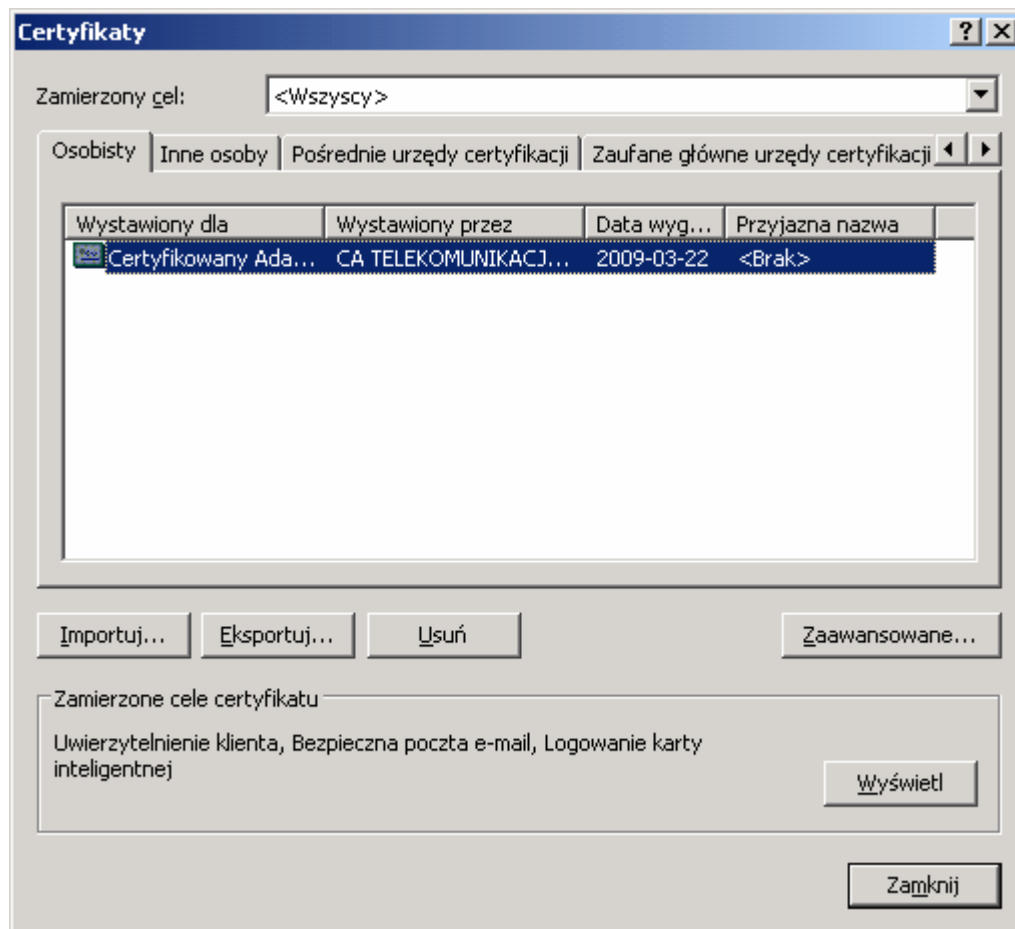
Dla certyfikatów do szyfrowania wyświetlana jest informacja:



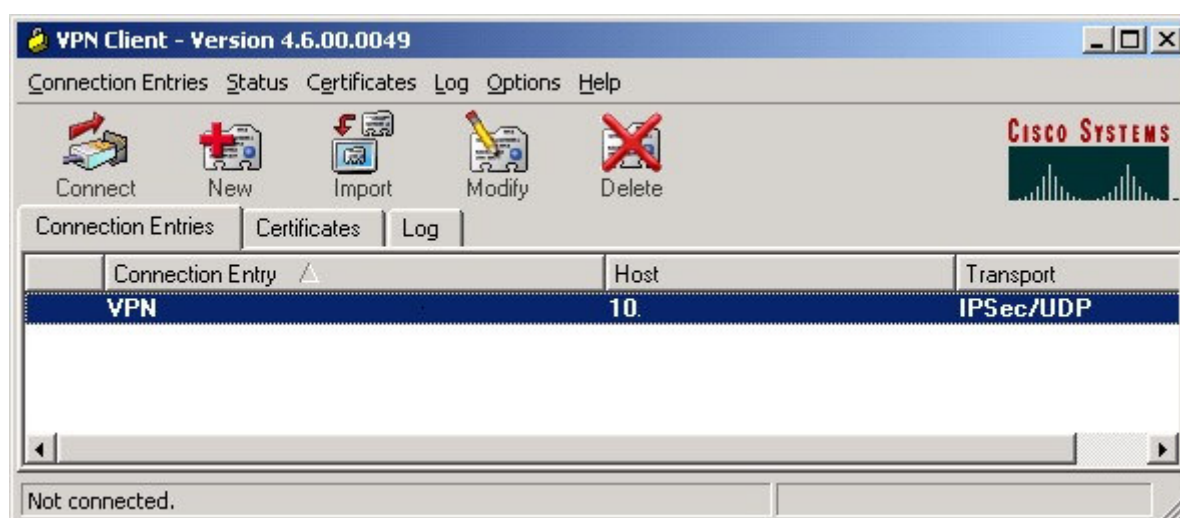
Ponieważ chcemy skonfigurować w kliencie Cisco certyfikat do podpisu dokonamy chwilowego usunięcia pozostałych certyfikatów z systemu certyfikatu poprzez:

- a) zaznaczenie certyfikatu do szyfrowania BPTP
- b) naciśnięcie przycisku **Usuń**
- c) potwierdzenie zgody na usunięcie certyfikatu

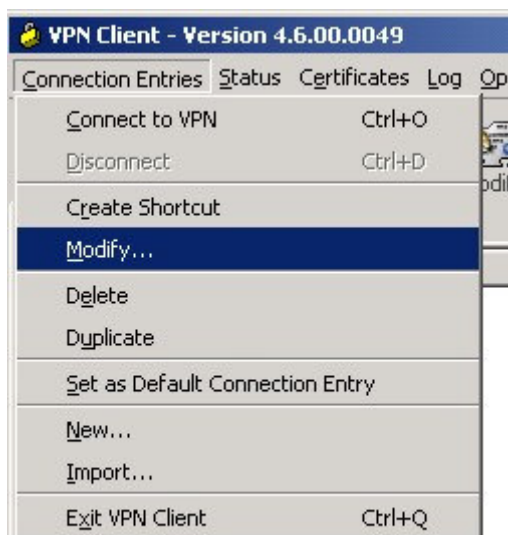
Po wykonaniu tych operacji pozostanie w systemie tylko jeden certyfikat BPTP - do podpisu wystawiony przez *CA Telekomunikacja Polska*



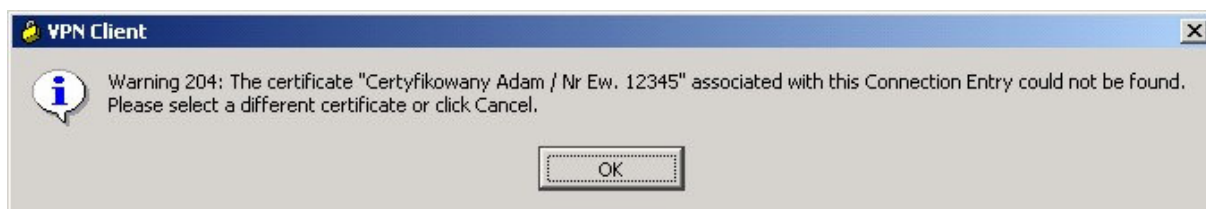
6. Naciskamy przycisk **Zamknij** aby zamknąć okno **Certyfikaty** a następnie zamykamy **Internet Explorer**
7. Z menu **Start** wybrać **Programy->Cisco Systems-> VPN ClientVPN Klient**
8. Aplikacja po uruchomieniu ma widok zbliżony do poniższego



Następnie z menu **Conection Entries** wybrać opcję **Modify**.

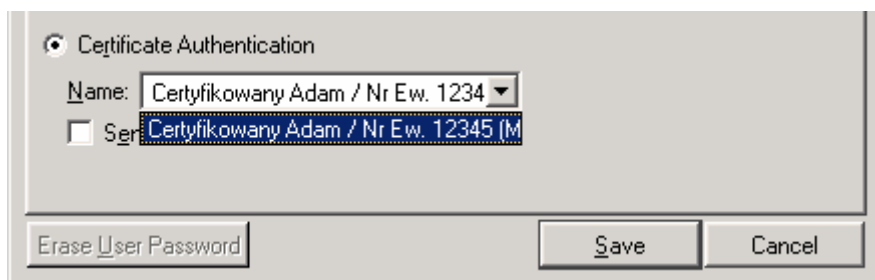


Może pojawić się okno o braku w systemie poprzednio użytego certyfikatu



W treści ostrzeżenia będą dane wskazujące na certyfikat, który był poprzednio używany i obecnie nie ma go w systemie. Naciskamy przycisk **OK**.

9. W oknie właściwości połączenia VPN przejść do grupy **Certificate Authentication**.



Z rozwijanego menu **Name** wybrać jedyny istniejący w systemie certyfikat wystawiony przez *CA Telekomunikacja Polska* następnie nacisnąć przycisk **Save**.

10. Zamknąć aplikację **Cisco VPN Client** i odłączyć token od komputera lub wyjąć kartę z czytnika.

11. Podłączyć token do komputera lub włożyć kartę do czytnika i odczekać kilka sekund aby wszystkie certyfikaty zostały ponownie zainstalowane w systemie.