

## **Informacje ogólne**

### **1. Wymagania dla aplikacji eToken RTE oraz tokenu Aladdin eToken PRO**

- Komputer PC z minimum 10 MB wolnej przestrzeni dyskowej
- Windows 2000 SP4, Windows XP
- Wolny port USB
- Włączony interfejs USB

### **2. Informacja o funkcjonalności tokenu Aladdin eToken PRO**

- Dla nowych użytkowników usługi BPTP na tokenie znajdują się 2 certyfikaty (do podpisu i do szyfrowania) wraz z 2 kluczami prywatnymi
- Dla dotychczasowych użytkowników usługi BPTP na tokenie znajdują 2 nowe certyfikaty (do podpisu i do szyfrowania) wraz z 2 kluczami prywatnymi oraz uprzednio posiadane certyfikaty i klucze do szyfrowania
- Token umożliwia wygenerowanie/osadzenie do 7 kluczy RSA 1024 bity
- Token posiada zarówno PIN użytkownika jak i administratora
- Korzystający z usługi BPTP znają jedynie PIN użytkownika
- Limit błędnych wprowadzeń PINu (użytkownika jak i administratora) wynosi 3

### **3. Informacja o funkcjonalności oprogramowania eToken Properties**

- Nie pokazuje informacji o liczbie pozostałych prób wprowadzenia PINu
- Posiada funkcjonalność autorejestracji certyfikatów w systemie
- Umożliwia zmianę PINu użytkownika
- Posiada zablokowaną funkcjonalność instalacji/usuwania certyfikatów i kluczy
- Wymusza stosowanie złożonych PINów

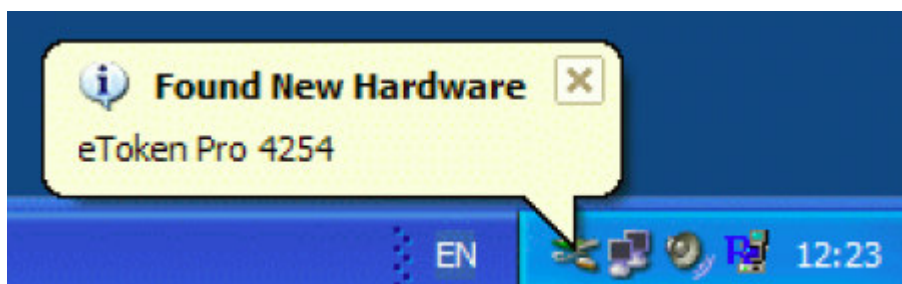
### **4. Uwagi**

- Pierwsze podłączenie tokenu do komputera należy wykonać dopiero po instalacji oprogramowania.
- Do wykonania wielu czynności konfiguracyjnych niezbędne jest posiadanie konta Administratora lokalnego z uprawnieniami umożliwiającymi instalację/usuwanie oprogramowania
- W aplikacji Cisco VPN Client, użycie opcji Delete w zakładce Certificate powoduje nieodwracalne usunięcie obiektów z tokenu
- Może powodować utrudnienia w jednoczesnym korzystaniu z kart Gemplus

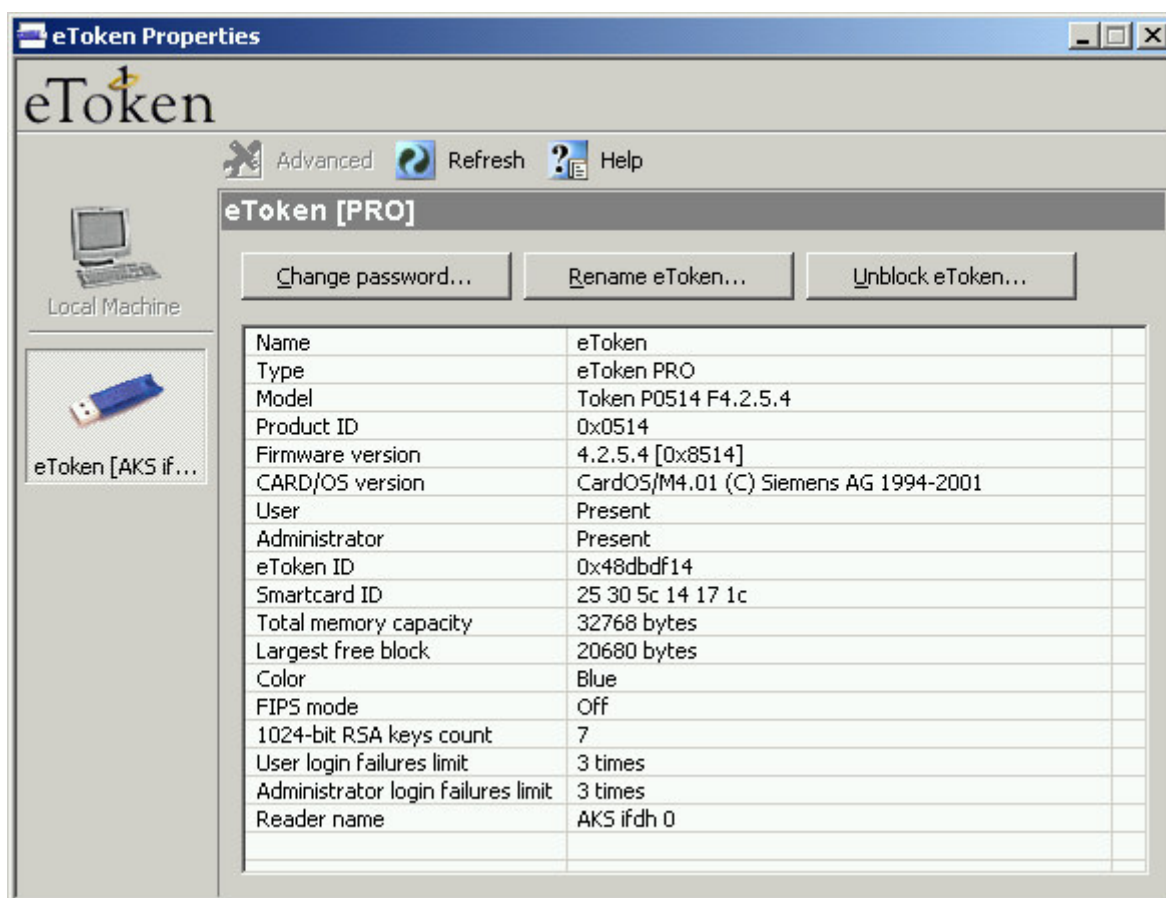
## Sprawdzenie poprawności instalacji

Poniższe czynności można wykonać na dowolnym koncie użytkownika

Zalogować się na konto użytkownika a następnie włożyć po raz pierwszy token Aladdin do portu USB. Przez kilka sekund będzie trwało wykrywanie urządzenia przez system oraz konfiguracja w systemie. Widoczne jest wówczas migotanie czerwonej diody umieszczonej w tokenie. Pojawi się także informacja wykryciu nowego sprzętu:

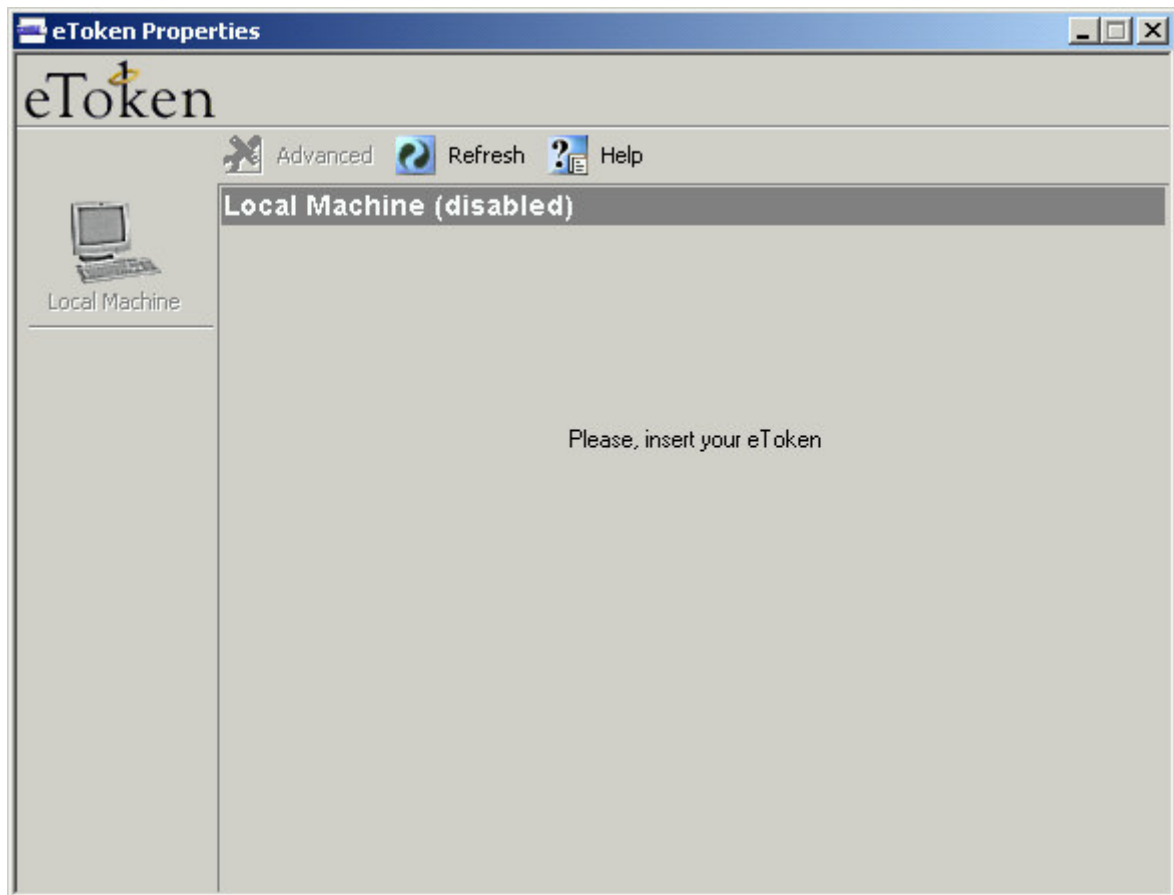


Z menu **Start** wybrać **Programy->eToken->eToken Properties**, pojawi się następujące okno:



W oknie tym można zobaczyć podstawowe informacje o posiadanym tokenie oraz wykonać kilka prostych operacji z zakresu zarządzania tokenem. Szczególnie istotna jest informacja zapisana w polu **eToken ID** będąca numerem seryjnym pozwalającym na

jednoznaczną identyfikację tokenu. Jeżeli w trakcie przeglądania informacji w aplikacji **eToken Properties** usuniemy token z portu USB wówczas zniknie ikona symbolizująca token oraz znikną informacje o własnościach tego urządzenia.



Zamknąć aplikację **eToken Properties** i ponownie umieścić token w porcie USB - sprawdzimy działanie autorejestracji certyfikatów w systemie:

1. Otworzyć przeglądarkę **Microsoft Internet Explorer** a następnie z menu **Narzędzia** wybrać **Opcje internetowe**
2. Odnaleźć i wskazać zakładkę **Zawartość** a następnie nacisnąć przycisk **Certyfikaty**
3. W oknie **Certyfikaty** w zakładce **Osobisty** odszukać certyfikaty wystawione przez *CA Telekomunikacja Polska*.
4. Powinny być widoczne co najmniej 2 certyfikaty wystawione dla użytkownika będącego posiadaczem tokenu

## Używanie tokenu w aplikacjach i informacje o PIN'ie

Większość aplikacji, które chcą wykorzystać klucze prywatne znajdujące się na tokenie będzie wyświetlała okno **eToken Base Cryptographic Provider** żądające podania PIN'u użytkownika.



PIN wprowadzamy w polu **Password** a następnie naciskamy przycisk **OK**.

**Każdy użytkownik posiada 3 próby wprowadzenia PIN'u.**

Jeżeli w oknie do wprowadzania PIN'u zostanie wprowadzony błędny PIN aplikacja wyświetli okno **eToken Error** z ostrzeżeniem o nieudanym uwierzytelnieniu.



Akceptujemy ostrzeżenie naciskając przycisk **OK**.

Pojawi się ponownie okno do wprowadzenia PIN'u ale tym razem zawiera ostrzeżenie o możliwości zablokowania tokenu poprzez wprowadzanie nieprawidłowego PIN'u



Jeżeli nie wprowadzimy poprawnego PIN'u każde następne okno z monitem o PIN będzie zawierało ostrzeżenie o możliwości zablokowania tokenu (prawy, górny róg okna).

**Jeżeli 3 krotnie zostanie wprowadzony niepoprawny PIN wówczas funkcja PIN'u użytkownika zostaje zablokowana.**

Możliwość odblokowania takiego tokenu jest możliwa jedynie poprzez znajomość PIN'u administratora będącego w posiadaniu Centrum Certyfikacji Signet.

Niestety oprogramowanie dostarczane przez producenta nie zawiera funkcjonalności pozwalającej na sprawdzenie ilości pozostałych prób wprowadzenia PIN'u. Ponadto informacja o tym, że dany token posiada zablokowany PIN użytkownika nie jest nigdzie bezpośrednio widoczna. Jedynie gdy PIN użytkownika jest już zablokowany po wprowadzeniu PIN'u (niezależnie czy jest poprawny czy też nie) pokazuje się okno z ostrzeżeniem o jego blokadzie.



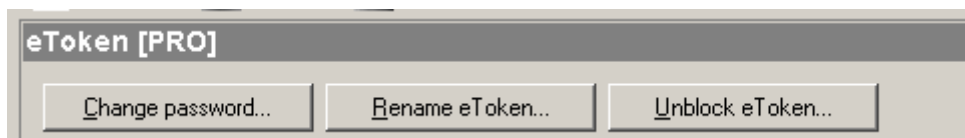
Aplikacja **eToken Properties** przez cały czas pokazuje jedynie informację o ilości dostępnych standardowo prób wprowadzenia PIN, niezależnie od jego stanu co może dodatkowo komplikować sytuację.

FIPS mode	Off
1024-bit RSA keys count	7
User login failures limit	3 times
Administrator login failures limit	3 times
Reader name	AKS ifdh 0

## Zmiana PIN'u

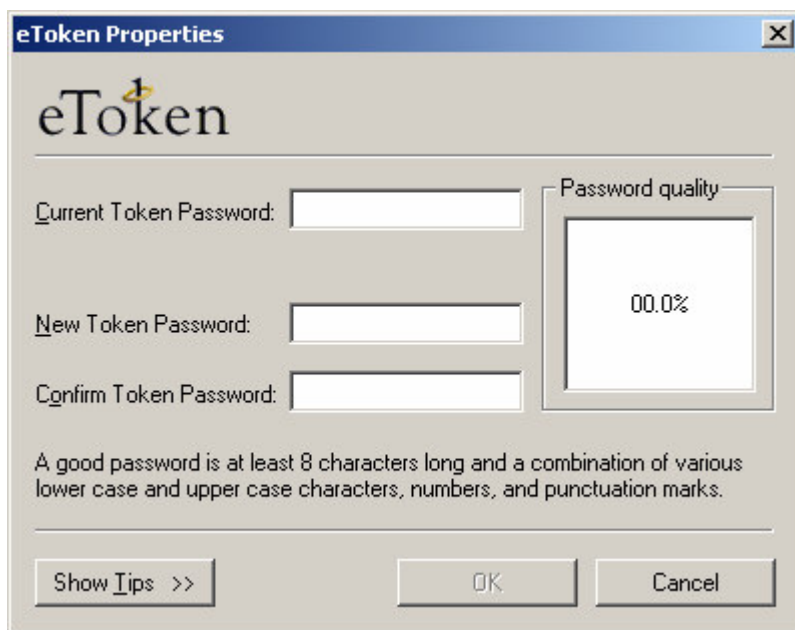
Każdy token Aladdin w usłudze Bezpieczna Poczta TP posiada nadany PIN użytkownika, który zostaje przesłany e-mailem na adres w poczcie korporacyjnej (podany w certyfikacie). Jest wskazane aby użytkownik samodzielnie zmienił otrzymany PIN na swój własny, które będzie mu łatwiej zapamiętać oraz będzie miał pewność, że nikt poza nim go nie zna.

Aplikacja **eToken Properties** umożliwia w prosty sposób zmianę PIN'u wymuszając stosowanie złożonych PIN'ów. Z menu **Start** wybrać **Programy->eToken->eToken Properties**, pojawi się okno aplikacji w którym naciskamy przycisk **Change Pasword**.

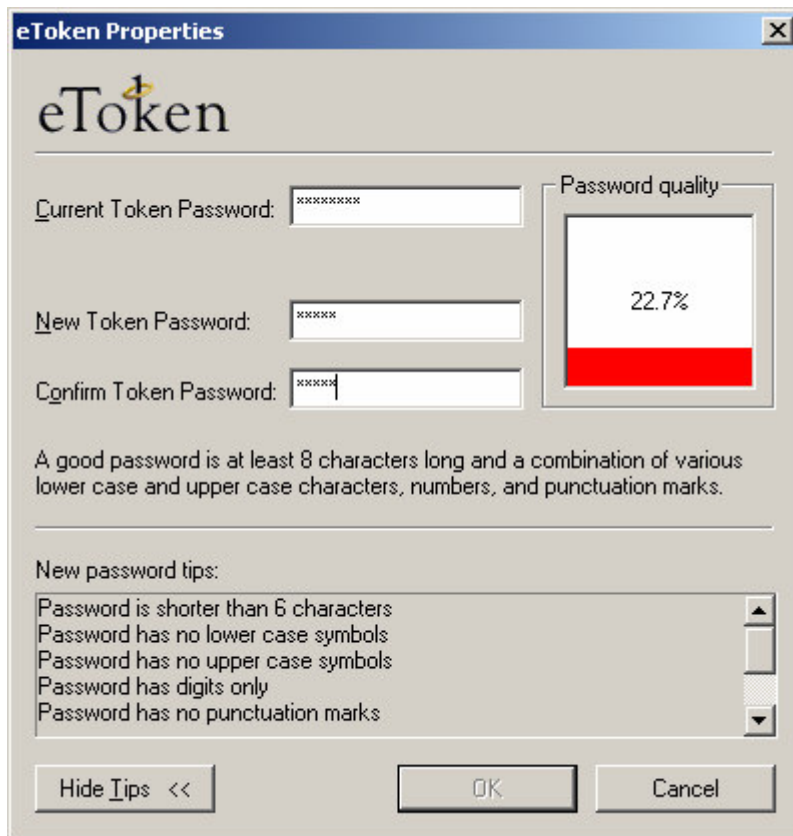


W oknie do zmiany PIN'u widoczne są pola:

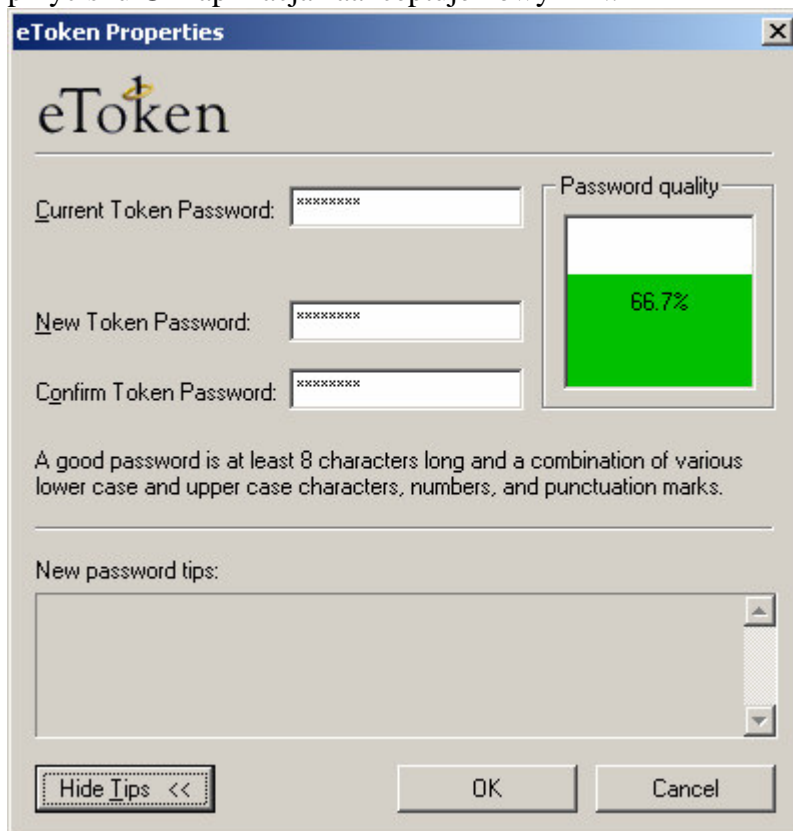
- **Current Token Password** - wprowadzenie aktualnego PIN'u
- **New Token Password** - wprowadzenie nowego PIN'u
- **Confirm Token Password** - potwierdzenie nowego PIN'u
- **Password quality** - wskaźnik jakości nowego PIN'u



Okno **Password Quality** w miarę wprowadzania nowego PIN'u w polu **New Token Password** będzie wskazywać jakość PIN'u. Wymagany jest co najmniej 6 znakowy PIN, dla którego wskaźnik jakości osiągnie wartość co najmniej 30%. Jeżeli wprowadzimy zbyt prostą propozycję PIN'u aplikacja uniemożliwi akceptację takiego PIN'u oraz w sekcji **New password tips** (widoczne po naciśnięciu przycisku **Show Tips>>**) wskaże wady zaproponowanego PIN'u.



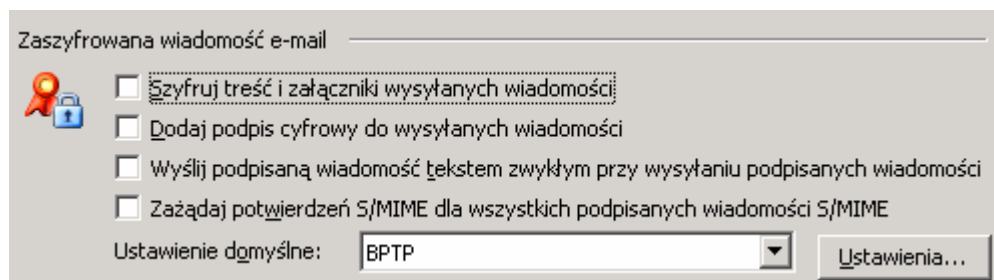
Jeżeli wprowadzimy natomiast jako nowy PIN ciąg znaków składający się z nie powtórzonych cyfr, małych i dużych liter (nie można wprowadzać polskich liter!) oraz znaków specjalnych wówczas wskaźnik przekroczy wartość 30% i po naciśnięciu przycisku **OK** aplikacja zaakceptuje nowy PIN.



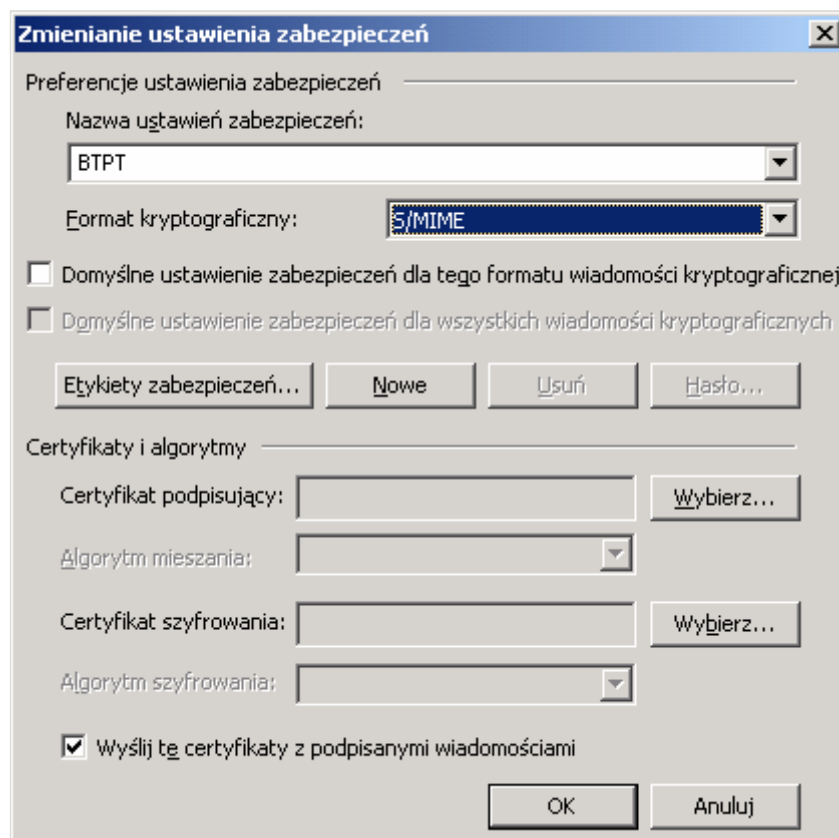
## Konfiguracja klienta pocztowego Outlook

*Poniższe czynności należy wykonać na koncie użytkownika*

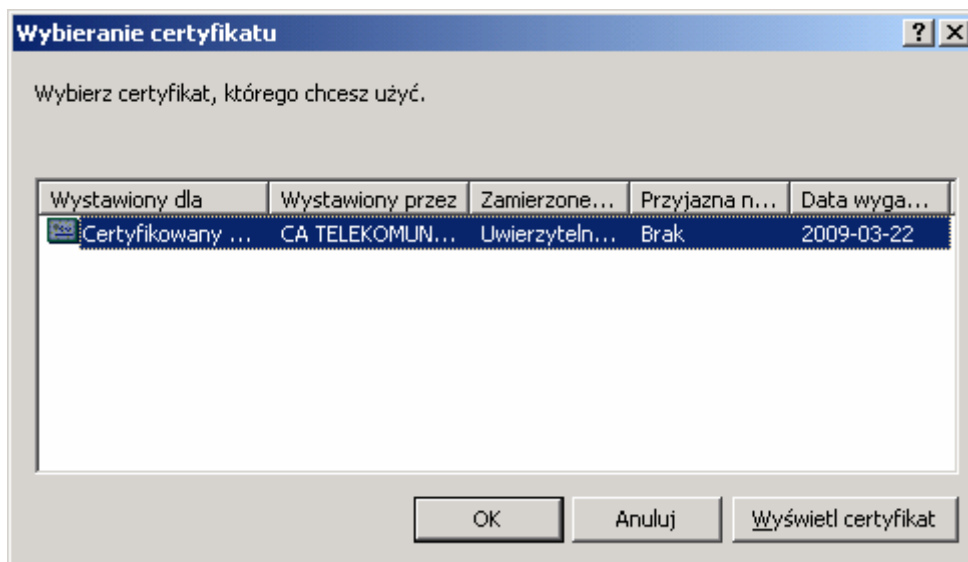
1. Uruchomić klienta pocztowego **Microsoft Outlook**
2. Z menu **Narzędzia** wybrać **Opcje**
3. W oknie **Opcje** przejść do zakładki **Zabezpieczenia**
4. W sekcji **Zaszyfrowana wiadomość e-mail** naciskamy przycisk **Ustawienia**



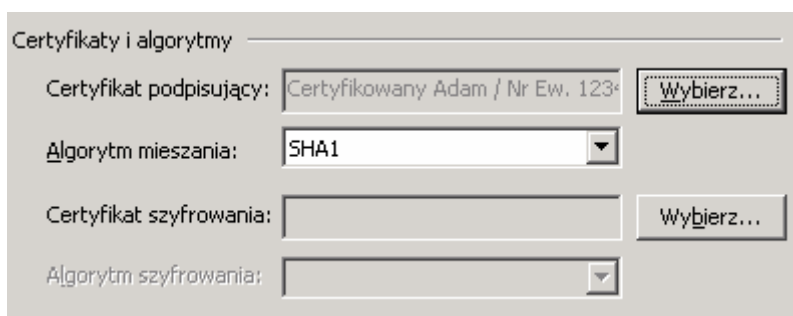
5. W oknie **Zmianie ustawienia zabezpieczeń** przechodzimy do sekcji **Certyfikaty i algorytmy**



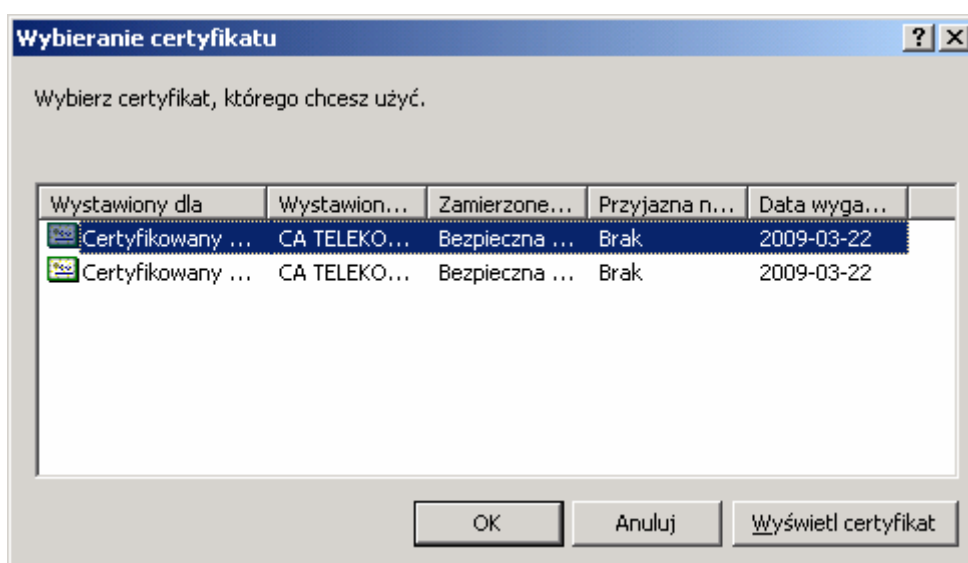
6. Pola wskazujące na certyfikaty do podpisu i do szyfrowania powinny być puste gdyż w punkcie **Odrejestrowanie certyfikatów** usunęliśmy certyfikaty z systemu. Następnie przy polu **Certyfikat podpisujący** naciskamy przycisk **Wybierz**. Pojawi się okno **Wybieranie certyfikatu**, w którym będzie widoczny zawsze tylko jeden certyfikat do podpisu wystawiony przez **CA TELEKOMUNIKACJA POLSKA**



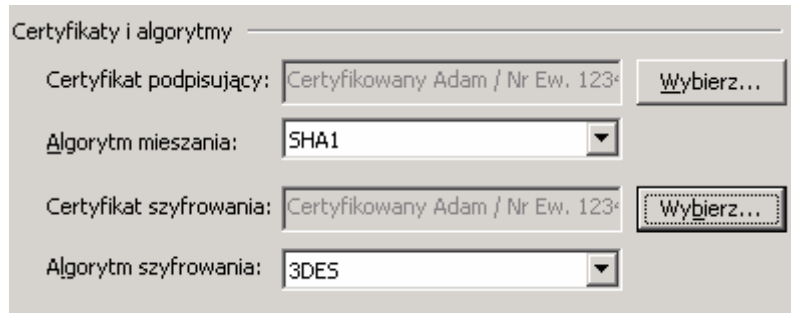
Zaznaczamy certyfikat i naciskamy przycisk **OK**. Outlook zaktualizuje informacje o certyfikacie podpisującym.



Następnie przy polu **Certyfikat szyfrowania** naciskamy przycisk **Wybierz**. Pojawi się okno **Wybieranie certyfikatu**, w którym będzie widoczny zawsze jeden lub więcej certyfikatów do szyfrowania wystawionych przez *CA TELEKOMUNIKACJA POLSKA*



Należy przyjąć zasadę, żeby spośród tych certyfikatów zawsze wskazywać na certyfikat najnowszy, który posiada zapisana w polu **Data wygaśnięcia** późniejszą datę. Zaznaczamy certyfikat i naciskamy przycisk **OK**. Outlook zaktualizuje informacje o certyfikacie szyfrującym.



The image shows a dialog box titled "Certyfikaty i algorytmy". It contains four rows of settings:

- Certyfikat podpisujący:** A text box containing "Certyfikowany Adam / Nr Ew. 123" and a "Wybierz..." button.
- Algorytm mieszania:** A dropdown menu with "SHA1" selected.
- Certyfikat szyfrowania:** A text box containing "Certyfikowany Adam / Nr Ew. 123" and a "Wybierz..." button.
- Algorytm szyfrowania:** A dropdown menu with "3DES" selected.

Zamykamy wszystkie otwarte okna akceptując wprowadzone zmiany. Konfiguracja Outlooka została zakończona.

## Problemy z konfiguracją Cisco VPN Client

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

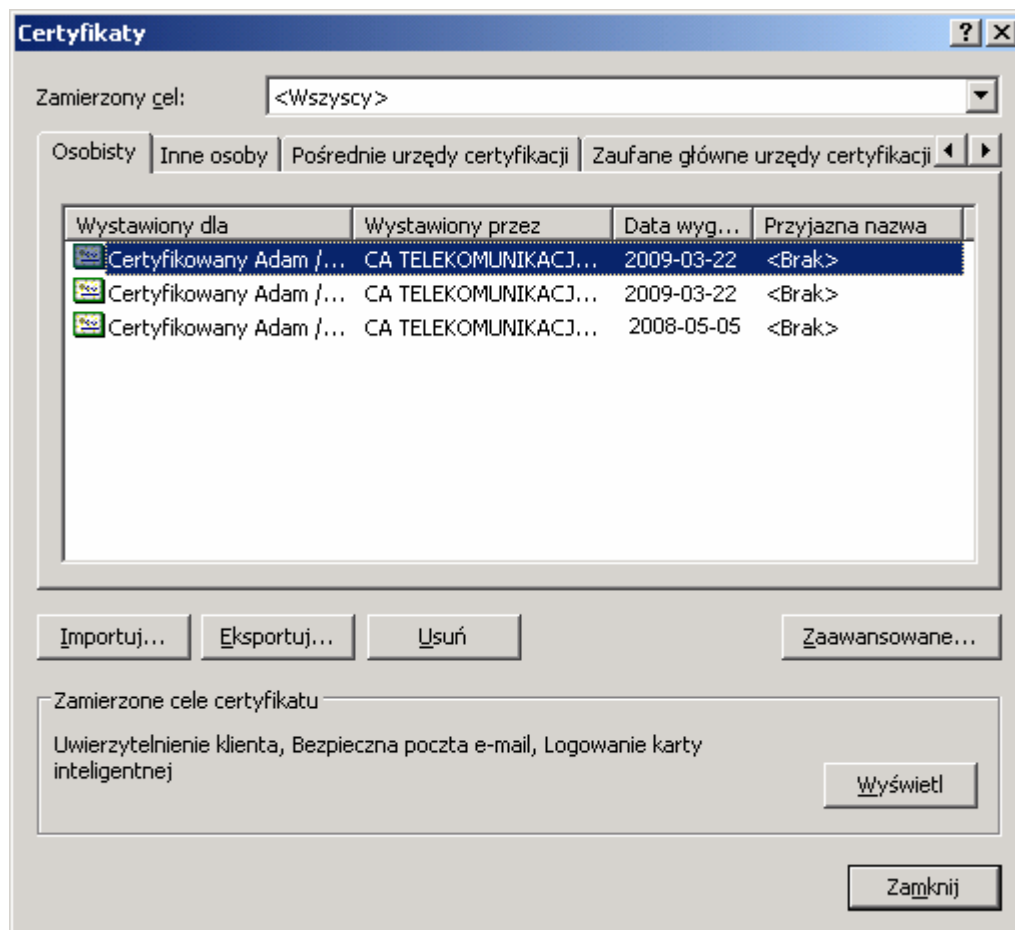
Aplikacja **Cisco VPN Client** nie posiada funkcjonalności umożliwiającej rozróżnienie certyfikatów oraz sprawdzenia ich ważności na podstawie listy CRL. Umożliwia jedynie wyświetlenie listy posiadanych w systemie certyfikatów oraz blokuje użycie certyfikatów wygasłych.

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.

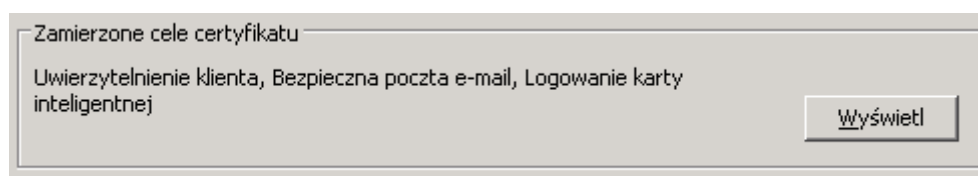
**W aplikacji Cisco VPN Client, użycie opcji Delete w zakładce Certificate powoduje nieodwracalne usunięcie obiektów z tokenu**

1. Zamknąć wszystkie aplikacje, które korzystają z certyfikatów (**Internet Explorer, Outlook, Cisco VPN Client**)
2. Podłączyć token do komputera i odczekać kilka sekund aby certyfikaty zostały zainstalowane w systemie
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

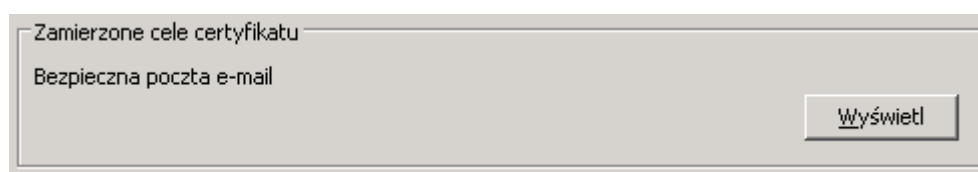


Certyfikaty rozróżniamy na podstawie informacji wyświetlanych w sekcji **Zamierzone cele certyfikatu**.

Dla certyfikatów do podpisu wyświetlana jest informacja:



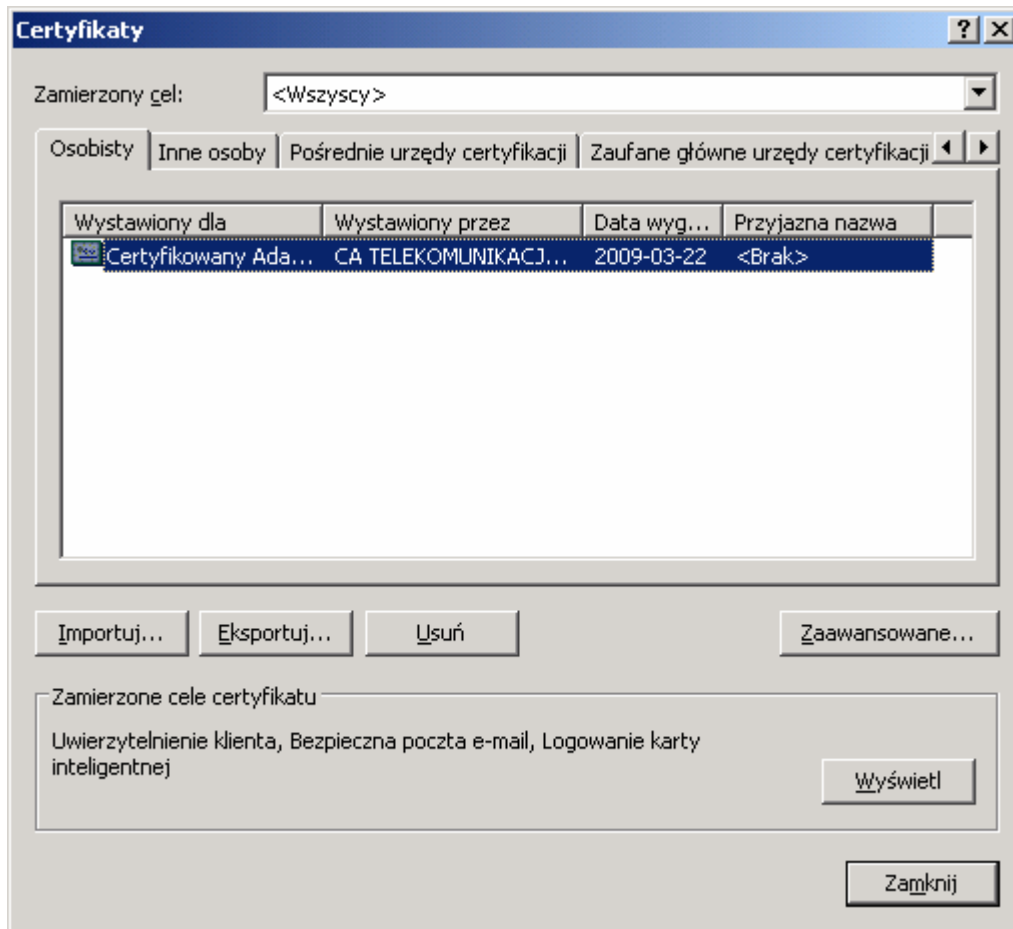
Dla certyfikatów do szyfrowania wyświetlana jest informacja:



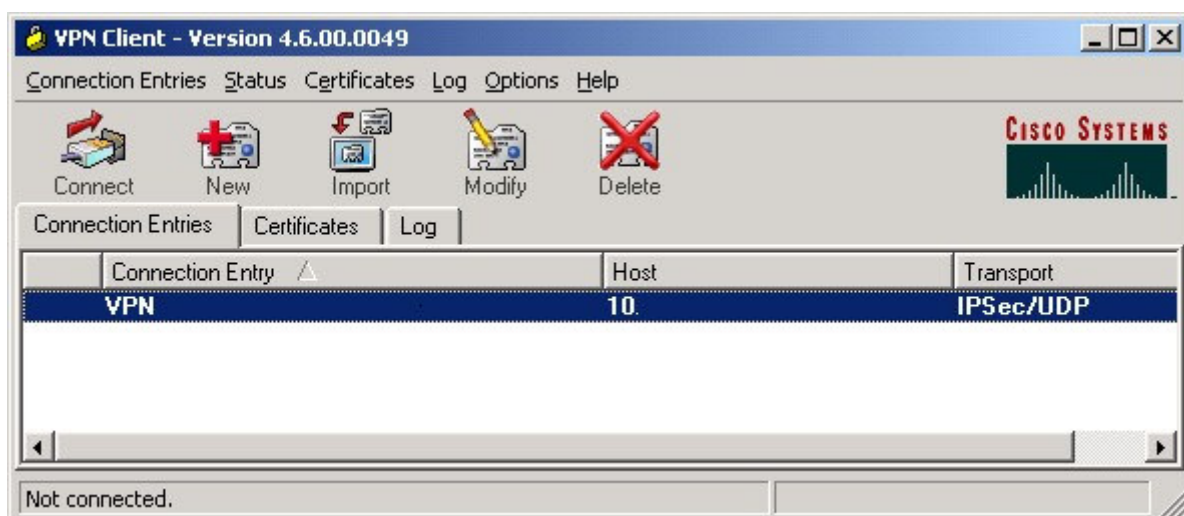
Ponieważ chcemy skonfigurować w kliencie Cisco certyfikat do podpisu dokonamy chwilowego usunięcia pozostałych certyfikatów z systemu certyfikatu poprzez:

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

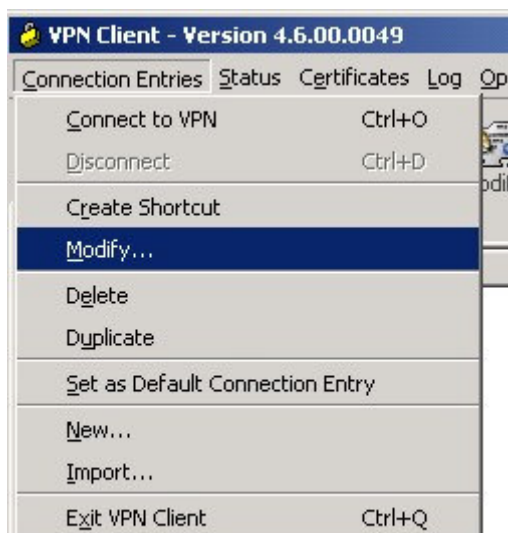
Po wykonaniu tych operacji pozostanie w systemie tylko jeden certyfikat BPTP - do podpisu wystawiony przez *CA Telekomunikacja Polska*



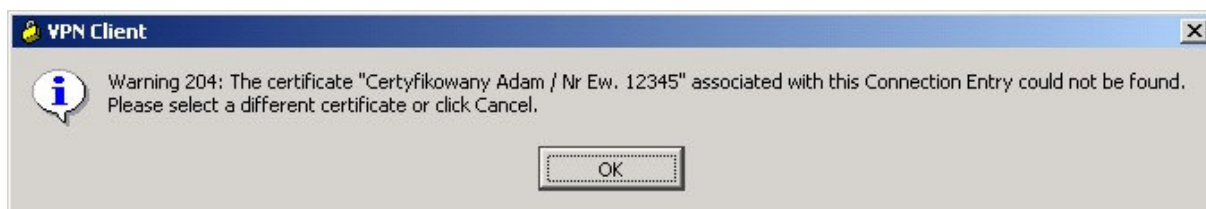
6. Naciskamy przycisk **Zamknij** aby zamknąć okno **Certyfikaty** a następnie zamykamy **Internet Explorer**
7. Z menu **Start** wybrać **Programy->Cisco Systems-> VPN ClientVPN Klient**
8. Aplikacja po uruchomieniu ma widok zbliżony do poniższego



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

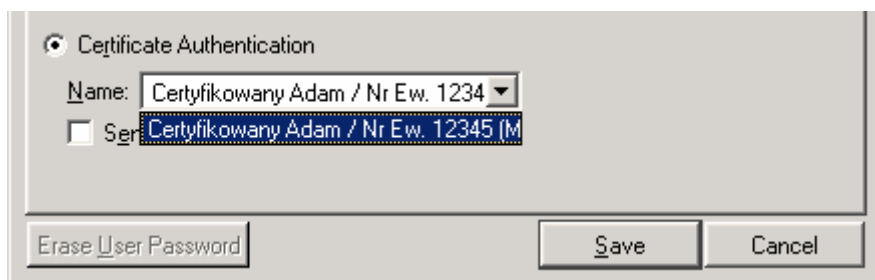


Może pojawić się okno o braku w systemie poprzednio użytego certyfikatu



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

11. Podłączyć token do komputera i odczekać kilka sekund aby certyfikaty zostały ponownie zainstalowane w systemie