

**CryptoTech**  
eSECURITY SOLUTIONS

# **Oprogramowanie CryptoCard Suite**

---

**Podręcznik użytkownika**

Wersja dokumentu: 0.9.6  
Data aktualizacji: 2004-07-16

# Spis treści

<b>1. WPROWADZENIE .....</b>	<b>3</b>
1.1. KONWENCJE DOKUMENTACJI .....	3
1.2. O ZESTAWIE CRYPTO CARD SET .....	3
1.3. SŁOWNIK POJĘĆ .....	4
<b>2. INSTALACJA PAKIETU CRYPTOCARD SUITE .....</b>	<b>6</b>
2.1. WYMAGANIA SYSTEMOWE APLIKACJI CRYPTO CARD SUITE .....	6
2.2. INSTALACJA PAKIETU CRYPTO CARD SUITE .....	6
2.3. SPRAWDZENIE POPRAWNOŚCI INSTALACJI .....	7
2.4. PRZYGOTOWANIE KARTY DO PRACY .....	9
2.5. BLOKOWANIE MOŻLIWOŚCI UŻYCIA KWALIFIKOWANEJ CZĘŚCI KARTY CRYPTO CARD MULTISIGN ....	12
2.6. KONFIGURACJA PROGRAMU CRYPTO CARD SUITE .....	13
2.7. ODINSTALOWANIE PAKIETU CRYPTO CARD SUITE .....	14
2.8. GDY WYSTĄPIĄ PROBLEMY .....	15
<b>3. UZYSKANIE CERTYFIKATU .....</b>	<b>17</b>
3.1. PRZYGOTOWANIE WNIOSKU O CERTYFIKACJĘ W FORMACIE PKCS#10 .....	17
3.2. IMPORT CERTYFIKATÓW ORAZ KLUCZY NA KARTĘ .....	19
3.3. REJESTRACJA CERTYFIKATU W SYSTEMIE .....	22
3.4. UZYSKANIE CERTYFIKATU ON-LINE NA PRZYKŁADZIE CENTRUM CERTYFIKACJI W DOMENIE ACTIVE DIRECTORY .....	23
3.5. KONFIGURACJA CERTYFIKATU DO LOGOWANIA W WINDOWS .....	27
<b>4. ZASTOSOWANIE KARTY CRYPTOCARD MULTISIGN DO ZABEZPIECZANIA POCZTY ELEKTRONICZNEJ (NA PRZYKŁADZIE MS OUTLOOK EXPRESS 6.0) .....</b>	<b>29</b>
4.1. INSTALACJA CERTYFIKATÓW W PROGRAMIE OUTLOOK EXPRESS .....	29
4.2. PODPISYWANIE WIADOMOŚCI POCZTY ELEKTRONICZNEJ .....	30
4.3. WERYFIKACJA POPRAWNOŚCI PODPISU W OTRZYMANEJ WIADOMOŚCI E-MAIL .....	31
4.4. SZYFROWANIE WIADOMOŚCI POCZTY ELEKTRONICZNEJ .....	32
4.5. DESZYFROWANIE WIADOMOŚCI POCZTY ELEKTRONICZNEJ .....	33

# 1. Wprowadzenie

## 1.1. Konwencje dokumentacji

W celu ułatwienia posługiwania się niniejszym podręcznikiem przyjęliśmy następujące konwencje.

Krój czcionki	Znaczenie
<b>tekst wytłuszczony</b>	termin, który należy zapamiętać. Są to pojęcia, które są szeroko używane w dokumentacji i ich zapamiętanie ułatwi zrozumienie tego podręcznika jak i pozostałej dokumentacji pakietu CryptoCard Suite 1.0
<i>kursywa</i>	Oznacza przytoczenie terminu obcojęzycznego.

## 1.2. O zestawie CryptoCard Set

CryptoCard Set to zestaw składający się z karty mikroprocesorowej CryptoCard multiSIGN i towarzyszącego jej oprogramowania CryptoCard Suite.

Karta CryptoCard multiSIGN jest specjalizowaną, kryptograficzną kartą mikroprocesorową przeznaczoną do realizacji kwalifikowanego i niekwalifikowanego podpisu elektronicznego oraz funkcji identyfikacji i silnego uwierzytelniania użytkowników. Karta ta, uzupełniona o oprogramowanie podpisujące i uwierzytelniające, stanowi doskonałe narzędzie wspierające szeroką gamę rozwiązań pracujących w ramach Infrastruktury Klucza Publicznego (PKI). Wsparcie dla dominujących na rynku standardów pozwala na użycie karty w typowych zastosowaniach wewnątrz organizacji (takich jak dostęp do komputerów, sieci czy innych zasobów) oraz w pełni realizować ideę podpisu elektronicznego. CryptoCard multiSIGN wyróżnia się podwójną strukturą obsługiwanych aplikacji, co oznacza, iż potrafi jednocześnie zawierać aplikację do podpisu niekwalifikowanego oraz certyfikowaną aplikację podpisu kwalifikowanego. W tym drugim przypadku karta stanowi komponent techniczny spełniający wymagania prawa polskiego stawiane bezpiecznym urządzeniom do składania kwalifikowanego podpisu elektronicznego.

Karta CryptoCard multiSIGN odznacza się następującymi cechami:

- 32 kB pamięci
- szyfrowanie RSA 1024 bity
- DES, 3DES i MAC realizowane na karcie
- generowanie kluczy na karcie
- wsparcie dla standardów przemysłowych (PKCS#11, PKCS#15, MS CryptoAPI, PC/SC)
- certyfikowane bezpieczeństwo systemu operacyjnego karty ITSEC E3 High
- certyfikowane bezpieczeństwo układu elektronicznego karty ITSEC E4 High

Bezpieczeństwo mechanizmów zarządzania kluczami jest zlokalizowane na karcie. Karta zarówno generuje klucze, jak również podpisuje nimi dane na zlecenie zewnętrznych aplikacji

po weryfikacji kodu PIN. Aplikacje umieszczone na karcie – kwalifikowana i niekwalifikowana są odseparowane i chronione oddzielnymi kodami PIN.

Oprogramowanie CryptoCard Suite realizuje standardy PKCS#11 w wersji 2.01 i 2.11 a wewnętrzne struktury aplikacji są zgodne z PKCS#15. Oprogramowanie to zawiera również certyfikowany przez Microsoft moduł CSP dedykowany do pracy przez interfejs CryptoAPI 2.0. Ponieważ interfejsy te korzystają ze standardu PC/SC możliwe jest korzystanie z szerokiej gamy czytników kart w środowisku Windows.

Zestaw CryptoCard Set współpracuje z oprogramowaniem liderów rynku PKI: Baltimore, RSA Security, Entrust, CheckPoint, Microsoft, Netscape, PGP, Novell i wielu innych.

Najnowsze informacje na temat zmian w oprogramowaniu CryptoCard Suite, znajdują się w pliku ReadMe.txt dołączonym do pakietu instalacyjnego. Plik ten można znaleźć w katalogu, w którym zostało zainstalowane oprogramowanie.

### 1.3. Słownik pojęć

Aby móc szybko rozpocząć używanie aplikacji CryptoCard Suite należy poznać terminologię stosowaną w świecie bezpieczeństwa i kryptografii. Zrozumienie tych kilku pojęć stanowi klucz do swobodnego poruszania się w aplikacji CryptoCard Suite jak i w innych systemach związanych z bezpieczeństwem.

Termin	Znaczenie
PIN	<i>Personal Identification Number</i> . Kod (składający się ze znaków alfanumerycznych), który zabezpiecza aplikację na karcie przed niepowołanym użyciem.
SO PIN	<i>Security Officer Personal Identification Number</i> . Numer podobny do PINu użytkownika jednak ten jest używany tylko w wypadku zablokowania niekwalifikowanej aplikacji karty lub podczas inicjalizacji.
PUK	Personal Unlocking Key. 8-cyfrowy numer, który służy do odblokowania kwalifikowanej części karty CryptoCard multiSIGN. Numer ten jest ustawiany przez użytkownika w trakcie aktywacji kwalifikowanej części karty i <b>nie</b> może zostać zmieniony w trakcie użytkowania.
PASSPHRASE	Hasło dostępu. Pełni taką samą rolę jak numer PIN.
MASTER PASSWORD	Inaczej hasło główne. Nie należy mylić tego hasła z kodem SO PIN ani PUK. Jest to hasło, które uwierzytelnia użytkownika do karty umożliwiając znaczną ingerencję w strukturę niekwalifikowanej części karty CryptoCard multiSIGN.
PKCS	<i>Public Key Cryptography Standard</i> . Nazwa zestawu standardów kryptografii klucza publicznego opracowanych i opublikowanych przez firmę RSA Security.
CA	<i>Certification Authority</i> . Urząd świadczący usługi certyfikacyjne oraz zarządzający wydanymi certyfikatami.
CRL	<i>Certificate Revocation List</i> . Specjalna lista zawierająca wykaz unieważnionych certyfikatów wydanych przez dane CA.

Wszelkie uwagi dotyczące niniejszego dokumentu prosimy kierować pod adres e-mail [dokumentacja@cryptotech.com.pl](mailto:dokumentacja@cryptotech.com.pl).

## 2. Instalacja pakietu CryptoCard Suite

### 2.1. Wymagania systemowe aplikacji CryptoCard Suite

Pakiet CryptoCard Suite jest przeznaczony do pracy w całej rodzinie współczesnych systemów Microsoft Windows. Dokładną listę wspieranych systemów operacyjnych można znaleźć poniżej:

- MS Windows 95 OSR2 \*
- MS Windows 98, 98 SE \*
- MS Windows Me (Millenium Edition) \*
- MS Windows NT 4 (wymagany jest Service Pack 6a)
- MS Windows 2000 (wymagany jest Service Pack 4)
- MS Windows XP (wymagany jest Service Pack 1)

Dodatkowo w systemie musi być zainstalowany Microsoft Internet Explorer w wersji co najmniej 4.0. Na systemach MS Windows 95/98/Me oraz NT 4 konieczne jest zainstalowanie Microsoft Smart Card Base Component, który jest dostępny za darmo do pobrania z Internetu pod adresem <http://www.microsoft.com/downloads/details.aspx?FamilyID=ecbb6433-df44-44f8-a439-e4262d049c1c&DisplayLang=en>

Do używania aplikacji CryptoCard Suite konieczne jest również posiadanie zainstalowanego czytnika kart elektronicznych zgodnego ze standardem PC/SC.

Minimalne wymagania sprzętowe pakietu CryptoCard Suite są zgodne z minimalnymi wymaganiami systemów operacyjnych, w których można zainstalować to oprogramowanie. Jednak w celu bezproblemowej i płynnej pracy zaleca się następująca minimalną konfigurację:

- procesor Celeron 266 MHz
- 64 MB RAM
- co najmniej 10 MB wolnej przestrzeni na dysku (potrzebne do instalacji)

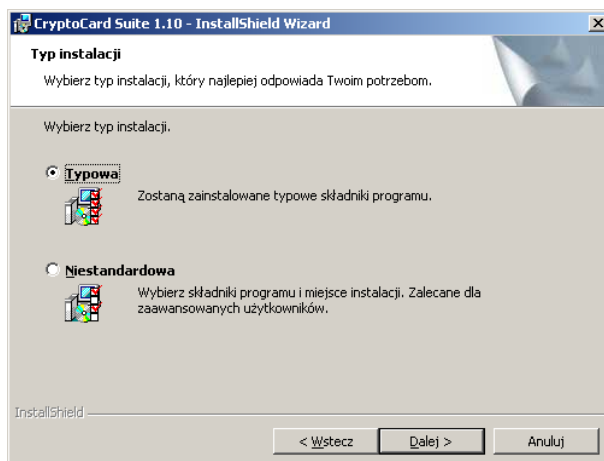
### 2.2. Instalacja pakietu CryptoCard Suite

**UWAGA:** Na systemach NT, 2000 i XP instalacja musi się odbyć z poziomu użytkownika z prawami lokalnego administratora danej maszyny lub administratora domeny NT/Active Directory.

---

\* system wspierany do wersji CryptoCard Suite 1.04.0104. W razie pytań dotyczących wsparcia tego systemu w nowszych wersjach oprogramowania CryptoCard Suite, prosimy o bezpośredni kontakt.

Oprogramowanie CryptoCard Suite jest dostarczane jako pojedynczy plik wykonywalny „setup.exe”. Po uruchomieniu instalatora użytkownik jest prowadzony przez kolejne ekrany, gdzie może dokonać wyboru niektórych ustawień aplikacji CryptoCard Suite. Dostępne są dwie metody instalacji – standardowa, która odznacza się tym, że aplikacja CryptoCard Suite jest instalowana w domyślnym katalogu (C:\Program Files\CryptoTech\CryptoCard) wraz z domyślnym zestawem bibliotek. Druga metoda instalacji – zaawansowana - przeznaczona jest dla użytkowników, którzy chcą dostosować instalację CryptoCard Suite do swoich indywidualnych potrzeb. W obu przypadkach program instalacyjny prowadzi użytkownika przez szereg intuicyjnych ekranów.



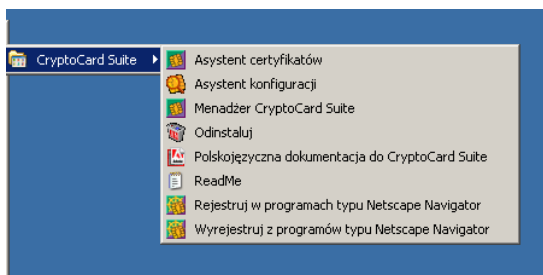
**UWAGA:** W systemach 95/98/Me instalator może poprosić o ponowne uruchomienie komputera. Jest to poprawne zachowanie, gdyż program instalacyjny pakietu CryptoCard Suite w razie konieczności uaktualnia systemowego instalatora MSI (Microsoft Installer). Restart jest konieczny, aby zmiany odniosły skutek.

**UWAGA:** Ze względów na stabilność działania aplikacji w systemie operacyjnym, newralgiczne biblioteki programu są kopiowane do katalogu %WINDOWS%\System32 bez względu na wybrany katalog, w którym ma być zainstalowana aplikacja.

Gdy program instalacyjny zakończy kopiowanie plików oraz rejestrowanie składników aplikacji CryptoCard Suite w systemie operacyjnym, pojawi się końcowy ekran instalatora (podobny do poniższego obrazka), gdzie użytkownik może zdecydować, czy chce przeczytać plik ReadMe.txt dołączony do tej wersji (jest to zalecane).

### **2.3. Sprawdzenie poprawności instalacji**

W celu weryfikacji poprawności instalacji należy sprawdzić czy na pulpicie widoczna jest ikona „Menadżer CryptoCard Suite” a w grupie start pojawiła się grupa programów „CryptoTech”.



Poszczególne elementy oznaczają:

- „Asystent certyfikatów” – uruchamia zestaw narzędzi, które są pomocne w zarządzaniu certyfikatami na karcie.
- „Asystent konfiguracji” – program pomagający sprawdzić, czy wymagane elementy systemu operacyjnego są zainstalowane i czy działają poprawnie.
- „Menadżer CryptoCard Suite” – program umożliwiający przeglądanie zawartości karty, zarządzanie jej zawartością. Z poziomu menadżera można uruchomić w/w programy.
- „Odinstaluj” – opcja umożliwiająca odinstalowanie pakietu CryptoCard Suite.
- „Polskojęzyczna dokumentacja do CryptoCard Suite” – niniejsza dokumentacja
- „ReadMe” – plik readme.txt zawierający opis zmian w danej wersji, opis znanych problemów itp.
- „Rejestruj w programach typu Netscape Navigator” – program pomagający zarejestrować tzw. „Security device” umożliwiający korzystanie z kart CryptoCard w programach typu Netscape Navigator czy Mozilla.
- „Wyrejestruj z programów typu Netscape Navigator” – program pomagający wyrejestrować „Security Device” z programów typu Netscape Navigator czy Mozilla.

Kolejnym krokiem jest uruchomienie asystenta konfiguracji. Aby to osiągnąć należy z menu Start → Programy → CryptoTech → CryptoCard Suite wybrać opcję „Asystent konfiguracji”. Jest to aplikacja, która pomoże sprawdzić czy pakiet CryptoCard Suite działa poprawnie oraz czy system operacyjny spełnia założone minimalne wymagania sprzętowo-systemowe.



Efektem działania Asystenta konfiguracji jest raport tekstowy, który jest osiągalny z poziomu ostatniego ekranu asystenta pod klawiszem „Raport”. Zawiera on informacje na temat



systemu operacyjnego, bibliotek powiązanych z aplikacją CryptoCard Suite oraz informacje dotyczące zainstalowanych systemie czytników kart elektronicznych.

Raport nie zawiera żadnych informacji dotyczących danych osobowych użytkownika ani żadnych informacji na temat kluczy czy certyfikatów użytkownika. Raport jest automatycznie zapisywany do pliku CryptoCardTest.log w katalogu, w którym jest zainstalowana aplikacja.

## 2.4. Przygotowanie karty do pracy

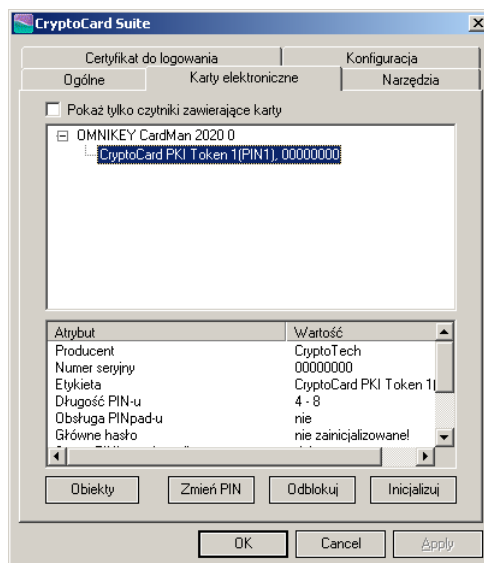
Karta CryptoCard multiSIGN fabrycznie jest przygotowana zarówno do obsługi kwalifikowanego jak i niekwalifikowanego podpisu elektronicznego.

Część niekwalifikowana jest gotowa do pracy od razu po zakupie. Domyślny PIN użytkownika to 1111 a SO PIN to 2222. Ze względów bezpieczeństwa zaleca się zmianę tych kodów przy rozpoczęciu pracy z kartą CryptoCard multiSIGN. Odpowiednia funkcjonalność jest dostępna w zakładce „Karty elektroniczne” pod przyciskiem „Zmień PIN”. Długość numerów PIN to minimalnie 4 znaki a maksymalnie 8 znaków dla części niekwalifikowanej oraz 6-8 znaków dla części do podpisu kwalifikowanego.

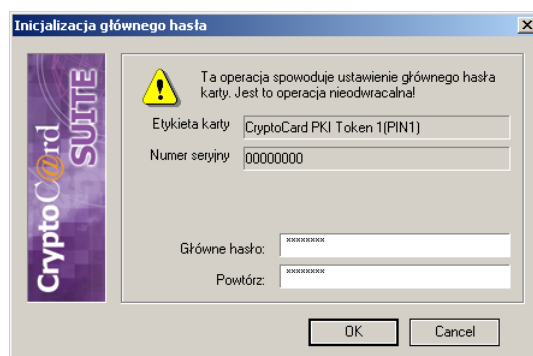
**UWAGA: Poczawszy od wersji 1.03.03 oprogramowanie CryptoCard Suite umożliwia ustawienie tzw. głównego hasła dla niekwalifikowanej części karty CryptoCard multiSIGN. Ustawienie takiego hasła umożliwi użytkownikowi późniejsze zarządzanie jej strukturą. Pomimo tego, że oprogramowanie CryptoCard Suite w obecnej wersji nie umożliwia jeszcze ingerencji w strukturę karty, ustawienie głównego hasła karty jest bardzo zalecane ze względów bezpieczeństwa.**

Główne hasło karty powinno składać się z 8 (minimalna akceptowana długość hasła) do 32 znaków alfanumerycznych, używanie polskich znaków diakrytycznych jest niezalecane i może powodować późniejsze problemy. Raz ustawionego hasła nie można zmienić, dlatego też powinno to być hasło nietrywialnie, niemożliwe do łatwego odgadnięcia dla innych osób. Hasło główne nie podlega mechanizmowi blokowania, co oznacza, że dopuszczalna jest dowolna ilość prób uwierzytelnienia się do karty z użyciem tego hasła. Użytkownik powinien zachować hasło w bezpiecznym miejscu – absolutnie niedopuszczalne jest zapisywanie hasła na karcie lub przechowywanie hasła razem z kartą. Zapomnienie głównego hasła może spowodować w przyszłości niemożliwość zmiany struktury części niekwalifikowanej karty CryptoCard multiSIGN.

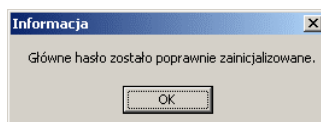
W celu ustawienia hasła głównego należy po włożeniu karty CryptoCard multiSIGN dwukrotnie kliknąć na pozycji „Główne hasło”, która jest widoczna jako atrybut karty w zakładce „Karty elektroniczne” Menadżera CryptoCard Suite. Status głównego hasła powinien być „nie zainicjowane!”.



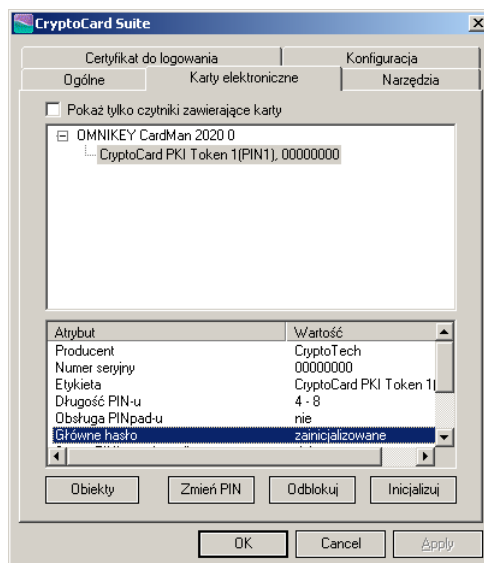
Następnie, należy wprowadzić hasło, które użytkownik chce ustawić jako hasło główne. Okno dialogowe jest skonstruowane w ten sposób, że nie pozwoli ustawić hasła krótszego niż 8 znaków.



Jeżeli wszystko przebiegnie pomyślnie, program poinformuje o ustawieniu hasła głównego przy pomocy odpowiedniego komunikatu.

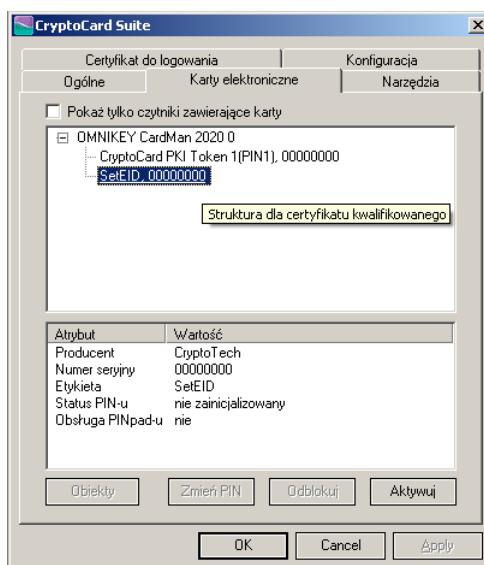


Po ustawieniu hasła głównego zmieni się jego status, który jest widoczny w dolnej części zakładki „Karty elektroniczne” Menadżera CryptoCard Suite. Status powinien być: „zainicjalizowane”.



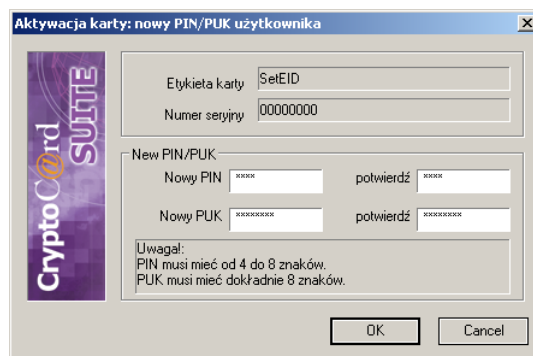
Kwalifikowaną część karty CryptoCard multiSIGN, należy aktywować przez ustawienie kodów PIN i PUK. Karta jest dostarczana w stanie pre-inicjalizowanym, co oznacza, że jest założona część kwalifikowana ale nie jest ona jeszcze gotowa do użycia ponieważ brakuje kodu PIN do części kwalifikowanej karty.

Kwalifikowana część karty jest widoczna w Menadżerze CryptoCard Suite w zakładce „Karty elektroniczne” pod nazwą „SetEID”.

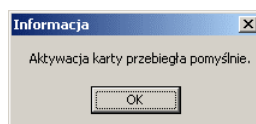


W celu aktywowania karty należy kliknąć przycisk „Aktywuj” i w okienku, które się pojawi podać nowe kody PIN i PUK. PIN powinien zawierać od 6 do 8 znaków, natomiast kod PUK musi zawierać dokładnie 8 znaków.

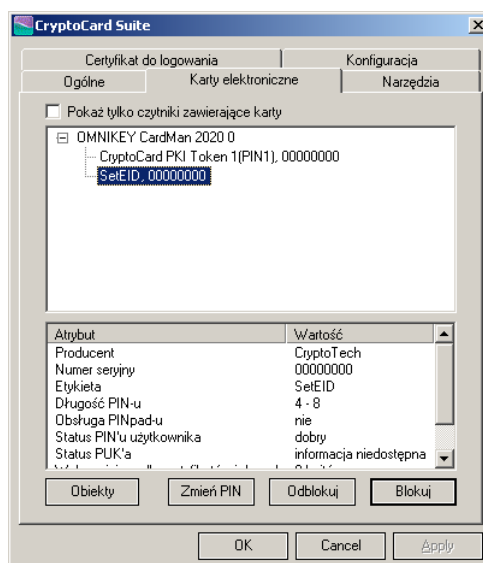
**UWAGA:** Kod PUK jest niezmienny – nie ma możliwości jego zmiany w trakcie używania karty! Kod PIN można zmieniać w trakcie używania karty.



Poprawny przebiegający proces inicjalizacji części kwalifikowanej karty kończy się komunikatem:



Po aktywacji karta jest gotowa do użycia. Miejsce przycisku „Aktywuj” zajmuje przycisk „Blokuj” – szczegóły użycia tej funkcjonalności są opisane w kolejnym rozdziale. Teraz można obejrzeć zawartość kwalifikowanej części karty klikając przycisk „Obiekty” i logując się do kwalifikowanej części karty ustawionym wcześniej kodem PIN.



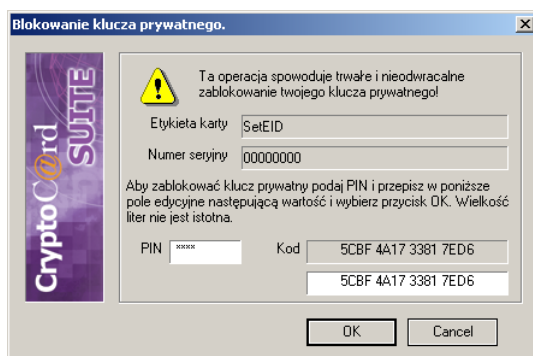
Atrybut	Wartość
Producent	CryptoTech
Numer seryjny	00000000
Etykieta	SetEID
Długość PIN-u	4 - 8
Obsługa PINpad-u	nie
Status PIN-u użytkownika	dobry
Status PUK'a	informacja niedostępna

## 2.5. Blokowanie możliwości użycia kwalifikowanej części karty CryptoCard multiSIGN

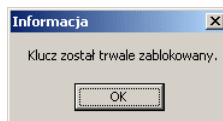
Ustawa o podpisie elektronicznym nakłada wymóg, żeby można było trwale uniemożliwić złożenie podpisu kwalifikowanego z użyciem danego klucza. CryptoCard Suite umożliwia trwale zablokowanie kwalifikowanej części karty CryptoCard multiSIGN.

Na powyższej ilustracji widać, że w miejsce przycisku „Aktywuj” pojawił się przycisk „Blokuj”. Po kliknięciu tego przycisku pojawi się okno dialogowe, w którym należy podać kod PIN do części kwalifikowanej oraz przepisać losowy kod.

**UWAGA:** Program nakłada na użytkownika takie wymagania, ponieważ operacja blokowania jest nieodwracalna i nie powinna być wykonywana pochopnie lub przypadkowo.

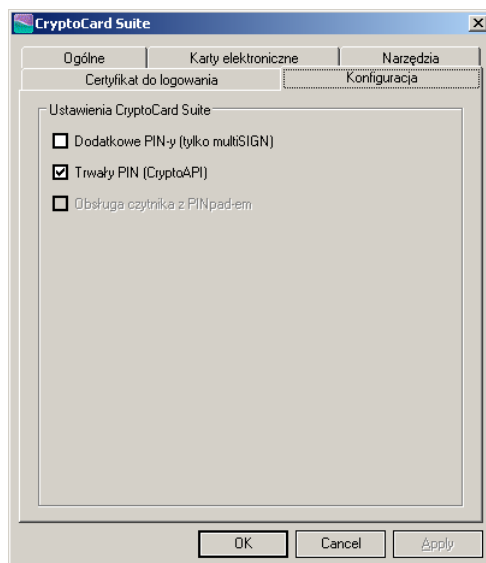


Po przepisanie kodu i kliknięciu OK, program jeszcze raz poprosi o potwierdzenie chęci trwałego zablokowania możliwości złożenia podpisu kwalifikowanego z użyciem tej karty, a po potwierdzeniu przystąpi do blokowania kwalifikowanej części karty CryptoCard multiSIGN. O zakończeniu operacji blokowania program poinformuje odpowiednim komunikatem.



## 2.6. Konfiguracja programu CryptoCard Suite

Pakiet CryptoCard Suite posiada możliwość dopasowania pewnych możliwości do indywidualnych potrzeb użytkownika. Konfiguracji można dokonać za pomocą zakładki „Konfiguracja” w Menadżerze CryptoCard Suite.



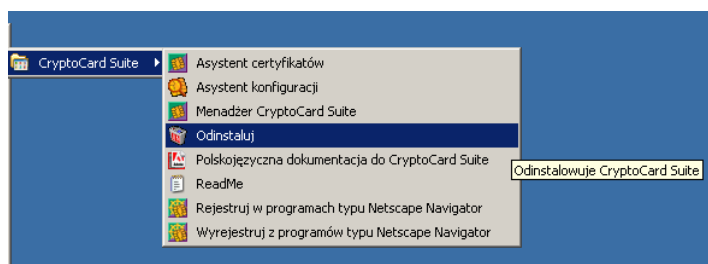
Możliwe do ustawienia są dwie opcje:

- „Dodatkowe PIN-y” – opcja możliwa tylko dla kart CryptoCard multiSIGN, powoduje, że użytkownik ma do dyspozycji dwie dodatkowe niekwalifikowane części karty
- „Trwały PIN” – włącza/wyłącza tymczasowe przechowywanie kodu PIN dla programu korzystającego z CryptoAPI, w którym podano kod PIN.

**UWAGA:** Korzystanie z funkcjonalności Trwały PIN obniża bezpieczeństwo korzystania z kart ponieważ wymusza przechowywanie kodu PIN w pamięci komputera.

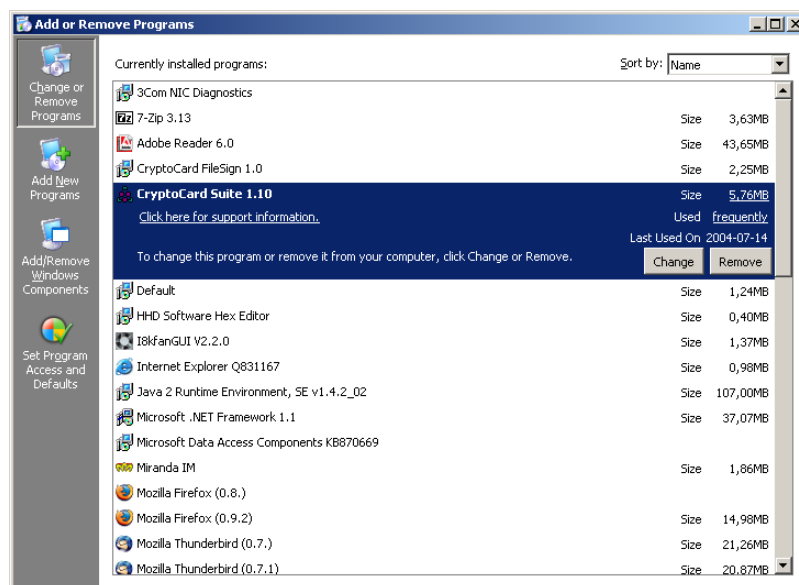
## 2.7. Odinstalowanie pakietu CryptoCard Suite

Najprostszym sposobem na odinstalowanie pakietu CryptoCard Suite jest wybranie opcji „Odinstaluj” z grupy CryptoTech-> CryptoCard Suite w menu Start.



Proces deinstalacji przebiega w sposób zautomatyzowany. Program usuwa pliki oraz wpisy systemowe pakietu CryptoCard Suite.

Oczywiście w celu odinstalowania pakietu CryptoCard Suite można skorzystać ze standardowego narzędzia do deinstalacji pakietów – „Dodaj/usuń programy” dostępnego w Panelu Sterowania.



**UWAGA:** Proces deinstalacji, podobnie jak proces instalacji musi odbywać się z konta administratora danej maszyny (bądź konta użytkownika posiadającego prawa administratora). Uwaga ta dotyczy systemów NT/2000/XP/2003.

**UWAGA:** W systemach Windows 95/98/Me program deinstalacyjny poprosi o ponowne uruchomienie komputera. Jest to poprawne zachowanie i należy zezwolić na restart komputera. Dopiero po ponownym uruchomieniu proces deinstalacji zostanie ukończony.

**UWAGA:** Może się okazać, że na dysku pozostał katalog, w którym była zainstalowana aplikacja CryptoCard Suite. Zazwyczaj w takiej sytuacji znajduje się w nim plik z logiem, który jest wynikiem działania Asystenta Konfiguracji. W takiej sytuacji cały katalog może zostać usunięty ręcznie.

## 2.8. Gdy wystąpią problemy

W sytuacji, gdy przez przypadek lub nieuwagę użytkownika zostanie usunięty któryś plik z pakietu CryptoCard Suite (np. TestKonfiguracji.exe) można go doinstalować w następujący sposób. Należy uruchomić program instalacyjny „setup.exe” i wybrać opcję „Napraw”. Program instalacyjny sprawdzi integralność instalacji i spróbuje naprawić wykryte błędy.

**UWAGA:** Opcja „Napraw” nie umożliwi odzyskania danych (kluczy, certyfikatów) z zainicjalizowanej karty. Nie umożliwia też odzyskania certyfikatów usuniętych nieopatrznie z systemu.

W przypadku, gdy nadal występują problemy w działaniu aplikacji CryptoCard Suite, należy

przede wszystkim uruchomić Asystenta Konfiguracji (menu Start → Programy → CryptoTech → CryptoCard Suite → Asystent konfiguracji) a raport, który powstanie należy zapisać do pliku. Zapisany raport wraz z opisem błędu należy wysłać pocztą elektroniczną pod adres [pomoc.techniczna@cryptotech.com.pl](mailto:pomoc.techniczna@cryptotech.com.pl).



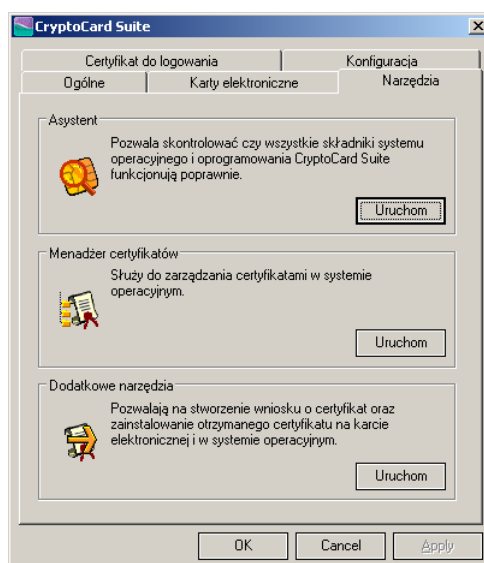
### 3. Uzyskanie certyfikatu

Certyfikaty klucza publicznego można uzyskać na wiele różnych sposobów.

Można samodzielnie wygenerować parę kluczy a następnie przygotować wniosek o certyfikację w formacie zgodnym ze standardem PKCS#10. O ile taka metoda może być stosowana w przypadku niekwalifikowanego podpisu elektronicznego, to w przypadku podpisu kwalifikowanego nie jest możliwa. Wynika to z przepisów prawa oraz regulaminów podmiotów świadczących usługi certyfikacyjne, które wyraźnie precyzują, że do otrzymania takiego użytkownik musi osobiście zarejestrować się w odpowiednim centrum rejestracyjnym (*Registration Authority, RA*). Dopiero po weryfikacji tożsamości użytkownika następuje stworzenie wniosku o certyfikację zgodnego z polityką przyjętą przez dane centrum a częścią tego wniosku jest wygenerowany klucz.

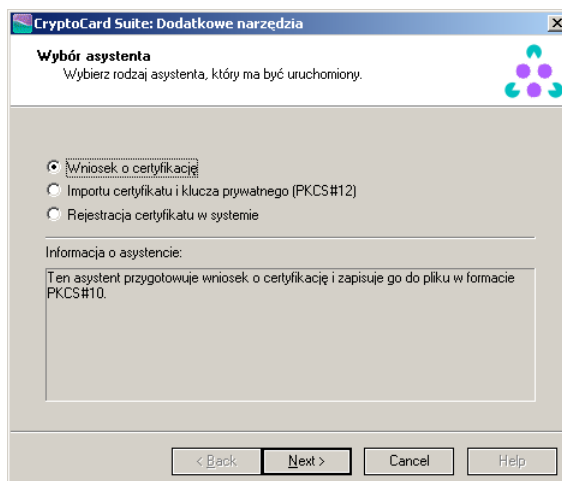
Listę podmiotów świadczących kwalifikowane usługi certyfikacyjne można znaleźć w Internecie pod adresem <http://www.centrast.pl/?i=10>. Certyfikaty niekwalifikowane można wydać lokalnie bądź też udać się do komercyjnych centrów certyfikacji i kupić.

Pakiet CryptoCard Suite oferuje zestaw trzech asystentów, które pomagają użytkownikowi zarządzać certyfikatami, które znajdują się na karcie elektronicznej. Są one dostępne po przejściu do zakładki „Narzędzia” i kliknięciu przycisku „Uruchom” w sekcji „Narzędzia dodatkowe”.



#### 3.1. Przygotowanie wniosku o certyfikację w formacie PKCS#10

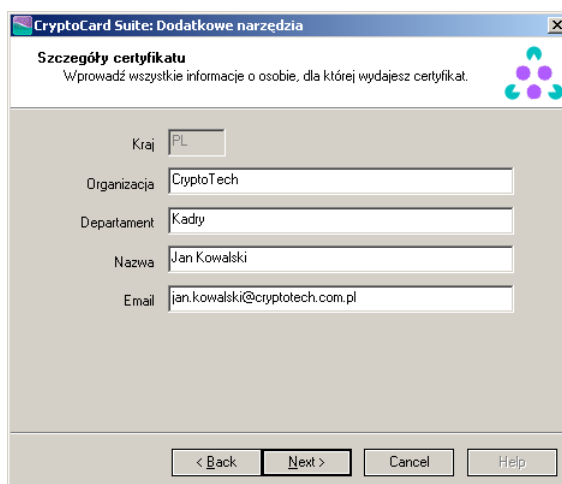
Aplikacja CryptoCard Suite udostępnia asystenta, który przeznaczony jest do stworzenia wniosku o certyfikację i zapisania go w formacie PKCS#10.



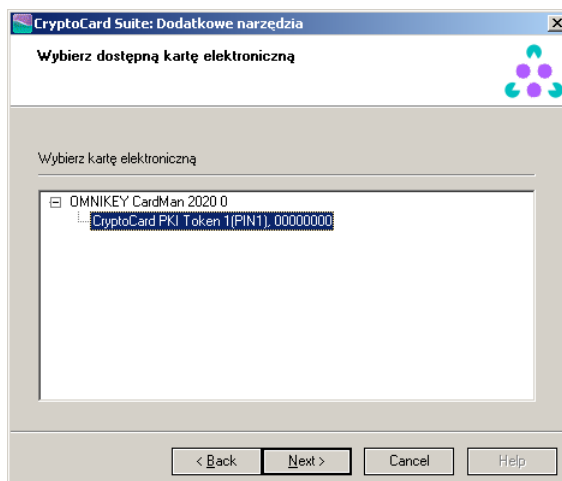
**UWAGA: Asystent nie może być używany do tworzenia wniosków o certyfikat kwalifikowany, czyli zgodny z ustawą o podpisie elektronicznym.**

Do wygenerowania wniosku konieczne jest podanie podstawowych informacji o osobie, która generuje wniosek. Oczywiście dane te nie są nigdzie weryfikowane, ale wpisanie nieprawdziwych danych może utrudnić zorientowanie się co to za certyfikat i dla kogo wydany.

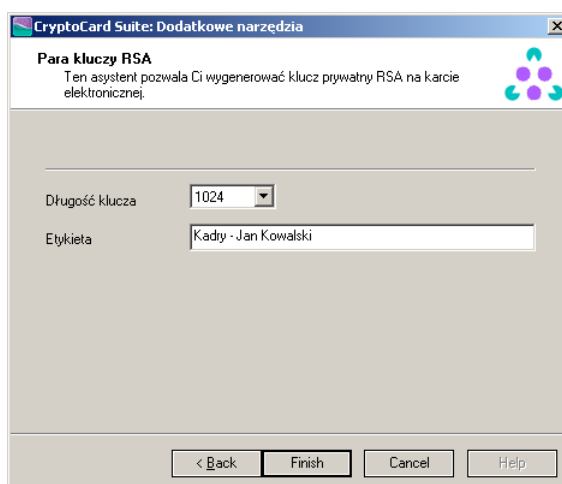
Adres e-mail jest weryfikowany syntaktycznie co oznacza, że jego format powinien być zgodny z zaleceniami dokument RFC 2822 (tekst tego dokumentu jest dostępny pod tym adresem: <http://www.faqs.org/rfcs/rfc2822.html>).



Następnie należy wskazać kartę, na której zostanie wygenerowana para kluczy, z której klucz prywatny będzie certyfikowany.



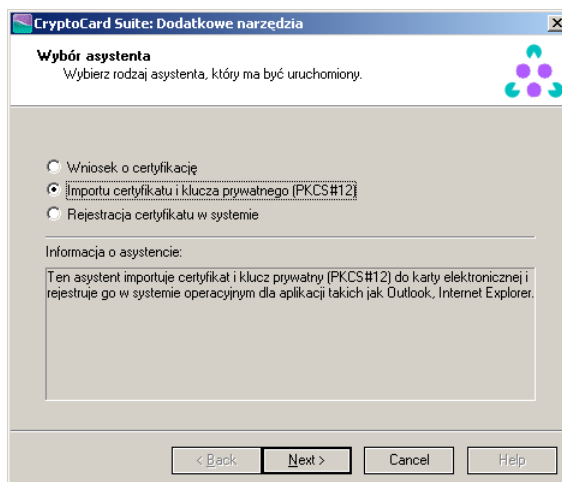
Następnie należy wybrać długość klucza, który ma zostać wygenerowany (zaleca się używanie klucza o długości 1024 bitów), oraz wybrać etykietę, pod którą klucz zostanie zapisany na karcie. Jest to nazwa, która ma na celu ułatwienie użytkownikowi rozpoznanie klucza gdyby na karcie znalazło się kilka kluczy).



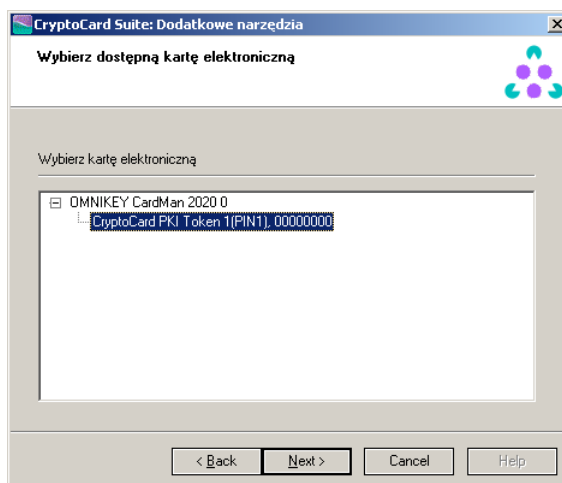
Następnie użytkownik musi podać PIN do karty po czym następuje generacja pary kluczy. Proces generacji może potrwać kilkadziesiąt sekund. Czas ten jest niezależny od szybkości komputera, na którym uruchomiona jest aplikacja CryptoCard Suite, gdyż generacja kluczy odbywa się na karcie. Ze względów bezpieczeństwa, wygenerowany klucz prywatny nie może być z niej wyeksportowany.

### 3.2. Import certyfikatów oraz kluczy na kartę

Jeżeli zaistniałaby sytuacja, że użytkownik posiada certyfikat w postaci pliku na dysku (np. zapisanego w formacie pliku PKCS#7 zawierającego certyfikat) lub plik w formacie PKCS#12 zawierający klucz prywatny oraz certyfikat, aplikacja CryptoCard Suite umożliwia umieszczenie takiego certyfikatu na karcie. Opcja taka może być użyteczna, jeżeli chcemy wykorzystać kartę jako nośnik dla certyfikatów. Odpowiednie narzędzie jest dostępne jako asystent o nazwie „Asystent importu certyfikatu i klucza prywatnego (PKCS#12)” w zakładce Narzędzia → Dodatkowe Narzędzia.



Po uruchomieniu odpowiedniego asystenta, należy wskazać kartę, na którą chcemy importować certyfikat.

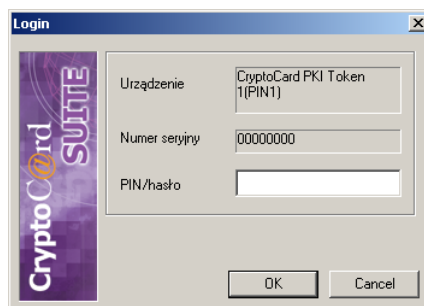


**UWAGA:** Niemożliwe jest samodzielne importowanie jakiegokolwiek certyfikatu do kwalifikowanej części karty CryptoCard multiSIGN. Jediną instytucją władną do umieszczania certyfikatów tej części jest wybrane przez nas centrum certyfikacji.

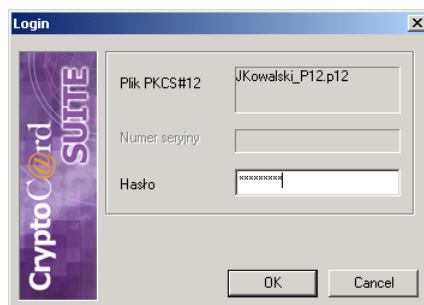
Następnie należy wskazać plik z certyfikatem, który chcemy importować. Mogą to być pliki zawierające certyfikaty X.509 (pliki z rozszerzeniami .der, .crt, .cer) lub pliki zawierające certyfikat oraz klucz zapisane w formacie PKCS#12v (pliki z rozszerzeniami .p12 lub .pfx).

**UWAGA:** Jeżeli chcemy importować plik PKCS#12 to musi on zawierać klucz prywatny i odpowiadający mu certyfikat. W innym przypadku próba importu zakończy się błędem.

Następnie użytkownik zostanie poproszony o podanie kodu PIN a w przypadku plików PKCS#12 również o hasło do tego pliku.



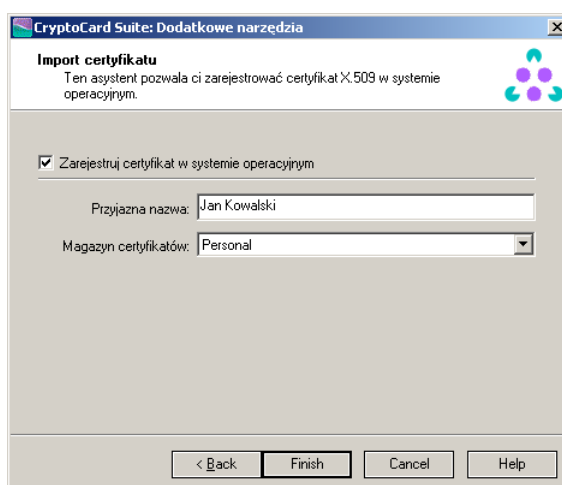
Dialog box "Login" z logo "CryptoCard SUITE" po lewej stronie. Zawiera trzy pola tekstowe: "Urządzenie" z wartością "CryptoCard PKI Token 1(PIN1)", "Numer seryjny" z wartością "00000000" oraz "PIN/hasło" (pusty). Na dole znajdują się przyciski "OK" i "Cancel".



Dialog box "Login" z logo "CryptoCard SUITE" po lewej stronie. Zawiera trzy pola tekstowe: "Plik PKCS#12" z wartością "JKowalski\_P12.p12", "Numer seryjny" (pusty) oraz "Hasło" (z maskowanymi znakami). Na dole znajdują się przyciski "OK" i "Cancel".

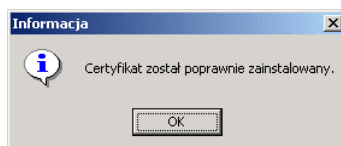
Jako ostatni krok, program zaoferuje możliwość zarejestrowania importowanego certyfikatu w systemie. Nie jest to krok konieczny, więc można kliknąć „Zakończ” w celu zamknięcia asystenta lub skorzystać z możliwości rejestracji.

Jeżeli użytkownik zdecydował się na rejestrację certyfikatu, należy zaznaczyć opcję „Zarejestruj certyfikat w systemie operacyjnym”, podać tzw. przyjazną nazwę (*friendly name*, jest to nazwa, która ma pomóc użytkownikowi zidentyfikować dany certyfikat) oraz wybrać tzw. magazyn systemowy (*certificate store*). Wybór magazynu jest dość istotną kwestią, ponieważ jeżeli rejestrujemy własny certyfikat to powinien on się znaleźć w Osobistym magazynie certyfikatów podczas gdy rejestrujemy certyfikat osoby, do której będziemy później wysyłać szyfrowaną pocztę elektroniczną, to taki certyfikat powinien się znaleźć w magazynie „Inne osoby”. Program nie pozwoli zarejestrować certyfikatu bez podania przyjaznej nazwy.



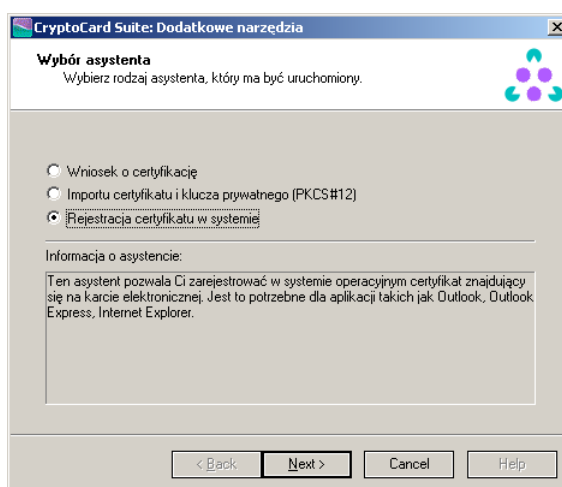
Dialog box "CryptoCard Suite: Dodatkowe narzędzia" z tytułem "Import certyfikatu". Zawiera komunikat: "Ten asystent pozwala ci zarejestrować certyfikat X.509 w systemie operacyjnym." i przycisk "Import". Poniżej znajduje się sekcja z opcją ☒ "Zarejestruj certyfikat w systemie operacyjnym". W tym trybie widoczne są pola: "Przyjazna nazwa:" z wartością "Jan Kowalski" oraz "Magazyn certyfikatów:" z menu rozwiniętym na "Personal". Na dole znajdują się przyciski "< Back", "Finish", "Cancel" i "Help".

Odpowiedni komunikat informuje, że cały proces dobiegł końca.

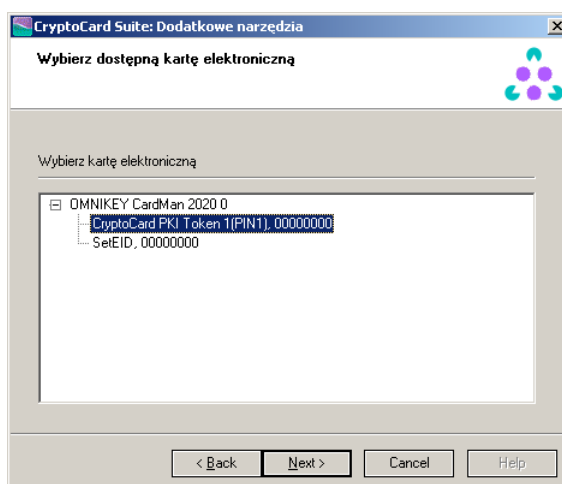


### 3.3. Rejestracja certyfikatu w systemie.

W celu skorzystania z klucza i skojarzonego z nim certyfikatu, należy ten certyfikat zarejestrować w systemie operacyjnym. Pakiet CryptoCard Suite umożliwia zarejestrowanie certyfikatów za pomocą wygodnego asystenta „Rejestracja certyfikatu w systemie”.

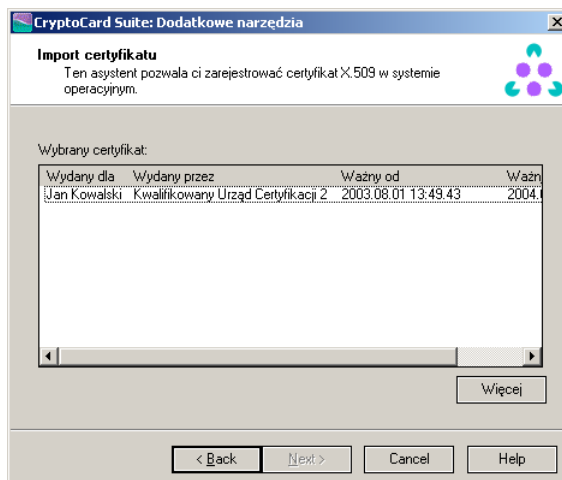


W pierwszym kroku użytkownik musi wybrać kartę (ew. część karty) z której chce zarejestrować certyfikat.



Następnie należy wybrać, który certyfikat z wybranej karty zostanie zarejestrowany. W okienku będą wyświetlone certyfikaty, które są na karcie albo na wybranej części karty. Może się jednak zdarzyć, że certyfikat będzie dostępny dopiero po podaniu PIN-u. W tym

celu trzeba kliknąć przycisk „Więcej” i po podaniu PIN-u program wyświetli wszystkie certyfikaty dostępne na danej karcie elektronicznej.

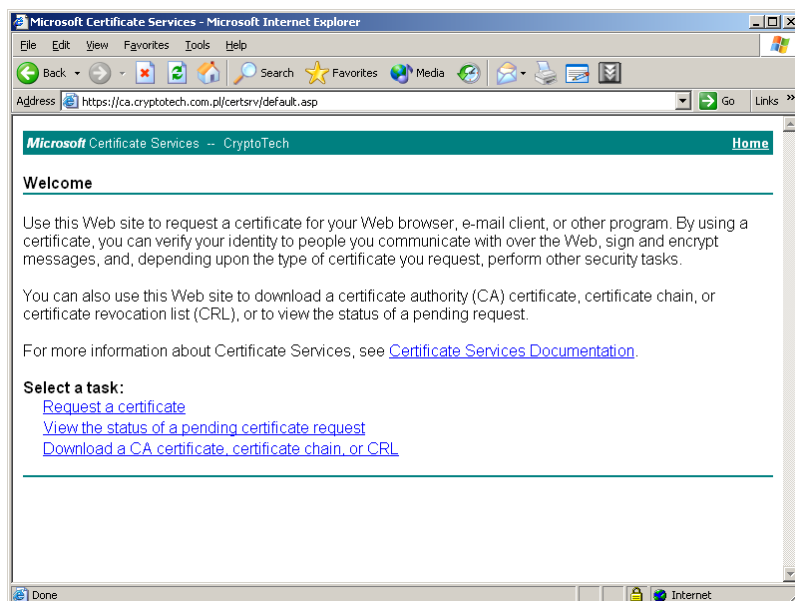


W ostatnim kroku użytkownik zostanie poproszony o podanie tzw. przyjaznej nazwy oraz wybranie „systemowego magazynu certyfikatów”, w którym zostanie zapisany certyfikat. Przyjazna nazwa jest nadawana w celu ułatwienia użytkownikowi wyszukiwania certyfikatów w systemie. Może to być dowolna nazwa. Oprogramowanie nie pozwoli zarejestrować certyfikatu bez podanej przyjaznej nazwy. Początkowe i końcowe znaki spacji zostaną automatycznie usunięte.

### **3.4. Uzyskanie certyfikatu on-line na przykładzie centrum certyfikacji w domenie Active Directory**

Ten rozdział jest przeznaczony głównie dla użytkowników kart CryptoCard multiSIGN, którzy zamierzają wykorzystać możliwości, jakie oferuje karta w zakresie logowania się do domeny Active Directory w MS Windows 2000 lub 2003. Jest to rozwiązanie przeznaczone głównie do zastosowań korporacyjnych ale stanowi doskonały przykład zastosowania koncepcji PKI i wykorzystania w niej kart elektronicznych.

Serwerowe wersje systemów firmy Microsoft posiadają wbudowane oprogramowanie Centrum Certyfikacji (CA, *Certification Authority*), które może wydawać certyfikaty dla użytkowników domeny. Udostępnia ono interfejs w postaci przejrzystych stron WWW, dzięki którym użytkownicy mogą samodzielnie uzyskać certyfikat.



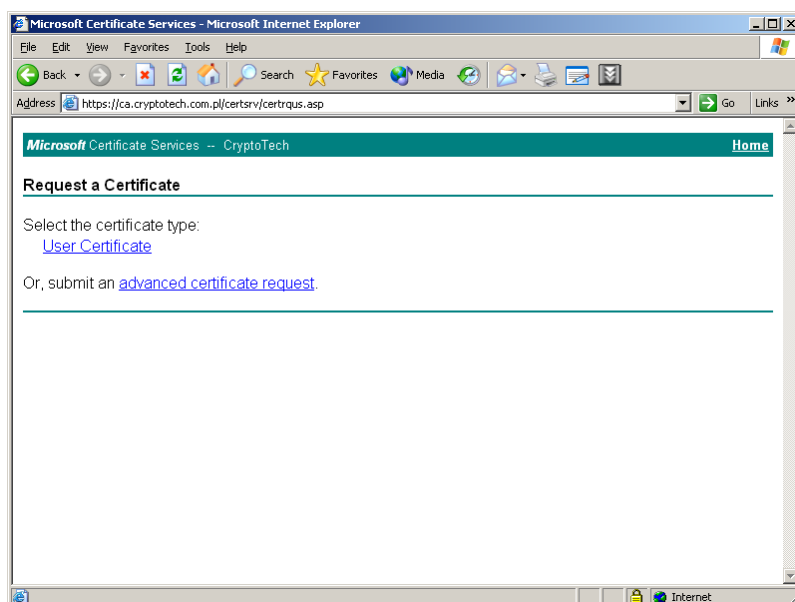
Na pierwszej stronie można wybrać następujące opcje:

„*Request a certificate*” – złożenie wniosku o certyfikację

„*Show status of a pending certificate request*” – pokazuje status już złożonych wniosków

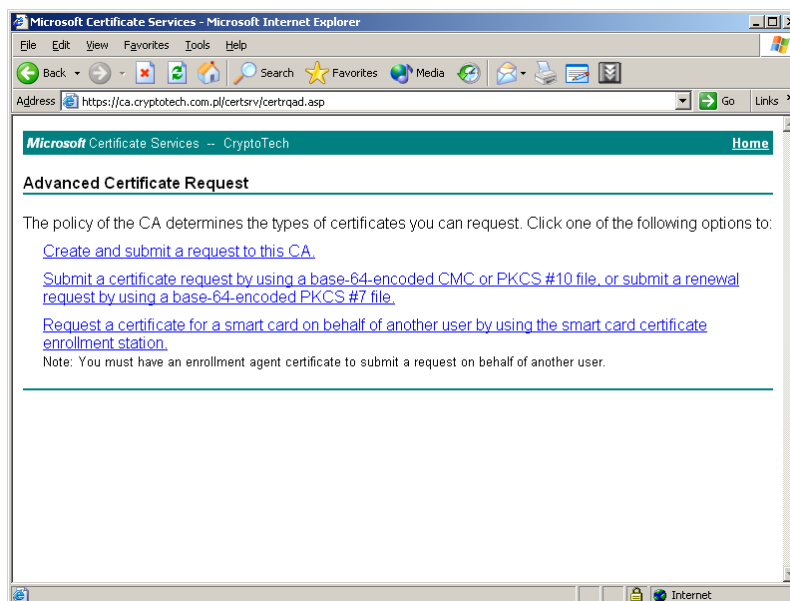
„*Download a CA certificate, certificate chain or CRL*” – udostępnia certyfikat samego CA ew. wszystkich pośrednich ośrodków (jeżeli takie istnieją) albo listę CRL

W naszym przypadku należy wybrać pierwszą opcję – „*Request a certificate*”.



Na kolejnej stronie możemy wybrać rodzaj procedury przy składaniu wniosku. W zależności od konfiguracji CA może zaproponować kilka standardowych typów np. „*User Certificate*” czy „*Smart Card logon certificate*”. Na potrzeby tego przykładu należy wybrać jednak „*Advanced certificate request*”, która to opcja pozwoli na większą kontrolę nad składanym wnioskiem.





Trzecia strona wyświetlana przez CA pozwala na wybranie typu certyfikatu, jaki chcemy uzyskać. Do wyboru dostępne są następujące możliwości:

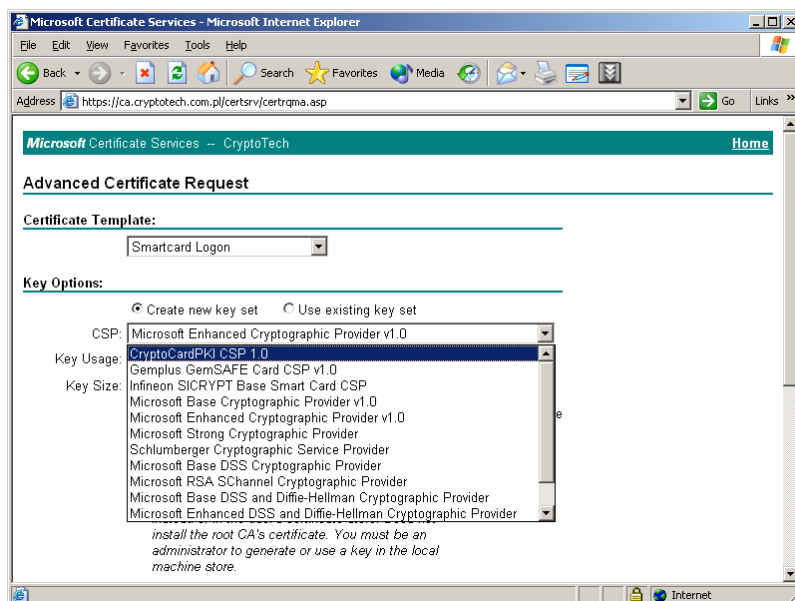
„*Create and submit a request to this CA*” – wystąpienie o certyfikat we własnym imieniu, wniosek jest od razu przesyłany do CA a wydany certyfikat zostaje osadzony na karcie oraz zainstalowany w systemie w profilu aktualnie zalogowanego użytkownika jako jeden z jego certyfikatów osobistych.

„*Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file*” – pozwala wysłać do CA wcześniej przygotowany wniosek w postaci pliku PKCS#10 lub CMC. Umożliwia też wystąpienie o odnowienie certyfikatu przez przesłanie odpowiednio przygotowanego pliku w formacie PKCS #7. Wszystkie pliki muszą być zakodowane przy pomocy algorytmu BASE64.

„*Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station*” – pozwala na wystąpienie z wnioskiem o certyfikację w imieniu innej osoby. Skorzystanie z tej opcji wymaga posiadania dodatkowego certyfikatu tzw. „*Enrollment agent certificate*”.

W omawianym przypadku należy wybrać pierwszą opcję oferowaną nam przez CA.

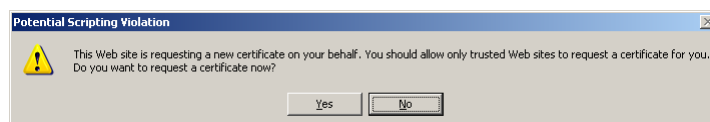
**UWAGA:** w tym miejscu Internet Explorer będzie usiłował załadować kontrolkę ActiveX, która jest konieczna do dalszych czynności związanych z wydaniem certyfikatu. W przypadku problemów należy zweryfikować ustawienia bezpieczeństwa dla programu MS Internet Explorer.



Wyżej przedstawiony ekran oferuje nam możliwość wybrania konkretnego typu certyfikatu, o który wystąpimy do CA. Należy zdecydować, do czego będziemy używać certyfikatu – typ „Smartcard Logon” pozwala jedynie na logowanie się do domeny AD przy pomocy karty. Bardziej użyteczny jest typ „Smartcard User”, który pozwala na logowanie się oraz na zabezpieczanie poczty elektronicznej (podpisywanie i szyfrowanie) oraz szyfrowanie plików.

**UWAGA: Aby korzystać z kart CryptoCard multiSIGN należy koniecznie wybrać CSP: „CryptoCardPKI CSP 1.0”!**

Pozostałe ustawienia można zostawić z wartościami domyślnymi.  
W celu kontynuowania procesu należy kliknąć przycisk „Submit >”.



W zależności od ustawień bezpieczeństwa programu MS IE, może pojawić się komunikat pokazany na powyższym obrazku. Na pytanie należy odpowiedzieć Yes.



Po podaniu numeru PIN do części niekwalifikowanej, karta wygeneruje nową parę kluczy. Klucz publiczny zostanie osadzony w nowo wydany certyfikacie. Jeżeli wszystko przebiegnie pomyślnie, powinien pojawić się strona taka jak na poniższym obrazku. Po kliknięciu „Install this certificate” certyfikat zostanie zainstalowany w systemie oraz osadzony na karcie elektronicznej. W trakcie rejestracji certyfikatu w systemie użytkownik zostanie poproszony o podanie kodu PIN. Dodatkowo oprogramowanie CryptoCardPKI CSP ustawi ten certyfikat jako domyślny certyfikat na karcie, co oznacza, że taką kartą będzie można się załogować do domeny MS Windows 2000/2003 bez konieczności wykonywania żadnych dodatkowych czynności.

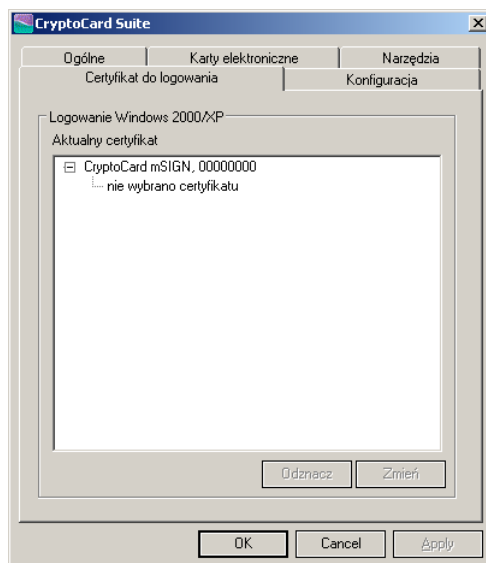
**UWAGA: Certyfikat ten nie jest certyfikatem kwalifikowanym!**

Omówienie wykorzystania pozostałych opcji oferowanych przez CA systemów MS Windows 2000/2003 wykracza poza ramy niniejszego dokumentu. W celu zapoznania się z nimi zaleca się lekturę odpowiednich rozdziałów dokumentacji do wyżej wspomnianych systemów operacyjnych.

### **3.5. Konfiguracja certyfikatu do logowania w Windows**

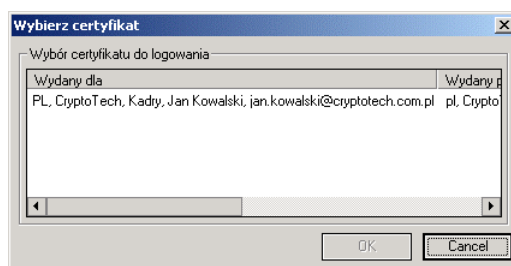
W wypadku gdy użytkownik posiada certyfikat w postaci pliku na dysku i chciałby użyć tego certyfikatu do logowania (certyfikat musi posiadać odpowiednie rozszerzenie – SmartCardLogon).

Procedura importu certyfikatu na kartę została opisana w rozdziale 3.2 niniejszego podręcznika. Gdy już certyfikat jest osadzony na karcie, można przystąpić do ustawienia go jako certyfikatu do logowania. Narzędzie przeznaczone do tego jest dostępne w zakładce „Certyfikat do logowania” w Menedżerze CryptoCard Suite.

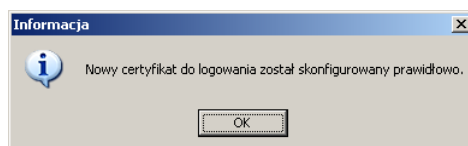


W celu ustawienia certyfikatu jako domyślnego, należy wybrać kartę, na której mamy certyfikat a następnie wcisnąć przycisk „Zmień”.

Program zapyta się o PIN do karty i po jego pomyślnej weryfikacji pokaże się okienko z listą certyfikatów dostępnych na danej karcie.



Następnie należy zaznaczyć wybrany certyfikat przez kliknięcie na nim i wcisnąć OK. Program dokona odpowiedniego wpisu na karcie i od tej chwili będzie można się zalogować przy użyciu karty CryptoCard multiSIGN.



Odpowiedni komunikat informuje użytkownika o pomyślnym zakończeniu procesu ustawiania certyfikatu domyślnego.

## 4. Zastosowanie karty CryptoCard multiSIGN do zabezpieczania poczty elektronicznej (na przykładzie MS Outlook Express 6.0)

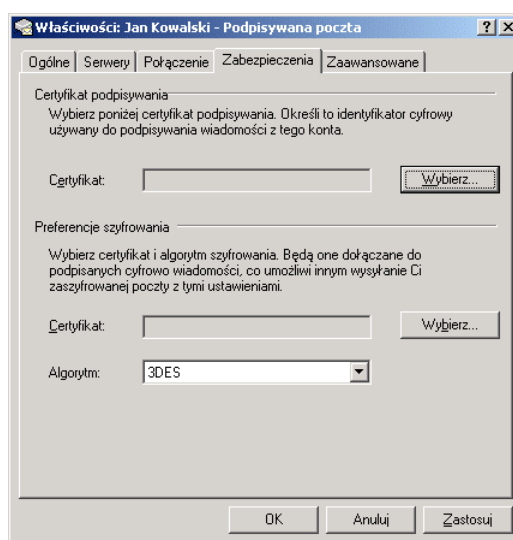
Posiadając już ważny certyfikat można przystąpić do jego używania. Jednym z najpopularniejszych zastosowań certyfikatów i Infrastruktury Klucza Publicznego jest zabezpieczanie korespondencji elektronicznej. Zastosowanie to nie dotyczy certyfikatów kwalifikowanych, które są przeznaczone do innych celów (określonych przy wydawaniu takiego certyfikatu).

### 4.1. Instalacja certyfikatów w programie Outlook Express

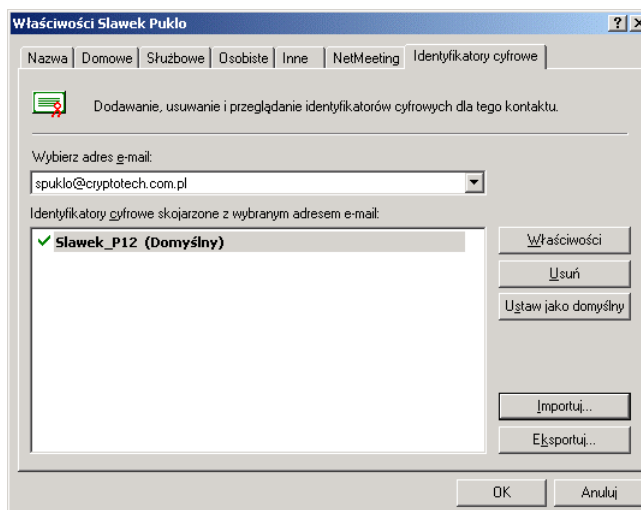
Przed przystąpieniem do podpisywania czy szyfrowania poczty należy odpowiednio skonfigurować program pocztowy. Konieczne jest też posiadanie zainstalowanego w systemie certyfikatu oraz konieczne jest posiadanie karty a kluczem prywatnym odpowiadającym kluczowi publicznemu z certyfikatu.

W celu zainstalowania certyfikatu w systemie można skorzystać z asystenta dostarczonego wraz z aplikacją CryptoCard Suite, co zostało opisane w rozdziale 3.3.

Następną czynnością, którą należy wykonać jest ustawienie certyfikatu, którego Outlook Express użyje do podpisywania poczty oraz do jej szyfrowania. Można to zrobić w zakładce „Zabezpieczenia” we właściwościach konta, z którego będzie wysyłana poczta podpisana elektronicznie. W tym samym miejscu należy określić algorytm, którego Outlook Express będzie używał do szyfrowania poczty.



Kolejnym krokiem jest zainstalowanie certyfikatów osób, do których będzie adresowana zaszyfrowana poczta. Można to zrobić za pośrednictwem wbudowanej Książki Adresowej. Jeżeli adresat już tam figuruje to należy wyświetlić Właściwości tego wpisu i wybrać zakładkę „Identyfikatory cyfrowe”. Jeżeli posiadamy certyfikat adresata, można go dodać klikając przycisk „Importuj”.

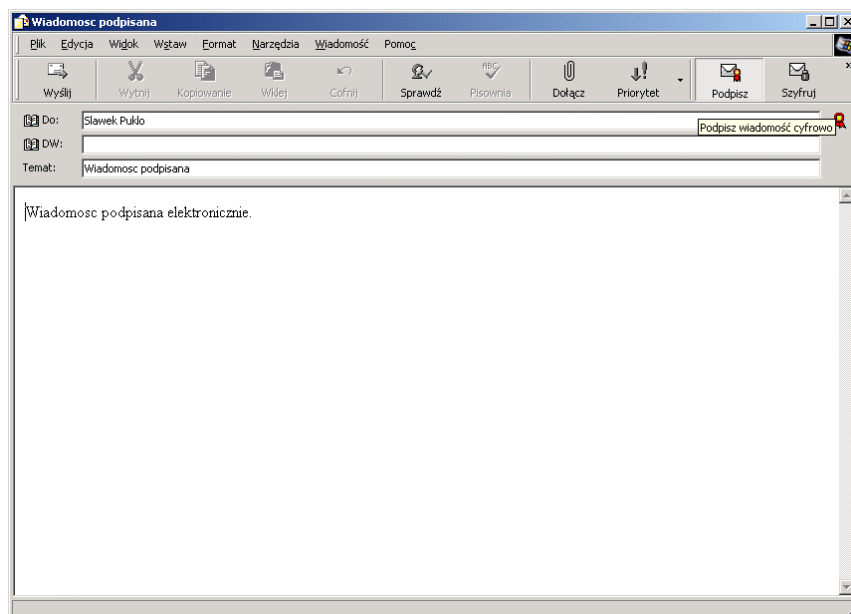


**UWAGA:** Posiadanie certyfikatu adresata jest koniecznym warunkiem, jeżeli chcemy wysłać zaszyfrowaną wiadomość e-mail.

**UWAGA:** Jeżeli certyfikat został wystawiony przez CA, które nie jest domyślnie uznawane przez Windows jako zaufane, niemożliwe będzie używanie takiego certyfikatu. Konieczne jest zainstalowanie w systemie certyfikatu urzędu, który wystawił certyfikaty użytkowników. Jest to szczególnie ważne przy korzystaniu z wewnętrznych, firmowych CA, które nie są ujęte na liście zaufanych wystawców certyfikatów. Uwaga ta dotyczy zarówno własnego certyfikatu jak i certyfikatów innych osób.

## 4.2. Podpisywanie wiadomości poczty elektronicznej

Jeżeli konfiguracja MS Outlook Express jest poprawna, stworzenie podpisanego maila jest łatwą czynnością. Wystarczy w trakcie tworzenia maila wcisnąć przycisk „Podpisz”, dostępny na belce narzędziowej.



W momencie wysyłania maila, użytkownik zostanie poproszony o podanie numeru PIN.



Program automatycznie podpisze i wyśle wiadomość.

W celu zweryfikowania, czy wiadomość została faktycznie podpisana można sprawdzić zawartość folderu „Elementy wysłane”. Przy wiadomości powinien widnieć symbol oznaczający mail podpisany elektronicznie.

Do	Temat	Wysłano	Konto
Sławek Pukło	Wiadomość podpisana	2003-08-08 15:09	Jan Kowalski - Podpisywan...

#### 4.3. Weryfikacja poprawności podpisu w otrzymanej wiadomości e-mail

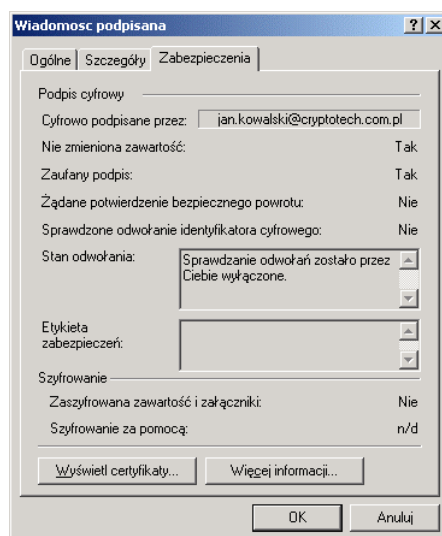
Aby zweryfikować podpis elektroniczny otrzymanej wiadomości wymagane jest posiadanie certyfikatu osoby, która tą wiadomość nadała. Domyślnym ustawieniem programu MS Outlook Express jest dołączanie certyfikatu nadawcy do podpisanych wiadomości, więc jeżeli

użytkownik nie posiada jeszcze certyfikatu nadawcy wystarczy go dodać w sposób opisany w rozdziale 4.1.

Przy próbie odczytania podpisanej wiadomości MS Outlook Express wyświetli komunikat informujący o tym, że wiadomość została podpisana. Umożliwi też zweryfikowanie podpisu – wystarczy kliknąć symbol



aby wyświetlić okienko informujące o podpisie i jego ważności.

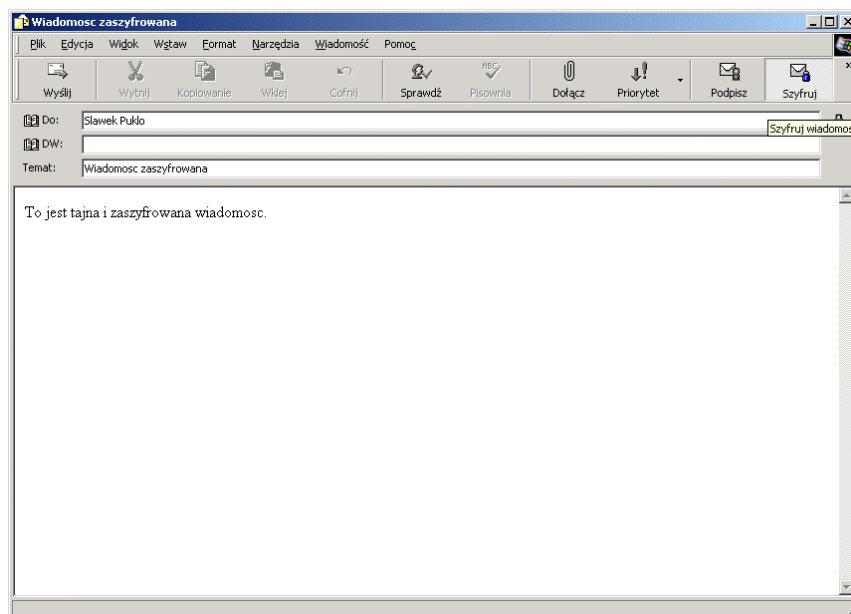


#### 4.4. Szyfrowanie wiadomości poczty elektronicznej

Wysłanie zaszyfrowanej wiadomości wymaga posiadania ważnego certyfikatu osoby, do której wysyłamy poufną wiadomość. Certyfikat musi być skojarzony z adresatem w książce adresowej – patrz rozdział 4.1.

Gdy wszystko jest już poprawnie skonfigurowane, wystarczy nacisnąć przycisk „Szyfruj” dostępny w belce narzędziowej, a Outlook Express automatycznie zaszyfruje pocztę w momencie jej wysyłania.



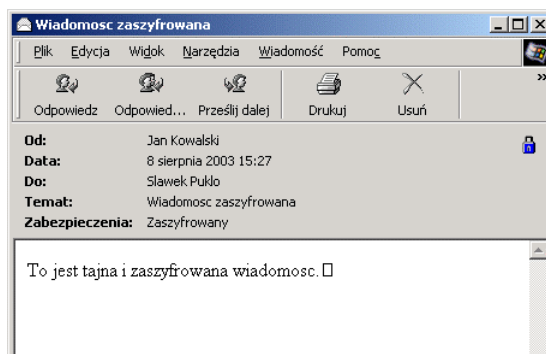


Przy szyfrowaniu poczty nie jest konieczne podawanie żadnych kodów PIN gdyż szyfrowanie odbywa się za pomocą klucza publicznego dostępnego w certyfikacie adresata.

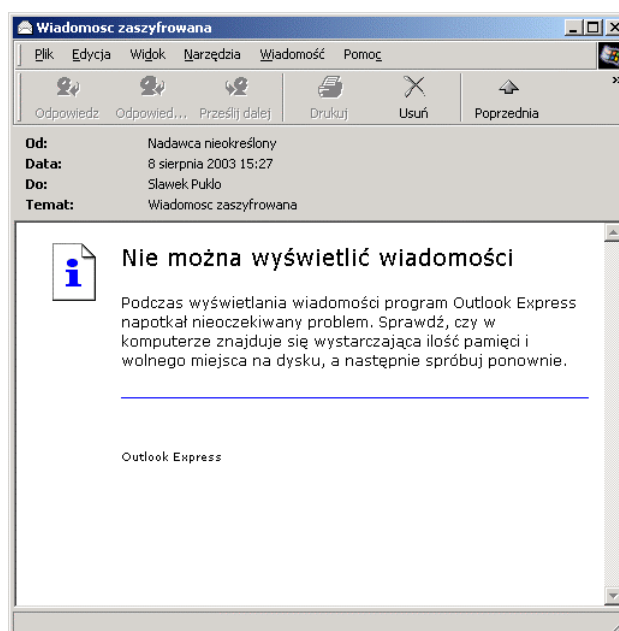
#### 4.5. Deszyfrowanie wiadomości poczty elektronicznej

Jeżeli użytkownik dostał zaszyfowaną wiadomość email, to w celu jej odczytania musi użyć swojego klucza prywatnego, który jest bezpiecznie przechowywany na karcie elektronicznej (w części niekwalifikowanej). Konieczne jest posiadanie zarejestrowanego certyfikatu z odpowiednim kluczem publicznym w systemowym, osobistym magazynie certyfikatów. Outlook automatycznie przystąpi do odszyfrowania wiadomości w momencie kliknięcia na nią – pojawi się okienko z pytaniem o kod PIN.

Jeżeli PIN jest poprawny to po chwili powinna pojawić się treść zaszyfowanej depeszy. O fakcie zaszyfowania przypomina symbol zamkniętej kłódki, widoczny w rogu ekranu.



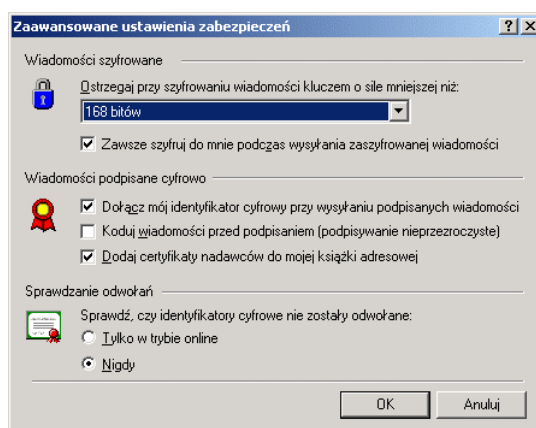
Gdy jednak operacja deszyfrowania nie powiedzie się, pojawi się odpowiedni komunikat.



Możliwe przyczyny takiego błędu to:

- brak klucza prywatnego komplementarnego do klucza, którym została zaszyfrowana wiadomość
- w osobistym systemowym magazynie certyfikatów nie ma zarejestrowanego odpowiedniego certyfikatu

Możliwe też jest przeczytanie zaszyfrowanej poczty przez jej nadawcę. Wiadomość taka zazwyczaj znajduje się w folderze „Wysłane”. Aby móc ją przeczytać należy wiadomość zaszyfrować również do samego siebie w trakcie jej wysyłania. Outlook Express uczyni tak automatycznie, pod warunkiem, że będzie włączona opcja „Zawsze szyfruj do mnie podczas wysyłania zaszyfrowanej wiadomości”. Można sprawdzić to ustawienie w „Zaawansowanych ustawieniach zabezpieczeń” dostępnych w menu Narzędzia → Opcje → Zabezpieczenia → Zaawansowane.



Opcja ta jest domyślnie włączona. Pozostałe kroki do przeczytania zaszyfrowanej wiadomości są takie same jak w przypadku wspomnianym wyżej.