PWPW
POLSKA WYTWÓRNIA
PAPIERÓW WARTOŚCIOWYCH

INSTRUKCJA OBSŁUGI KARTY DARK

CENTRUM USŁUG ZAUFANIA SIGILLUM

Wersja 1.2

Spis treści

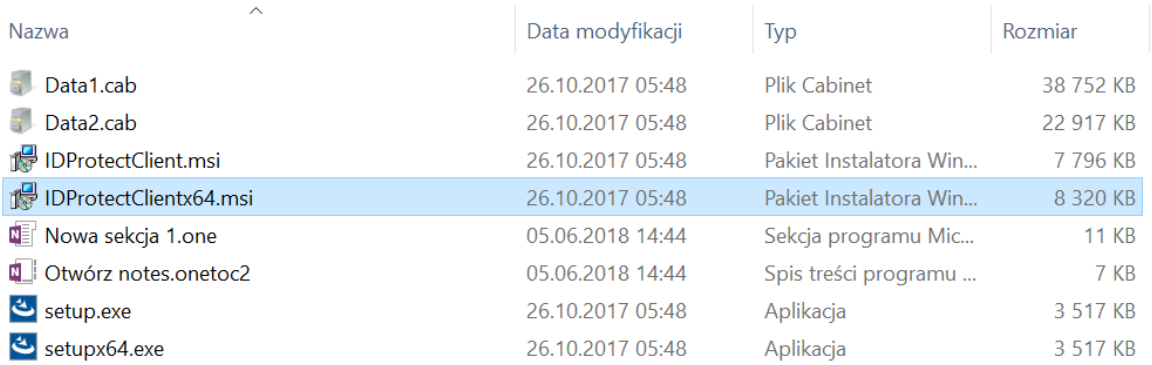
1. Wstęp

Niniejszy dokument stanowi instrukcję instalacji oraz użytkowania oprogramowania służącego do obsługi karty DARK. Dokument zawiera opisy podstawowych funkcjonalności niezbędnych do prawidłowego działania oprogramowania. Szczegółowa instrukcja jest dostarczana przez dostawcę kart i jest instalowana wraz z opisywanym oprogramowaniem. Można ją znaleźć w C:\Program Files (x86)\NXP Semiconductors\IDProtect Client\Docs\IDProtect for Windows User Guide.pdf (wersja angielska).

Karta DARK dostępna jest w poniższym wzorze:

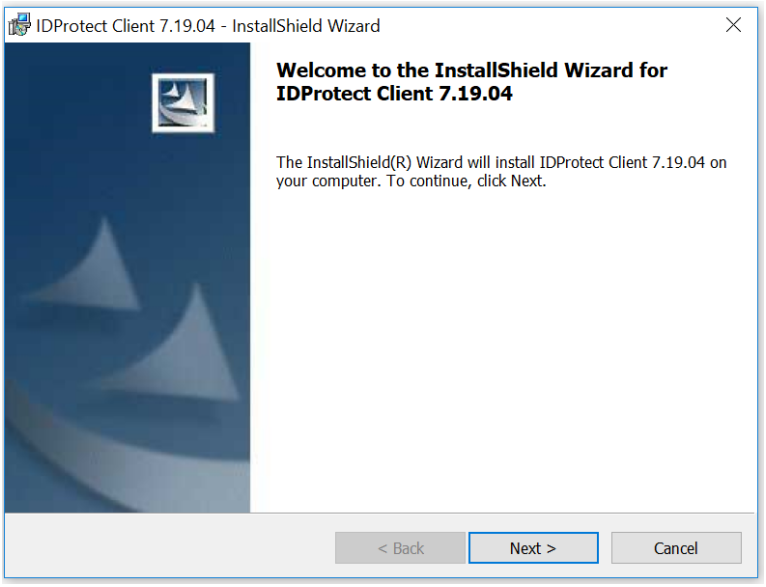
2. Instalacja oprogramowania

W celu umożliwienia zarządzania kartą, należy zainstalować odpowiednie oprogramowanie dostarczone przez PWPW (https://sigillum.pl/Pliki). Instalację oprogramowania do karty należy rozpocząć od wybrania właściwej wersji instalacyjnej: dla Windows 32 bitowego - plik „IDProtectClient.msi", dla Windows 64 bitowego - plik „IDProtectClientx64.msi".

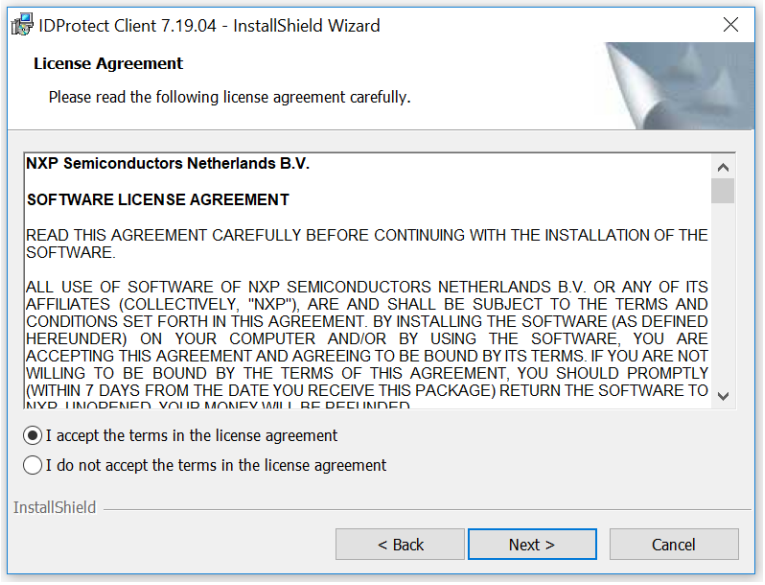


Nazwa	Data modyfikacji	Typ	Rozmiar
Data1.cab	26.10.2017 05:48	Plik Cabinet	38 752 KB
Data2.cab	26.10.2017 05:48	Plik Cabinet	22 917 KB
IDProtectClient.msi	26.10.2017 05:48	Pakiet Instalatora Win...	7 796 KB
IDProtectClientx64.msi	26.10.2017 05:48	Pakiet Instalatora Win...	8 320 KB
Nowa sekcja 1.one	05.06.2018 14:44	Sekcja programu Mic...	11 KB
Otwórz notes.onetoc2	05.06.2018 14:44	Spis treści programu ...	7 KB
setup.exe	26.10.2017 05:48	Aplikacja	3 517 KB
setupx64.exe	26.10.2017 05:48	Aplikacja	3 517 KB

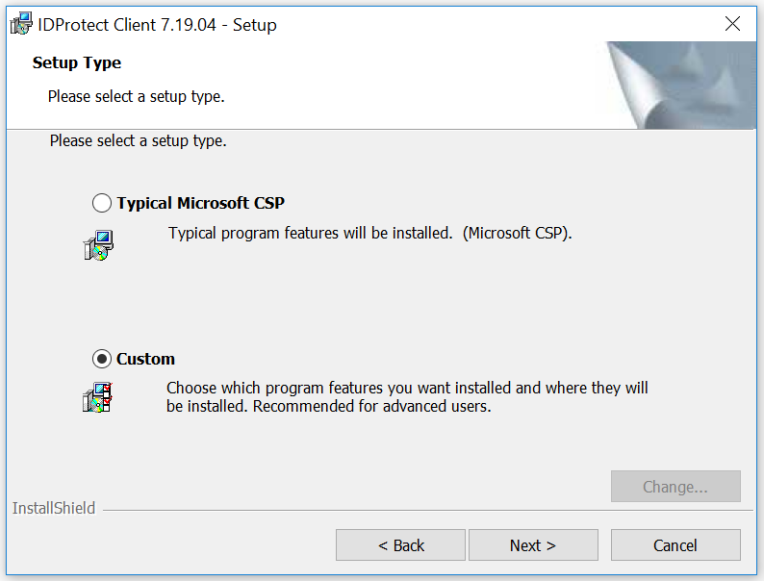
Po włączeniu instalatora pojawi się ekran powitalny, z którego przechodzimy do następnego ekranu, klikając w przycisk „Next".



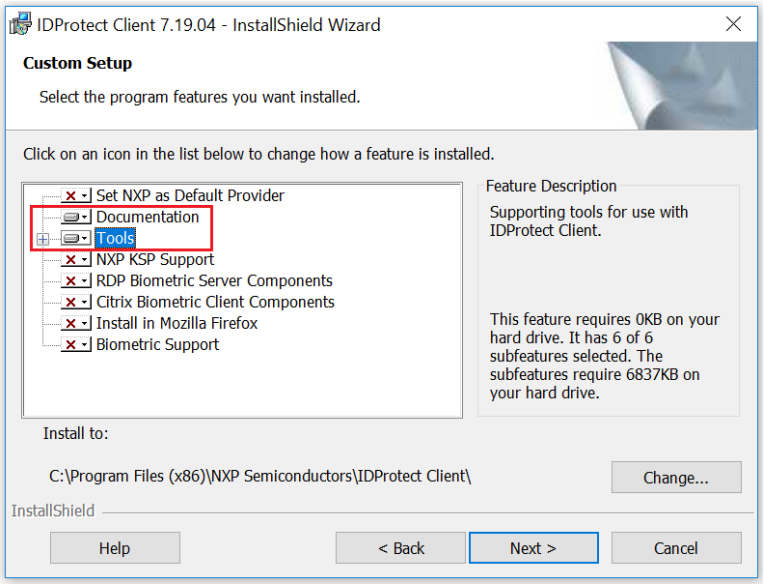
Kolejny krok to potwierdzenie umowy licencyjnej – wybieramy „I accept the terms in the license agreement":



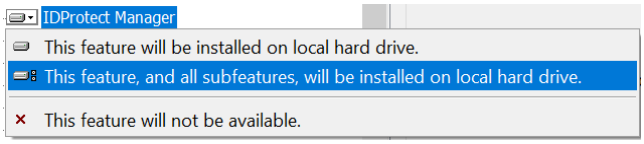
Na następnym ekranie należy wybrać typ instalacji „Custom”:



Następnie wybieramy komponenty, które mają zostać zainstalowane:



Aby zainstalować wybrany komponent, należy kliknąć w ikonkę  , a następnie wybrać „This feature, and all subfeatures, will be installed on local hard drive.”.

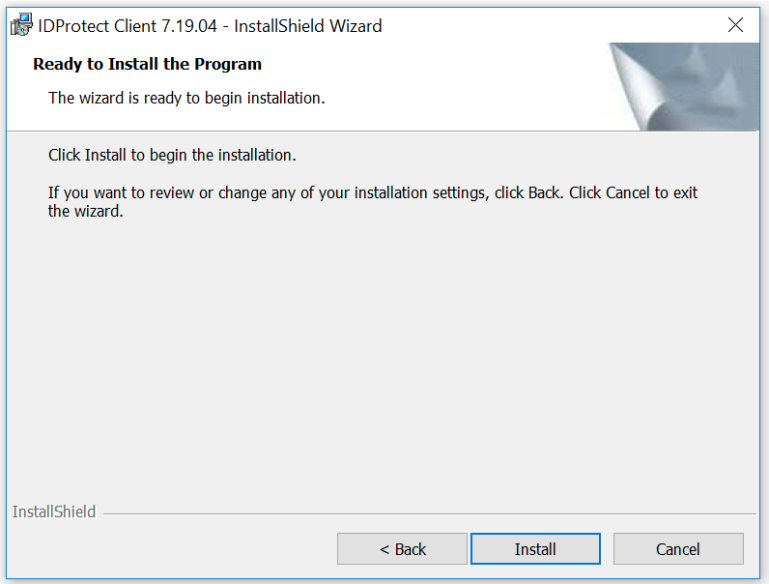


Należy zainstalować następujące komponenty:

- Documentation: zostanie zainstalowana szczegółowa instrukcja obsługi narzędzi do karty DARK (wersja angielska);
- Tools – wszystkie z poniższych (kliknąć obok komponentu Tools, aby rozwinąć więcej opcji):
  - IDProtect Manager
  - IDProtect Format
  - IDProtect Options
  - IDProtect PINTool
  - IDProtect Admin PIN Tool

UWAGA: proszę nie instalować komponentu „Set NXP as Default Provider”. Może to powodować nieoczekiwane problemy w działaniu oprogramowania do zarządzania kartą, jak i narzędzi do składania podpisu.

Po wybraniu wszystkich wymaganych komponentów przechodzimy dalej do następnego ekranu, gdzie potwierdzamy instalację przyciskiem „Install”:



Następuje instalacja oprogramowania. Po jej zakończeniu nie ma potrzeby restartowania systemu.

3. Korzystanie z oprogramowania

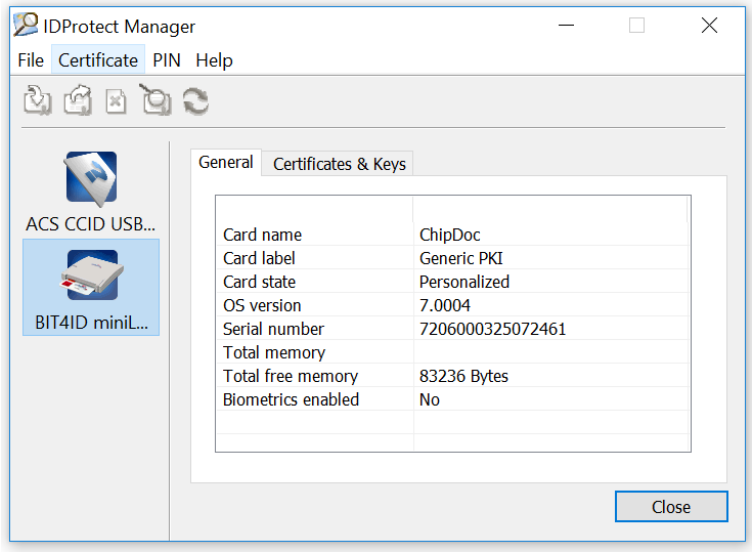
Po wykonaniu instalacji w systemie operacyjnym dostępne są następujące aplikacje:

- **IDProtect Manager**: Pozwala podejrzeć klucze i certyfikaty na karcie. Działa w tle i jest widoczny w na pasku zadań pod ikonką  Domyślnie uruchamia się przy starcie systemu;
- **IDProtect Format**: umożliwia sformatowanie karty (wyczyszczenie całej zawartości – kluczy i certyfikatów);
- **IDProtect PINTool**: umożliwia zmianę PINu do karty;
- **IDProtect Admin PIN Tool**: umożliwia zmianę PUKu do karty.

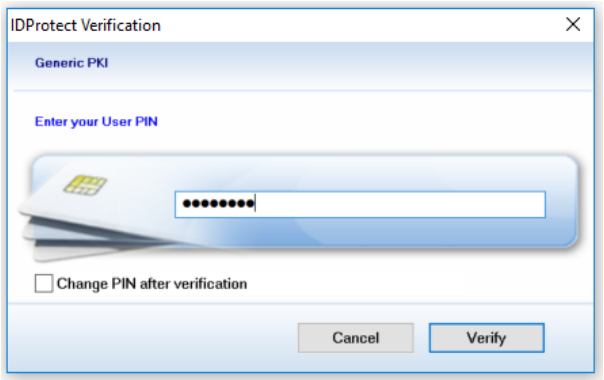
W dalszej części zostały opisane najważniejsze funkcjonalności opisanych powyżej aplikacji.

3.1. IDProtect Manager

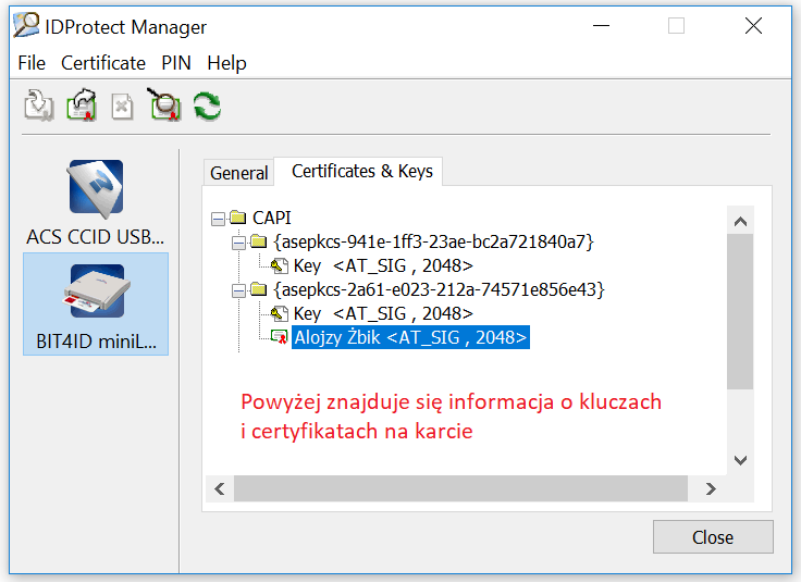
Po włączeniu aplikacji w lewej sekcji widoczne są wszystkie podłączone czytniki. Należy wybrać czytnik, w którym znajduje się karta DARK. Aplikacja wyświetli podstawowe informacje o karcie w zakładce „General". Są to przede wszystkim nazwa karty (ChipDoc), wersja systemu operacyjnego (OS version), nr seryjny karty (Serial number) oraz rozmiar pozostałego miejsca na karcie (Total free memory).



Aby wyświetlić zawartość karty należy przełączyć się na zakładkę „Certificates & Keys". Aplikacja poprosi o podanie PINu:



Użytkownik wprowadza PIN, a następnie klika w przycisk „Verify”. Następuje weryfikacja poprawności wprowadzonego PINu. Jeśli jest niepoprawny, aplikacja wyświetli komunikat błędu oraz liczbę pozostałych prób wprowadzania PINu (max. 3). Jeżeli PIN jest prawidłowy, aplikacja wyświetli wszystkie klucze i certyfikaty istniejące na karcie. Aby podejrzeć szczegóły certyfikatu należy dwukrotnie kliknąć w jego nazwę, która pochodzi z pola „Nazwa powszechna” (Common Name) certyfikatu. Można to również zrobić zaznaczając certyfikat, a następnie wybierając z menu głównego „Certificate” -> „View”.

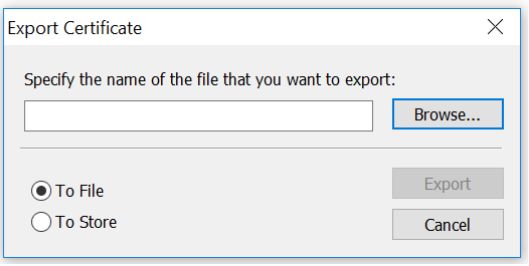


Opcjonalnie, podczas wprowadzania PINu, można zaznaczyć opcję „Change PIN after verification” co będzie skutkowało możliwością zmiany PINu do karty, od razu po tym, jak obecny PIN zostanie poprawnie zweryfikowany.

Aplikacja umożliwia wyeksportowanie certyfikatu do pliku. Operację można wykonać na dwa sposoby:

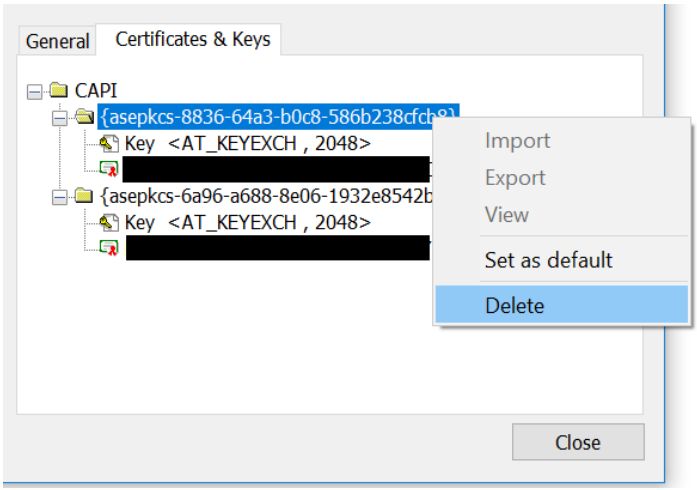
- Klikamy w certyfikat prawym przyciskiem myszy i wybieramy „Export”;
- Zaznaczamy certyfikat, po czym z menu głównego wybieramy „Certificate” -> „Export”.

W obu przypadkach aplikacja wyświetli następujące okienko:



Aby dokończyć operację, należy wybrać opcję „To File” oraz kliknąć w przycisk „Browse”, aby wprowadzić nazwę pliku i miejsce jego wyeksportowania. Na koniec wybieramy „Export”. Operacja zostanie potwierdzona stosownym komunikatem.

Aplikacja umożliwia również ręczne skasowanie wybranych kluczy i certyfikatów z karty. W tym celu należy w sekcji „Certificates & Keys” kliknąć prawym przyciskiem myszy folder, w którym znajdują się klucze i/lub certyfikat:

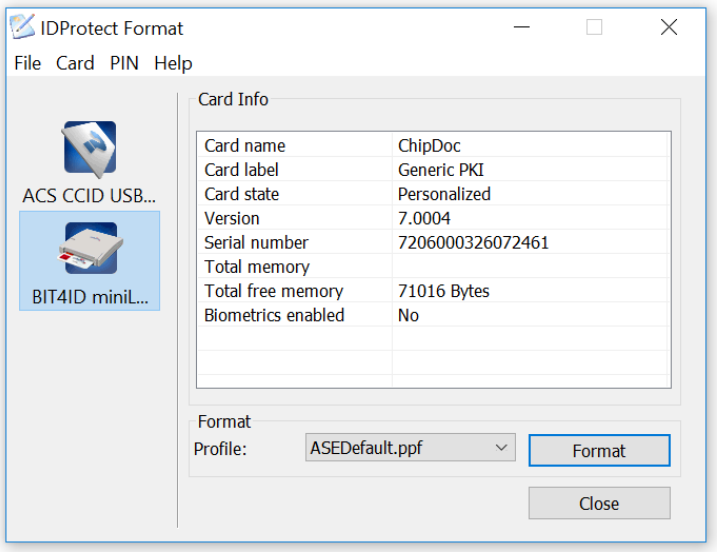


Następnie należy wybrać opcję „Delete” i potwierdzić operację w wyskakującym okienku klikając w przycisk „Tak”. Folder zostanie usunięty i nie będzie już widoczny na karcie.

UWAGA: w wyniku powyższej operacji wykasowane zostaną bezpowrotnie certyfikaty i klucze znajdujące się na karcie.

3.2. IDProtect Format

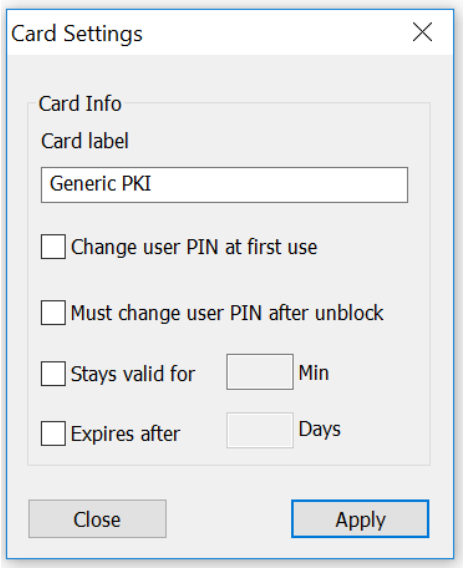
Aplikacja umożliwia wyczyszczenie karty ze wszystkich istniejących na niej kluczy oraz certyfikatów. Wybieramy w sekcji „Format” profil „ASEDefault.ppf” i klikamy w przycisk „Format”:



Aplikacja wyświetli okienko ostrzegawcze. Aby kontynuować wybieramy „Tak”, po czym następuje operacja formatowania karty. Jej zakończenie zostanie potwierdzone stosownym komunikatem.

UWAGA: w wyniku powyższej operacji wykasowane zostaną bezpowrotnie certyfikaty i klucze znajdujące się na karcie. Aplikacja nadaje karcie domyślne wartości PIN i PUK, odpowiednio ‘11111111’ i ‘00000000’. PIN i PUK można zmienić za pomocą narzędzi IDProtect PINTool i IDProtect AdminPINTool.

Za pomocą narzędzia IDProtect Format można również zmienić wybrane atrybuty karty, jak np. czas przez jaki nie będzie wymagane podawanie ponownie PINu podczas użycia karty. W tym celu należy włożyć kartę do czytnika, a następnie wybrać w aplikacji opcję „File” -> „Modify Admin Settings”. Zostanie wyświetlone następujące okienko:



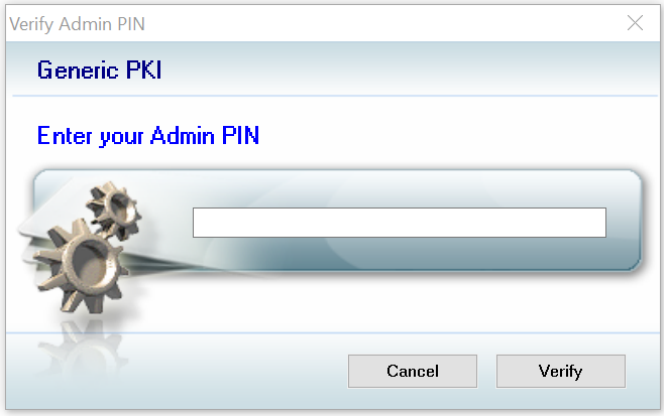
Opcje możliwe do modyfikacji:

- Card label – możliwość nadania nazwy własnej karty, która będzie wyświetlana w narzędziach do obsługi karty;

- Change user PIN at first use – zaznaczenie powoduje wymuszenie zmiany PINu podczas jego pierwszego użycia;
- Must change user PIN after unblock – zaznaczenie spowoduje, że wymagana będzie zmiana PIN przy pierwszym jego użyciu, po wcześniejszym odblokowaniu PINu;
- Stays valid for – możliwość ustawienia czasu, przez jaki PIN będzie ważny i nie będzie konieczności ponownego jego podawania. Po upłynięciu ustawionego czasu (w minutach) użytkownik ponownie zostanie zapytany o PIN podczas np. składania podpisu. **Aby PIN był wymagany przy każdej operacji należy zaznaczyć niniejszą opcję i wpisać wartość '0' (zero);**
- Expires after – liczba dni, po których wymagana będzie zmiana PINu.

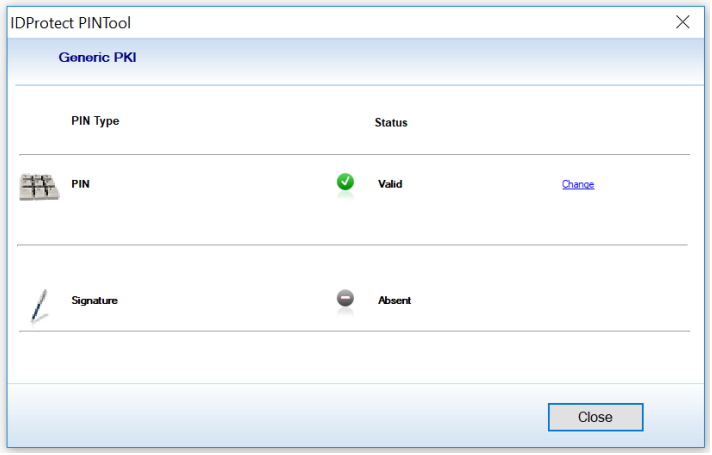
UWAGA: po wykonaniu zmiany każdego z powyższych parametrów, należy dodatkowo zrestartować komputer. Inaczej zmiany nie zostaną zapamiętane.

Każdą zmianę wyżej opisanych ustawień należy potwierdzić przyciskiem „Apply", a następnie podać PUK (Admin PIN) i kliknąć w przycisk „Verify":

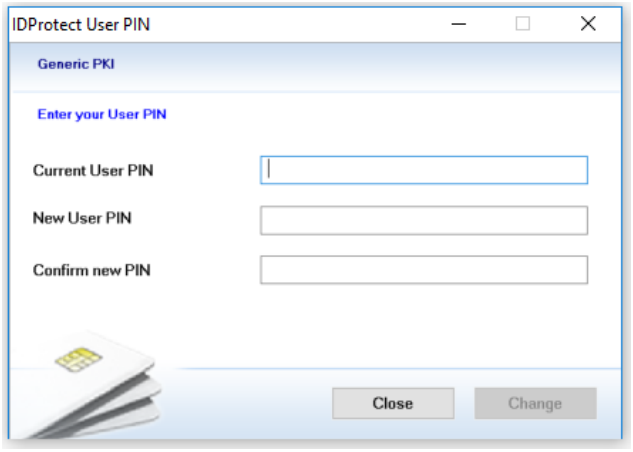


3.3. IDProtect PINTool

W celu zmiany PINu do karty należy kliknąć przycisk „Change" w sekcji „PIN":

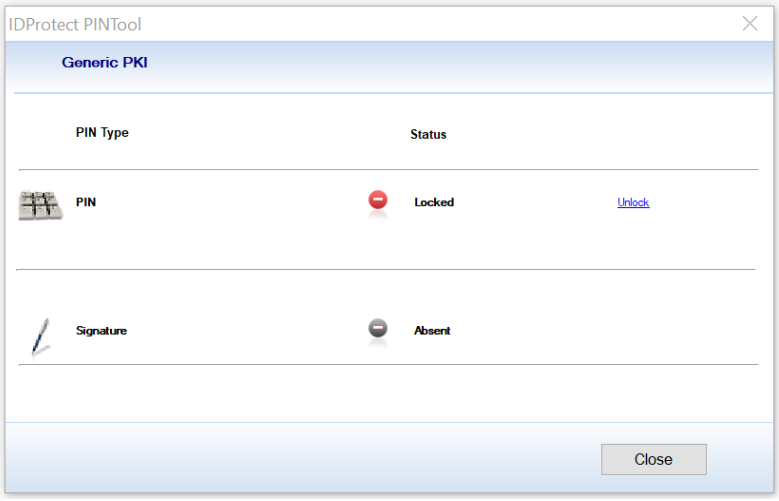


Aplikacja poprosi o wpisanie obecnego PINu oraz dwukrotne podanie nowego (minimum 6 znaków). Następnie należy potwierdzić operację przyciskiem „Change”.



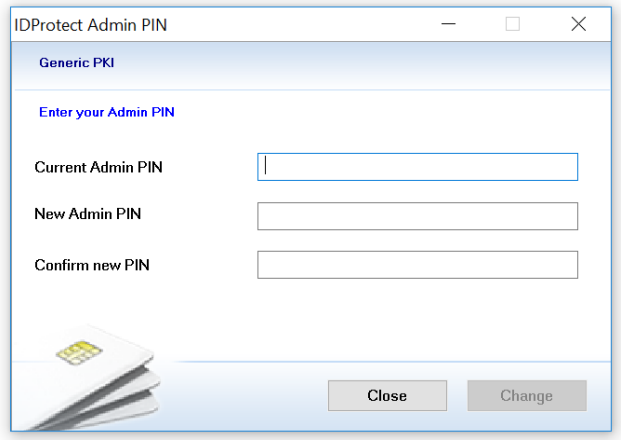
Operację zmiany PINu można również wykonać w z poziomu aplikacji IDProtectManager. W menu głównym należy wybrać „PIN” -> „Manage…”.

W przypadku, gdy PIN do karty został zablokowany (wykorzystano maksymalną liczbę powtórzeń podania PINu), na ekranie będzie widniała informacja o statusie karty „Locked”.



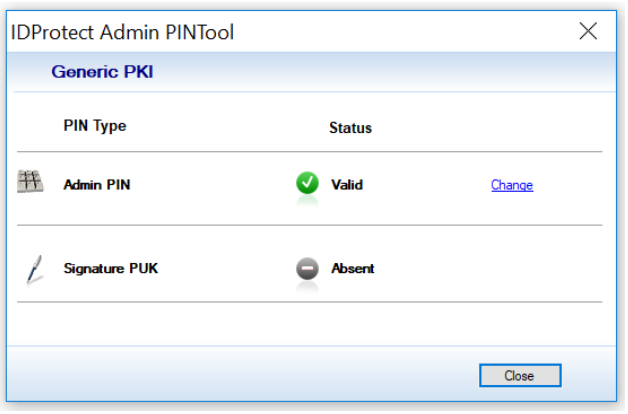
W celu odblokowania PINu należy kliknąć w przycisk „Unlock”, a na kolejnym ekranie wprowadzić PUK i nadać nowy PIN (należy podać PIN inny niż dotychczas używany). Na koniec należy potwierdzić operację przyciskiem „OK”. Prawidłowe odblokowanie PIN zostanie potwierdzone zmianą statusu na „Valid”.

UWAGA: pięciokrotne wprowadzenie błędnego PUKu skutkuje trwałym zablokowaniem karty.



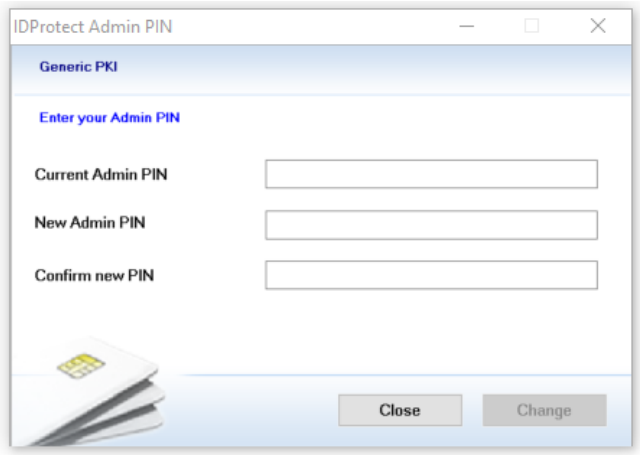
3.4. IDProtect AdminPINTool

W celu zmiany PUKu do karty należy kliknąć przycisk „Change” w sekcji „Admin PIN”:



Aplikacja poprosi o wpisanie obecnego PUKu oraz dwukrotne podanie nowego (minimum 8 znaków). Następnie należy potwierdzić operację przyciskiem „Change”.

UWAGA: pięciokrotne wprowadzenie błędnego PUKu skutkuje trwałym zablokowaniem karty.


IDProtect Admin PIN
Generic PKI
Enter your Admin PIN
Current Admin PIN
New Admin PIN
Confirm new PIN
Close
Change

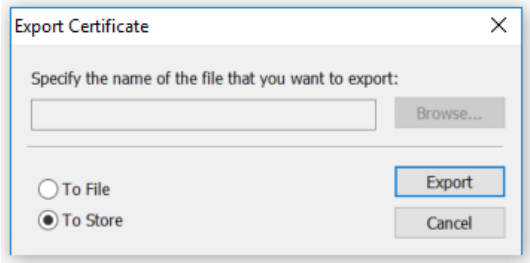
4. Obsługa potencjalnych problemów

4.1. Certyfikat nie jest widoczny w magazynie certyfikatów

Źródłem takiej sytuacji może być:

1. Brak karty w czytniku. Po wyjęciu karty z czytnika certyfikat nie jest widoczny w magazynie certyfikatów. Jest to zamierzone działanie karty. Po włożeniu karty do czytnika certyfikat ponownie pojawi się w magazynie certyfikatów.
2. Konfiguracja komputera. W pewnych przypadkach konfiguracja komputera może powodować, że certyfikat nie dodał się automatycznie do magazynu certyfikatów. Wobec tego należy dodać certyfikat ręcznie za pomocą narzędzia IDProtect Manager poprzez:
    a. Kliknięcie w certyfikat prawym przyciskiem myszy i wybranie „Export”;
    b. Zaznaczenie certyfikatu, po czym z menu głównego wybranie „Certificate” -> „Export”.

    W obu przypadkach aplikacja wyświetli następujące okienko:



    Aby dokończyć operację, należy wybrać opcję „To Store” oraz kliknąć w przycisk „Export”. Operacja zostanie potwierdzona stosownym komunikatem. Certyfikat został dodany do magazynu certyfikatów.