INSTRUKCJA UŻYTKOWNIKA

Instalacja i konfiguracja czytników kart kryptograficznych oraz aplikacji proCertum CardManager w systemie Linux

Wersja 2.0

Certum by asseco

Spis treści

1. Wstęp

Celem dokumentu jest opisanie czynności niezbędnych do korzystania z certyfikatów kwalifikowanych i niekwalifikowanych zapisanych na karcie kryptograficznej. Poniższy opis dotyczy instalacji i konfiguracji czytników kart kryptograficznych, instalacji aplikacji proCertum CardManager oraz podstawowej obsługi tej aplikacji.

2. Instalacja czytników kart kryptograficznych w systemach Linux

W systemach Linux muszą być zainstalowane biblioteki do obsługi czytników kart kryptograficznych w zależności od jego rodzaju.

- libccid - PC/SC driver for USB CCID smart card readers
- libacr38u - PC/SC driver for the ACR38U smart card readers
- libacsccid1 - PC/SC driver for ACS USB CCID smart card readers

Dodatkowo będą potrzebne będą komponenty:

- pcscd
- pcsc-tool
- libpcsclite1

3. Instalacja aplikacji proCertum CardManager w systemach Linux

Plik instalacyjny aplikacji proCertumCardManager dla systemu Linux należy pobrać w zależności od rodzaju architektury, wersji glibc oraz QT ze strony:
http://www.certum.pl/certum/cert,oferta_proCertum_CardManager.xml

Plik binarny należy uruchomić w konsoli. Po zakończeniu instalacji zostanie wyświetlona lista komponentów do zainstalowania z pkt 2.

Aplikacja proCertumCardManager będzie umieszczona w katalogu */opt/proCertumCardManager*

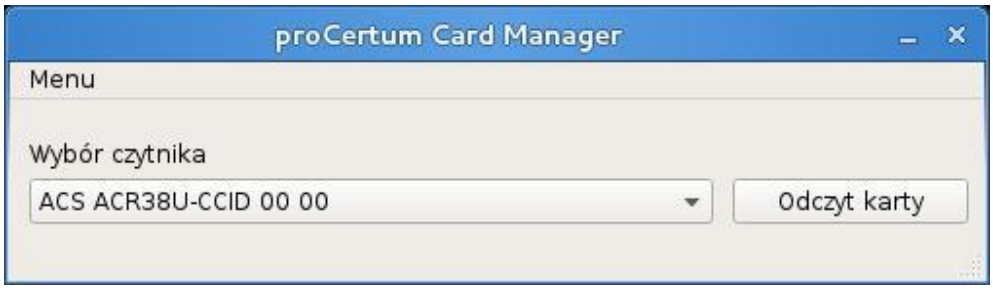
4. Deinstalacja aplikacji proCertumCardManager w systemach Linux

W celu usunięcia aplikacji proCertumCardManager należy uruchomić skrypt ***proCertumCardManager_uninstall*** znajdujący się w katalogu aplikacji */opt/proCertumCardManager*

Skrypt deinstalacyjny nie usuwa bibliotek ani komponentów **pcsc**.

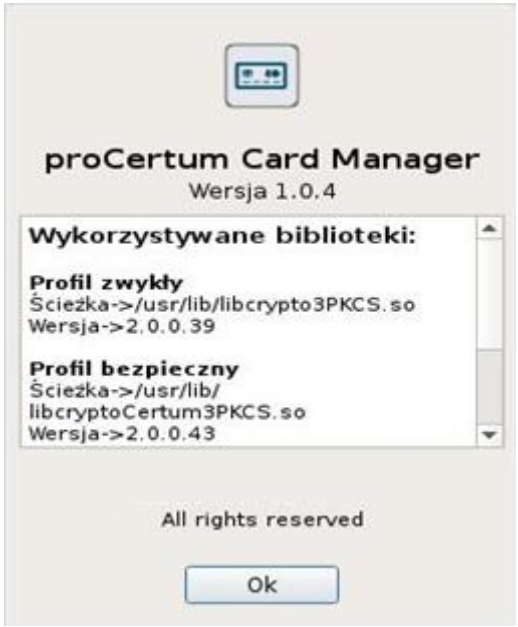
5. Obsługa aplikacji proCertum CardManager w systemach Linux

Przed uruchomieniem aplikacji proCertum CardManager należy do portu USB podłączyć czytnik kart kryptograficznych. Do czytnika należy włożyć kartę kryptograficzną i uruchomić aplikację **proCertumCardManager.**



Rysunek 1 – aplikacja proCertumCardManager

Po chwili na ekranie pojawi się aplikacja **proCertumCardManager**.
Po wywołaniu opcji **O programie** użytkownik może zapoznać się z informacjami o programie.



Rysunek 2 – o programie

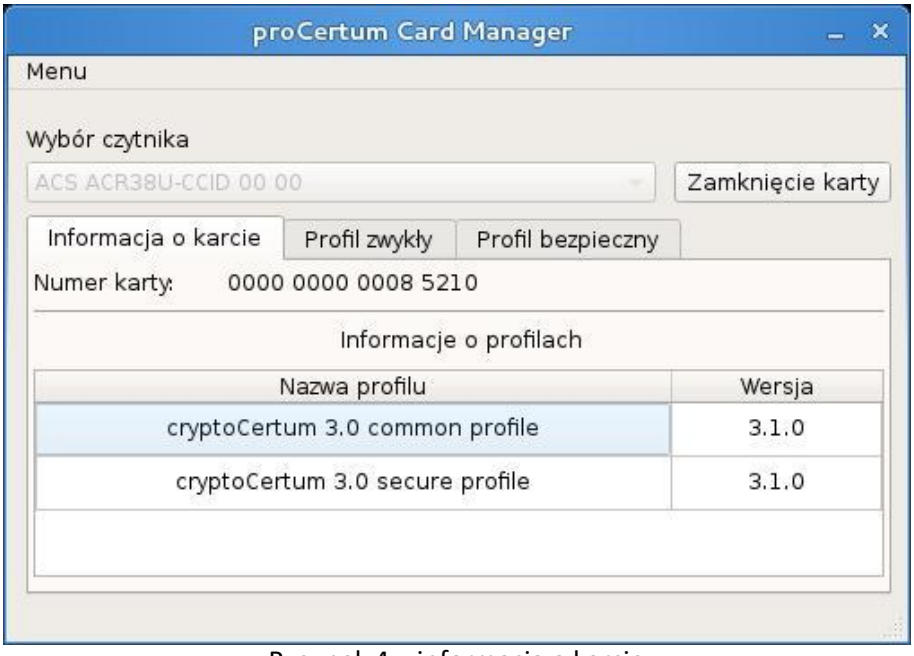
Domyślnie aplikacja ukrywa przyciski **Usunięcie certyfikatu.** W celu ich wyświetlenia należy z menu wybrać **Opcje**.

Rysunek 3 – opcje

W celu zakończenia pracy z aplikacją należy wybrać opcję **Zakończ**.

W listy rozwijalnej wybierz czytnik, którego używasz. Odczytaj zawartość kart przyciskiem **Odczyt karty**. Interfejs aplikacji podzielony jest na 3 zakładki:

Informacja o karcie – podstawowe informacje o karcie

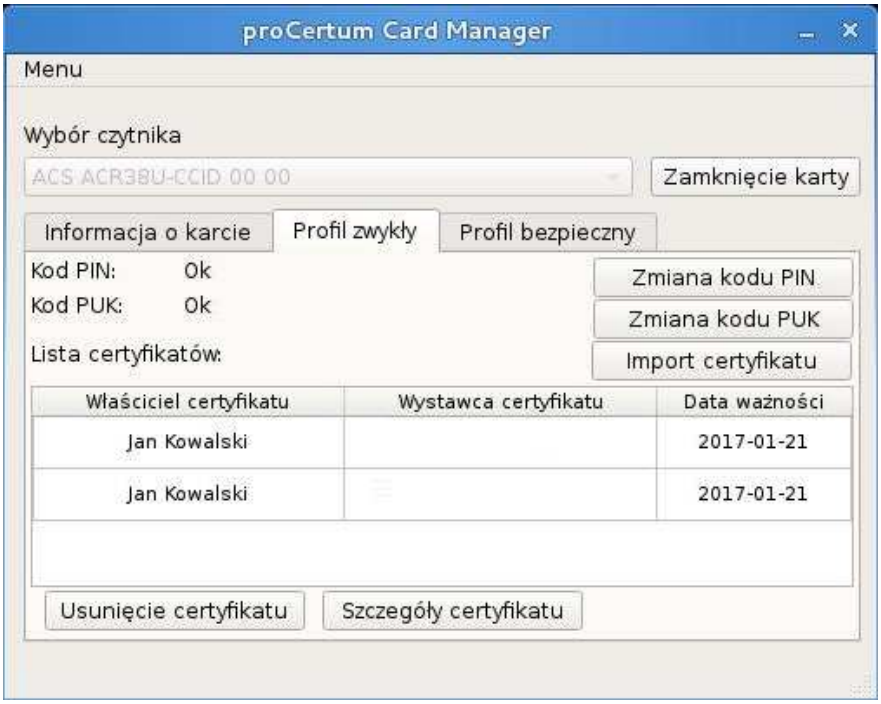


Rysunek 4 – informacja o karcie

W zakładce tej użytkownik może odczytać numer karty oraz sprawdzić jakie zostały utworzone profile.

5.1. Profil zwykły – certyfikaty niekwalifikowane

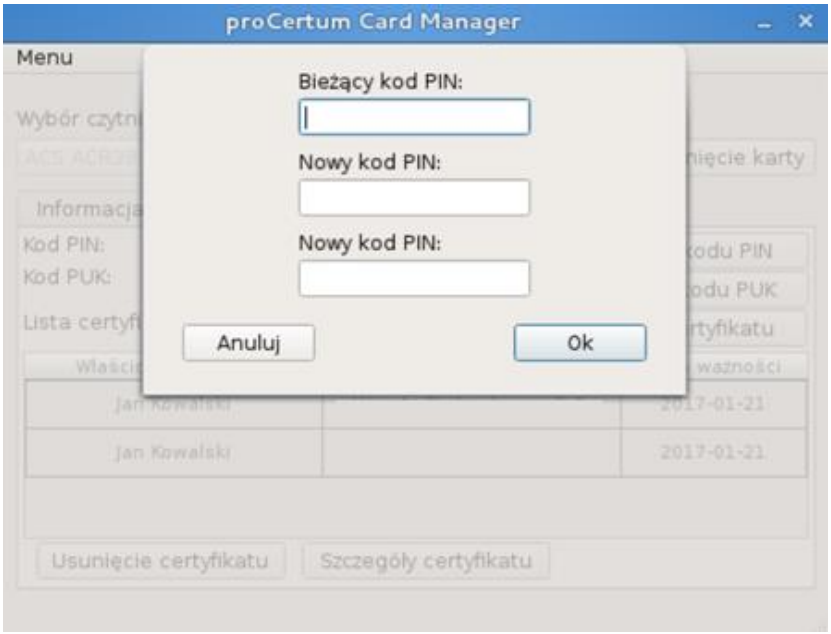
Profil zwykły – informacje na temat profilu i zawartych w nim certyfikatów



Rysunek 5 – profil zwykły karty

W zakładce tej użytkownik może odczytać: listę certyfikatów niekwalifikowanych, szczegóły poszczególnych certyfikatów, status kodu PIN/PUK.

W celu zmiany kodu PIN należy wybrać opcję **Zmiana kodu PIN**. Należy podać bieżący PIN a następnie zdefiniować nowy PIN.

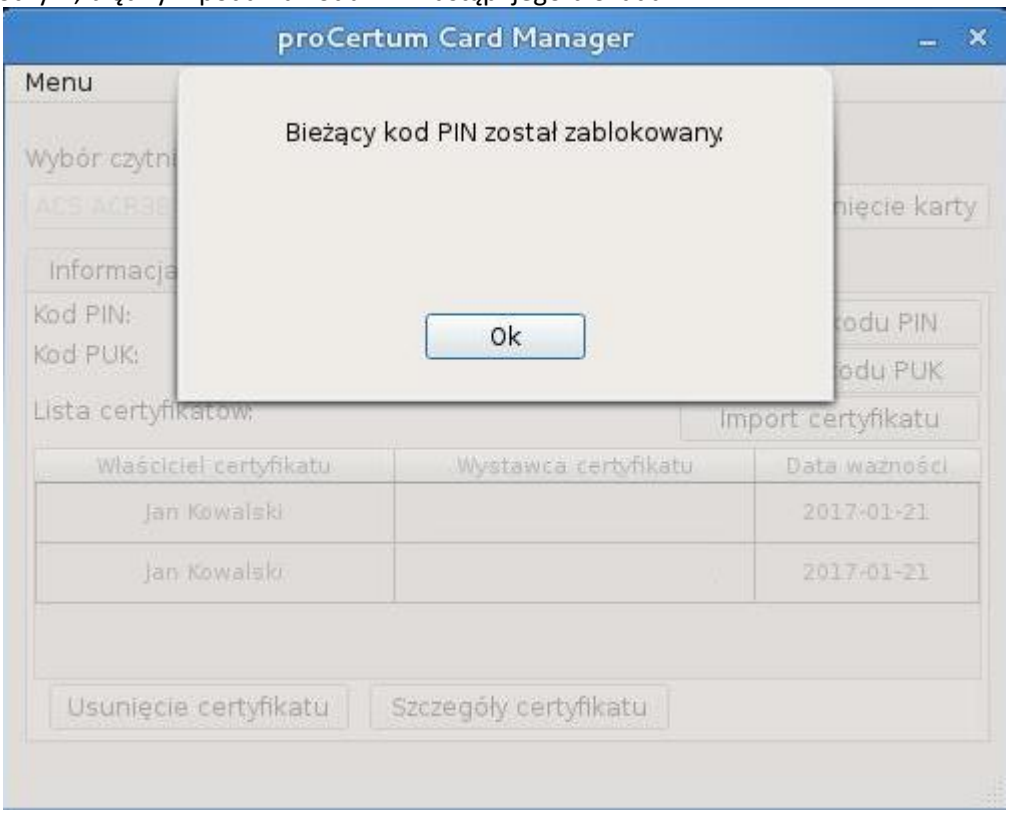


Rysunek 6 – profil zwykły karty – zmiana PIN

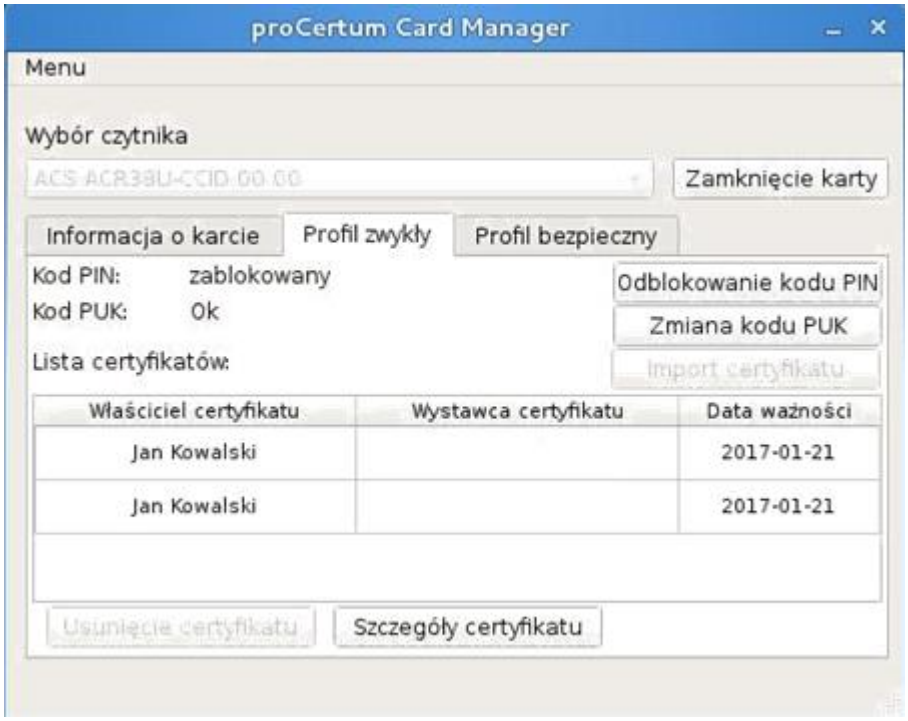
Minimalna długość PIN to 6 znaków a maksymalna długość PIN to 8 znaków. Po zdefiniowaniu nowego PIN na ekranie pojawi się komunikat:

Rysunek 7 – profil zwykły karty – potwierdzenie zmiany PIN

Po trzykrotnym, błędnym podaniu kodu PIN nastąpi jego blokada.

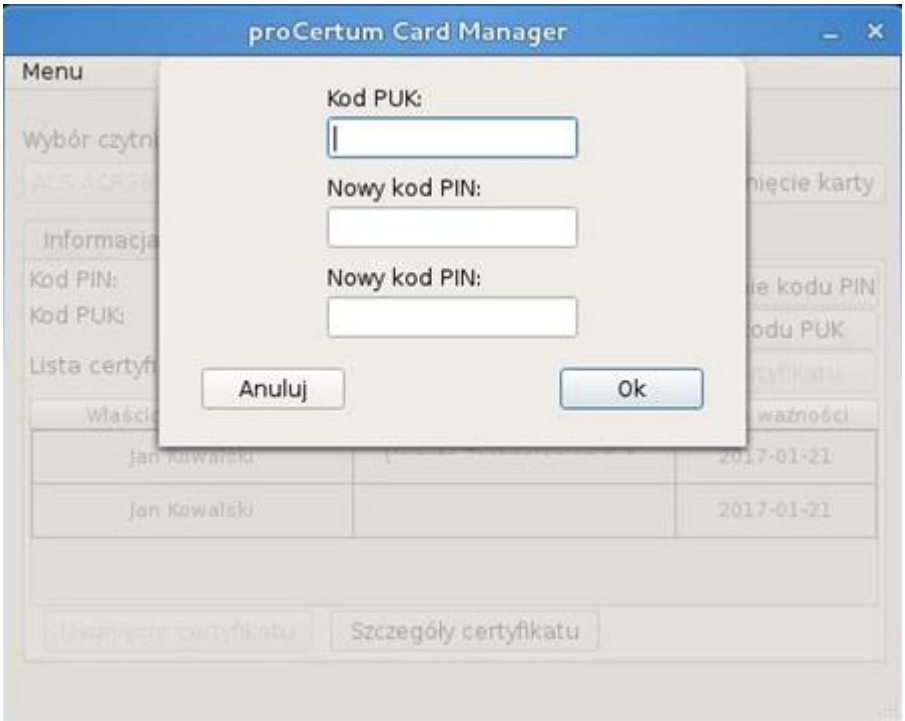


Rysunek 8 – profil zwykły karty – Zablokowany kod PIN



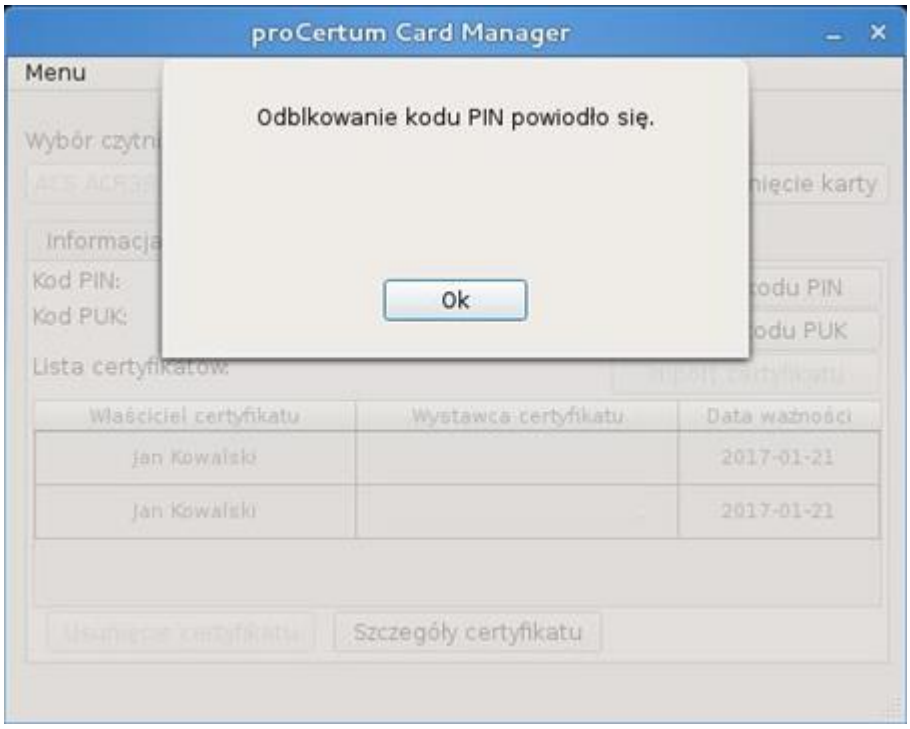
Rysunek 9 – profil zwykły karty – Zablokowany kod PIN

W celu odblokowania kodu PIN należy wybrać opcję ***Odblokowanie kodu PIN***



Rysunek 10 – profil zwykły karty – Odblokowanie kod PIN

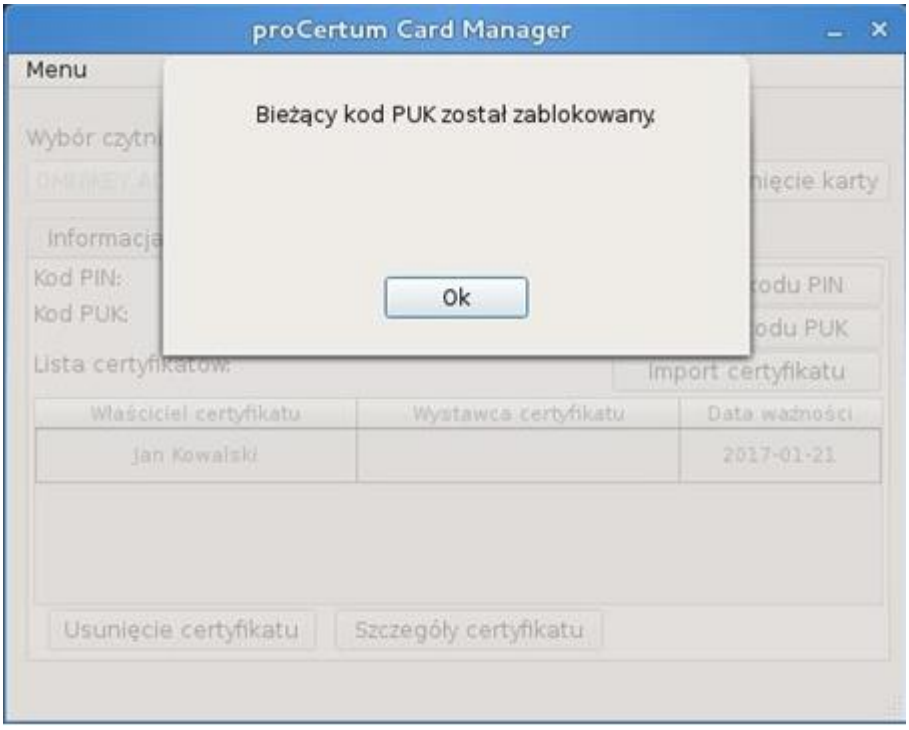
Po podaniu kodu PUK należy dwukrotnie podać nowy kod PIN



Rysunek 11 – profil zwykły karty – Odblokowany kod PIN

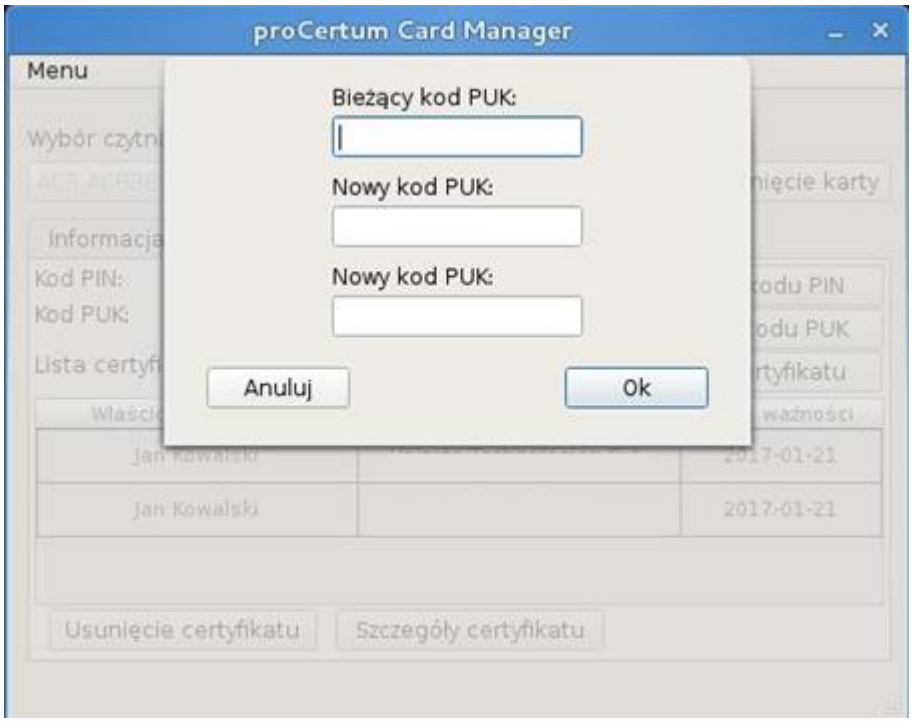
Odblokowanie kodu PIN na profilu bezpiecznym odbywa się w analogiczny sposób jak na profilu zwykłym.

UWAGA: Na obu profilach, po trzykrotnym, błędnym podaniu kodu PUK nastąpi jego **trwała** blokada.



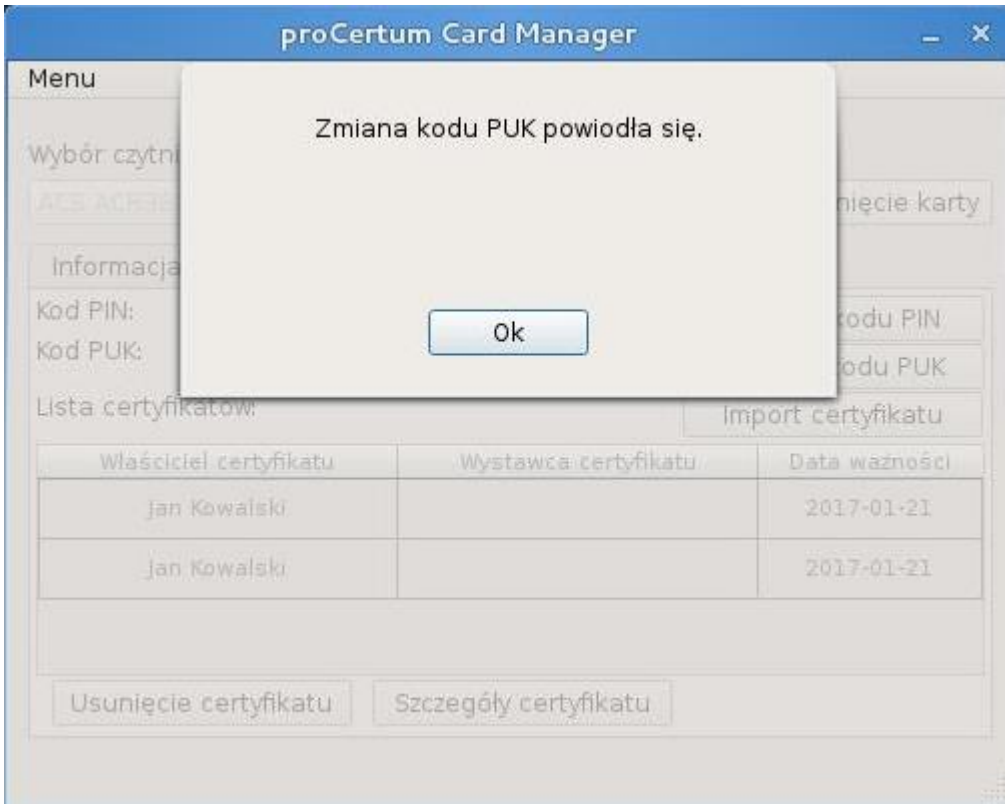
Rysunek 12 – profil zwykły karty – Blokada kodu PUK

Jeśli istnieje konieczność zmiany kodu PUK to należy wybrać opcję **Zmiana PUK**.



Rysunek 13 – profil zwykły karty – zmiana PUK

Minimalna długość PUK to 4 znaki a maksymalna długość PUK to 8 znaków. Po zdefiniowaniu nowego PUK na ekranie pojawi się komunikat:



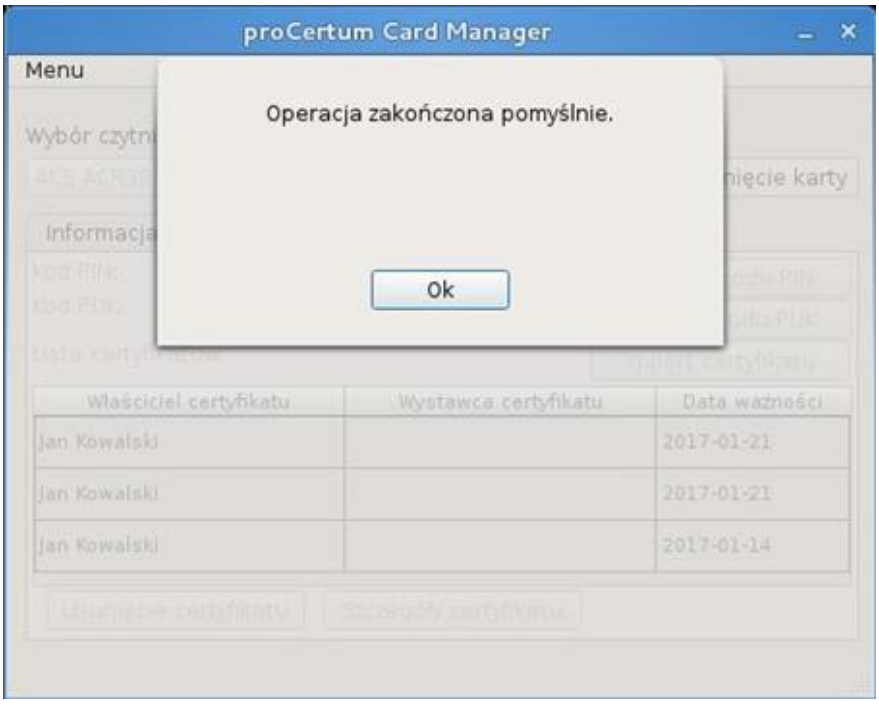
Rysunek 14 – profil zwykły karty – potwierdzenie zmiany PUK

Aplikacja **proCertum CardManager** pozwala na import do **profilu zwykłego certyfikatu niekwalifikowanego** z pliku p12 lub pfx (format zgodny z PKCS#12). W celu importu wybierz opcję **Import Certyfikatu**. Następnie wskaż plik z certyfikatem.

Po wskazaniu pliku z certyfikatem i potwierdzeniu wyboru przyciskiem **Otwórz** podaj hasło do pliku p12/pfx chroniące klucz prywatny. Ponadto należy podać bieżący PIN dla profilu zwykłego.

Rysunek 15 – profil zwykły karty – import certyfikatu

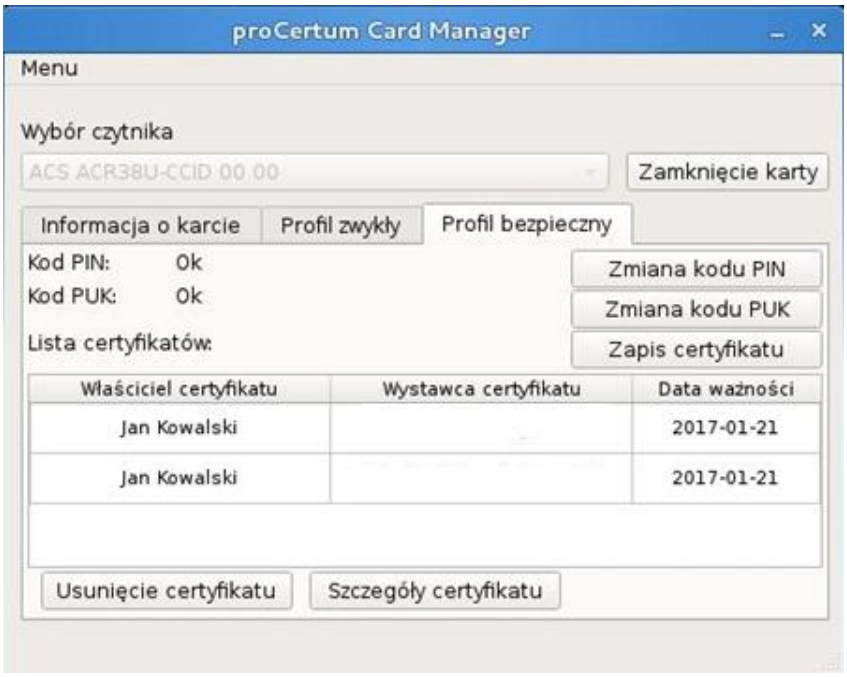
Podane dane należy potwierdzić przyciskiem **OK**. Proces importu zostanie potwierdzony poniższym komunikatem:



Rysunek 16 – profil zwykły karty – import certyfikatu

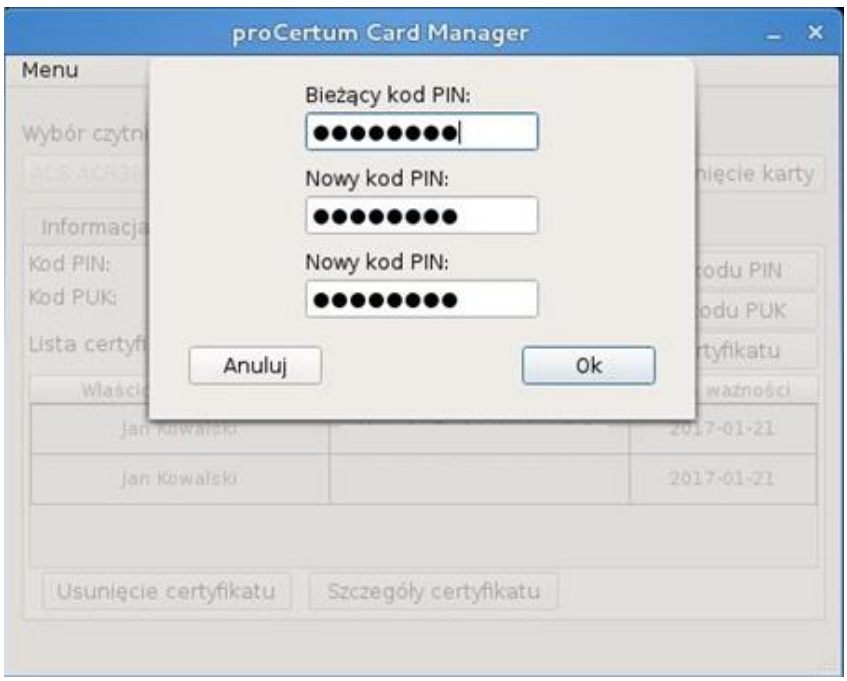
5.2. Profil bezpieczny – certyfikaty kwalifikowane

Profil bezpieczny – informacje na temat profilu i zawartych w nim certyfikatów



Rysunek 17 – profil bezpieczny karty

W zakładce tej użytkownik może odczytać: listę certyfikatów kwalifikowanych, szczegóły poszczególnych certyfikatów, status kodu PIN/PUK.
W celu zmiany kodu PIN należy wybrać opcję **Zmiana kodu PIN**. Należy podać bieżący PIN a następnie zdefiniować nowy PIN.

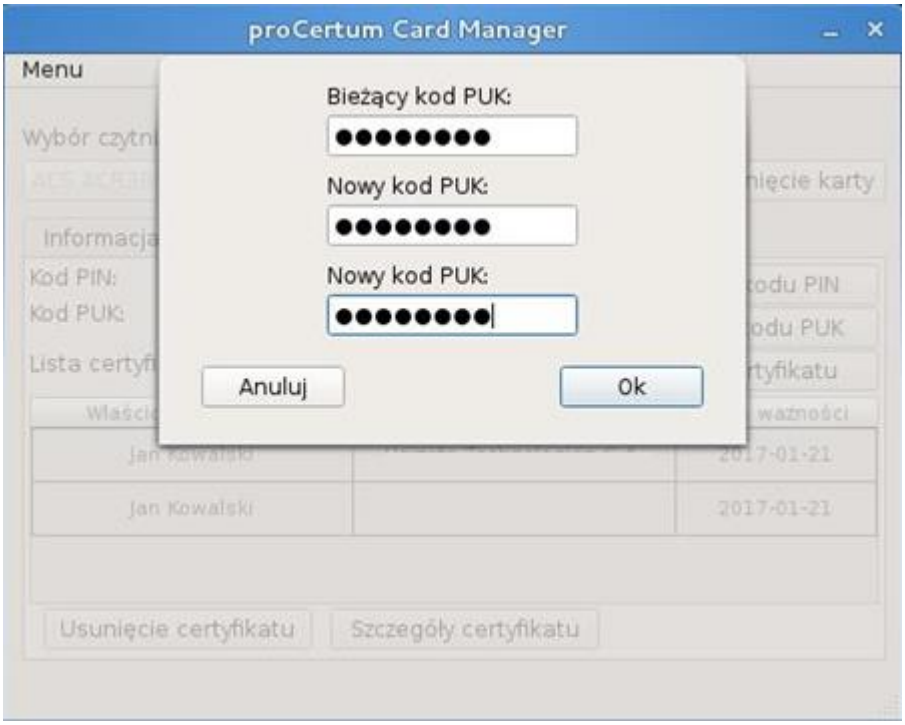


Rysunek 18 – profil bezpieczny karty – zmiana PIN

Minimalna długość PIN to 6 znaki a maksymalna długość PIN to 8 znaków. Po zdefiniowaniu nowego PIN na ekranie pojawi się komunikat:

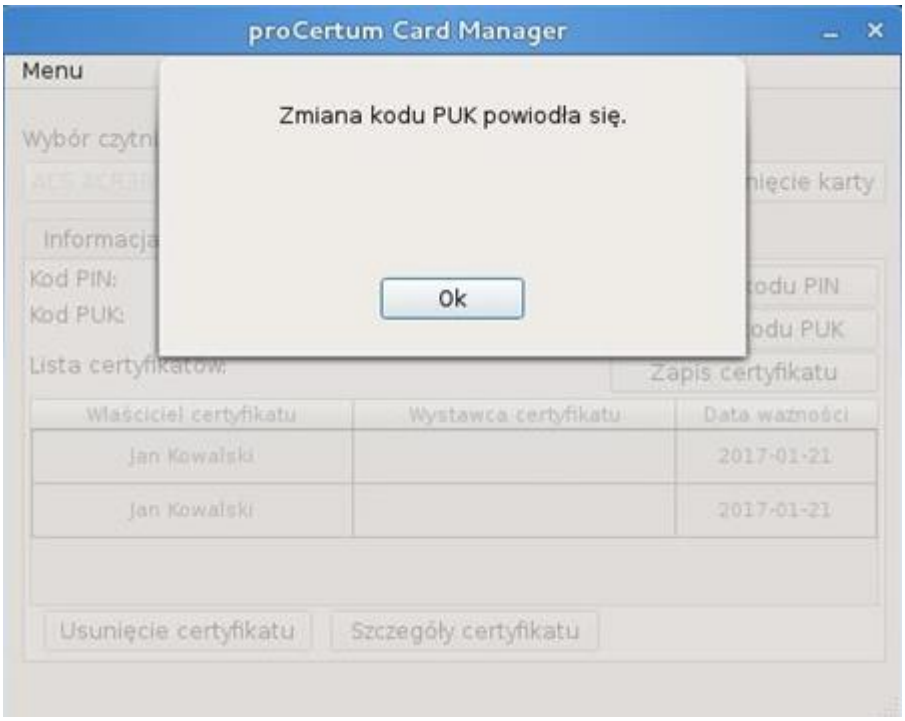
Rysunek 19 – profil bezpieczny karty – potwierdzenie zmiany PIN

Jeśli istnieje konieczność zmiany kodu PUK to należy wybrać opcję **Zmiana PUK**.
UWAGA: Na obu profilach, po trzykrotnym, błędnym podaniu kodu PUK nastąpi jego **trwała** blokada.



Rysunek 20 – profil bezpieczny karty – zmiana PUK

Minimalna długość PUK to 4 znaki a maksymalna długość PUK to 8 znaków. Po zdefiniowaniu nowego PUK na ekranie pojawi się komunikat:

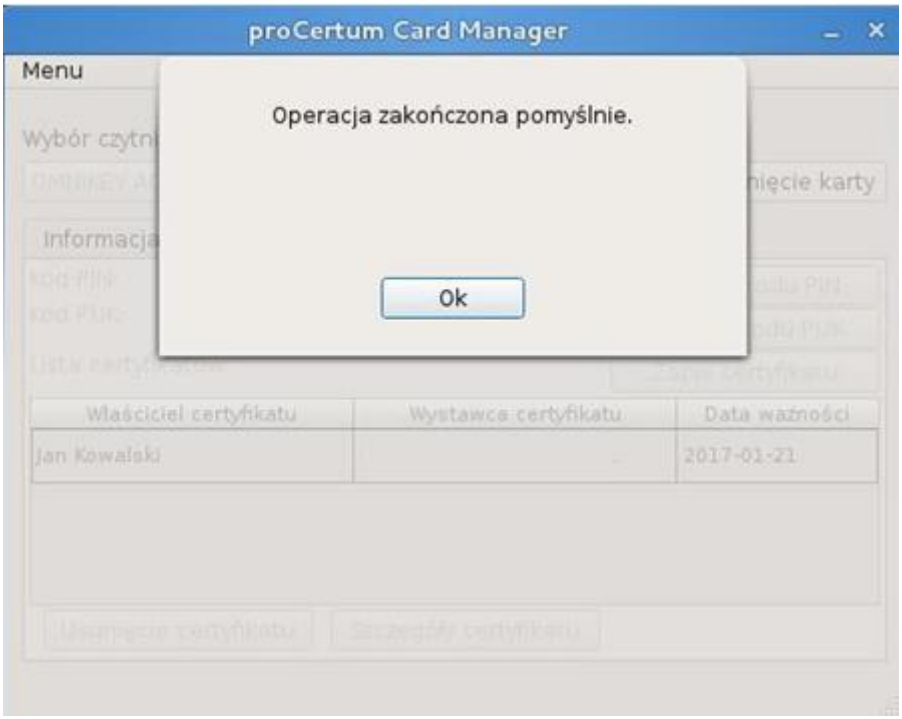


Rysunek 21 – profil bezpieczny karty – potwierdzenie zmiany PUK

Aplikacja **proCertum CardManager** pozwala na import do **profilu bezpiecznego certyfikatu kwalifikowanego** z pliku cer. lub der. (format X509). Warunkiem koniecznym jest posiadanie zapisanego klucza prywatnego na karcie w profilu bezpiecznym.
Po wskazaniu pliku z certyfikatem o potwierdzeniu wyboru przyciskiem. Należy podać bieżący PIN dla profilu bezpiecznego.

Rysunek 22 – profil bezpieczny karty – import certyfikatu

Podane dane należy potwierdzić przyciskiem **OK**. Proces importu zostanie potwierdzony poniższym komunikatem:



Rysunek 23 – profil bezpieczny karty – import certyfikatu