eKonto 2.0

Zarządzanie kartą elektroniczną

Wersja 20151028

Politechnika Poznańska
Pl. Marii Skłodowskiej-Curie 5
60-965 Poznań
http://www.put.poznan.pl/

Dział Rozwoju Oprogramowania
http://intranet.put.poznan.pl/department/at

Spis treści

1 Niezbędne oprogramowanie

Aby korzystać z obsługi certyfikatu na karcie musisz zainstalować sterowniki do karty oraz oprogramowania SmartCard Suite. Wszystkie pliki są dostępne w systemie **eProgramy**.

1.1 Oprogramowanie do zarządzania kartą

1.1.1 Pobranie oprogramowania SmartCard Suite

Zaloguj się do systemu eLogin a następnie przejdź do systemu **eProgramy**. Przejdź do zakładki **Dostępne oprogramowanie**, a następnie rozwiń gałąź **SmartCard**. Wciśnij przycisk **Szczegóły** obok nazwy **SmartCard Suite**. W kolejnym oknie wciśnij przycisk **Pobierz** aby pobrać najnowszą wersję aplikacji.

1.2 Sterowniki do karty

1.2.1 Uzyskanie kodu PIN do karty

Pracownicy Politechniki Poznańskiej mogą uzyskać kod PIN w Dziale Spraw Pracowniczych.

Studenci mogą sprawdzić swój początkowy PIN w systemie eStudent 2.0, w zakładce **Legitymacje**.

1.2.2 Sprawdzenie rodzaju karty

Pracownicy Politechniki Poznańskiej korzystają z kart Oberthur Cosmo 5.4 i Oberthur Cosmo 7, które wymagają sterowników **Oberthur Authentic Webpack**.

Studenci mogą sprawdzić rodzaj karty w systemie **eStudent 2.0** w zakładce **Legitymacje**.

1.2.3 Pobranie sterowników

Jeśli posiadasz kartę Oberthur Cosmo 5.4 lub Oberthur Cosmo 7 rozwiń gałąź **SmartCard** w systemie **eProgramy** i wciśnij przycisk **Szczegóły** obok pozycji **Oberthur Authentic Webpack**. W nowym oknie wciśnij przycisk **Pobierz** obok pliku **AWP 5.1.0 SR1 P11 Only.msi** lub **AWP 5.1.0 SR1 P11 Only 64-bit.msi** w zależności od wersji systemu operacyjnego, z którego korzystasz.

Jeśli posiadasz kartę Gemalto Optelio R5 rozwiń gałąź **SmartCard** w systemie **eProgramy** i wciśnij przycisk **Szczegóły** obok pozycji **Gemalto Classic Client**. W nowym oknie wciśnij przycisk **Pobierz** obok pliku **Classic_Client_32_User_setup.msi** lub **Classic_Client_64_User_setup.msi** w zależności od wersji systemu operacyjnego, z którego korzystasz.

Jeśli posiadasz kartę Gemalto Optelio R7 rozwiń gałąź **SmartCard** w systemie **eProgramy** i wciśnij przycisk **Szczegóły** obok pozycji **Gemalto IDGo 800**. W nowym oknie wciśnij przycisk **Pobierz** obok pliku **IDGo800_PKCS11_Library.msi**.

2 Instalowanie certyfikatu na karcie

2.1 Pobieranie certyfikatu

W celu pobrania certyfikatu należy wejść na stronę https://elogin.put.poznan.pl i się zalogować do swojego eKonta.

2.1.1 Rodzaje certyfikatów

Istnieje możliwość pobraniach dwóch rodzajów certyfikatów.

2.1.1.1 Certyfikat ogólnego przeznaczenia

Certyfikat ogólnego przeznaczenia może być wykorzystany, między innymi, do:

- uwierzytelnienia w uczelnianej sieci WiFi - na komputerze lub telefonie,
- podpisywania i szyfrowania listów e-mail - w kliencie pocztowym,
- logowania do serwisu eLogin - w przeglądarce komputera.

2.1.1.2 Certyfikat logowania do Windows

Certyfikat ten umożliwia logowanie się do systemu Windows za pomocą karty inteligentnej (legitymacji pracowniczej, studenckiej lub doktoranckiej). Możliwość ta dostępna jest na komputerach dodanych do domeny Active Directory Politechniki Poznańskiej.

2.1.2 Generowanie certyfikatu

Certyfikat możesz wygenerować z kluczem prywatnym utworzonym przez CA Politechniki Poznańskiej, lub dla klucza prywatnego wygenerowanego na karcie na podstawie pliku żądania wygenerowania certyfikatu (CSR).

2.1.2.1 Generowanie certyfikatu z systemowym kluczem prywatnym

Przed pobraniem certyfikatu należy go wygenerować. Jeśli wygenerowałeś certyfikat wcześniej i jego data ważności nie minęła, możesz przejść do punktu 2.1.3.

Aby wygenerować certyfikat zaloguj się do systemu eLogin i przejdź do zakładki **Certyfikaty**. Następnie wciśnij przycisk **Wygeneruj certyfikat – klucz CA** (**Wygeneruj Nowy Certyfikat**) w części odpowiadającej wybranemu rodzajowi certyfikatu.

2.1.2.2 Generowanie certyfikatu z kluczem prywatnym wygenerowanym na karcie (na podstawie CSR)

Przed wygenerowaniem certyfikatu należy na karcie wygenerować parę kluczy (patrz: 2.2.2.1). Jeśli na karcie znajduje się para kluczy, dla której chcesz wygenerować nowy certyfikat, należy utworzyć plik z żądaniem wygenerowania certyfikatu (CSR, patrz: 2.2.2.2).

W systemie eLogin odblokuj zaawansowane funkcje strony z certyfikatami. W tym celu przejdź do strony **Ustawienia** i zaznacz pole wyboru przy opcji **Chcę korzystać z zaawansowanych opcji na stronie z certyfikatami**. Na dole strony wciśnij przycisk **Zapisz**.

Jeśli masz już przygotowany plik CSR, w systemie eLogin przejdź do zakładki **Certyfikaty** i wciśnij przycisk **Wygeneruj certyfikat – żądanie CSR** dla wybranego rodzaju certyfikatu (2.1.1). Na następnym ekranie wskaż plik CSR i wciśnij **Wygeneruj certyfikat**.

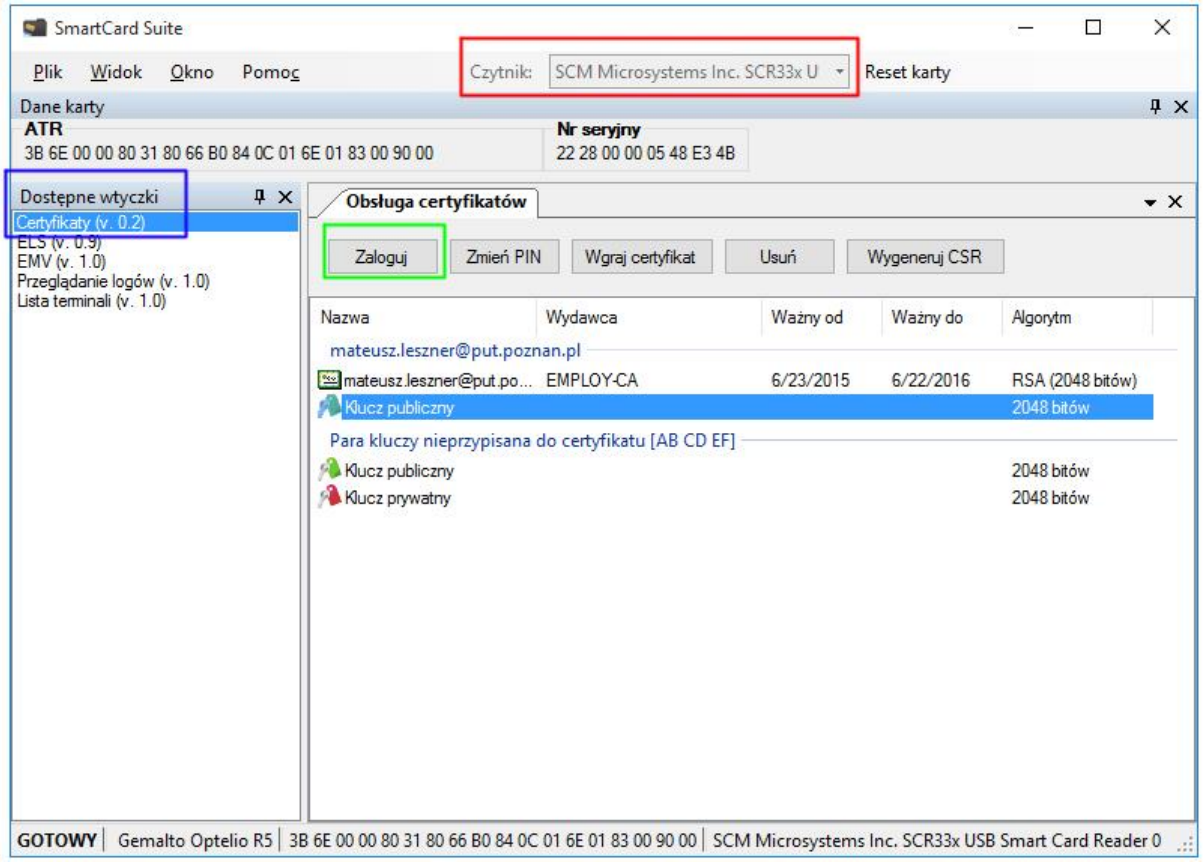
2.1.3 Pobieranie certyfikatu

Zaloguj się w systemie eLogin i przejdź do zakładki **Certyfikaty**. Następnie, w części odpowiadającej wybranemu rodzajowi certyfikatu wciśnij przycisk **Pobierz certyfikat publiczny**, aby pobrać certyfikat wygenerowany na podstawie żądania CSR, lub **Pobierz certyfikat z kluczem prywatnym**, aby pobrać certyfikat z kluczem prywatnym wygenerowanym przez CA Politechniki Poznańskiej. W przypadku certyfikatu z kluczem prywatnym na następnej stronie podaj aktualne hasło do eKonta oraz dowolne, wybrane przez siebie hasło do pliku z certyfikatem a następnie wciśnij przycisk **Pobierz certyfikat**.

2.2 Zarządzanie certyfikatami na karcie

Przed wykonaniem dalszych kroków upewnij się, że masz zainstalowaną aplikację do obsługi kart **SmartCard Suite** (patrz: 1.1.1) oraz odpowiednie sterowniki do karty (patrz: 1.2).

W aplikacji **SmartCard Suite** upewnij się, że w polu **Czytnik** (czerwony kolor) wybrany jest czytnik kart, z którego korzystasz. Następnie z listy w lewej części okna wybierz **Certyfikaty** (niebieski kolor) i dwukrotnie kliknij na tę pozycję. Zostanie załadowane okno umożliwiające zarządzanie certyfikatami.



Rysunek 1 Okno programu SmartCard Suite

2.2.1 Odczyt listy certyfikatów na karcie

Wciśnij przycisk **Zaloguj** (zielony kolor), a w nowym oknie podaj kod pin do karty (patrz: 1.2.2). Po poprawnym wprowadzeniu kodu pin zostanie odczytana i wyświetlona lisa certyfikatów i kluczy na karcie. Jeżeli kod pin jest zablokowany zobacz pkt. 3.1.

2.2.2 Generowanie pliku żądania CSR

2.2.2.1 Generowanie pliku żądania CSR dla nowej pary kluczy

Jeśli chcesz wygenerować nową parę kluczy na karcie, upewnij się, że na liście certyfikatów i kluczy nie jest zaznaczona żadna opcja (kliknij w białe pole na liście) a następnie wciśnij przycisk **Wygeneruj CSR**. Zostanie wygenerowana nowa para kluczy na karcie a następnie program wyświetli okno zapisywania pliku – wskaż w nim miejsce, w których chcesz zapisać plik CSR, który później użyjesz w systemie eLogin.

2.2.2.2 Generowanie pliku żądania CSR dla istniejącej pary kluczy

Na liście certyfikatów i kluczy zaznacz klucz prywatny, do którego chcesz wygenerować plik żądania CSR. Wciśnij przycisk **Wygeneruj CSR** a w kolejnym oknie wskaż miejsce, w którym chcesz zapisać plik CSR, który później użyjesz w systemie eLogin.

2.2.3 Wgrywanie certyfikatu na kartę

Przed wgraniem certyfikatu na kartę należy pobrać plik certyfikatu z systemu eLogin (patrz: 2.1.3).

W aplikacji **SmartCard Suite** zaloguj się do karty (patrz: 2.2.1) a następnie wciśnij przycisk **Wgraj certyfikat**. W nowym oknie wskaż plik certyfikatu pobrany z systemu eLogin. Jeśli wgrywasz certyfikat z kluczem prywatnym wygenerowanym przez CA Politechniki Poznańskiej zostanie wyświetlone pytanie o hasło – należy w nim podać hasło do certyfikatu wprowadzone w systemie eLogin (patrz: 2.1.3, **nie** jest to hasło do systemu eLogin). Certyfikat zostanie wgrany na kartę i wyświetlony na liście certyfikatów i kluczy.

2.2.4 Usuwanie certyfikatu z karty

Zaloguj się do karty (patrz: 2.2.1), a następnie na liście certyfikatów i kluczy wybierz certyfikat, który chcesz usunąć. Wciśnij przycisk **Usuń**.

Usuwanie certyfikatu nie powoduje usunięcia kluczy.

2.2.5 Usuwanie pary kluczy z karty

Zaloguj się do karty (patrz: 2.2.1), a następnie na liście certyfikatów i kluczy wybierz jeden z kluczy pary, którą chcesz usunąć. Wciśnij przycisk **Usuń**.

Usunięcie kluczy nie jest możliwe, jeżeli są one powiązane z certyfikatem – najpierw usuń certyfikat (2.2.4).

3 Zmiana kodu PIN

W aplikacji **SmartCard Suite** w oknie **Certyfikaty** wciśnij przycisk **Zmień PIN**. W nowym oknie wprowadź bieżący kod PIN. Po wciśnięciu **OK** zostanie wyświetlone okno z pytaniem o nową wartość kodu PIN. W obu polach wprowadź identyczną wartość nowego kodu PIN składającego się z liter i cyfr (wielkość liter ma znaczenie). Po wciśnięciu przycisku **OK** kod PIN zostanie zmieniony.

3.1 Zablokowany kod PIN

Pracownik, którego karta ma zablokowany kod PIN powinien zgłosić się do Działu Rozwoju i Oprogramowania.

Student, którego karta ma zablokowany kod PIN powinien zgłosić się do dziekanatu w celu zresetowania kodu PIN.

Rejestr zmian dokumentu	
Wersja	Opis
20120718	Utworzenie dokumentu
20120914	Opisanie odblokowania kodu PIN
20150421	Aktualizacja dla eProgramy i eCertyfikat
20151028	Nowa wersja dla SmartCard Suite i certyfikatów w eLogin