WYMAGANIA

dla stacji roboczych stanowisk obsługi dla użytkowników końcowych SRP

ŹRÓDŁO
Otwórz, kliknij, załatw sprawę

INNOWACYJNA GOSPODARKA
NARODOWA STRATEGIA SPÓJNOŚCI

pl.ID

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka

Ministerstwo
Spraw Wewnętrznych

COI
centralny ośrodek informatyki

1. Wymagania sprzętowe

Każde stanowisko do obsługi aplikacji ŹRÓDŁO, w zależności od poszczególnych komponentów powinno składać się z:

- Zestaw komputerowy (komputer/monitor/klawiatura/mysz)
- Czytnik kart kryptograficznych
- Drukarka
- Skaner (wymagany w przypadku obsługi RDO)

Dodatkowo stacja musi posiadać połączenie sieciowe z dostępem do Internetu. Każda osoba upoważniona do pracy z aplikacją powinna posiadać personalną kartę z ważnym certyfikatem, wydanym przez Centrum certyfikacji MSW.

2. Wymagania systemowe

Każda stacja robocza powinna spełniać następujące wymagania:

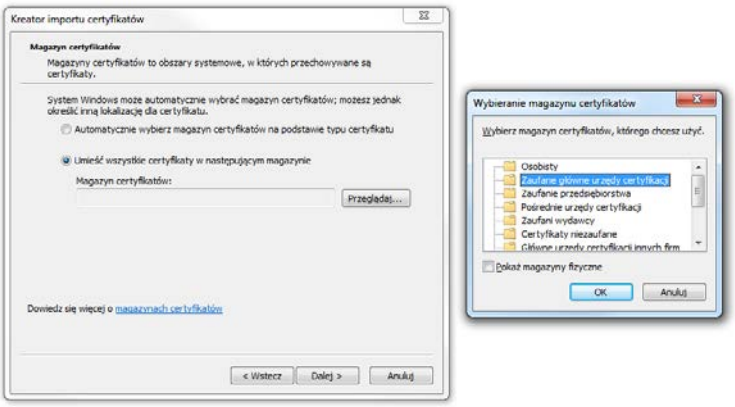
- System operacyjny MS Windows (Vista, Win 7, Win 8)
- Oprogramowanie Java SE 7 Runtime Environment (JRE) Update 45 lub nowsze
- Przeglądarka plików PDF (np. Adobe Reader)
- Aktualne oprogramowanie antywirusowe
- Przeglądarka Internetowa umożliwiająca uruchamianie apletów języka Java:
    - Mozilla Firefox (wersja 24 lub nowsza)
    - Internet Explorer (wersja 10 lub nowsza)
    - Google Chrome (wersja 30 lub nowsza)
- Zainstalowane sterowniki dla następujących urządzeń peryferyjnych:
    - Drukarka A4
    - Skaner obsługujący sterownik skanowania TWAIN (np. EPSON V33 lub HP ScanJet G2710)

3. Przygotowanie stanowiska

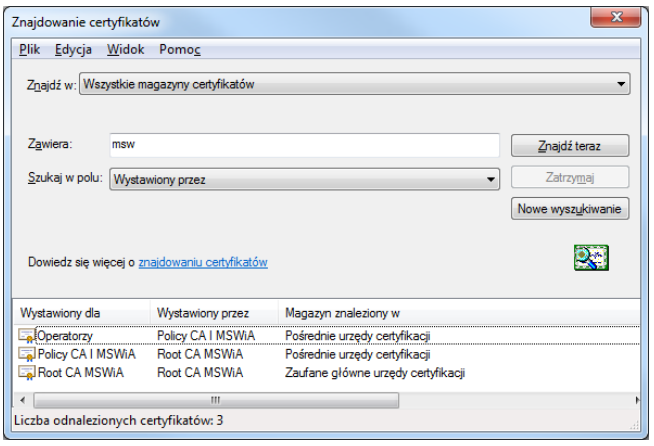
3.1. Instalacja certyfikatów

W celu pobrania certyfikatów niezbędny jest dostęp do strony https://ankiety.obywatel.gov.pl/

Po zalogowaniu się wybieramy z menu po lewej ***Pliki do Pobrania*** i pobieramy na stację paczkę z certyfikatami, które trzeba będzie zainstalować dla konta lokalnego komputera. Certyfikat o nazwie *„root.cer" instalujemy wskazując ręcznie magazyn certyfikatów* ***Zaufane główne urzędy certyfikacji.*** *Pozostałe certyfikaty tj. „policy.cer" oraz „operatorzy.cer" instalujemy wskazując ręcznie magazyn* ***Pośrednie urzędy certyfikacji.***



Poprawną instalację można zweryfikować za pomocą konsoli wpisując w menu start -> uruchom: **certmgr.msc** i wyszukując certyfikatów wystawionych przez MSW.

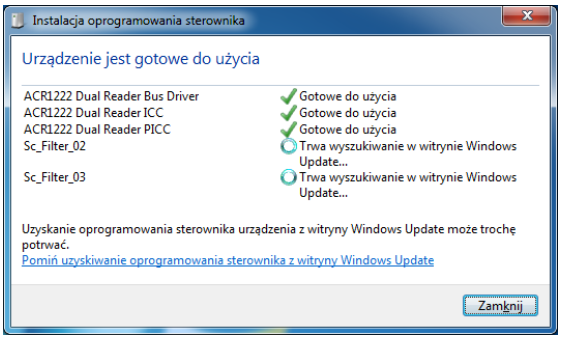


3.2. Instalacja czytnika kart kryptograficznych

Każda stacja powinna posiadać zainstalowany jeden z czytników kart inteligentnych:

- Czytnik kart ACS ACR85 PINPad
- Czytnik kart ACS ACR1222
- Czytnik kart SCM Microsystem SDI011

Przykładowy czytnik kart ACS ACR1222



Instalacja sterowników w systemie MS Windows 7

Aby czytnik umożliwiał poprawną komunikację z kartą, należy zainstalować aktualne sterowniki. Zalecaną formą pobrania sterowników jest wyszukanie ich w witrynie Windows Update. Dopuszcza się czytniki kart inteligentnych innych firm pod warunkiem, że są zgodne ze standardami ISO/IEC 14443, ISO/IEC 7816 oraz ISO/IEC 18092. W razie problemów z wintryną Windows Update sterowniki można pobrać ze strony https://ankiety.obywatel.gov.pl/ w dziale ***Pliki do pobrania.***

3.3. Modele kart kryptograficznych

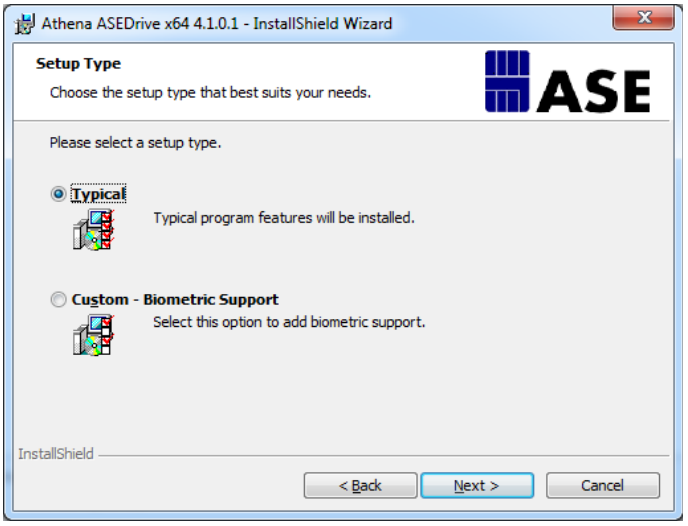
Pracownik musi posiadać kartę kryptograficzną wraz z zainstalowanym certyfikatem, upoważniający do pracy z SRP, wydanym przez Centrum Certyfikacji MSW. Certyfikaty wydawane są na następujących rodzajach kartach:

Athena IDProtect DuO *Gemalto ID Prime MD3810*

W zależności od modelu wykorzystywanej karty (patrz kształt chip'a) należy zainstalować do niej odpowiednie sterowniki. Zaleca się instalację oprogramowania dla obu kart kryptograficznych.

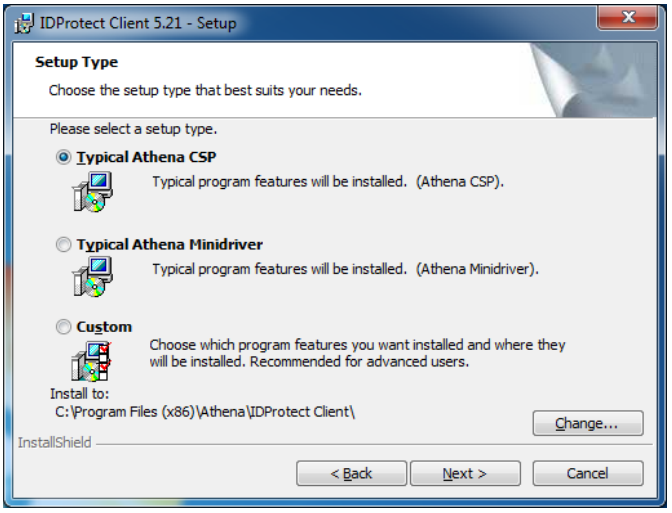
3.4. Instalacja i konfiguracja karty Athena

Pobieramy sterowniki ***ASEDrive IIIe*** w wersji 32-bit lub 64-bit ze strony producenta: http://www.athena-scs.com/support/software-driver-downloads Podczas instalacji przeglądarka Firefox musi być zamknięta. W kreatorze instalacji należy wybrać opcję ***Typical*** jako rodzaj instalacji.

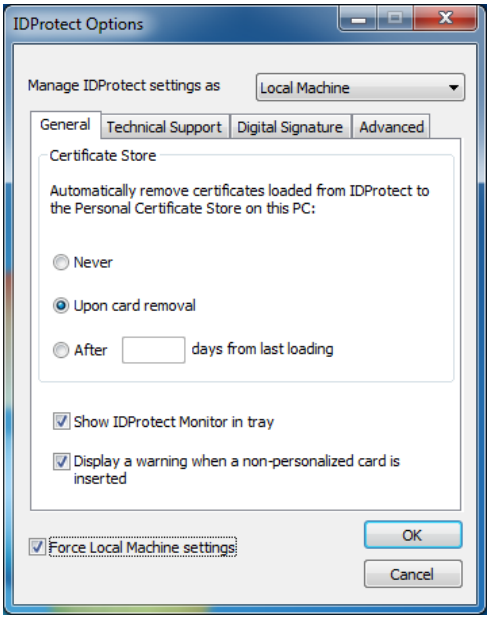


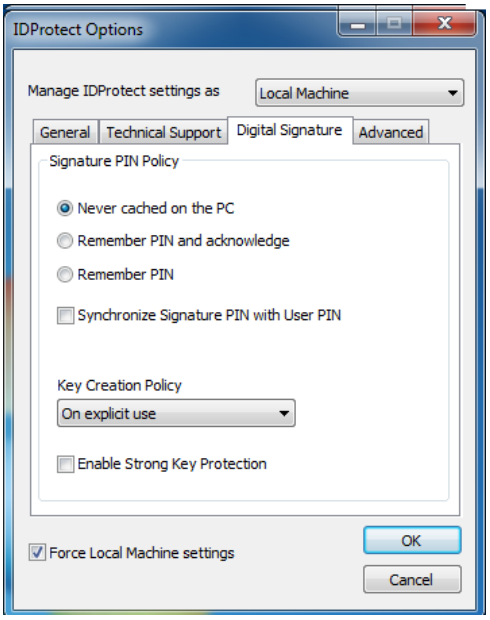
W celu pobrania plików instalacyjnych niezbędny jest dostęp do strony https://ankiety.obywatel.gov.pl/

Po zalogowaniu się wybieramy z meniu po lewej ***Pliki do Pobrania***. Pobieramy na stację program do instalacji sterowników ***IDProtectClient***. Uruchamiamy instalator za pomocąpliku ***Setup*** lub ***Setupx64*** w zależności od wersji systemu operacyjnego. Podczas instalacji należy wybrać opcję ***Typical Athena CSP.***



Będąc zalogowanym na stacji jako lokalny administrator uruchamiamy na stacji program **IDProtetc Options** i zmieniamy opcję ***Manage IDProtect settings*** na *„Local Machine”*. Dalej w zakładce ***General*** ustawiamy *„Upon card removal”* i zaznaczamy *„Force Local Machine settings”.* W zakładce ***Digital signature*** ustawiamy opcję *„Never cached on the PC”* i zaznaczamy *„Force Local Machine settings”*. Poniżej zaprezentowano przykład poprawnej konfiguracji.





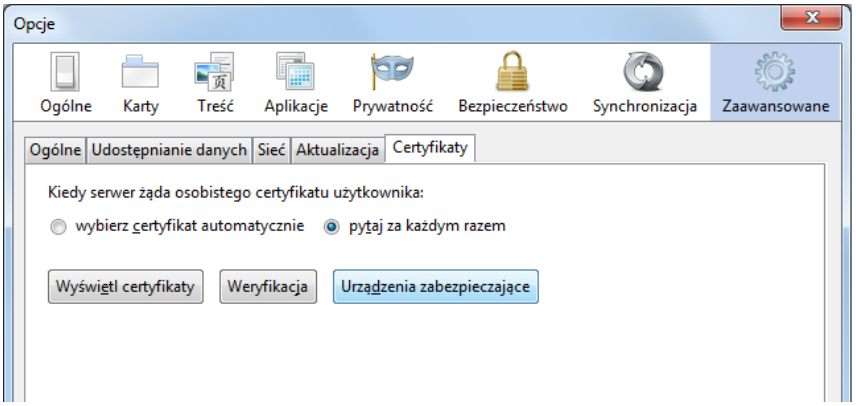
Instalacja i konfiguracja oprogramowania *IDProtect Client* oraz Athena *ASEDrive III* umożliwi korzystanie na stanowisku z kart kryptograficznych **Athena *IDProtect DuO***.

3.5. Instalacja i konfiguracja karty Gemalto

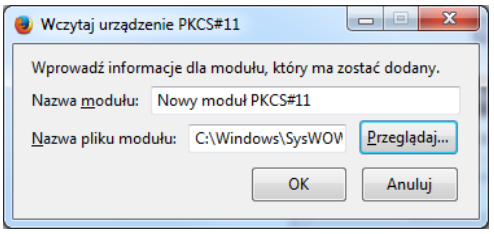
Zalecaną formą pobrania sterowników dla kart Gemalto jest wyszukanie ich w witrynie Windows Update. W przypadku niepowodzenia instalacji należy sprawdzić czy sterowniki nie oczekują w kolejce na instalację wraz z innymi aktualizacjami systemowymi na danej stacji. Można je również zainstalować ręcznie, pobierając ze strony Microsoft Update (link do zasobu dostępny jest na stronie https://ankiety.obywatel.gov.pl/)

Dodatkowo dla przeglądarki **Firefox** konieczne jest załadowanie modułu urządzenia zabezpieczającego. W tym celu niezbędny jest dostęp do strony https://ankiety.obywatel.gov.pl/ Po zalogowaniu się wybieramy z meniu po lewej ***Pliki do Pobrania***. Wybieramy **PKCS11** i zapisujemy plik ***IDPrimePKCS11.dll*** w folderze C:\Windows\SysWOW64 lub C:\Windows\System32 w zależności od wersji systemu.

Następnie w przeglądarce Firefox wybieramy z głównego menu *„Opcje”* następnie *„Zaawansowane”* i zakładkę *„Certyfikaty”* i kliakmy na przycisk *„Urządzenia zabezpieczające”.*



Za pomocą przycisku *„Wczytaj”* wskazujemy plik ***IDPrimePKCS11.dll*** w folderze systemowym który przenieśliśmy chwilę wcześniej. Zaleca się zmianę nazwy nowego modułu na **Gemalto PKCS#11**

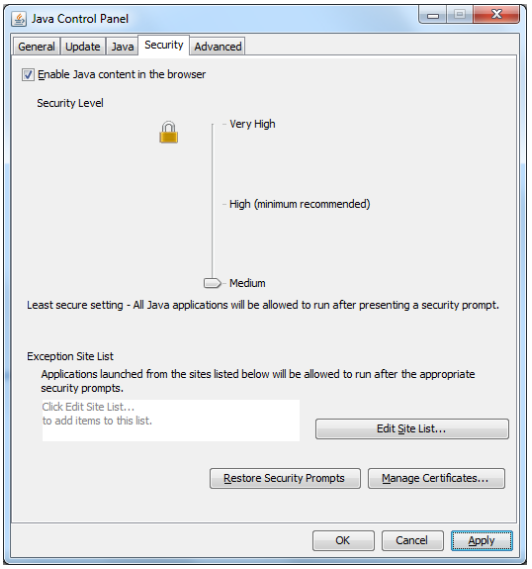


Nowy moduł PKCS#11 wczytujemy wyłącznie dla przeglądarki Firefox.

3.6. Konfiguracja oprogramowania Java

W przypadku braku oprogramowania Java należy zainstalować jego najnowszą wersję, która dostępna jest na stronie producenta: https://www.java.com/pl/download/

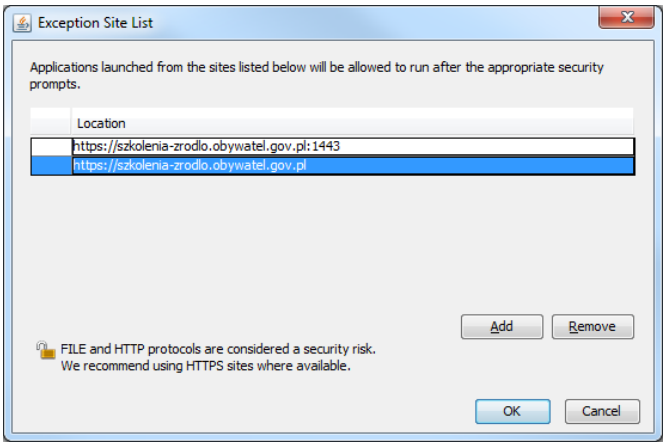
W panelu sterowania odnajdujemy **Java Control Panel** i ustawiamy poziom zabezpieczeń na *„Medium”:*



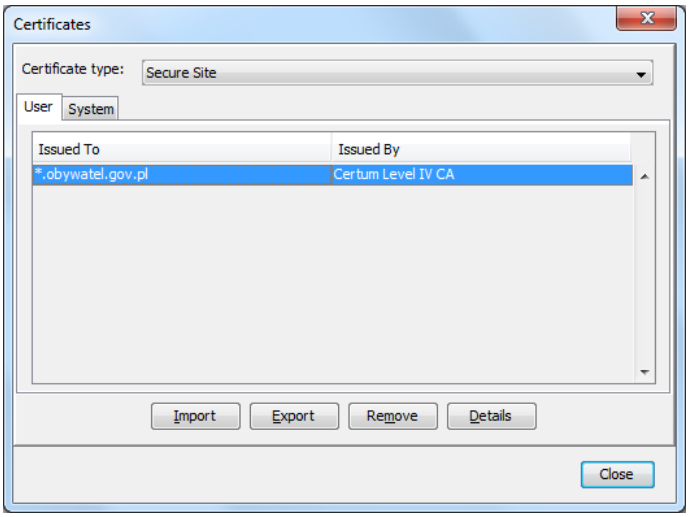
Następnie za pomocą przycisku **Edit Site List ...** dodajemy dwa adresy:

https://szkolenia-zrodlo.obywatel.gov.pl:1443

https://szkolenia-zrodlo.obywatel.gov.pl



Ponownie w zakładce Security wybieramy przycisk **Manage Certificates**. W nowo otwartym oknie wybieramy rodzaj certyfikatu jako **Secure Site** i importujemy jeden z pobranych wcześniej certyfikatów o nazwie „obywatel.cer”.



3.7. Sprawdzenie drukarki i skanera

Należy zweryfikować czy sterowniki do urządzeń peryferyjnych są zainstalowane poprawnie. W tym celu należy wydrukować stronę testową oraz zeskanować przykładowy dokument (na stacjach które są wyposażone w skaner).

4. Wymagania sieciowe

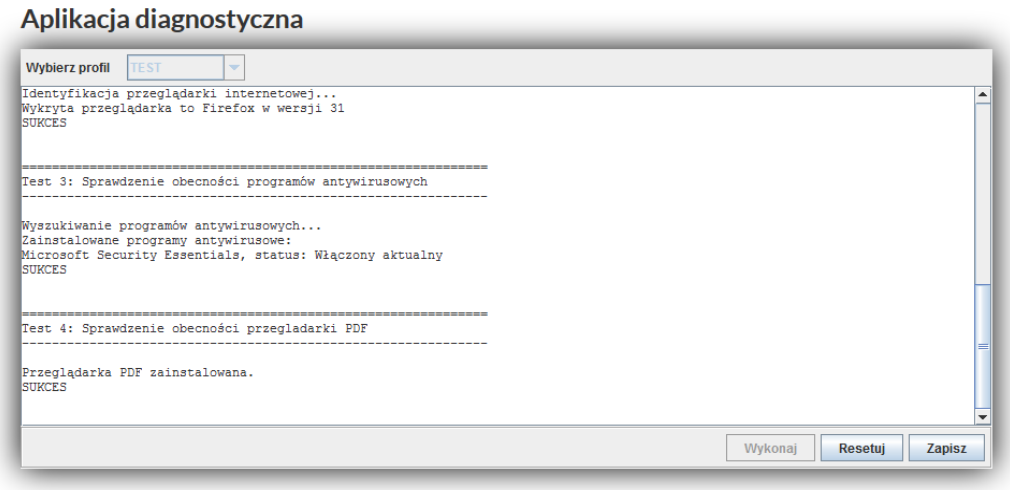
W celu poprawnej komunikacj z aplikacją ŹRÓDŁO, należy zezwolić na ruch w sieci pomiędzy stacją a systemem SRP w oparciu o następujące numery portów: **443, 1443, 20443**. W zależności od topologii sieci w danej lokalizacj, reguły dotyczące wymienionych portów należy wdrożyć we właściwych miejscach i na adekwatnych urządzeniach.

5. Lista kontrolna

Na koniec lista sprawdzająca wykonanie wszystkich niezbędnych kroków do poprawnego przygotowania stacji:

- Instalacja certyfikatów
  - wybranie odpowiednich magazynów
- Instalacja czytnika kart
- Instalacja / konfiguracja karty Athena
  - instalacja sterowników producenta ASEDrive IIIe
  - instalacja oprogramowania IDProtect Client
  - zmiana ustawień w programie IDProtect Option
- Instalacja / konfiguracja karty Gemalto
  - podpięcie biblioteki dla przeglądarki Firefox
- Instalacja / konfiguracja oprogramowania JAVA
  - zmiana poziomu zabezpieczeń w panelu
  - dodanie adresów jako wyjątki
  - instalacja certyfikatu
- Testy drukowania i skanowania

Dodatkowe narzędzie do weryfikacji konfiguracji stanowiska do obsługi SRP znajduje się na stronie https://ankiety.obywatel.gov.pl Po zalogowaniu się wybieramy z meniu po lewej **Diagnostyka** a następnie wybieramy profil „Test” i uruchamiamy przyciskiem „Wykonaj”.



Podczas diagnostyki sprawdzane są następujące elementy:

- Test 1: Sprawdzenie wersji Java i systemu operacyjnego
- Test 2: Sprawdzenie przeglądarki internetowej
- Test 3: Sprawdzenie obecności programów antywirusowych
- Test 4: Sprawdzenie obecności przegladarki PDF

Pomyślne zakończenie każdego z testów opatrzone będzie słowem **SUKCES** w oknie aplikacji diagnostycznej.

6. Zgłaszanie problemów

Wszelkie problemy należy zgłaszać poprzez Service Desk (aplikację ITSM) dostępną pod adresem https://pomoc.coi.gov.pl lub poprzez dedykowaną linie telefoniczną – (42) 253 54 99 – obsługiwaną przez zespół przeszkolonych konsultantów. Usługa ta będzie dostępna w dni robocze w godzinach od 8:00 do 16:00.

UWAGA! Preferowanym formą kontaktu w zgłaszaniu błędów jest korzystanie z systemu zgłoszeń ITSM, m.in. z uwagi na fakt, że skuteczne zgłoszenie błędu wymaga dołączenia załączników np. takich jak zrzut ekranu, które nie są możliwe do przekazania drogą telefoniczną.

Instrukcja w jaki sposób korzystać z aplikacji ITSM dostępna jest na stronie www.obywatel.gov.pl w zakładce dedykowanej Lokalnym Administratorom Systemu.