WYMAGANIA

dla stacji roboczych stanowisk obsługi dla użytkowników końcowych SRP











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



Ministerstwo Spraw Wewnętrznych





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:
 - o 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.*

Magazyn certyfikatów	
Magazyny certyfikatów to obszary systemowe, w których przechowywane są certyfikaty.	
System Windows może automatycznie wybrać magazyn certyfikatów; możesz jednak określić inną lokalizację dla certyfikatu.	Wybieranie magazynu certyfikatów
Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu	Wybierz magazyn certyfikatów, którego chcesz uży
Umieść wszystkie certyfikaty w następującym magazynie	Osobisty
Magazyn certyfikatów:	Zaufane glówne urzędy certyfikacj
Przeglądaj	Zaufanie przedsiębiorstwa Pośrednie urzędy certyfikacii
	Zaufani wydawcy
	Glówne urzedy certyfikarii innych firm
	Pokaż magazyny fizyczne
	OK Anulus
Dowiedz się więcej o <u>magazynach certyfikatów</u>	

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

najdowanie certyi	fikatów		×
Plik Edycja <u>w</u>	idok Pomo <u>c</u>		
Z <u>n</u> ajdź w: Wszyst	kie magazyny certyfikatów		•
Z <u>a</u> wiera: m	ISW		Znajdź teraz
Szukaj w polu: Wystawiony przez		Zatrzy <u>m</u> aj	
Nowe wysz <u>u</u> kiwa		Nowe wysz <u>u</u> kiwanie	
Dowiedz sie wiece	ej o znajdowaniu certyfikatów	L	
Wystawiony dla	Wystawiony przez	Magazyn znaleziony w	
Wystawiony dla	Wystawiony przez Policy CA I MSWiA	Magazyn znaleziony w Pośrednie urzędy certyfikacji	
Wystawiony dla Operatorzy Policy CA I MSV	Wystawiony przez Policy CA I MSWiA ViA Root CA MSWiA	Magazyn znaleziony w Pośrednie urzędy certyfikacji Pośrednie urzędy certyfikacji	
Wystawiony dla Operatorzy Policy CA I MSV Root CA MSWi/	Wysławiony przez Policy CA I MSWiA ViA Root CA MSWiA & Root CA MSWiA	Magazyn znaleziony w Pośrednie urzędy certyfikacji Pośrednie urzędy certyfikacji Zaufane główne urzędy certyfikacji	
Wystawiony dla Operatorzy Policy CA I MSV Root CA MSWi <i>l</i>	Wystawiony przez Policy CA I MSWIA VIA Root CA MSWIA Root CA MSWIA	Magazyn znaleziony w Pośrednie urzędy cettyfikacji Pośrednie urzędy cettyfikacji Zaufane główne urzędy cettyfikacji	



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



📋 Instalacja oprogramowania sterownika	×	
Urządzenie jest gotowe do użyc	ia	
ACR1222 Dual Reader Bus Driver	✓ Gotowe do użycia	
ACR1222 Dual Reader ICC	Gotowe do uzycia	
ACR1222 Dual Reader PICC	Gotowe do uzycia	
Sc_Filter_02	Trwa wyszukiwanie w witrynie Windows Update	
Sc_Filter_03	Trwa wyszukiwanie w witrynie Windows Update	
Uzyskanie oprogramowania sterownika urządzenia z witryny Windows Update może trochę potrwać. Pomiń uzyskiwanie oprogramowania sterownika z witryny Windows Update		
	Zam <u>k</u> nij	

Instalacja sterowników w systemie MS Windows 7

Przykładowy czytnik kart ACS ACR1222

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

3.3. Modele kart kryptograficznych

https://ankiety.obywatel.gov.pl/ w dziale Pliki do pobrania.

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:

<u>http://www.athena-scs.com/support/software-driver-downloads</u> Podczas instalacji przeglądarka Firefox <u>musi</u> <u>być zamknięta</u>. 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.

IDProtect O	ptions	Į	- • ×
Manage ID	Protect settings as	Local Machine	e 🔻
General	Technical Support	Digital Signature	Advanced
Certific	ate Store		
Automatically remove certificates loaded from IDProtect to the Personal Certificate Store on this PC:			IDProtect to
© Nev	/er		
O Upo	Upon card removal		
© Afb	er days f	from last loading	
 Show IDProtect Monitor in tray Display a warning when a non-personalized card is inserted 			
Force L	ocal Machine setting	9	OK Cancel





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 <u>https://ankiety.obywatel.gov.pl/</u>)

Dodatkowo dla przeglądarki **Firefox** konieczne jest załadowanie modułu urządzenia zabezpieczającego. W tym celu niezbędny jest dostęp do strony <u>https://ankiety.obywatel.gov.pl/</u> 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**



🕘 Wczytaj urządzen	e PKCS#11	
Wprowadź informacje dla modułu, który ma zostać dodany.		
Nazwa <u>m</u> odułu: N	lowy moduł PKCS#11	
<u>N</u> azwa pliku moduł	u: C:\Windows\SysWOV	<u>P</u> rzeglądaj
	ОК	Anuluj

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: <u>https://www.java.com/pl/download/</u>

W panelu sterowania odnajdujemy Java Control Panel i ustawiamy poziom zabezpieczeń na "Medium":

🛃 Java Control Panel	
General Update Java Security Advanced	
Enable Java content in the browser	
Security Level	
C Very High	
- High (minimum recommended)	
- Medium	
Least secure setting - Ail Java applications will be allowed to run after presenting.	a security prompt.
Exception Site List	
Applications launched from the sites listed below will be allowed to run after the security prompts.	e appropriate
Click Edit Site List to add items to this list.	List
Restore Security Prompts Manag	e Certificates
OK Car	cel <u>Apply</u>

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

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



List	x
Applications launched from the sites listed below will be allowed to run af prompts.	ter the appropriate security
Location	
https://szkolenia-zrodlo.obywatel.gov.pl:1443	
FILE and HTTP protocols are considered a security risk.	Add <u>R</u> emove
	OK Cancel

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".

Certificates	×
Certificate type: Secure Site	
User System	
Issued To Issued By	
*.obywatel.gov.pl Certum Level IV CA	^
	Ŧ
Import Export Remove Details	
	Close

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

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



Aplikacja diagnostyczna

Wybierz profil TEST 💌	
Identyfikacja przeglądarki internetowej	
Wykryta przeglądarka to Firefox w wersji 31 SUKCES	
Test 3: Sprawdzenie obecności programów antywirusowych	
Wyszukiwanie programów antywirusowych	
Zainstalowane programy antywirusowe: Migrosoft Segurity Fagentiala, status, Wiscorpy aktualny	
SUKCES	
Test 4: Sprawdzenie obecności przegladarki PDF	
	=
Przeglądarka PDF zainstalowana.	
SURCES	
	Wykonaj Posotuj Zapisz
	vyronaj Resetuj Zapisz

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 <u>https://pomoc.coi.gov.pl</u> 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 <u>www.obywatel.gov.pl</u> w zakładce dedykowanej Lokalnym Administratorom Systemu.