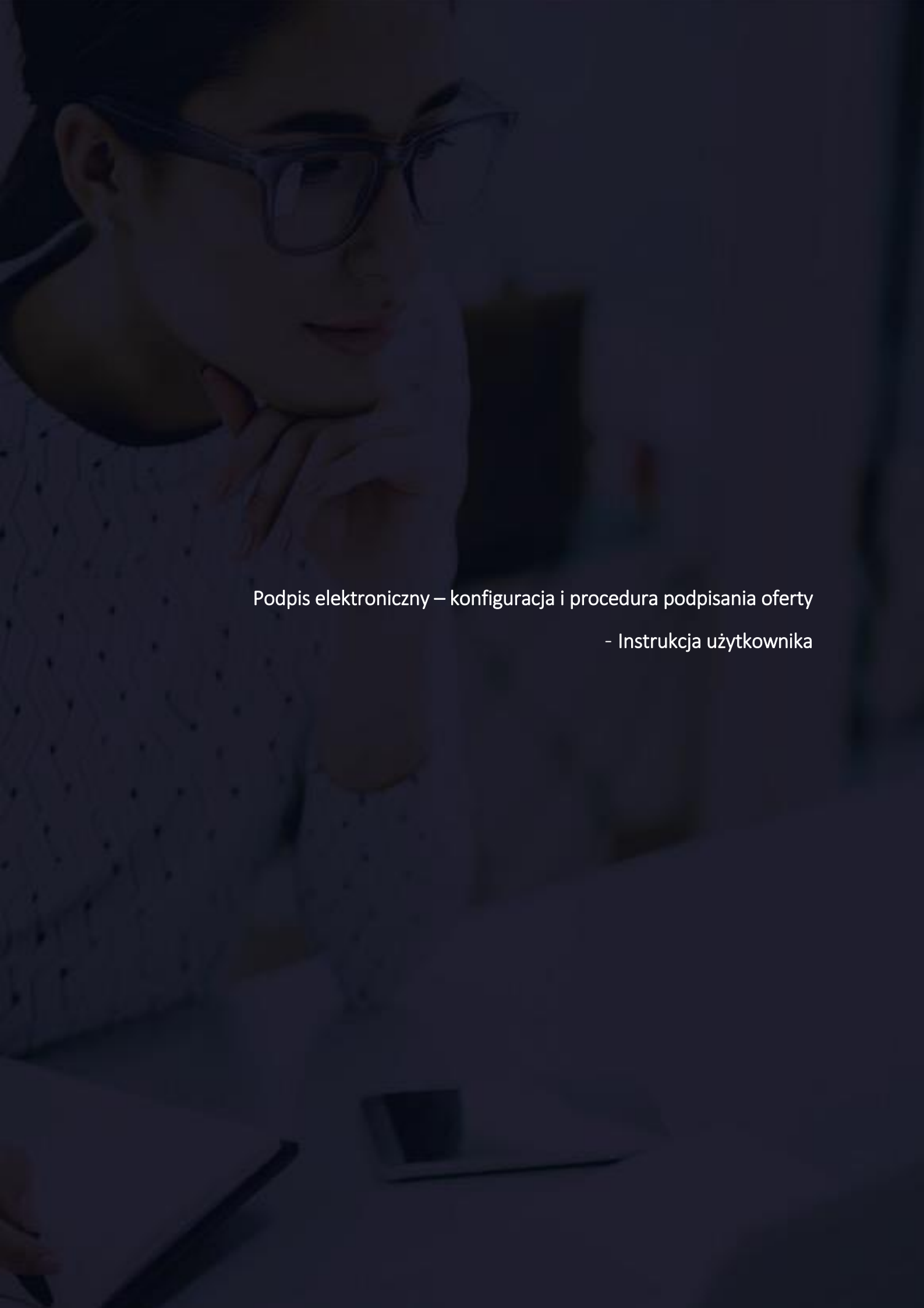


Podpis elektroniczny – konfiguracja i procedura podpisania oferty

- Instrukcja użytkownika

Spis treści

1 Kwalifikowany podpis elektroniczny

1.1 Czym jest podpis elektroniczny

Podpis elektroniczny to dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny. Bezpieczny podpis elektroniczny lub inaczej podpis kwalifikowany stanowi elektroniczny odpowiednik podpisu odręcznego i zawiera wszystkie jego najistotniejsze cechy, tzn.:

- potwierdza jednoznacznie tożsamość osoby podpisującej,
- uniemożliwia zaprzeczenie faktu podpisania,
- jest powiązany z treścią, która została podpisana,
- uniemożliwia wprowadzenie jakichkolwiek, niezauważalnych zmian w podpisanej treści.

Dzięki zastosowaniu podpisu elektronicznego dysponujemy niepodważalnym dowodem złożenia oferty przez ściśle określona osobę.

Tzw. bezpieczny podpis elektroniczny, podpis kwalifikowany można uzyskać w placówkach kwalifikowanych podmiotów świadczących usługi certyfikacyjne, zwane obecnie usługami zaufania lub ich partnerów. Uzyskaniu bezpiecznego podpisu elektronicznego towarzyszy przedłożenie wymaganych dokumentów i zaświadczeń potwierdzających jednoznacznie tożsamość strony ubiegającej się o podpis.

Podpis kwalifikowany składa się kilku elementów tworzących tzw. bezpieczne środowisko:

- karta kryptograficzna
- czytnik
- oprogramowanie
- certyfikat kwalifikowany
- wystawca certyfikatu wpisany do rejestru uprawnionych podmiotów Narodowe Centrum Certyfikacji

1.2 Procedura uzyskiwania podpisu elektronicznego

1.2.1 Jaki podpis jest potrzebny w zamówieniu publicznym?

Podpis tzw. Kwalifikowany, czyli weryfikowany certyfikatem kwalifikowanym. Taki sam jaki jest stosowany np. w kontaktach z ZUS (program Płatnik)

1.2.2 Na kogo podpis ma być wystawiony?

Podpis elektroniczny jest podpisem osobistym, a więc musi być wystawiony na osobę. To musi być osoba, która jest uprawniona do składania oświadczeń woli w imieniu firmy. Jeżeli podpisem będzie posługiwać się ktoś kto nie jest uwidoczniony w dokumentach firmowych (KRS, EDG) jako reprezentant, to Zamawiający powinien zostać poinformowany o udzieleniu pełnomocnictwa

przez Wykonawcę wyznaczonej osobie. To pełnomocnictwo może być udzielone np. tylko do jednego postępowania lub na określony czas.

1.2.3 Do kogo kierować się po podpis?

Kwalifikowany podpis elektroniczny można zakupić u jednego z dostawców, akredytowanego przez Ministerstwo Cyfryzacji m.in.: Eurocert, KIR, PWPW, Certum by Asseco. Pełna lista znajduje się na stronie NcCert. Obowiązujące są również podpisy wydane przez kwalifikowane podmioty w dowolnym kraju EU. Zarówno urządzenie, jak i sam podpis Zamawia się bezpośrednio na stronie internetowej producenta.

Procedura zakupu i instalacji podpisu elektronicznego – na przykładzie CERTUM - dostępna jest do pobrania pod adresem:
https://www.certum.pl/pl/wsparcie/cert_wiedza_podpis_elektroniczny_zakup_zestaw_certum/

1.2.4 Koszt podpisu

Koszt stosowania podpisu elektronicznego jest postrzegany przez uczestników rynku zamówień publicznych jako istotna bariera w stosowaniu elektronicznych środków komunikacji. Ceny zestawów różnią się od siebie – w zależności od długości ważności certyfikatu (wydawany na rok lub dwa lata) oraz rodzaju nośnika do składania podpisu (np. czytnik kart usb). Średnio koszt bezpiecznego podpisu elektronicznego (cena zestawu z odpowiednim urządzeniem) wynosi około 300 zł brutto. Należy doliczyć do tego również roczny abonament, którego koszt to około 120 zł brutto. Abonament wymaga odnowienia w kolejnych latach. Warto pamiętać, że zakup podpisu elektronicznego na potrzeby działalności gospodarczej może być zakwalifikowany, jako koszt uzyskania przychodu w ramach prowadzonej działalności gospodarczej.

1.3 Instalacja

Procedury instalacji mogą się różnić w zależności od producenta podpisu, ale można wyodrębnić trzy główne kroki:

- Instalacja oprogramowania oraz odpowiednich sterowników do czytników na komputerze – należy mieć zaktualizowane oprogramowanie Java w wersji 1.8.0_65 lub nowszej, **koniecznie w wersji 32-bitowej i 64-bitowej;**
- Włożenie karty do czytnika w celu weryfikacji, czy podpis działa;
- Zainstalowanie odpowiednich certyfikatów.

Ścieżka certyfikacji to trzypoziomowy proces budowania zaufania do podpisu: certyfikat użytkownika podpisu jest poświadczany certyfikatem przez Centrum Certyfikacji. Następnie certyfikat wystawiany przez Narodowe Centrum Certyfikacji autoryzuje certyfikat Centrum Certyfikacji.

1.3.1 Czas potrzebny do uruchomienia podpisu

Czas niezbędny do instalacji i uruchomienia podpisu zależy od procedur wystawcy, możliwości umówienia weryfikacji tożsamości i tego czy wnioskodawca ma gotowe wszystkie wymagane dokumenty. Do tego trzeba jeszcze dodać czas na zainstalowanie podpisu na komputerze i skonfigurowanie stanowiska.

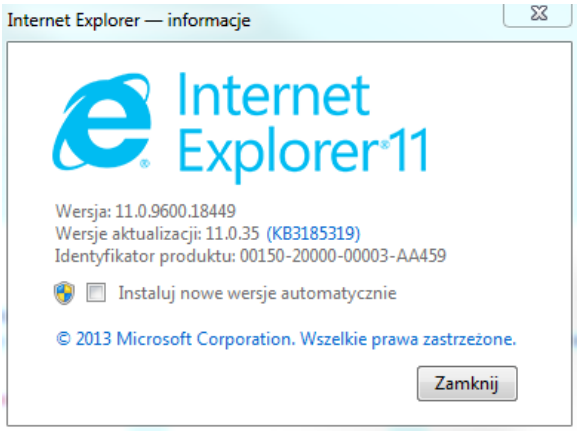
1.4 System operacyjny Windows

1.4.1 Konfiguracja przeglądarki – Internet Explorer

Celem niniejszego rozdziału jest dostarczenie Wykonawcom informacji z zakresu konfiguracji przeglądarki Internet Explorer w taki sposób, aby możliwe było pomyślne zakończenie procedury elektronicznego podpisywania dokumentów w Systemie Zakupowym .

1.4.1.1 Informacje wstępne i weryfikacja wersji przeglądarki:

- Wersje przeglądarki Internet Explorer wspierane podczas konfiguracji – v. 10 i wyżej;
- Przed przystąpieniem do pracy należy sprawdzić wersję przeglądarki – po kliknięciu na ikonę („Narzędzia”) należy wybrać opcję „Internet Explorer - Informacje”. Wyświetlony zostanie następujący ekran:

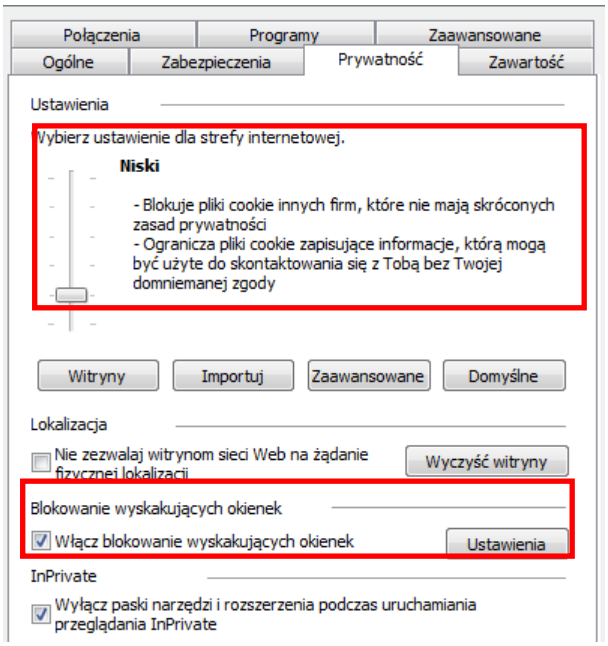


Rysunek 3 Sprawdzenie wersji przeglądarki Internet Explorer

- Osoba konfigurująca przeglądarkę musi być zalogowana z uprawnieniami administratora;
- Przeglądarka Internet Explorer rekomendowana jest do realizacji funkcjonalności w zakresie podpisu elektronicznego (w Systemie Zakupowym).

1.4.1.2 Blokada wyskakujących okienek

Prawidłowe działanie kontrolki Szafir KIR wymaga wyłączenia blokady wyskakujących okienek. W tym celu należy kliknąć na ikonę , a następnie wybierz „Opcje internetowe”. Przejdź na kartę „Prywatność”, gdzie dostępne są opcje sterowania poziomem ustawień dla strefy internetowej (zaleca się ustawienie poziomu na „Niski”).

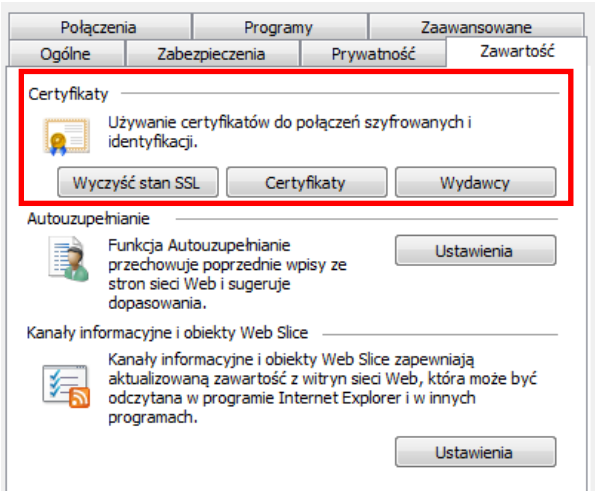


Rysunek 4 Wyłączenie blokady wyskakujących okienek

Z poziomu zakładki „Prywatność" należy zweryfikować jaką wartość widnieje przy opcji „Blokowanie wyskakujących okienek". Jeśli check-box jest zaznaczony, należ go odznaczyć i zastosować ustawienia.

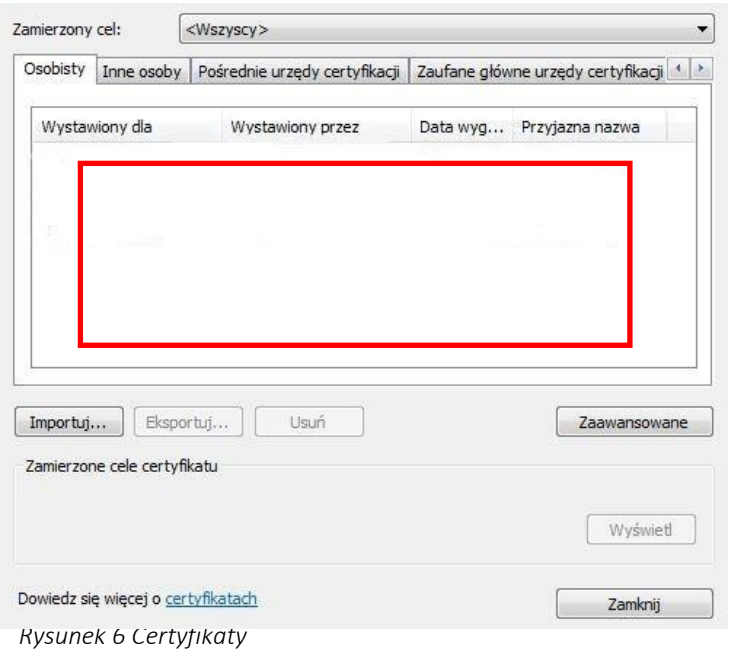
1.4.1.3 Używanie certyfikatów do połączeń szyfrowanych i identyfikacji

W celu prawidłowej realizacji podpisywania dokumentów w środowisku zamawiającego należy upewnić się, iż certyfikat, którym planowane jest podpisywanie dokumentów widoczny jest z poziomu przeglądarki IE. W tym celu należy kliknąć na ikonę , a następnie przejść do zakładki „Zawartość".



Rysunek 5 Zakładka "Zawartość" i przycisk „Certyfikaty"

W celu zweryfikowania listy używanych certyfikatów do połączeń szyfrowanych i identyfikacji należy kliknąć na przycisk „Certyfikaty". Otworzone zostanie okno, które zaprezentowano na poniższym obrazie (rys. 6).



Rysunek 6 Certyfikaty

Certyfikaty, które wykorzystane zostaną do podpisu, powinny być widoczne z poziomu przeglądarki w oknie „Certyfikaty". Pozwoli to zweryfikować czy certyfikat posiadany przez użytkownika prawidłowo komunikuje się z kontrolką Szafir KIR. Jeśli certyfikat nie pojawił się na liście, należy zweryfikować powód wystąpienia problemu – pomocne mogą okazać się informacje dostępne na stronie wystawcy certyfikatu.

1.4.1.4 Instalacja i uruchomienie kontrolki KIR Szafir w przeglądarce Internet Explorer

Krok 1

Wykonanie z poziomu przeglądarki Internet Explorer akcji rozpoczynającej procedurę podpisu elektronicznego w środowisku SWPP2 wywoła oko uruchomienia rozszerzenia Szafir.

Rysunek 7 Okno uruchomieniowe aplikacji Szafir dla przeglądarki Internet Explorer

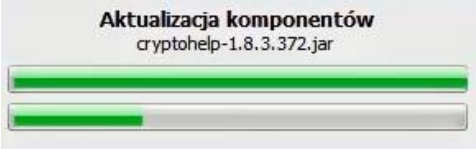
Celem finalizacji procedury należy kliknąć na przycisk „Run". W tym miejscu należy wskazać, do prawidłowej pracy z kontrolką KIR przeglądarka Internet Explorer wymaga aktualnej wersji środowiska

uruchomieniowego JAVA. Przycisk „Run” pozwoli uruchomić i zainstalować w przeglądarce rozszerzenie SDK Szafir KIR. Proces rozpocznie się automatycznie.

UWAGA – w zależności od ustawień bezpieczeństwa na komputerze oraz zainstalowanej wersji środowiska JAVA pierwszym oknem, które pojawi się po zainicjowaniu procedury podpisu może być alert zabezpieczeń (np. „Do you want to continue?”) lub sugestia dotycząca aktualizacji JAVA (np. „JAVA run of date?”). Po zapoznaniu się z komunikatami w obu przypadkach należy postąpić zgodnie z sugerowanymi przez alert działaniami.

Krok 2

Przycisk „Run” pozwoli zainstalować w przeglądarce rozszerzenie SDK Szafir KIR. Proces rozpocznie się automatycznie bezpośrednio po wydaniu polecenia.



Rysunek 8 Instalacja rozszerzenia SDK Szafir KIR dla przeglądarki Internet Explorer

Pomyślna aktualizacja rozszerzenia wywoła alert zabezpieczeń z prośbą o nawiązanie połączenia pomiędzy apletem Szafir KIR a zainstalowanym na komputerze środowiskiem JAVA. Proces wymaga wyrażenia zgodny na takie połączenie, dlatego należy nacisnąć przycisk „Allow”.

Rysunek 9 Alert zabezpieczeń z prośbą o zgodę na połączenie pomiędzy apletem Szafir a JAVĄ

Udzielenie zgody spowoduje uruchomienie aplikacji Szafir KIR i umożliwienie użytkownikowi złożenia podpisu elektronicznego.

1.4.2 Konfiguracja przeglądarki Mozilla FireFox

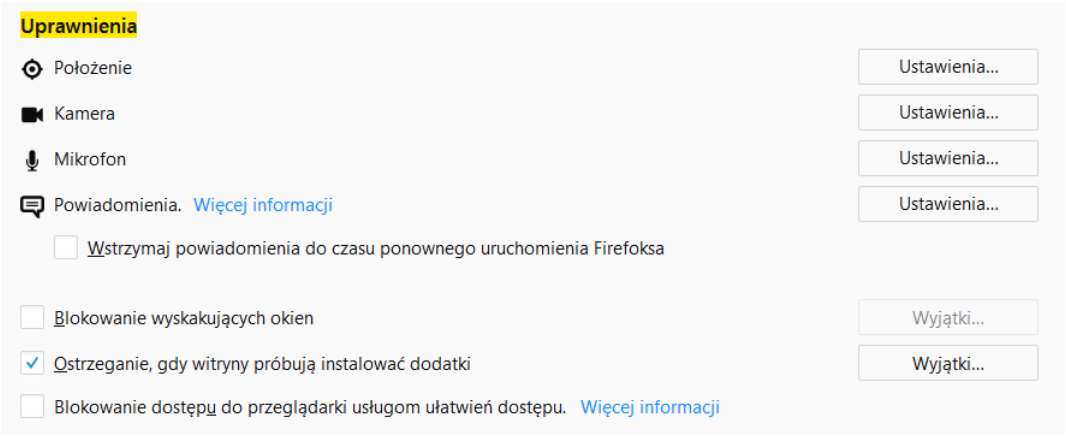
Prawidłowe działanie kontrolki Szafir KIR wymaga zainstalowania na stacji roboczej użytkownika dwóch dedykowanych elementów – rozszerzenia do przeglądarki SDK Szafir KIR oraz aplikacji Szafir Host.

Pomimo automatyzacji procesu pobierania i aktualizacji obu tych elementów (zaprezentowane w rozdziale 10.) w razie potrzeby można pobrać oba komponenty ręcznie za pośrednictwem linków wymienionych w rozdziale 6. niniejszej instrukcji.

1.4.2.1 Blokada wyskakujących okienek

Elementem, który może stanowić problem podczas realizacji podpisu elektronicznego w środowisku SWPP2 (zwłaszcza aktualizacji/ instalacji komponentów wymaganych do jego prawidłowego

działania) jest blokada wyskakujących okienek. W celu jej wyłączenia należy kliknąć na ikonę ☰, następnie wybrać „Opcje". Kolejnym krokiem jest przejście do sekcji „Prywatność i bezpieczeństwo".



Rysunek 10 Wyłączenie blokady wyskakujących okien (Mozilla FireFox)

W sekcji „Uprawnienia" należy odhaczyć opcję „Blokowanie wyskakujących okien" i zastosować ustawienia.

1.4.2.2 Instalacja i uruchomienie kontrolki KIR Szafir w przeglądarce Mozilla FireFox

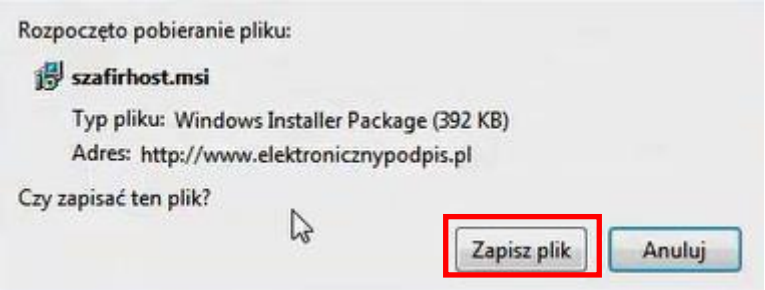
Krok 1

W celu instalacji i uruchomienia kontrolki KIR Szafir należy rozpocząć procedurę podpisu z poziomu Systemu Zakupowego za pomocą jednej z dedykowanych akcji np. „Złóż ofertę". Na ekranie pojawi się komunikat „Czekaj na uruchomienie podpisu elektronicznego".

Rysunek 11 Komunikat dedykowany instalacji Host App KIR

W celu instalacji Szafir Host dla Windows kliknij na przycisk „Instaluj na Windows".

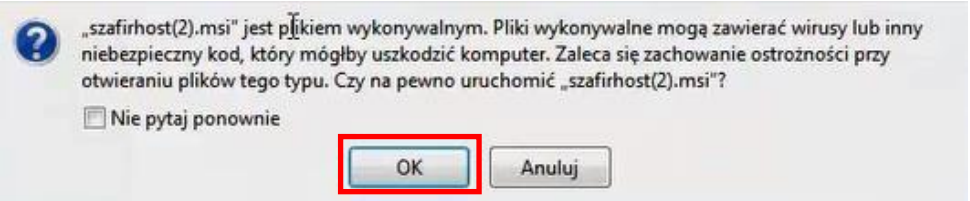
Rysunek 12 Informacja o pobieraniu instalatora Szafir Host



Po zakończeniu pobierania zapisany plik można otworzyć. Kliknij na przycisk „Zapisz plik" i poczekaj do końca instalacji.

Krok 2

Plik z instalatorem Szafir Host (szafirhost.msi) należy otworzyć. Może pojawić się alert „Uruchamianie pliku wykonywalnego". W takim przypadku naciśnij przycisk „Ok" na alercie.

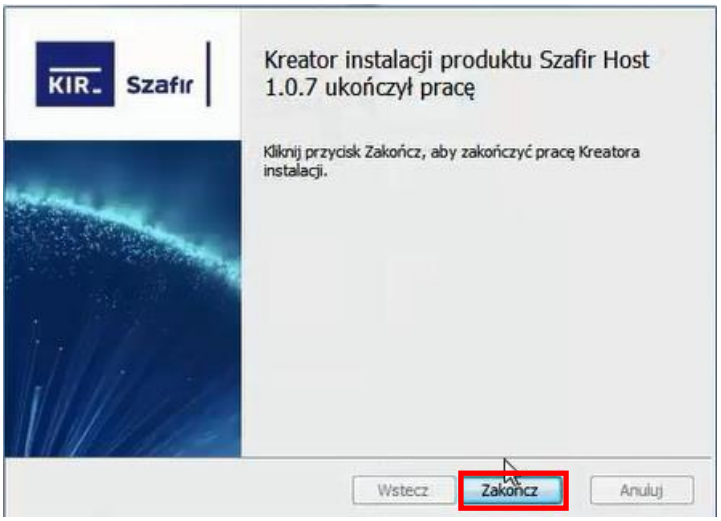


Rysunek 13 Alert o pliku wykonywalnym

Kolejnym możliwym elementem jest wyświetlenie się okna pop-up z informacjami o zabezpieczeniach. W celu dokończenia procedury kliknij na przycisk „Uruchom". Akcja uruchomi instalator aplikacji Szafir Host.

Rysunek 14 Instalator aplikacji Szafir Host

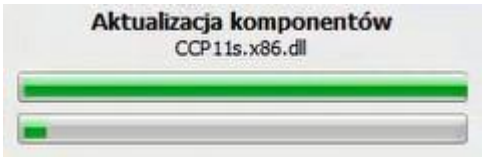
Aby zainstalować aplikację zaakceptuj warunki umowy licencyjnej, a następnie kliknij na przycisk „Zainstaluj”. Zaczekaj aż instalacja komponentu zakończy się. Instrukcje na ekranie poinformują Cię o koniecznych krokach – „Zakończ” instalację.



Rysunek 15 Kończenie pomyślnie zakończonej pracy instalatora Szafir

Krok 3

Po zainstalowaniu aplikacji Szafir Host nastąpi automatyczna instalacja i aktualizacja komponentu Szafir SDK. Paski postępu przedstawiono na poniższym rysunku.



Rysunek 16 Aktualizacja komponentów

Należy zaczekać, aż proces zakończy się powodzeniem. Po tym jak zostanie sfinalizowany, zwróć uwagę, że w pasku adresu przeglądarki pojawiło się nowe rozszerzenie – konsola Szafir KIR.

Rysunek 17 Rozszerzenie Szafir KIR

Finalizacja instalacji komponentów pozwoli na automatyczne uruchomienie aplikacji Szafir, za pomocą której możliwe jest opatrzenie dokumentów podpisem (patrz rys. 21 Uruchomiona aplikacja Szafir KIR).

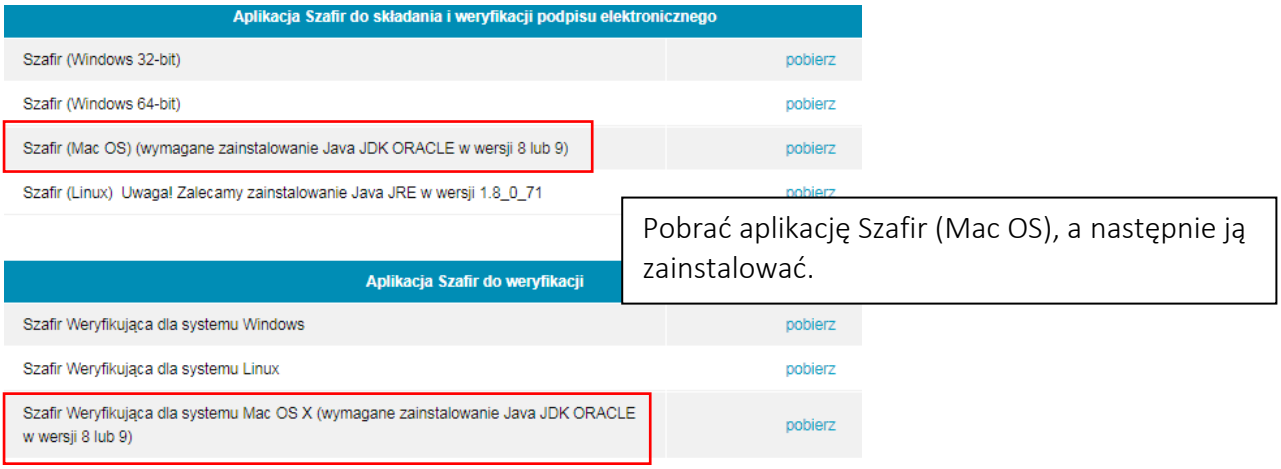
1.5 System operacyjny Macintosh (Mac)

1.5.1 Komponenty aplikacji Szafir

W celu prawidłowego użytkowania nakładki Szafir, rekomendujemy korzystanie z przeglądarki **Google Chrome**, która jest zalecaną przeglądarką w przypadku systemu MacOS.

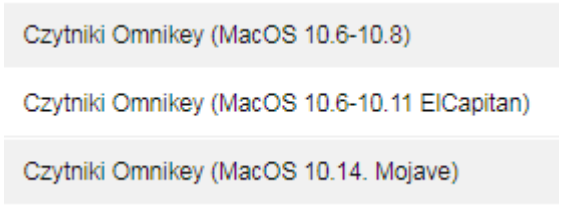
Przed dodaniem nakładki Szafir do przeglądarki na komputerach typu Macintosh należy, zainstalować niezbędne komponenty aplikacji Szafir. Użytkownik wykonuje czynności, według poniższych kroków:

- Wejść na stronę: http://www.elektronicznypodpis.pl/informacje/aplikacje/
  Pobrać aplikację **Szafir (Mac OS),** a następnie ją zainstalować.



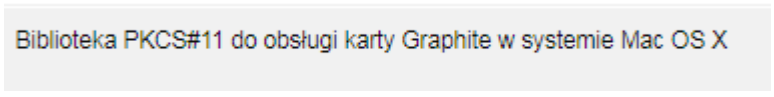
Rysunek 18 Aplikacje i sterowniki na stronie elektronicznypodpis.pl

- Pobrać sterowniki do **czytników Omnikey** dla odpowiedniej wersji systemu MacOS oraz je zainstalować.



Rysunek 19 lista czytników Omnikey na stronie elektronicznypodpis.pl

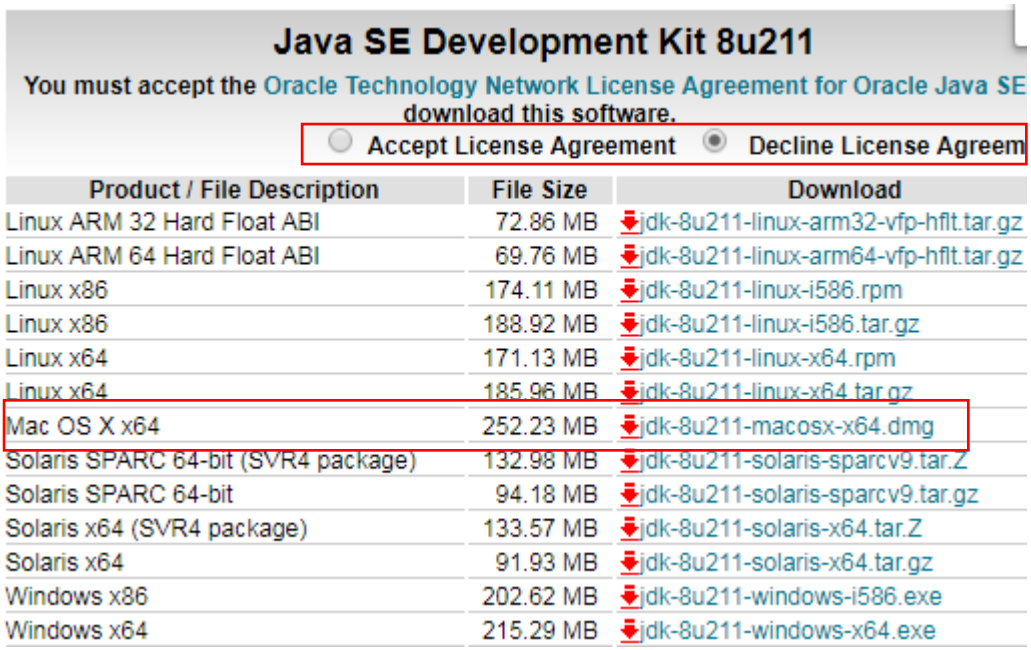
- W przypadku karty typu **Graphite** niezbędne jest również zainstalowanie Bibliotek PKCS#11 do obsługi karty Graphite w systemie Mac OS X.



Rysunek 20 karta typu Graphite na stronie elektronicznypodpis.pl

1.5.2 Javę JDK

Dla poprawnego działania aplikacji należy zainstalować również Javę JDK ze strony: https://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html
Należy oznaczyć „**Accept License Agreement**” i pobrać wersję o nazwie „**Mac OS x64**” z sekcji „Java SE Development Kit 8u211”.



Java SE Development Kit 8u211

You must accept the Oracle Technology Network License Agreement for Oracle Java SE to download this software.

Accept License Agreement Decline License Agreem

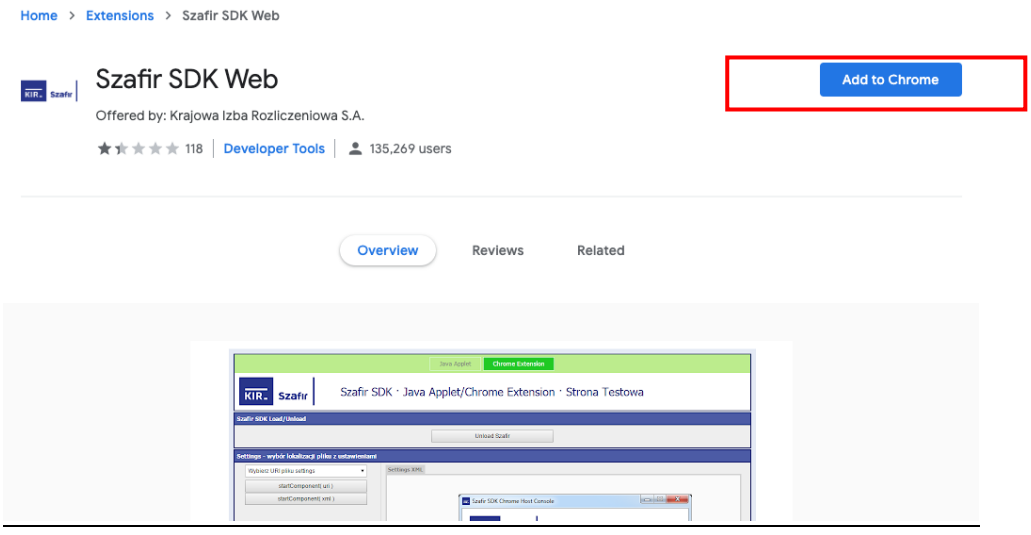
Product / File Description	File Size	Download
Linux ARM 32 Hard Float ABI	72.86 MB	jdk-8u211-linux-arm32-vfp-hflt.tar.gz
Linux ARM 64 Hard Float ABI	69.76 MB	jdk-8u211-linux-arm64-vfp-hflt.tar.gz
Linux x86	174.11 MB	jdk-8u211-linux-i586.rpm
Linux x86	188.92 MB	jdk-8u211-linux-i586.tar.gz
Linux x64	171.13 MB	jdk-8u211-linux-x64.rpm
Linux x64	185.96 MB	jdk-8u211-linux-x64.tar.gz
Mac OS X x64	252.23 MB	jdk-8u211-macosx-x64.dmg
Solaris SPARC 64-bit (SVR4 package)	132.98 MB	jdk-8u211-solaris-sparcv9.tar.Z
Solaris SPARC 64-bit	94.18 MB	jdk-8u211-solaris-sparcv9.tar.gz
Solaris x64 (SVR4 package)	133.57 MB	jdk-8u211-solaris-x64.tar.Z
Solaris x64	91.93 MB	jdk-8u211-solaris-x64.tar.gz
Windows x86	202.62 MB	jdk-8u211-windows-i586.exe
Windows x64	215.29 MB	jdk-8u211-windows-x64.exe

Rysunek 21 Javę JDK

W tym celu pobranie Java JDK wymaga posiadania darmowego konta na Oracle: https://login.oracle.com/oaam_server/login.do

1.5.3 Nakładka Szafir - Szafir SDK Web

Dodanie nakładki Szafir na przeglądarce Chrom jest możliwe, przez wejście w rozszerzenia przeglądarki Chrom:
https://chrome.google.com/webstore/detail/szafir-sdk-web/gjalhnomhafafofonpdihihjnbafkipc



Rysunek 22 Dodanie Szafir SDK Web do Chrome

1.6 Mamy już podpis elektroniczny od kilku miesięcy. Czy można go stosować?

Tak, pod warunkiem, że certyfikat jest jeszcze ważny. Należy to sprawdzić z odpowiednim wyprzedzeniem za pomocą oprogramowania dostarczonego z podpisem. W razie ryzyka utraty ważności w okolicach terminu przygotowania i składania oferty należy go przedłużyć. Przedłużanie w czasie ważności jest zazwyczaj prostsze niż uzyskiwanie nowego podpisu po wygaśnięciu ważności certyfikatu.

1.7 Procedura podpisania ofert z użyciem podpisu elektronicznego

Przy składaniu oferty przez Platformę automatycznie uruchamia się aplikacja z podpisem oraz zostaje wygenerowany dokument z ofertą. Przy zatwierdzeniu następuje podpisanie. Z kolei sam podpis potwierdza się PINem. Po zatwierdzeniu system automatycznie składa ofertę. Dodatkowo, wykonawca ma możliwość wygenerowania pliku pdf ze złożonej oferty. Należy również pamiętać, że wszystkie załączniki do oferty podpisywane są poza aplikacją. Instrukcja podpisywania dokumentów poza aplikacją – na przykładzie aplikacji Szafir jest dostępna do pobrania na stronie:

https://www.elektronicznypodpis.pl/gfx/elektronicznypodpis/userfiles/_public/informacje/instrukcje/instrukcja_podpis_i_weryfikacja_xades_pades_cades.pdf

W przypadku przeglądarki Google Chrome, Opera i Firefox (od wersji 52) wymagana jest instalacja dedykowanego rozszerzenia Podpis elektroniczny **Szafir SDK** oraz dodatkowej aplikacji **Szafir Host** udostępniającej funkcje podpisu elektronicznego.

Rozszerzenie Szafir SDK można pobrać z lokalizacji:	
	Google Chrome: https://chrome.google.com/webstore/detail/podpis-elektroniczny-szaf/gjalhnomhafafofonpdihihjnbafkipc/
	Opera: https://addons.opera.com/pl/extensions/details/podpis-elektroniczny-szafir-sdk/
	Firefox: https://www.elektronicznypodpis.pl/download/webmodule/firefox/szafir_sdk_web-0.0.10-anfx.xpi
Instalator aplikacji Szafir Host można pobrać z lokalizacji:	
Windows 64 bitowy	http://www.elektronicznypodpis.pl/gfx/elektronicznypodpis/pl/defaultstronaopisowa/146/1/1/szafirhost.msi
Windows 32 bitowy	http://www.elektronicznypodpis.pl/gfx/elektronicznypodpis/pl/defaultstronaopisowa/146/1/1/szafirhost_x86.msi

Po zainstalowaniu rozszerzenia **Szafir SDK** oraz aplikacji **Szafir Host** należy przeładować bieżącą stronę. Jeżeli rozszerzenie oraz aplikacja zostały prawidłowo zainstalowane i mimo to nadal podczas pracy z podpisem występują problemy, należy sprawdzić czy w przeglądarce

włączone jest rozszerzenie Szafir SDK oraz czy na komputerze zainstalowane jest środowisko uruchomieniowe Java JRE.

Środowisko Java JRE można pobrać i zainstalować z lokalizacji Java JRE: https://www.java.com/download/ - zainstalować oprogramowanie zgodnie z instrukcją umieszczoną na stronie, a następnie zrestartować komputer
Posiadaną wersję sprawdzić można zgodnie z instrukcją dostępną pod linkiem: https://www.java.com/pl/download/help/version_manual.xml

1.8 Wskazówki dotyczące rozwiązywania problemów z podpisem elektronicznym

1.8.1 Okno do podpisu elektronicznego nie pojawia się:

W przypadku, gdy nie pojawia się okno do podpisu elektronicznego, należy sprawdzić poprawność zainstalowania aplikacji Szafir.

- Czy pojawiło się okienko do automatycznej instalacji Szafira?
- Czy pojawił się komunikat o tym, że instalacja aplikacji dostała zablokowana przez system?

Jeśli nie pojawiła się żadna informacja, należy sprawdzić, czy ustawieniach przeglądarki opcja wyskakujących okien nie jest zablokowana.

1.8.2 Niewidoczny certyfikat

Jeżeli aplikacja Szafir zainstalowana jest prawidłowo, a mimo wszystko nie widać certyfikatu, należy sprawdzić, czy jest on prawidłowo dodany do danej przeglądarki.