

Instrukcja obsługi certyfikatów na karcie Graphite w środowisku macOS

Spis treści

1. WPROWADZENIE.....	2
1.1. Wersje systemu macOS od 2012 roku.....	2
1.2. Sprawdzenie wersji oprogramowania.....	2
1.3. Ilość wolnej pamięci na dysku	3
1.4. Preferencje systemowe.....	3
1.5. Zakładka Ochrona i prywatność w Preferencjach systemowych.....	4
1.6. Zakładka Użytkownicy i grupy w Preferencjach systemowych.....	6
1.7. Dodawanie nowego konta użytkownika.....	6
1.8. Sprawdzenie wersji sterownika do czytnika.....	7
2. AKTYWACJA KARTY.....	8
3. INSTALACJA APLIKACJI SZAFIR	10
4. ODBLOKOWANIE KARTY LUB ZMIANA PIN/PUK.....	14
5. ODNOWIENIE ONLINE.....	15
6. UŻYCIE CERTYFIKATU NA WWW	15

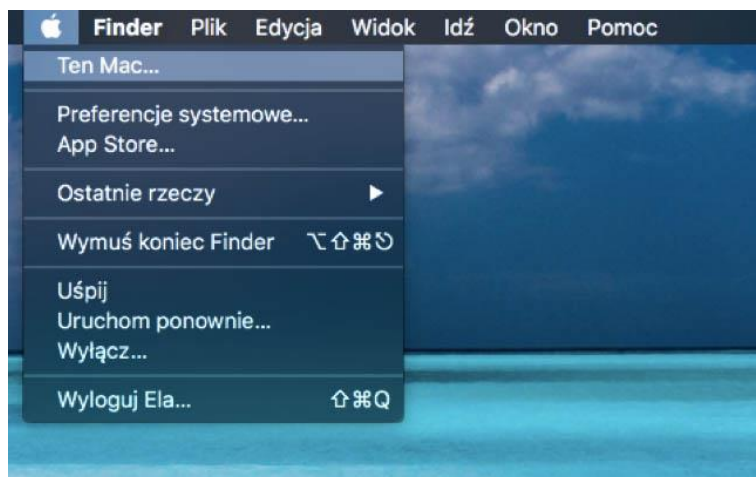
1. Wprowadzenie

1.1. Wersje systemu macOS od 2012 roku

Wersja	Nazwa kodowa
OS X 10.9	Mavericks
OS X 10.10	Yosemite
OS X 10.11	El Capitan
macOS 10.12	Sierra
macOS 10.13	High Sierra
macOS 10.14	Mojave
macOS 10.15	Catalina
macOS 11	Big Sur
macOS 12	Monterey

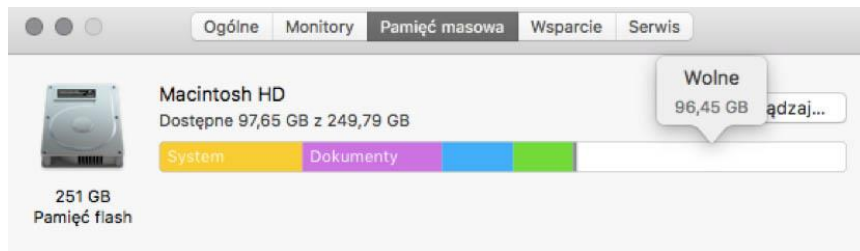
1.2. Sprawdzenie wersji oprogramowania

Kliknij w lewy górny róg ekranu w symbol „jabłka” i wybierz opcję **Ten Mac**. Następnie w zakładce **Ogólne** pojawi się informacja na temat wersji i nazwy kodowej.



1.3. Ilość wolnej pamięci na dysku

W tym celu ponownie wybierz symbol „jabłka” w lewym górnym rogu i opcję Ten mac, a następnie przejdź do zakładki Pamięć masowa.



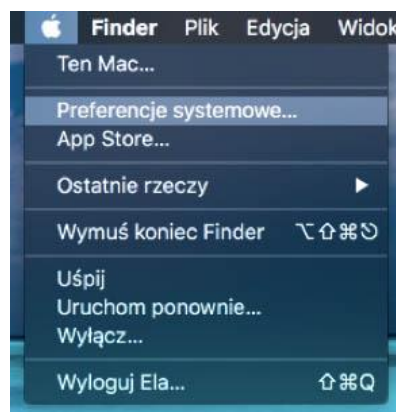
1.4. Preferencje systemowe

Funkcje systemową Preferencje systemowe można otworzyć na 3 sposoby:

a) wpisz Preferencje systemowe w pole spotlight – kombinacja klawiszy Command (skrót na klawiaturze cmd) + spacja:



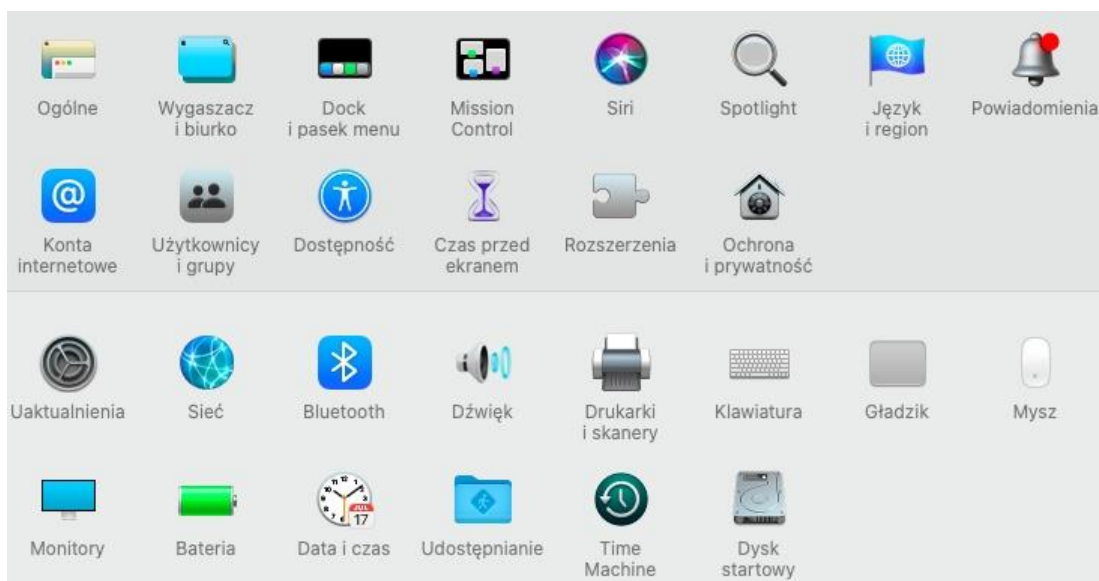
b) kliknij w symbol „jabłka” w lewym górnym rogu i wybierz Preferencje systemowe:




c) pasek Dock, gdzie należy odszukać Programy, a następnie Preferencje systemowe:

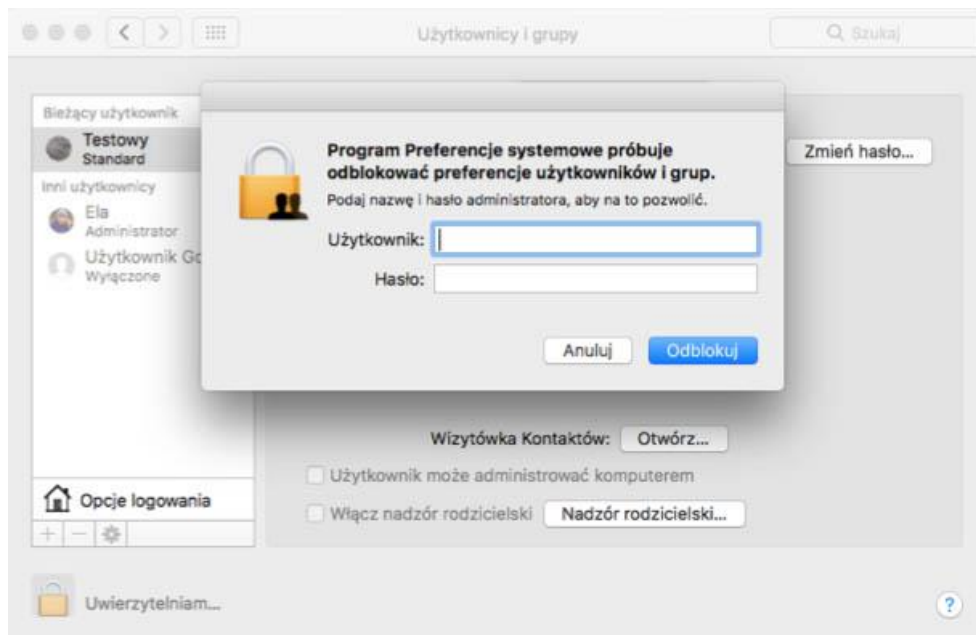


Po otwarciu Preferencji systemowych pojawi się okno, gdzie dostępne są ustawienia komputera.



1.5. Zakładka Ochrona i prywatność w Preferencjach systemowych

Zakładka ta umożliwia odblokowanie programu w celu np. jego instalacji. jeśli pochodzi z nieznanego źródła. Jeśli chcesz wprowadzić zmiany, odblokuj „kłódkę”  w lewym dolnym rogu i podaj hasło bieżącego konta użytkownika, który posiada uprawnienia administratora. Jeżeli nie posiada takich uprawnień, wprowadź login i hasło użytkownika, który jest administratorem na danym urządzeniu/koncie.



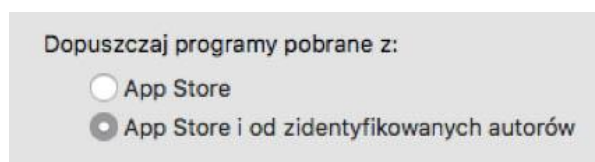
UWAGA!

W systemach niższych niż macOS Sierra dostępna jest opcja: „dopuszczaj programy z dowolnego źródła”.

a) systemy poniżej macOS Sierra:



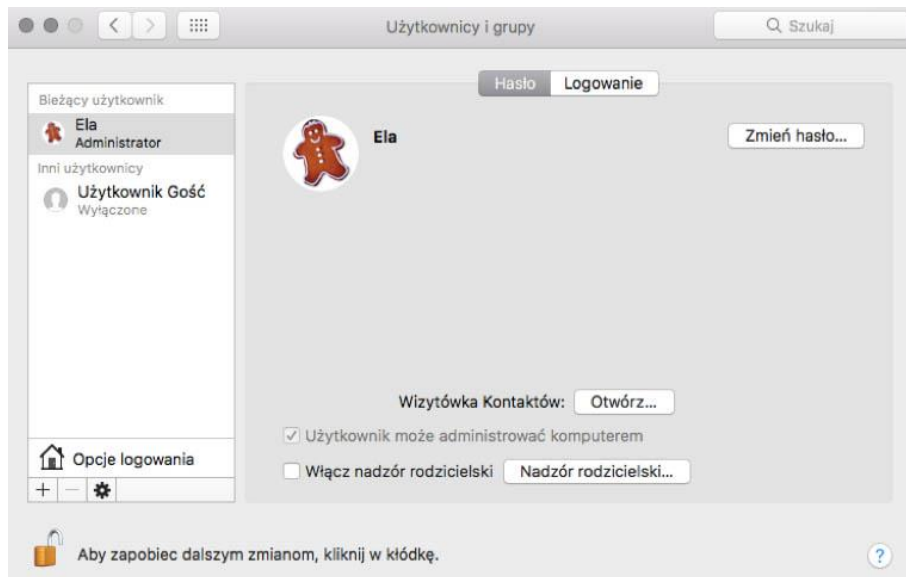
b) macOS Sierra i wyższy:



1.6. Zakładka Użytkownicy i grupy w Preferencjach systemowych

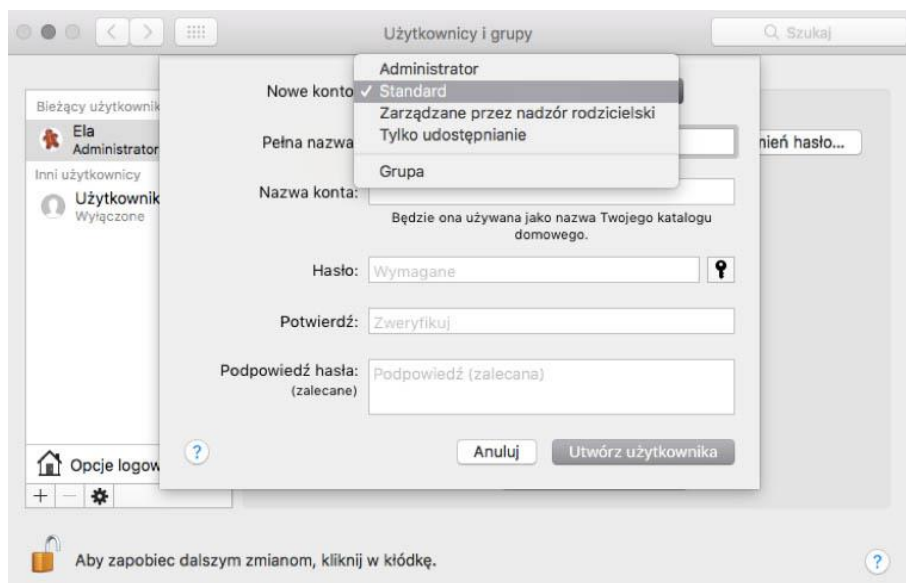
Dzięki tej zakładce można sprawdzić, czy użytkownik posiada uprawnienia administratora, a także dodać innych użytkowników komputera.

Zmiany w kontaktach może wprowadzić jedynie administrator.



1.7. Dodawanie nowego konta użytkownika

W tym celu w Preferencjach systemowych w zakładce Użytkownicy i grupy administrator powinien kliknąć w kłódkę, a następnie wprowadzić hasło i za pomocą sybolu „+” dodać nowe konto. Może to być konto standardowe (użytkownik nie ma możliwości wprowadzania zmian ani instalacji programów na komputerze) lub konto typu administrator (na jednym komputerze może być wielu administratorów).



1.8. Sprawdzenie wersji sterownika do czytnika

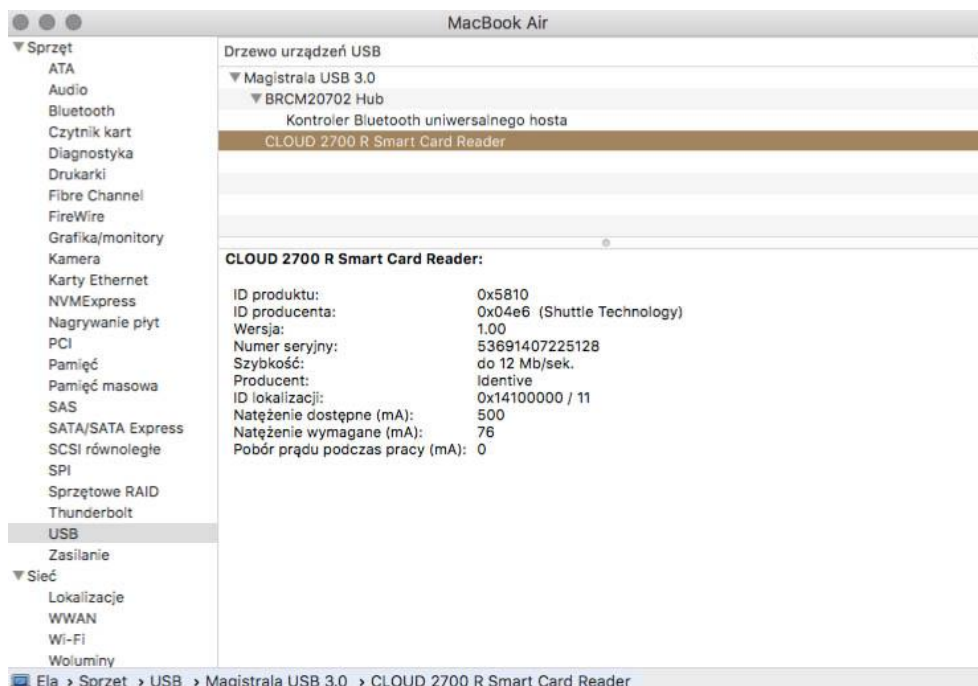
WAŻNE!

Sterowniki do czytnika powinny pobrać się automatycznie po umieszczeniu urządzenia w porcie USB komputera.

W pasku Dock odszukaj Programy, Narzędzia i dalej Informacje o systemie.



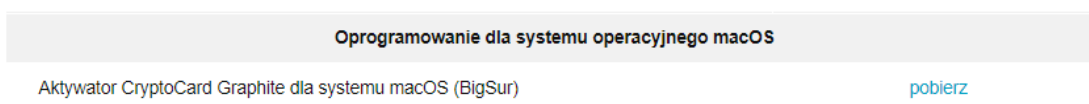
W zakładce **Sprzęt** na liście odszukaj **USB**. Po kliknięciu w środku ekranu pojawi się nazwa czytnika. Po zaznaczeniu pojawią się informacje techniczne o czytniku i wersji sterownika.



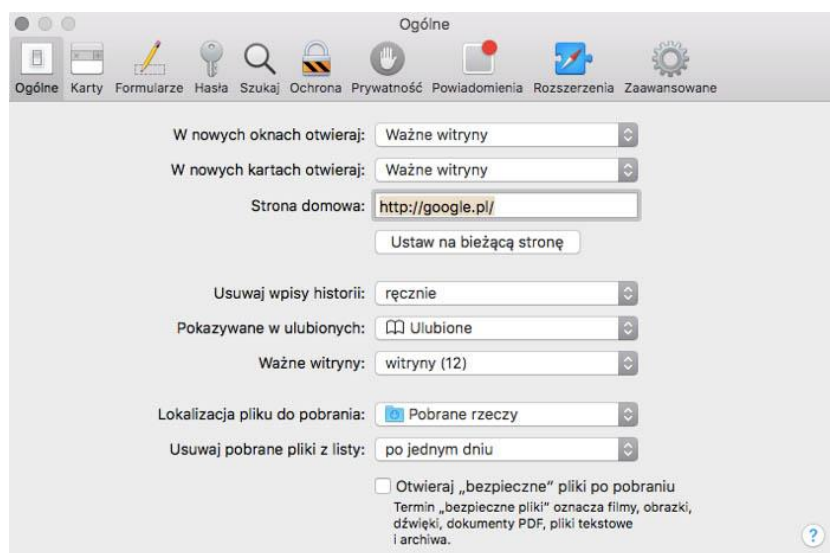
2. Aktywacja karty

Od wersji macOS 11 Big Sur istnieje możliwość aktywacji karty Graphite (numer na karcie 111...). Jest to proces jednorazowy.

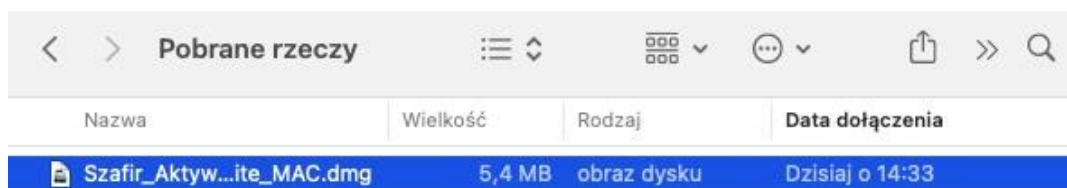
W tym celu pobierz oprogramowanie dostępne na stronie www.elektronicznypodpis.pl w zakładce Informacje -> Aplikacje i sterowniki:



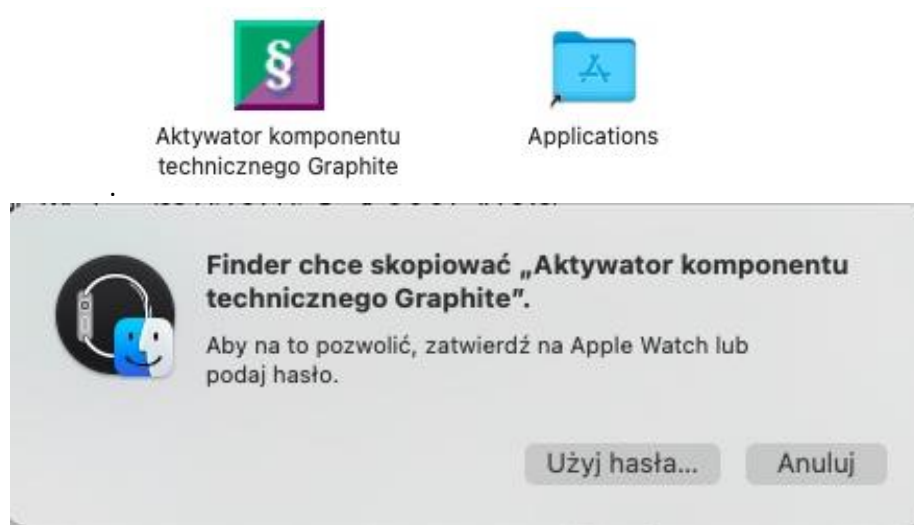
Jeżeli pobierasz oprogramowanie ze strony poprzez przeglądarkę Safari, to plik powinien zapisać się w folderze **Pobrane**. Gdyby było inaczej, sprawdź lokalizację pobranych plików. W tym celu otwórz Safari, przejdź do ustawień poprzez kombinację klawiszy Command (skrót na klawiaturze cmd) + przecinek. W zakładce **Ogólne** pojawi się informacja o folderze pobieranych plików.



Jeżeli plik został już pobrany i znajduje się na dysku komputera, przejdź do wybranego folderu i uruchom oprogramowanie.



Pojawi się okno z prośbą o przeciągnięcie ikonki programu do listy Aplikacji, co wymaga podania hasła administratora.



Od tego momentu aplikacja będzie widoczna na liście Aplikacji/Programów.

Przy pierwszym jej uruchomieniu może pojawić się następujące okno, które należy potwierdzić, klikając Otwórz.



Okno aplikacji wygląda następująco:

ccs

Szafir Aktywator CryptoCard Graphite

Niewłaściwe operacje z użyciem PUK mogą zablokować dostęp do karty. Wprowadź PUK zgodnie z instrukcją otrzymaną od wydawcy karty.

PUK

Niewłaściwe operacje z użyciem PIN-u transportowego mogą zablokować token kwalifikowany. Nowy kod PIN nadany przez użytkownika powinien mieć od 6 do 16 znaków i może składać się z cyfr oraz liter. Nie zaleca się stosowania polskich liter oraz znaków specjalnych.

PIN

Nowy PIN Potwierdź

Aktywuj **Zarejestruj certyfikat**

Aktywacja karty jest możliwa poprzez wpisanie kodu PUK z koperty i nadanie nowego PIN. Kod nie powinien zawierać polskich liter oraz znaków specjalnych. (Powyższe okno aplikacji prezentuje kartę już aktywowaną, dlatego pola mają kolor szary i nie umożliwiają wpisania żadnych znaków).

Aktywację karty potwierdź, klikając **Aktywuj** w lewym dolnym rogu.

3. Instalacja aplikacji Szafir

Program Szafir jest w wersji także dla systemów macOS. Link do aplikacji znajduje się na stronie internetowej: <http://www.elektronicznypodpis.pl/informacje/aplikacje/> pod hasłem Szafir (MacOS).

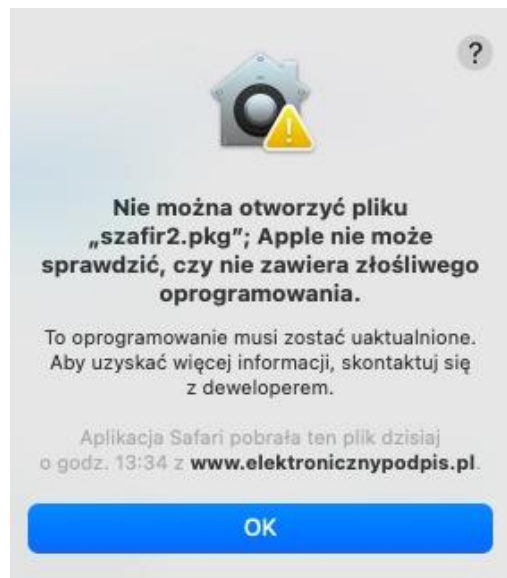
Aplikacja Szafir do składania i weryfikacji podpisu elektronicznego	
Szafir (Windows 32-bit, Szafir 2.0.0.build 642)	pobierz
Szafir (Windows 64-bit, Szafir 2.0.0.build 642)	pobierz
Szafir (macOS, Szafir 2.0.0.build 642)	pobierz
Szafir (Linux, Szafir 2.0.0.build 642, biblioteka dla kart Graphite , instrukcja instalacji) Uwaga! Zalecamy zainstalowanie Java JRE w wersji min. 1.8 (Oracle) lub Adopt OpenJDK od wersji 11	pobierz

Pakiet z aplikacją Szafir dostępny na stronie internetowej zawiera wymagane oprogramowanie Java.

Aplikacja Szafir pobrana ze strony zapisze się w folderze **Pobrane** bądź w innym folderze. Plik Szafir jest w formacie **.jar**, co oznacza, że po pobraniu i rozpakowaniu nie trzeba go instalować, ponieważ po kliknięciu w ten plik od razu uruchomi się aplikacja Szafir.

Nazwa	Wielkość	Rodzaj	Data dołączenia
szafir2.pkg	85,6 MB	pakiet i...talacyjny	Dzisiaj o 13:34
ccsmac	--	folder	Dzisiaj o 13:32
Szafir_Akt...2.02.mpkg	6,9 MB	pakiet i...talacyjny	Dzisiaj o 13:32
Instrukcja...MacOS.pdf	536 KB	Dokument PDF	Dzisiaj o 13:32
ccsuite-to....205.2.pkg	3 MB	pakiet i...talacyjny	Dzisiaj o 13:32

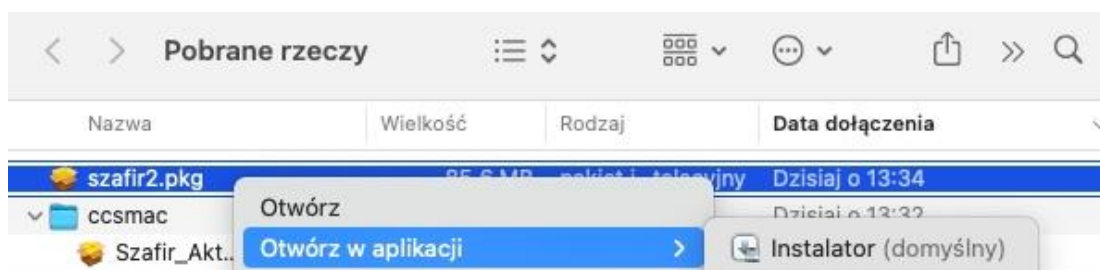
Po otwarciu może pojawić się komunikat dotyczący pobierania programów z nieznanych źródeł.



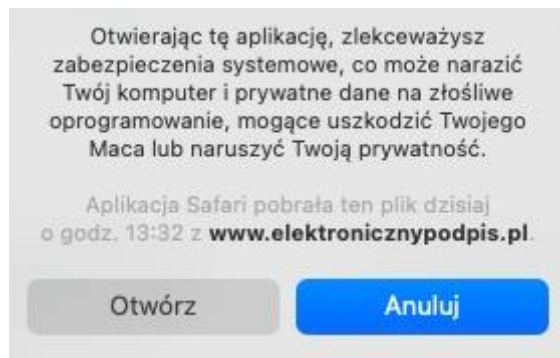
Należy postępować analogicznie, jak w przypadku instalacji Cryptocard Suite na stronie 12 instrukcji.

UWAGA!

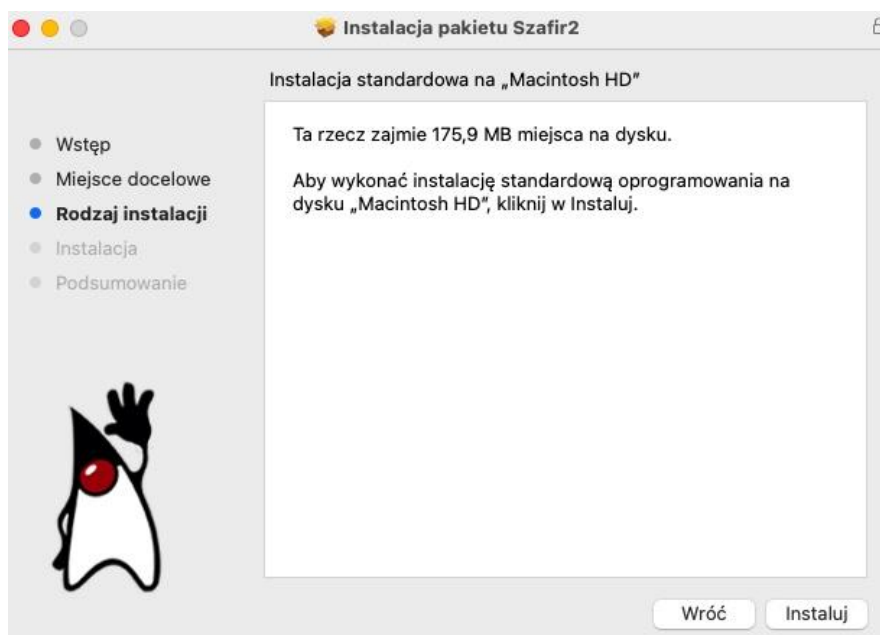
Wciśnięty klawisz Control + ikona programu Szafir -> Otwórz -> Instalator

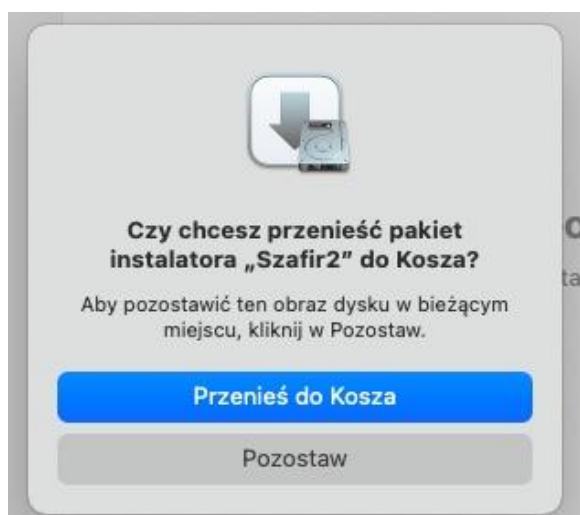
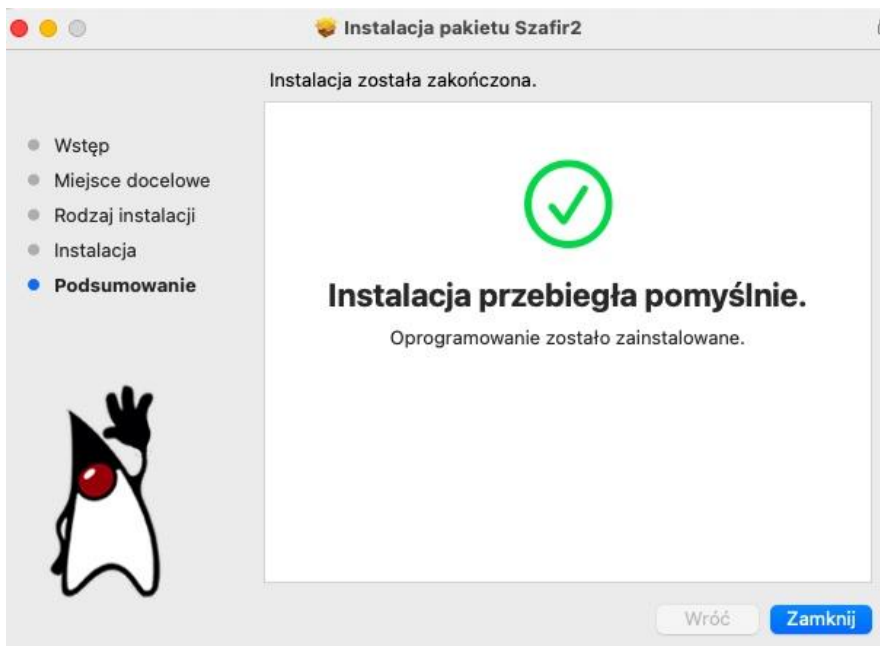
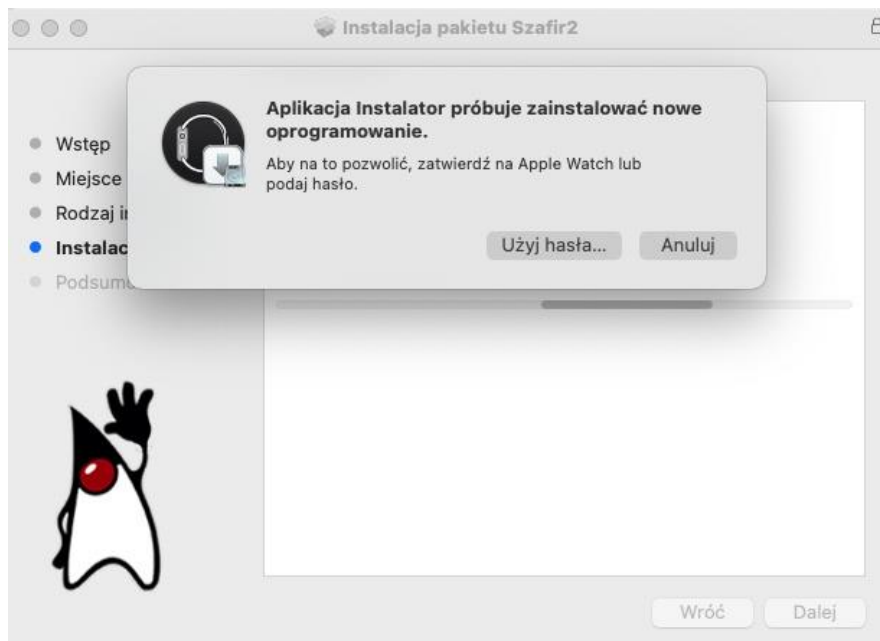


Powyższy komunikat nie zawsze się pojawia. W przypadku dodania wyjątku wyświetli się okno, które ponownie zapyta, czy otworzyć program, należy wybrać **Otwórz**.



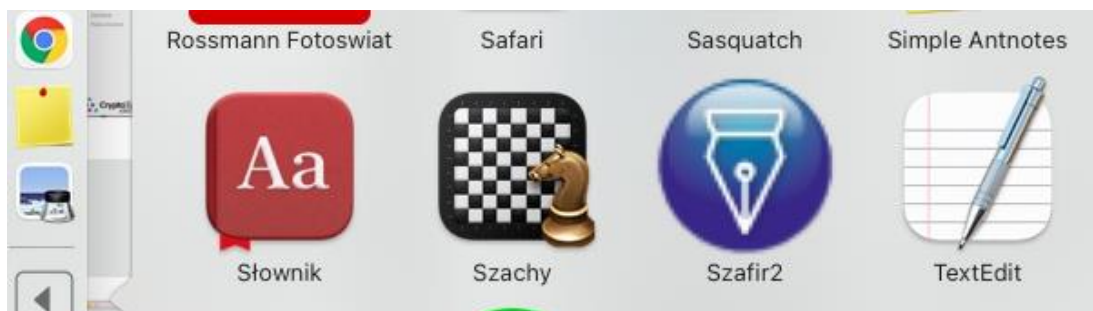
Po wykonaniu wszystkich czynności pojawi się okno z możliwością instalacji pakietu Szafir.





Samą instalkę można przenieść do kosza za pomocą przycisku **Przenieś do kosza**.

Aplikację można odnaleźć na liście programów lub poprzez wyszukiwanie. Nazwa programu to **Szafir2**:



Aby zweryfikować, czy podpis działa prawidłowo, wykonaj próbę złożenia podpisu w aplikacji.

4. Odblokowanie karty lub zmiana PIN/PUK

Od wersji macOS 11 Big Sur istnieje możliwość zmiany kodu PIN lub PUK oraz odblokowania karty w przypadku jej zablokowania.

Zmiana PIN/PUK jest możliwa w aplikacji **Szafir Aktywator CryptoCard Graphite** w zakładce **Zmiana PIN/PUK**. Proces instalacji tej aplikacji został przedstawiony w punkcie 2 niniejszej instrukcji. Wymaga on podania obecnego kodu PIN/PUK i nadania nowego kodu.

Interfjs aplikacji wygląda następująco:

A screenshot of the 'Szafir Aktywator CryptoCard Graphite' application window. The window title is 'ccs'. The application has a green header bar with the title. Below the header, there are four tabs: 'Aktywator', 'Zmiana PIN/PUK' (which is selected), 'Odblokowanie PIN', and 'O aplikacji'. The main content area contains a warning message: 'Niewłaściwe operacje z użyciem kodu PIN lub PUK mogą zablokować token kwalifikowany. Nowa wartość PIN lub PUK nie może być krótsza niż długość kodu PIN lub PUK z którym aktywowano kartę. Upewnij się, że znasz aktualną wartość kodu PIN lub PUK.' Below the warning, there are input fields for 'PIN', 'Nowy PIN', and 'Potwierdź'. There are also two buttons: 'PIN' (purple) and 'PUK' (grey). At the bottom, there is an 'OK' button.

Aplikacja umożliwia **odblokowanie karty** w przypadku jej zablokowania.

Karta zostanie zablokowana po 3 błędnych próbach wpisaniu kodu PIN. Jeśli certyfikat jest zablokowany, pola do wpisania kodów są aktywne. Przykładowa karta przedstawiona powyżej nie jest zablokowana, dlatego pola nie są aktywne.

Odblokowanie karty następuje w zakładce **Odblokowanie PIN**, po wpisaniu kodu PUK z koperty (która została wydana wraz z certyfikatem) i nadaniu **nowego kodu PIN**.

Interfejs aplikacji wygląda następująco:

ccs

Szafir Aktywator CryptoCard Graphite

Aktywator Zmiana PIN/PUK Odblokowanie PIN O aplikacji

Niewłaściwe operacje z użyciem PUK użytkownika mogą doprowadzić do trwałego zablokowania karty i utraty wszystkich danych znajdujących się na niej, takich jak certyfikaty lub klucze prywatne. Upewnij się, że znasz aktualną wartość kodu PUK.

PUK

Zmień PIN

Nowy PIN Potwierdź

OK

5. Odnowienie online

Procedura odnowienia online wymaga skorzystania z systemu Windows.

Instrukcja dotycząca tego procesu jest dostępna na stronie www.elektronicznypodpis.pl.

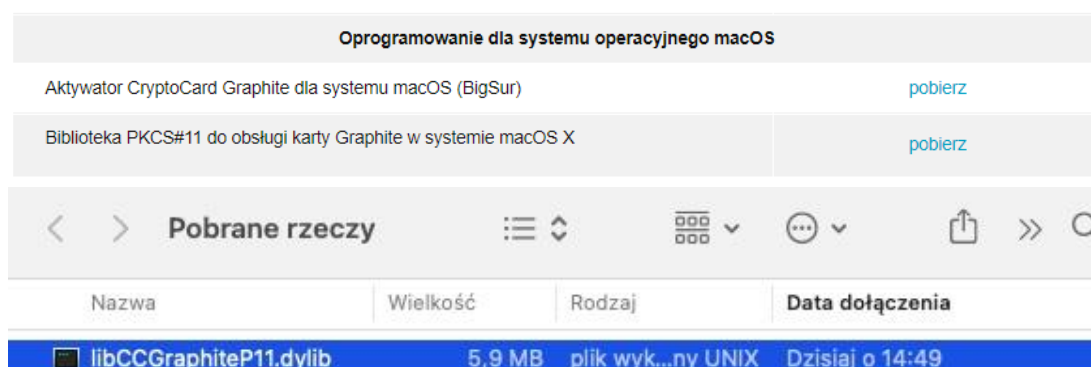
Po prawidłowym odnowieniu certyfikatu w dalszym ciągu, bez wykonywania dodatkowych czynności, można korzystać ze środowiska macOS.

6. Użycie certyfikatu na www

Niektóre strony www lub aplikacje wymagają wskazania biblioteki `.dylib` obsługującej kartę.

Biblioteka obsługująca kartę `libCCGraphiteP11.dylib` dostępna jest na stronie:

<https://www.elektronicznypodpis.pl/informacje/aplikacje/>



W przypadku pojawienia się problemów prosimy o kontakt:

e-mail: kontakt@kir.pl