DATA AKTUALIZACJI DOKUMENTU: 05/10/2022

PODRĘCZNIK
CENTAUR CHIRON GUI

TYP DOKUMENTU:WEWNĘTRZNY
STWORZONY PRZEZ ENIGMA SYSTEMY OCHRONY INFORMACJI SP. Z O.O. 02-230 WARSZAWA
UL. JUTRZENKI 116 | TELEFON: +48 22 570 57 10 | FAX: +48 22 570 57 15
WWW.ENIGMA.COM.PL

DATA UTWORZENIA DOKUMENTU: 11/01/2021

ENIGMA SYSTEMY OCHRONY INFORMACJI SP. Z O.O.
JUTRZENKI 116
02-230 WARSZAWA
POLSKA

TELEFON: +48 22 570 57 10
FAX: +48 22 570 57 15
STRONA INTERNETOWA: WWW.ENIGMA.COM.PL

HISTORIA ZMIAN W PROJEKCIE

WERSJA PROJEKTU	DATA	OPIS ZMIAN W PROJEKCIE
1.0	11.01.2021	Brak
1.1	05.10.2022	Aktualizacja dokumentu

SPIS TREŚCI

`

1 WSTĘP

Centaur Chiron jest modułem samoobsługi użytkowników systemu Centaur. Pozwala na odnowienie certyfikatów, odblokowanie i aktywację kart kryptograficznych, a także certyfikację przy wykorzystaniu kodów jednorazowych.

2 INSTALACJA

Oprogramowanie jest przeznaczone do pracy na systemie Windows. Instalację należy wykonać przy pomocy oryginalnego instalatora.

2.1 INSTALATOR CHIRONGUISETUP.EXE

Po uruchomieniu pojawi się okno wyboru.

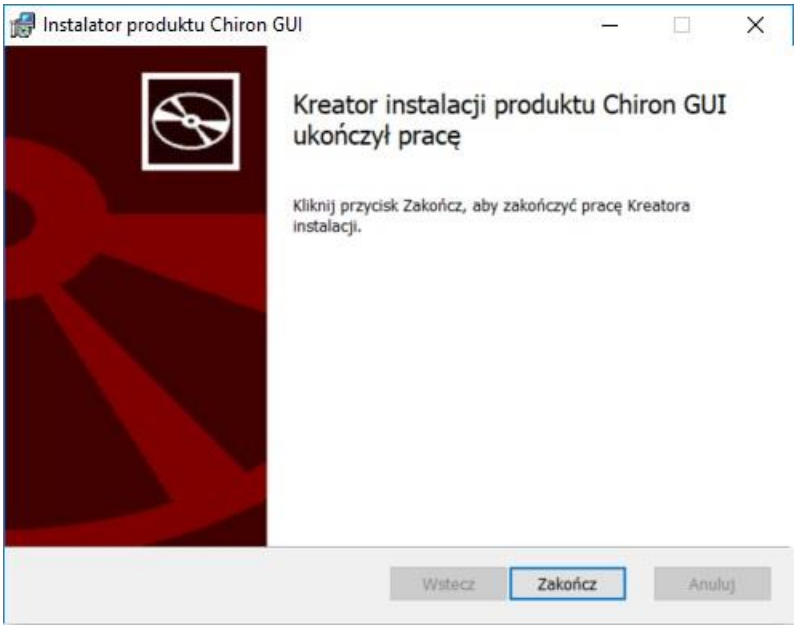
Rysunek 1 Okno instalacji z wykorzystaniem ChironGuiSetup.exe

Po wybraniu opcji **Zainstaluj** proszę poczekać do końca operacji. Program zostanie zainstalowany w katalogu ***C:\Program Files (x86)\Chiron GUI*** .

2.2 INSTALATOR CHIRONGUISETUP.MSI

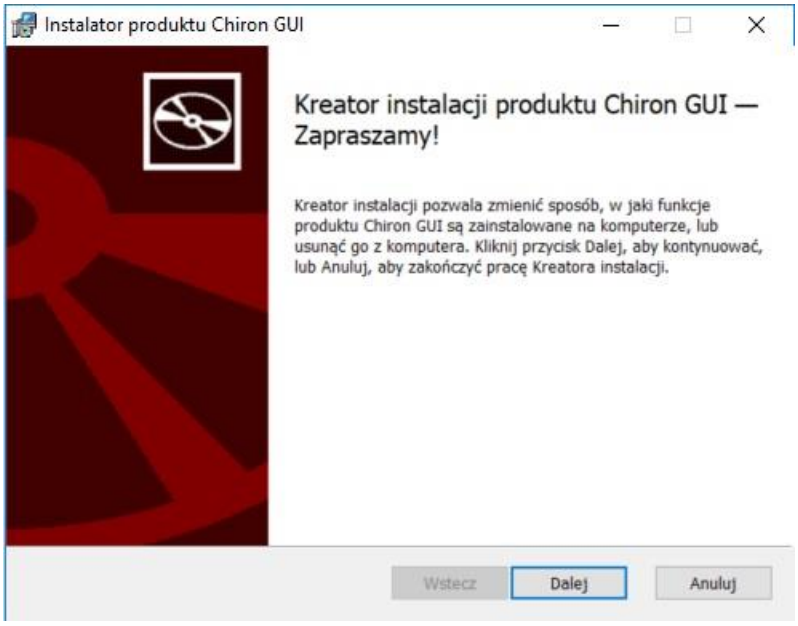
Przy pierwszym uruchomieniu instalatora, gdy na maszynie nie jest jeszcze zainstalowany program *Chiron GUI,* zostanie on automatycznie zainstalowany w lokalizacji ***C:\Program Files (x86)\Chiron GUI*** .

Po udanej instalacji pojawi się okno zakończenia operacji.



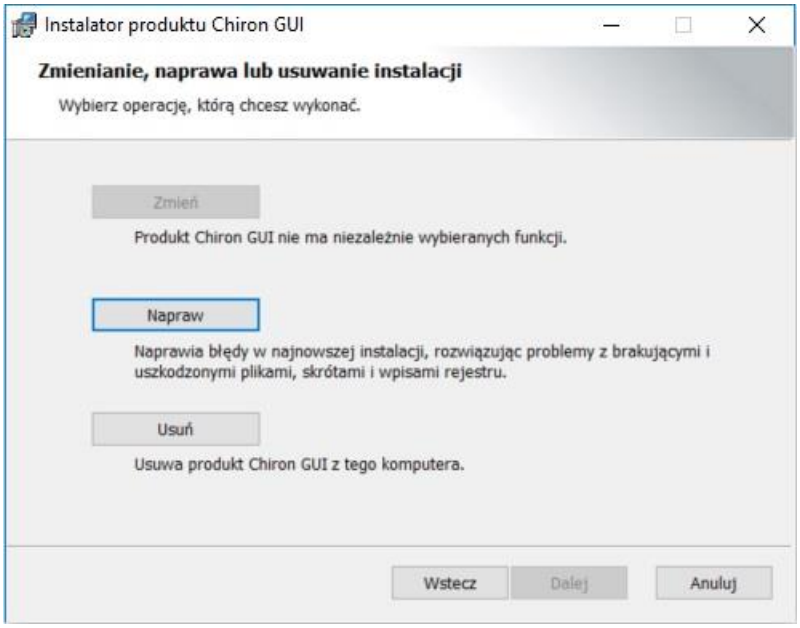
Rysunek 2 Okno zakończenia operacji ChironGuiSetup.msi

Po uruchomieniu instalatora w przypadku, gdy na komputerze jest zainstalowany *Chiron GUI,* pojawi się okno instalatora.



Rysunek 3 Okno instalatora z wykorzystaniem ChironGuiSetup.msi

Po wybraniu opcji **Dalej** pojawi się okno wyboru kreatora.



Rysunek 4 Okno wyboru kreatora ChironGuiSetup.msi

Z tego poziomu można dokonać operacji **Naprawienia** instalacji lub **Usunięcia** programu.

2.2.1 NAPRAW

Operacja naprawy instalacji skutkuje przywróceniem fabrycznej konfiguracji oprogramowania *Chiron GUI*.

Rysunek 5 Okno naprawy instalacji

2.2.2 USUŃ

Operacja usunięcia skutkuje odinstalowaniem programu *Chiron GUI.*

Rysunek 6 Okno usunięcia programu

2.2.3 INSTALACJA APLIKACJI W TRYBIE CICHYM

W celu instalacji oprogramowania Chiron GUI w trybie cichym należy uruchomić wiersz poleceń w miejscu gdzie znajduje się plik `ChironGuiSetup.msi`, a następnie wykonać:

```
msiexec /i ChironGuiSetup.msi /qn /quiet
```

2.2.4 DEINSTALACJA APLIKACJI W TRYBIE CICHYM

W celu instalacji oprogramowania Chiron GUI w trybie cichym należy uruchomić wiersz poleceń w miejscu gdzie znajduje się plik `ChironGuiSetup.msi`, a następnie wykonać:

```
msiexec /uninstall ChironGuiSetup.msi /qn /quiet
```

3 KONFIGURACJA

Oprogramowanie *Chiron GUI* jest przeznaczone dla użytkownika końcowego. Użytkownik może samodzielnie dokonać recertyfikacji certyfikatu na karcie lub odblokować kartę w przypadku zablokowania PINu.

Kontrolka bezpośrednio współpracuje z serwisem *Centaur WWW*, który dalej przekazuje odpowiednie żądania do Centaur CCK.

W przypadku wprowadzenia modyfikacji w pliku konfiguracyjnym należy ponownie uruchomić program.

3.1 KONFIGURACJA GŁÓWNA

Dla celów konfiguracji oprogramowania *Chiron GUI* należy edytować plik **config.json** znajdujący się w katalogu, w którym został zainstalowany program (katalog instalacji). Plik ten ma składnię JSON.

Parametry konfiguracyjne:

- **centaurWWWAddress** - adres pod którym dostępny jest serwis **v1** *Centaur WWW*. Przykładowy adres: *https://**10.13.13.32:9443**/services/v1/centaurWS/* . Wytłuszczony fragment adresu podlega konfiguracji.
    - **Należy pamiętać, że fragment adresu musi być taki sam jak CN w certyfikacie wystawionym dla Centaura WWW np. „centaurwww". Przy takiej konfiguracji w pliku hosts musi być skonfigurowane również mapowanie adresu IP, pod którym jest dostępny Centaur WWW i nazwy z certyfikatu.**

- **backupCentaurWWWAddress** adres pod którym dostępny jest alternatywny serwis **v1** *Centaur WWW*. Przykładowy adres: *https://**10.13.13.33:9443**/services/v1/centaurWS/* . Wytłuszczony fragment adresu podlega konfiguracji.

- **centaurOIMAddress** - adres pod którym dostępny jest serwis **oim** *Centaur WWW*. Przykładowy adres: *https://**10.13.13.32:9443**/services/oim/centaurWS/* . Wytłuszczony fragment adresu podlega konfiguracji.

- **kerberosWWWAuthenticationProxy** - adres serwera uwierzytelniającego dla serwisu **v1** *Cenatur WWW*. Pole może pozostać puste co oznacza użycie adresu z pola **centaurWWWAddress**.

- **kerberosOIMAuthenticationProxy -** adres serwera uwierzytelniającego dla serwisu **oim** *Cenatur WWW*. Pole może pozostać puste co oznacza użycie adresu z pola **centaurOIMAddress**.

- **pkcs11LibraryPath** – lokalizacja biblioteki PKCS#11 do obsługi kart. Dla przykładu obsługa kart typu ENCARD: *C:\\Program Files (x86)\\ENCARD\\enigmap11.dll*

Można skonfigurować jednoczesną obsługę kilku kart podając biblioteki PKCS#11 w formacie:
["C:\\Windows\\System32\\crypto3PKCS.dll", "C:\\Windows\\System32\\eTPKCS11.dll"]

- **tlsCaRootCertificatePath** – lokalizacja magazynu certyfikatów zaufanych wystawców. Magazyn certyfikatów zawierać certyfikat CA będącego wystawcą certyfikatu TLS dla serwisu Centaur WWW. Plik ten musi być w formacie PEM.

- **caName** – nazwa urzędu CCK który obsługuje dana kontrolka.

- **schemaName** – nazwa schematu certyfikacji wykorzystywanego w procesie Certyfikacji z kodem jednorazowym na karcie kryptograficznej.

  UWAGA! Nazwa ta nie jest wykorzystywana w procesie recertyfikacji z wykorzystaniem starego certyfikatu.

- **schemaNamePfx -** nazwa schematu certyfikacji wykorzystywanego w procesie Certyfikacji z kodem jednorazowym do pliku PKCS#12

- **chipdocTool** – lokalizacja programu chipdoc-tool odpowiedzialnego za proces aktywacji karty.

- **activateCardWorker -** rodzaj sposobu aktywacji karty. Dozwolone wartości pola to:

  - *chipdocTool*
  - *SSO (dla aktywacji z wykorzystaniem kerberosa)*

- **certificateUpdateWorker –** rodzaj sposobu aktualizacji karty. Dozwolone wartości pola to:
  - *cardUpdate (aktualizacja z wykorzystaniem konfiguracji w schemacie certyfikacji w CCK)*
  - *fromOldKey (ignoruje schemat CCK i wykorzystuje przy recertyfikacji parametry cleanupStrategy oraz oldKeyRecertification)*
    - **Parametry cleanupStrategy oraz oldKeyRecertification muszą być skonfigurowane, jeśli korzystamy z opcji „fromOldKey”**

- **logLevel** – Poziom logowania błędów do pliku. Dostępne wartości:

  0 – debug; **1** – info; **2** – warning; **3** – error; **4** – critical

- **ButtonDisable** – Sekcja do dezaktywacji przycisków w głównym oknie. Domyślnie wszystkie przyciski są aktywne (ustawione na *false*). W przypadku dezaktywacji przycisku należy ustawić poniższą wartość na *true*.
  - **unlockCardBtnDisable** – dezaktywacja przycisku Odblokowania karty.
  - **recertifyOldKeyBtnDisable** – dezaktywacja przycisku Certyfikacji z wykorzystaniem poprzedniego certyfikatu (Aktualizacja karty).
  - **certifyOneTimeCodeBtnDisable** – dezaktywacja przycisku Certyfikacji z wykorzystaniem kodu jednorazowego.

- **activateCardBtnDisable** – dezaktywacja przycisku Aktywacji karty.
- **changeCardPinBtnDisable –** dezaktywacja przycisku Zmiany PIN-u karty.
- **installCertificateBtnDisable –** dezaktywacja przycisku Instalacji certyfikatu na kartę
- **showCardInfoBtnDisable –** dezaktywacja przycisku Diagnostyka karty.
- **recertifyPkcs12OldKeyBtnDisable –** dezaktywacja przycisku recertyfikacji pliku pkcs#12 z wykorzystaniem poprzedniego certyfikatu.
- **certifyPkcs12OneTimeCodeBtnDisable –** dezaktywacja przycisku certyfikacji do pliku pkcs#12 z wykorzystaniem kodu jednorazowego.
- **revokeUserCertificatesBtnDisable –** dezaktywacja przycisku do Unieważnienia wszystkich certyfikatów użytkownika
- **configureAppBtnDisable –** dezaktywacja przycisku Konfiguracji oprogramowania

- **oldKeyRecertification –** Flaga mająca ustalić, czy opcja recertyfikacja przy użyciu starego certyfikatu ma wykorzystywać aktualnie istniejące na karcie klucze powiązane z odpowiednimi certyfikatami, czy też wygenerować nowe pary kluczy. Parametr jako wartość przyjmuje następne tryby:
  - **true (lub1) –** recertyfikacja z użyciem starych kluczy,
  - **false (lub 0) –** recertyfikacja z generowaniem nowych kluczy.

- **cleanupStrategy** – znacznik służy do definicji zachowania aplikacji podczas certyfikacji oraz recertyfikacji:
  - **Remove_nothing** - W obydwu przypadkach (Kod jednorazowy oraz recertyfikacja z wykorzystaniem starego certyfikatu) Chiron GUI pozostawia wszystkie obiekty na karcie (tj. certyfikaty stare, nowe oraz klucze urzędu).
  - **Remove_signing** - Certyfikacja z kodem jednorazowym nie usuwa zawartości karty; Recertyfikacja z wykorzystaniem starego certyfikatu usuwa z karty klucz do podpisu, który był recertyfikowany (pozostawia klucz do szyfrowania).
  - **Remove_all** - W obydwu przypadkach recertyfikacja usuwa z karty wszystkie dotychczasowe obiekty.
  - **Remove_all_my_ca** - W obydwu przypadkach recertyfikacja usuwa z karty wszystkie obiekty (poza certyfikatami z innego CA).
  - **Remove_recert_key_and_certs** - W obydwu przypadkach recertyfikacja usuwa z karty wszystkie obiekty związane z recertyfikacją (pozostawia inne certyfikaty użytkownika oraz certyfikaty innych użytkowników).
- configVersion – wersja zainstalowanego lokalnie pliku konfiguracyjnego, jeśli jest inna niż dystrybuowana przez Centaura WWW to jest nią nadpisywana przy uruchomieniu programu

3.1.1 PRZYKŁADOWY PLIK KONFIGURACYJNY

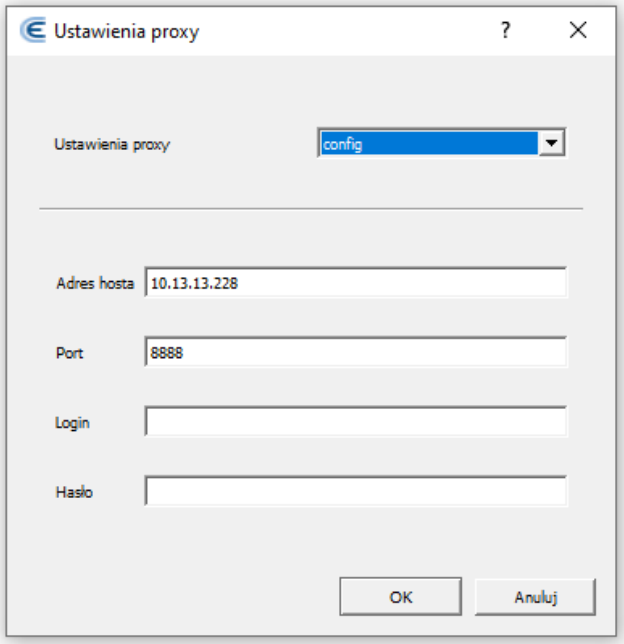
```
{
    "centaurWWWAddress": "https://centaurwww:9443/services/v1/centaurWS/",
    "centaurOIMAddress": "https://10.13.13.167:9443/services/oim/centaurWS/",
    "kerberosWWWAuthenticationProxy" : "",
    "kerberosOIMAuthenticationProxy" : "",
```

```
    "pkcs11LibraryPath":
["C:\\Windows\\System32\\crypto3PKCS.dll","C:\\Windows\\System32\\eTPKCS11.dll"],
    "tlsCaRootCertificatePath": "root.pem",
    "caName": "Enigma",
    "configVersion": "1.0",
    "schemaName": "Test podpis",
    "schemaNamePfx": "Test podpis",
    "chipdocTool": "chipdoc-tool.exe",
    "logLevel" :  "0",
    "activateCardWorker": "chipdocTool",
    "certificateUpdateWorker": "fromOldKey",
    "cleanupStrategy": "Remove_nothing",
    "ButtonDisable": {
        "unlockCardBtnDisable":  false,
        "recertifyOldKeyBtnDisable": false,
        "recertifyOneTimeCodeBtnDisable": false,
        "activateCardBtnDisable":  true
    },
}
```


3.2 KONFIGURACJA SERWERA PROXY

Konfiguracja serwera proxy możliwa jest po pierwszym uruchomieniu aplikacji Chiron. Po pierwszym uruchomieniu aplikacji konfiguracja proxy dostępna jest bezpośrednio w interfejsie graficznym Chirona po naciśnięciu przycisku **Konfiguracja proxy**. Po naciśnięciu tego przycisku otworzy się **okno ustawień proxy**, w którym możliwa jest konfiguracja parametrów takich jak:

- **Ustawienia proxy** – możliwość konfiguracji proxy, z którego będzie korzystało oprogramowanie, jeśli parametr nie jest skonfigurowany to przyjmuje domyślnie wartość „system”:
    - **none** – oprogramowanie nie korzysta z proxy,
    - **system** – oprogramowanie korzysta z systemowych ustawień proxy,
    - **config** – oprogramowanie korzysta z ustawień proxy zapisanych w pliku konfiguracyjnym, wymaga uzupełnienia sekcji proxyOptions.
- **Adres hosta** – adres serwera proxy bez dodatkowych znaków (np. 10.13.13.228),
- **Port** – port serwera proxy podany jako liczba (bez cudzysłowów),
- **Login** – login do serwera proxy,
- **Hasło** – hasło do serwera proxy.



Rysunek 7 Okno konfiguracyjne ustawienia proxy

Po zmianie ustawień proxy na **config** i zapisaniu ustawień proxy przyciskiem **OK** zostanie stworzony plik **.chiron-gui-proxy.json** w katalogu użytkownika, na którego koncie został zainstalowany Chiron. Plik ten zawiera parametry konfiguracyjne serwera proxy, które zostały wprowadzone i zapisane w **oknie ustawień proxy** takie jak:

- **proxyOptions** – sekcja zawierająca ustawienia proxy:
  - proxyHostAddress – adres serwera proxy bez dodatkowych znaków (np. 10.13.13.228),
  - proxyPort- port serwera proxy podany jako liczba (bez cudzysłowów),
  - proxyLogin – login do serwera proxy,
  - proxyPassword – hasło do serwera proxy.

- **proxySetting** – możliwość konfiguracji proxy, z którego będzie korzystało oprogramowanie, jeśli parametr nie jest skonfigurowany to przyjmuje domyślnie wartość „system”:
  - **none** – oprogramowanie nie korzysta z proxy,
  - **system** – oprogramowanie korzysta z systemowych ustawień proxy,
  - **config** – oprogramowanie korzysta z ustawień proxy zapisanych w pliku konfiguracyjnym, wymaga uzupełnienia sekcji proxyOptions.

Wprowadzenie zmian w **oknie ustawień proxy** spowoduje zmianę w pliku **.chiron-gui-proxy.json,** jak również wprowadzenie zmian w pliku **.chiron-gui-proxy.json** spowoduje zmianę ustawień w **oknie ustawień proxy**.

3.2.1 PRZYKŁADOWY PLIK KONFIGURACYJNY

```
{
  "proxyOptions": {
```

```
    "proxyHostAddress": "10.13.13.228",
    "proxyLogin": "przykłady_login",
    "proxyPassword": "przykładowe_hasło",
    "proxyPort": 8888
  },
  "proxySetting": "config"
}
```

3.3 KONFIGURACJA APLIKACJI NA SYSTEMACH OPERACYJNYCH LINUX I MACOS

Konfiguracja aplikacja na poszczególnych systemach operacyjnych jest taka sama. Jedynymi różnicami są nazwa pliku oraz ścieżki do plików wykorzystywanych przez oprogramowanie (bibliotek PKCS#11 oraz certyfikatu tls):

- Dla systemów Windows plik konfiguracyjny nosi nazwę config.json.
- Dla systemów Linux plik konfiguracyjny nosi nazwę linux-config.json.
- Dla systemów macOS plik konfiguracyjny nosi nazwę mac-config.json.

W poszczególnych plikach konfiguracyjnych należy wskazać prawidłowe ścieżki, w których umieszczone są biblioteki PKCS#11 dedykowane dla systemu.

3.4 KONFIGURACJA SŁOWNIKA

Nazwy przycisków w menu głównym są konfigurowalne. Znajdują się w pliku **guiTexts.json**, który jest w katalogu instalacji programu.

3.4.1 PRZYKŁADOWY PLIK KONFIGURACYJNY

```
{
    "MainWindow": {
        "unlockCardBtn": "Odblokuj kartę",
        "recertifyOldKeyBtn": "Recertyfikuj dla starego klucza",
        "recertifyOneTimeCodeBtn": "Recertyfikuj z kodem jednorazowym",
        "activateCardBtn": "Aktywuj kartę",
        "changeCardPinBtn": "Zmiana PIN-u karty",
        "installCertificateBtn": "Nagranie certyfikatu na kartę"
    }
}
```

4 LOGOWANIE BŁĘDÓW

Oprogramowanie Chiron GUI posiada własny system logowania błędów do pliku. W przypadku podania w głównym pliku konfiguracyjnym parametru **logLevel** (patrz pkt 3.1) zostanie utworzony plik **log.log** w katalogu instalacji programu.

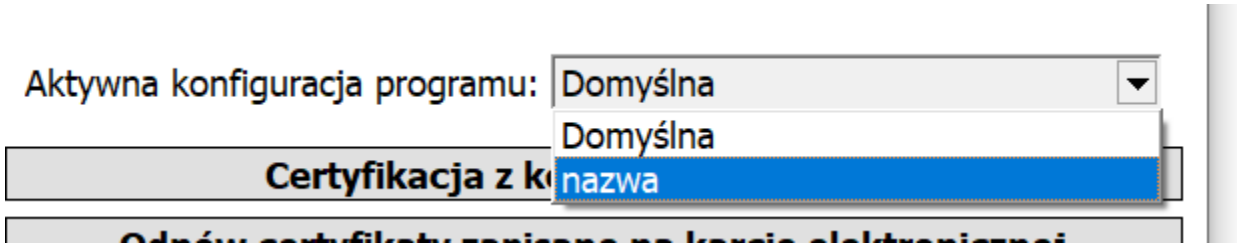
5 OBSŁUGA DWÓCH ŚRODOWISK W JEDNEJ ISTALACJI CHIRONA GUI

Aplikacja Chiron GUI ma możliwość współpracy z wieloma systemami Centrum Certyfikacji (Centaur) na jednej instalacji Chirona GUI.

Aby móc połączyć się do dwóch różnych środowisk za pomocą Chirona GUI w folderze instalacyjnym aplikacji powinny znajdować się:

1. Przykładowo dwa pliki konfiguracyjne:
    a. config.json – jest to „domyślna” konfiguracja
    b. config-nazwa.json – jest to druga konfiguracja

W powyższym przykładzie po uruchomieniu aplikacji Chiron GUI użytkownik będzie miał możliwość wyboru konfiguracji miedzy „Domyślna” a „nazwa”.



Rysunek 8 Aktywna konfiguracja programu - wybór konfiguracji

Konfiguracje są wczytywane z osobnych plików, których nazwy mogą mieć postać (program nie obsługuje polskich znaków):

- config-nazwa_konfiguracji.json,
- config - nazwa_konfiguracji.json,
- configNazwaKonfiguracji.json,
- config.json.

Konfiguracja o nazwie config.json jest uznawana za domyślną i jeśli istnieje jest wybierana automatycznie.

6 OBSŁUGA

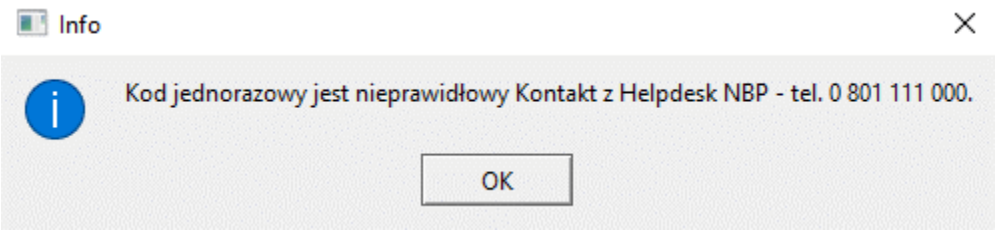
Po uruchomieniu programu dostępne jest okno główne. Wszystkie dostępne operacje są wykonywane w sposób prosty dla użytkownika.

Rysunek 9 Okno główne

W przypadku oczekiwania na wykonanie operacji zostanie wyświetlone animowane okno oczekiwania. W razie potrzeby okno to może być przeniesione w dowolne miejsce ekranu.

Rysunek 10 Okno oczekiwania

Komunikaty o błędach są wyświetlane w oknie błędu.



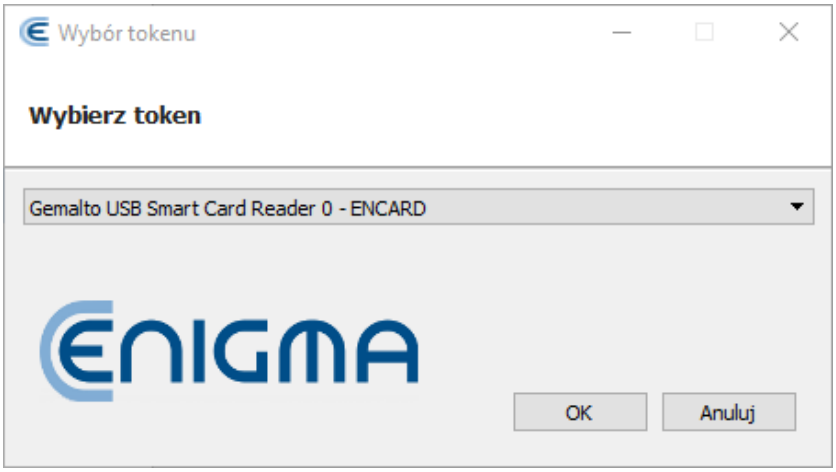
Rysunek 11 Okno błędu

6.1 CERTYFIKACJA Z KODEM JEDNORAZOWYM

Certyfikacja z kodem jednorazowym pozwala użytkownikowi wygenerować nowy certyfikat wykorzystując uzyskany z Centrum Certyfikacji kod jednorazowy.

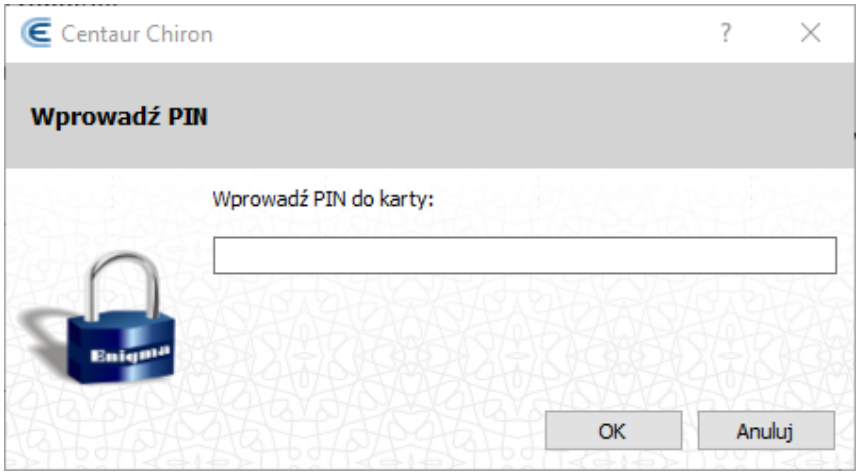
Aby wykonać certyfikację należy wybrać przycisk „Certyfikacja z kodem jednorazowym”.

Jeżeli podłączona jest więcej niż jedna karta lub karta posiada wiele tokenów zostanie wyświetlone okno wyboru tokenu:



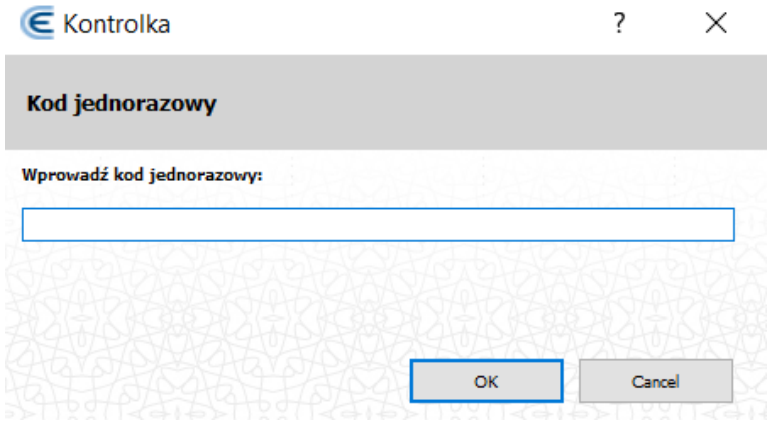
Rysunek 12. Okno wyboru tokenu

Z listy rozwijanej należy wskazać token na którym mają zostać wygenerowane certyfikaty, a następnie wybrać przycisk „OK”. Po wykonaniu powyższych kroków wyświetlone zostanie okno wprowadzania PINu chroniącego token:



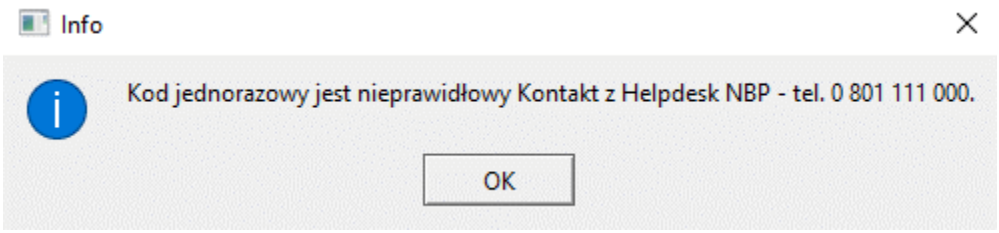
Rysunek 13. Wprowadzanie hasła do tokenu na karcie

Następnie należy podać kod jednorazowy uzyskany z Centrum Certyfikacji:



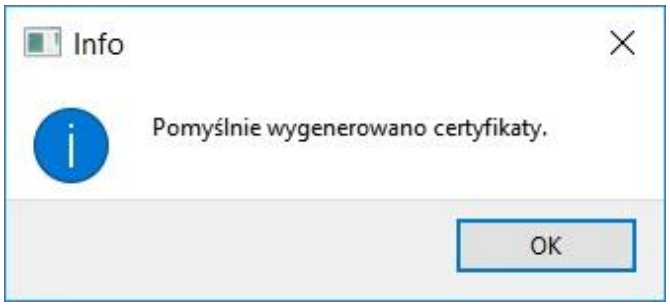
Rysunek 14. Wprowadzanie kodu jednorazowego

W sytuacji podania błędnego kodu jednorazowego zostanie wyświetlony komunikat:



Rysunek 15 komunikat o błędnym kodzie jednorazowym

Po pomyślnym przeprowadzeniu certyfikacji na karcie zostaną zainstalowane nowe certyfikaty kluczami i wyświetli się komunikat o zakończeniu procesu.



Rysunek 16 Zakończenie procesu certyfikacji

6.2 ODNÓW CERTYFIKATY ZAPISANE NA KARCIE ELEKTRONICZNEJ

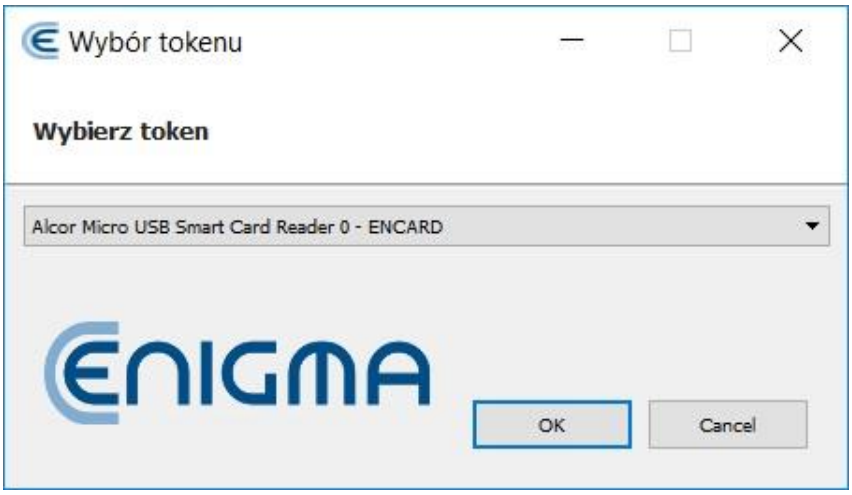
Odnowienie certyfikatów zapisanych na karcie elektronicznej pozwala użytkownikowi odnowić certyfikaty znajdujące się na karcie kryptograficznej.

Po wybraniu opcji „Odnów certyfikaty zapisane na karcie elektronicznej" program wyszuka karty.

W przypadku braku karty w czytniku lub niepoprawnej konfiguracji biblioteki PKCS11 (wskazana biblioteka w konfiguracji jest niekompatybilna z typem wprowadzonej karty) pojawi się komunikat z prośbą o włożenie karty do czytnika. Po włożeniu karty wciśnij **OK**.

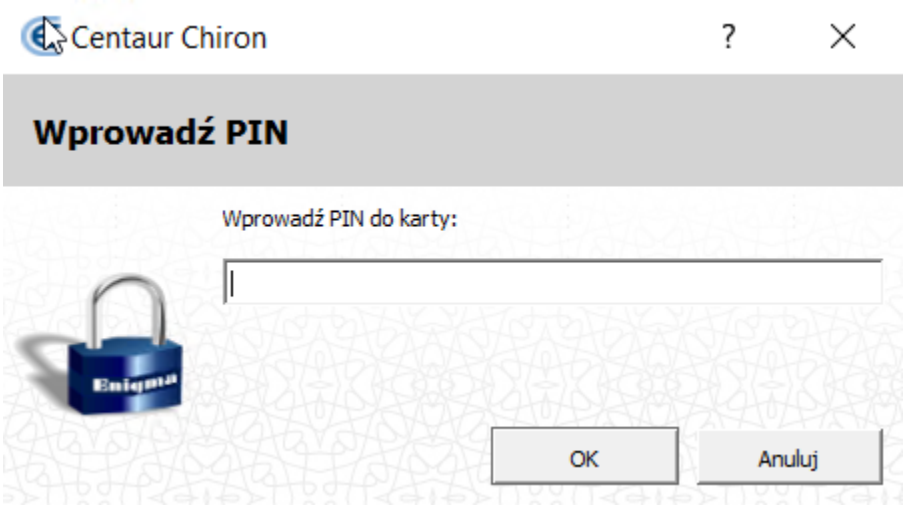
Rysunek 17 Włóż kartę do czytnika

W przypadku wykrycia większej liczby tokenów program wyświetli okno wyboru. Proszę wybrać token z listy i wcisnąć **OK**.



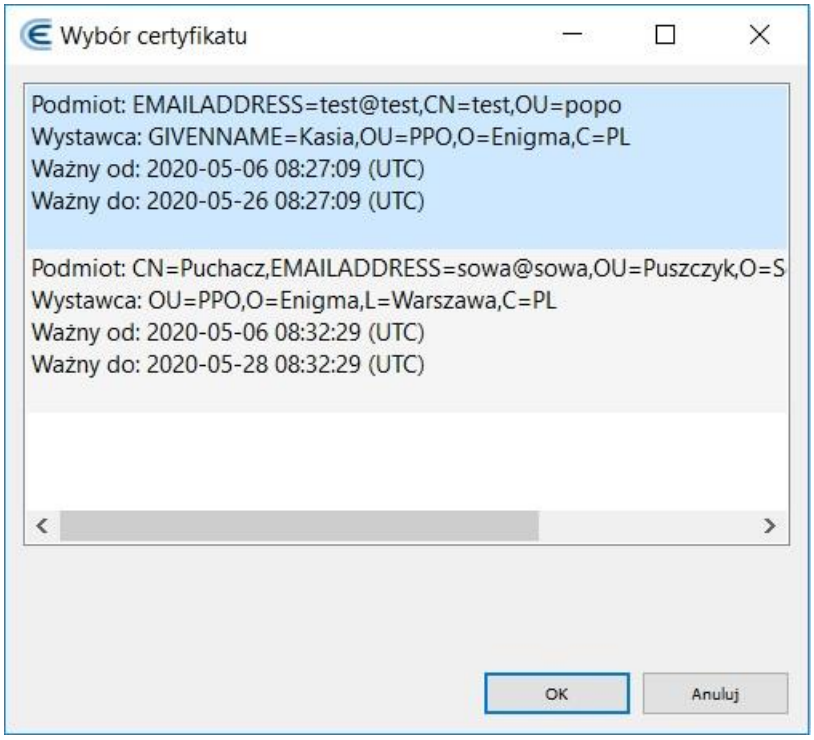
Rysunek 18 Okno wyboru tokenu

Po wyborze tokenu pojawi się okno z prośbą o PIN użytkownika w celu odczytania karty. Po wprowadzeniu PIN wciśnij **OK**.



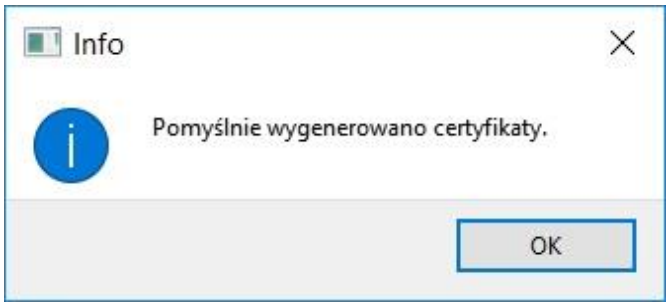
Rysunek 19 Wprowadź PIN

Gdy na karcie znajduje się tylko jeden certyfikat, zostanie on wybrany automatycznie. W innym przypadku pojawi się okno wyboru certyfikatu do odnowienia.



Rysunek 20 Okno wyboru certyfikatu

Po pomyślnym przeprowadzeniu certyfikacji na karcie zostaną zainstalowane nowe certyfikaty kluczami i wyświetli się komunikat o zakończeniu procesu.



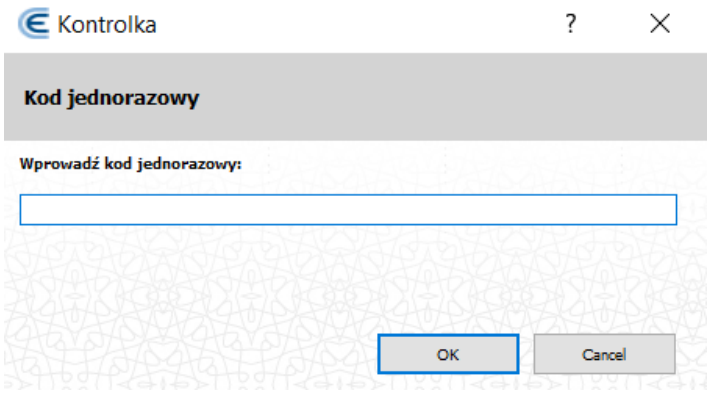
Rysunek 21 Zakończenie procesu certyfikacji

6.3 CERTYFIKACJA Z WYKORZYSTANIEM KODU JEDNORAZOWEGO DO PLIKU W FORMACIE PKCS#12

Certyfikacja z wykorzystaniem kodu jednorazowego do pliku w formacie PKCS#12 pozwala użytkownikowi wygenerować nowe certyfikaty wykorzystując uzyskany z Centrum Certyfikacji kod jednorazowy.

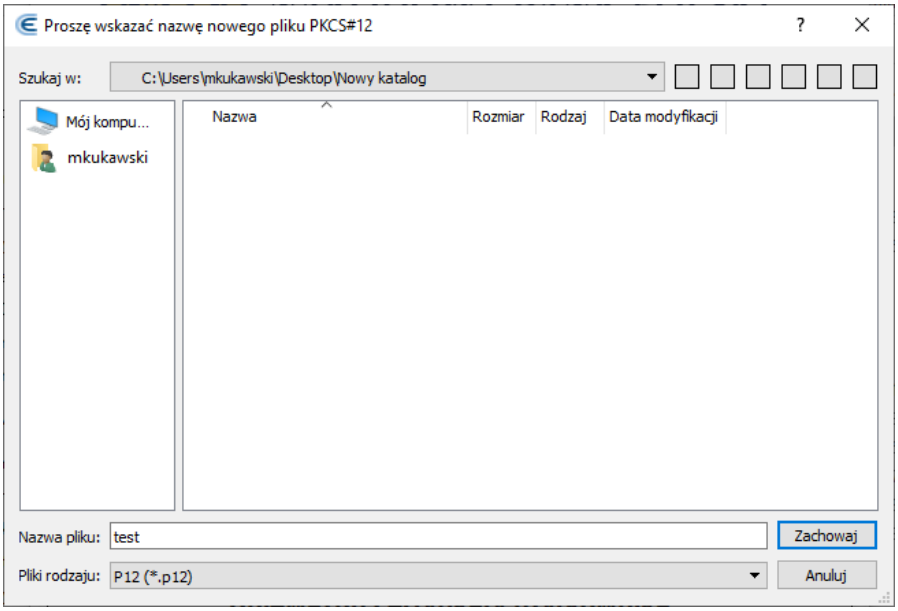
Aby wykonać certyfikację należy wybrać przycisk „Certyfikacja z wykorzystaniem kodu jednorazowego do pliku”.

Po wybraniu przycisku zostanie wyświetlono okno wprowadzania kodu jednorazowego, w którym należy podać kod uzyskany z Centrum Certyfikacji:



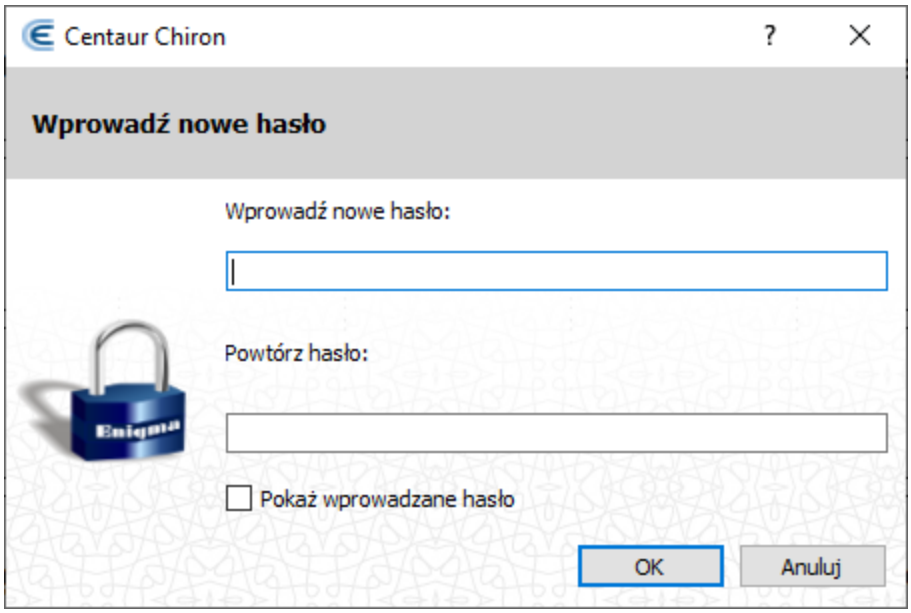
Rysunek 22. Wprowadzanie kodu jednorazowego

Następnie należy podać nazwę i lokalizację do zapisu wygenerowanego pliku PKCS#12:



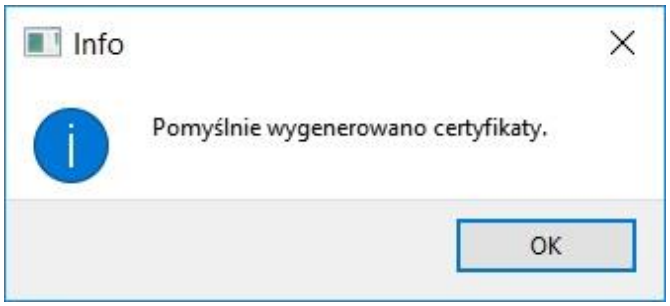
Rysunek 23. Wskazywanie nazwy i miejsca zapisu pliku PKCS#12

W kolejnym kroku trzeba wprowadzić oraz powtórzyć hasło, które będzie chroniło plik PKCS#12:



Rysunek 24. Ustalanie hasła do pliku

Po pomyślnym przeprowadzeniu certyfikacji w pliku zostaną zapisane nowe certyfikaty wraz z kluczami i wyświetli się komunikat o zakończeniu procesu.

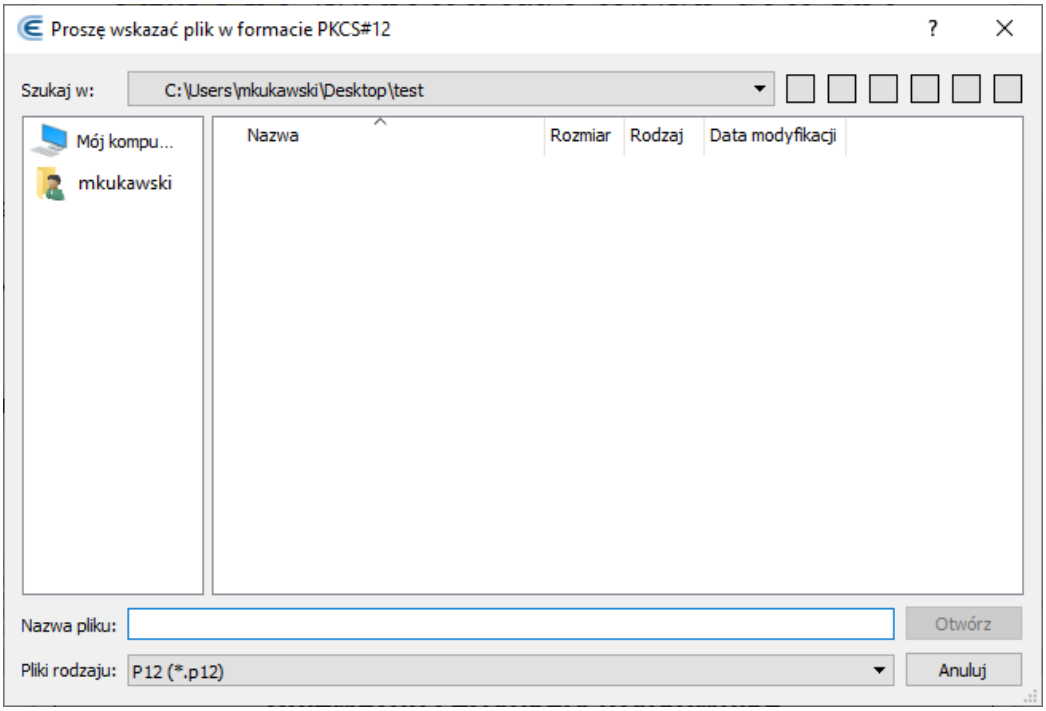


Rysunek 25. Zakończenie procesu certyfikacji

6.4 ODNOWIENIE CERTYFIKATU ZAPISANEGO W PLIKU W FORMACIE PKCS#12

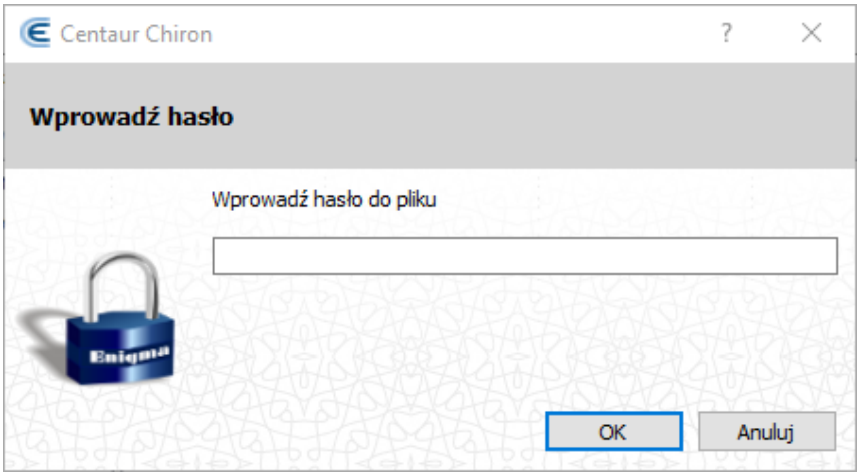
Aby wykonać akcję należy wybrać przycisk „Odnów certyfikat firmowy dla przeglądarki”

Zostanie wyświetlone okno wyboru pliku do odnowienia certyfikatu:



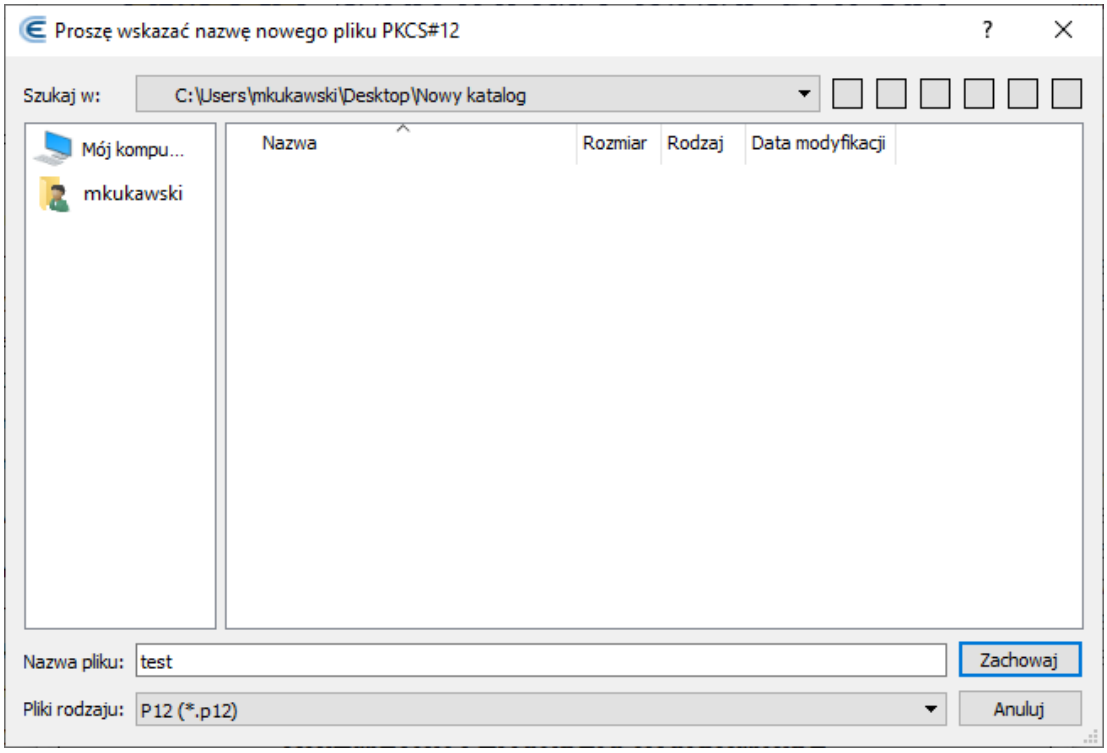
Rysunek 26. Wybór pliku do odnowienia certyfikatu

Następnie należy wprowadzić hasło chroniące plik:



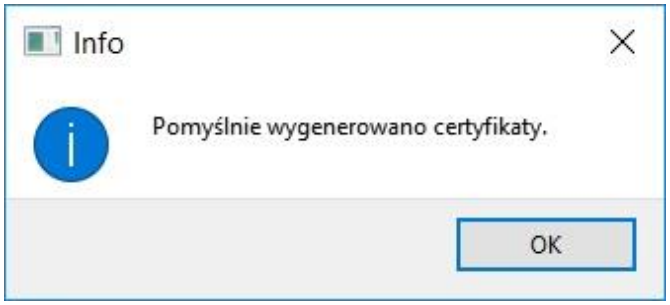
Rysunek 27. Wprowadzanie hasła do pliku

W kolejnym kroku należy podać nazwę i lokalizację do zapisu odnowionego pliku PKCS#12:



Rysunek 28. Wskazywanie nazwy i miejsca zapisu pliku PKCS#12

Po pomyślnym przeprowadzeniu odnowienia w pliku zostaną zapisane nowe certyfikaty wraz z kluczami i wyświetli się komunikat o zakończeniu procesu. Hasło do nowego pliku PKCS#12 jest takie samo jak chroniące dotychczasowy plik PKCS#12.

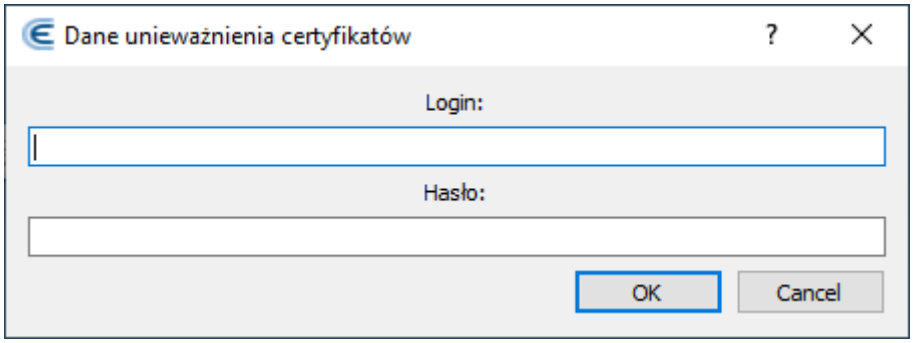


Rysunek 29. Zakończenie procesu certyfikacji

6.5 UNIEWAŻNIANIE CERTYFIKATÓW UŻYTKOWNIKA

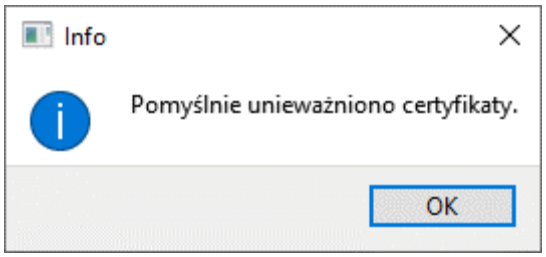
Przed rozpoczęciem unieważniania certyfikatów użytkownik musi przygotować swój unikalny identyfikator oraz hasło do komunikacji z Centrum Certyfikacji

Chcąc unieważnić wszystkie certyfikaty użytkownik powinien wybrać przycisk „Unieważnij certyfikaty użytkownika”. Spowoduje to wyświetlenie okna, w którym należy wprowadzić Login oraz Hasło użytkownika. Login jest unikalnym identyfikatorem użytkownika, a Hasło jest ustalonym hasłem do kontaktów z Centrum Certyfikacji.



Rysunek 30. Dane użytkownika do unieważnienia certyfikatów

Po wprowadzeniu poprawnych danych i zatwierdzeniu przyciskiem OK **wszystkie** certyfikaty użytkownika zostaną unieważnione, co zostanie potwierdzone komunikatem:



Rysunek 31. Potwierdzenie unieważnienia certyfikatów

7 SPIS ILUSTRACJI