NARODOWY
BANK POLSKI

CHIRON GUI

Departament Cyberbezpieczeństwa
Warszawa, 2024 r.

Opracował:
Wydział Kryptografii

email: cck@nbp.pl

Spis treści

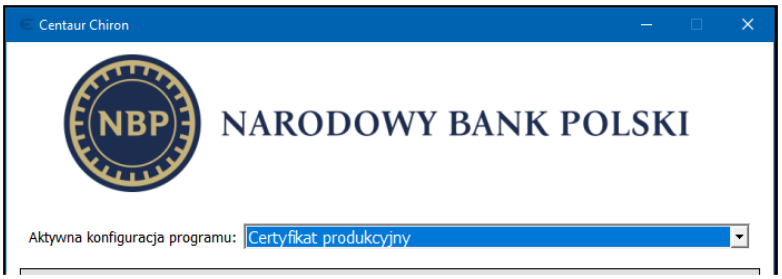
1. Informacje wstępne

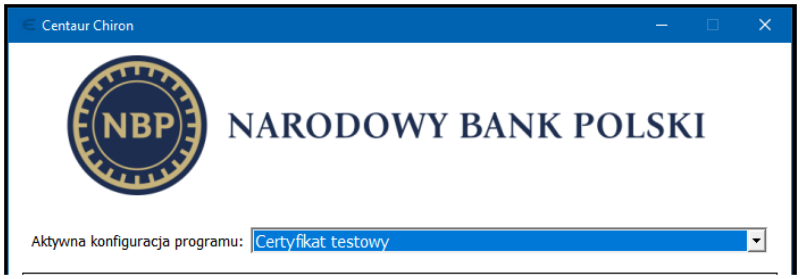
1. Od dnia 21.11.2022 r. dla wszystkich certyfikatów w systemie DOCert funkcjonuje nowy system zdalnej obsługi certyfikatów oparty o aplikację Chiron GUI.
2. Aplikacja Chiron GUI wymaga instalacji na stacji roboczej użytkownika.
3. Pliki instalacyjne aplikacji Chiron GUI dostępne są na stronie www.docert.nbp.pl w zakładce „Obsługa zdalna".
4. Instrukcja obsługi aplikacji Chiron GUI dostępna jest na stronie www.docert.nbp.pl w zakładce „Instrukcje".
5. Jedna aplikacja Chiron GUI obsługuje zarówno certyfikaty produkcyjne jak i testowe *(nie ma potrzeby instalacji osobnych aplikacji dla obu typów certyfikatów).*
6. Aplikacja Chiron GUI łączy się z serwerami systemu DOCert o następujących adresach:
    a. Środowisko testowe
        i. 193.109.212.15:443
        ii. 195.85.196.15:443
    b. Środowisko produkcyjne
        i. 193.109.212.32:443
        ii. 195.85.196.32:443
7. Ruch pomiędzy aplikacją Chiron GUI a ww. adresami jest szyfrowany – zastosowanie deszyfratorów lub innych urządzeń ingerujących w połączenie może spowodować brak możliwości wygenerowania/odnowienia certyfikatu *(sugerujemy dodanie wyjątków na urządzeniach deszyfrujących ruch).*
8. Aplikacja Chiron GUI obsługuje serwery PROXY konfiguracja możliwa jest z poziomu menu aplikacji po pierwszym jej uruchomieniu.
9. Logi aplikacji zapisywane są w pliku log.log znajdującym się w katalogu, w którym zainstalowano aplikację Chiron GUI *(w przypadku systemu Windows standardowo C:\Program Files(x86)\Chiron GUI\log.log).*

2. Uruchomienie aplikacji

1) Uruchomienie aplikacji Chiron GUI możliwe jest z poziomu menu systemu operacyjnego lub przy pomocy ikony umieszczonej na pulpicie.
2) Przy każdym uruchomieniu, aplikacja próbuje nawiązać połączenie z serwerami, w celu weryfikacji konfiguracji. W razie potrzeby aplikacja pobierze nową konfigurację.
3) Wygląd okna aplikacji *(wersja zainstalowanej aplikacji widoczna jest w lewym górnym rogu okna).*

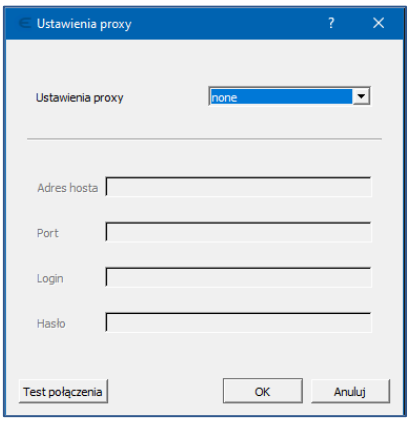
4) Po uruchomieniu aplikacji Chiron GUI należy wybrać, czy obsługa certyfikatów ma dotyczyć certyfikatów wydanych przez urząd produkcyjny **NBP CCK 2** czy testowy **NBP CCK TEST 2.**





2.1. Konfiguracja PROXY.

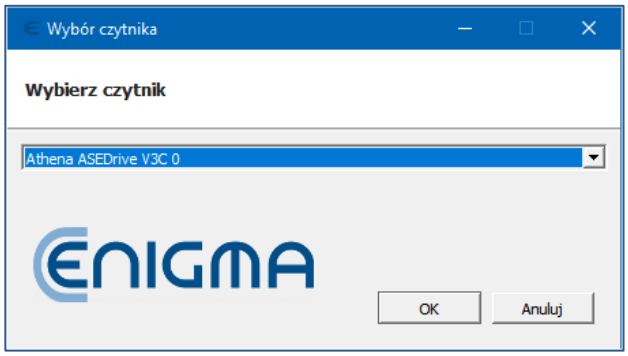
1) Po pierwszym uruchomieniu aplikacji Chiron GUI, z dostępnego menu możliwe jest wprowadzenie konfiguracji PROXY *(jeśli jest wymagane)*, w każdym przypadku możliwe jest wykonanie testu połączenia z systemem odnawiania certyfikatów.
    a. none – brak PROXY;
    b. system – konfiguracja pobierana jest z systemu operacyjnego;
    c. config – ręczne wprowadzenie danych;
        i. Adres hosta;
        ii. Port;
        iii. Login i hasło *(jeśli wymagane)*.



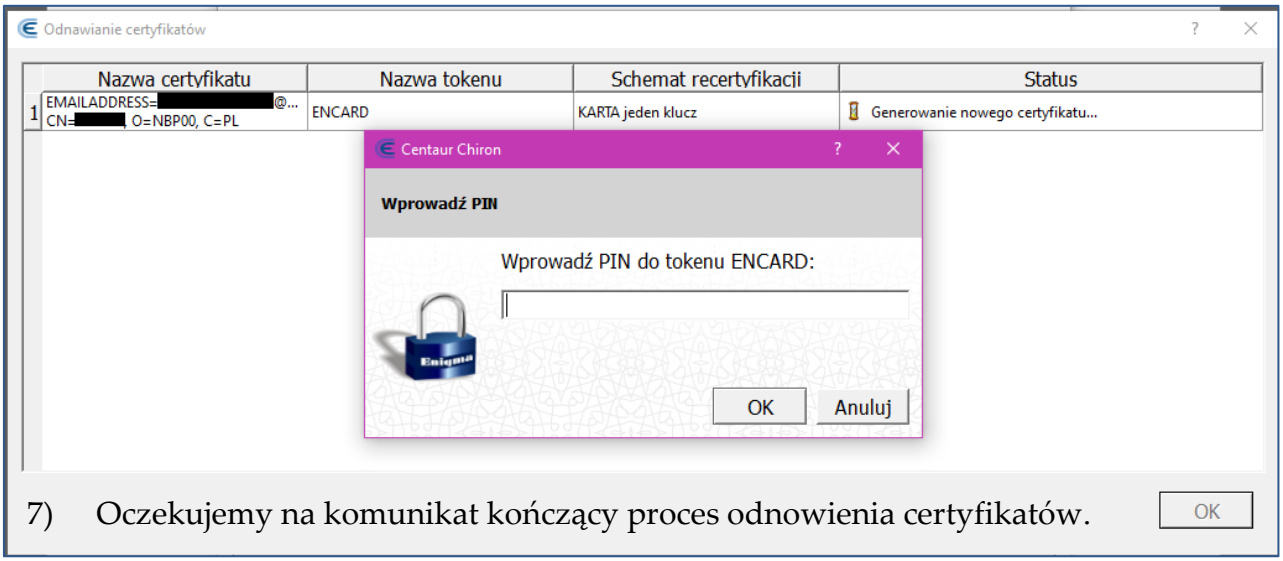
2.2. Odnów certyfikat zapisany na karcie elektronicznej.

1) Wkładamy kartę do czytnika;
2) Uruchamiamy aplikacje Chiron GUI;
3) Wybieramy środowisko *(Certyfikat testowy lub Certyfikat produkcyjny)*;

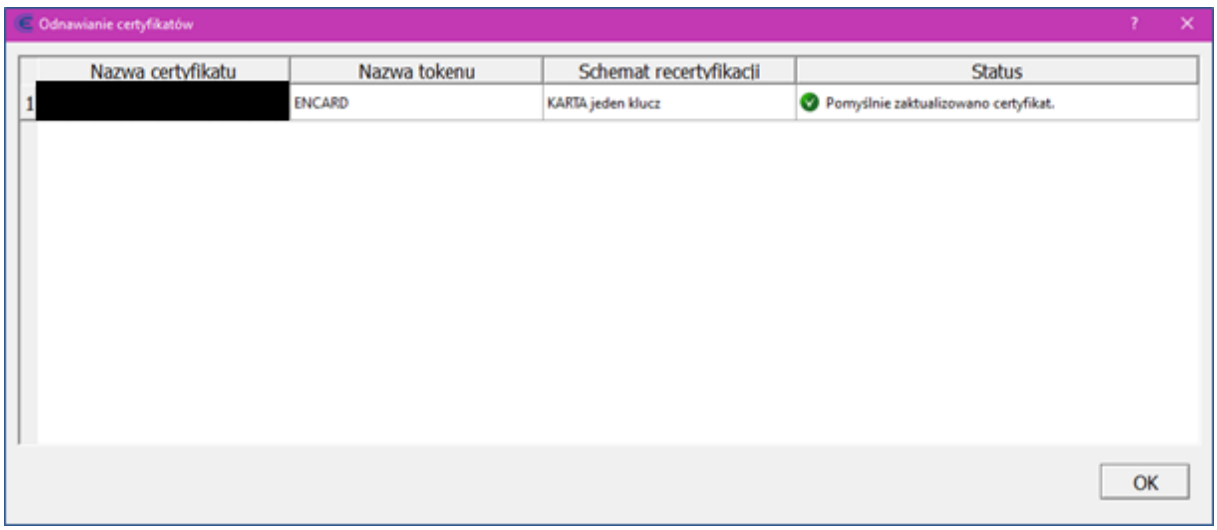
4) Wybieramy opcję *Odnów certyfikaty zapisane na karcie elektronicznej;*
5) Jeśli w komputerze zainstalowanych jest więcej niż jeden czytnik aplikacja poprosi o wybór czytnika z kartą, na której certyfikat ma zostać odnowiony;



6) Wprowadzamy pin do karty;



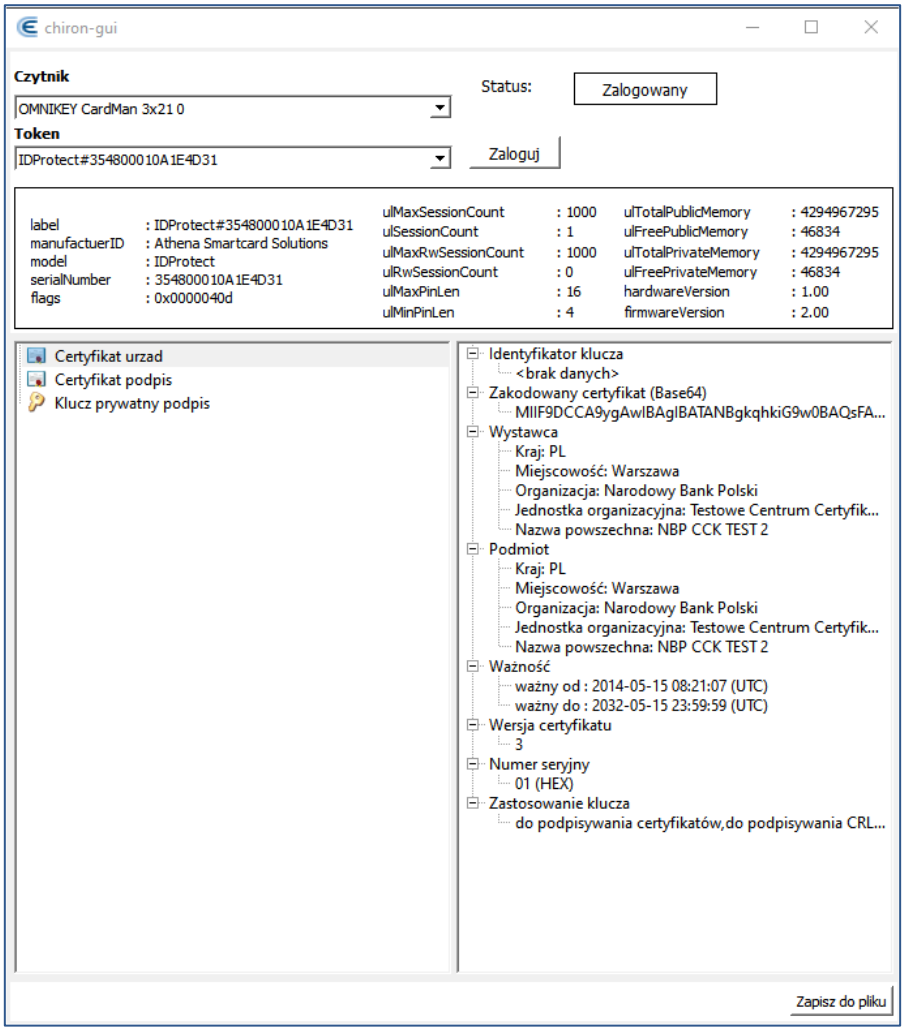
7) Oczekujemy na komunikat kończący proces odnowienia certyfikatów.



2.3. Wyświetl informacje o karcie.

1) Opcja umożliwia wyświetlenie informacji o certyfikatach i kluczach nagranych na kartę;
2) Wybranie tej opcji wywoła poniższe okno:

3) W oknie możliwe są operacje:

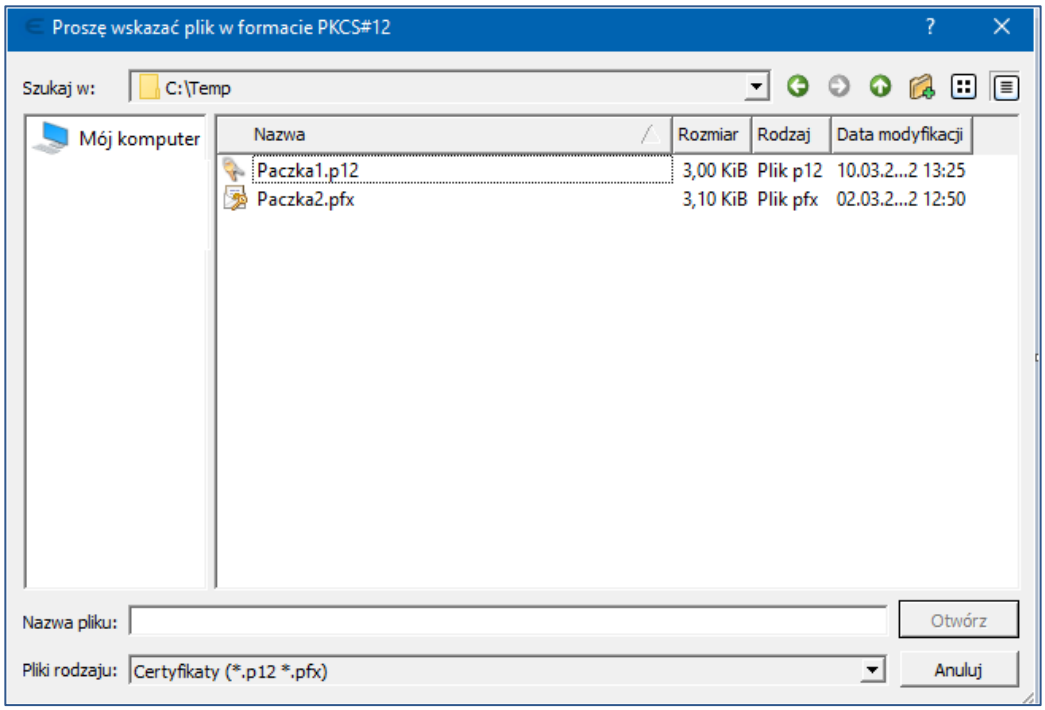


a. Zalogowanie do karty;
b. Podgląd certyfikatów i kluczy;
c. Wygenerowanie raportu z zawartości karty *(Zapisz do pliku)*.

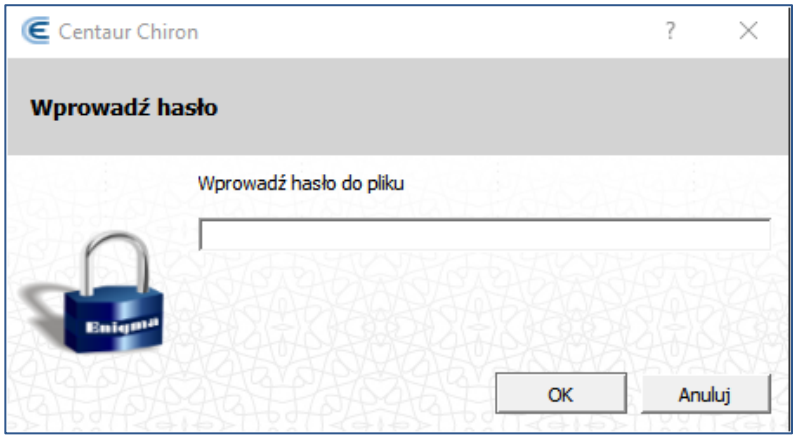
2.4. Odnów certyfikat firmowy dla przeglądarki

1) Opcja ta umożliwia odnowienie certyfikatu zapisanego w postaci pliku z rozszerzeniem .p12 lub .pfx;

2) Wskazujemy plik zawierający certyfikat, który będzie podlegał odnowieniu;



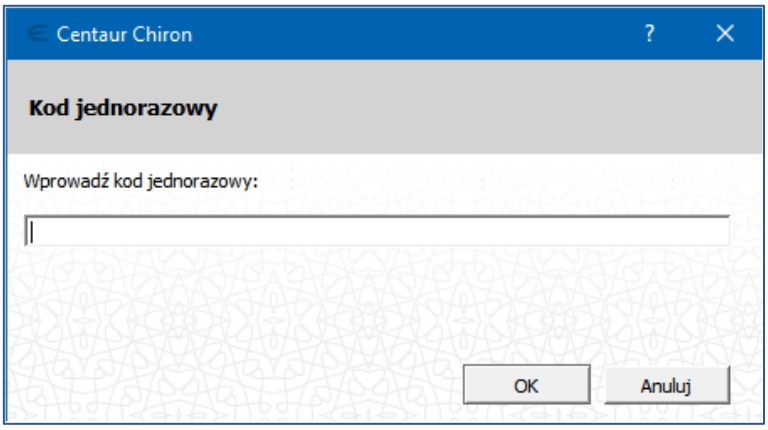
3) Wprowadzamy hasło do pliku wskazanego w ppkt 2;



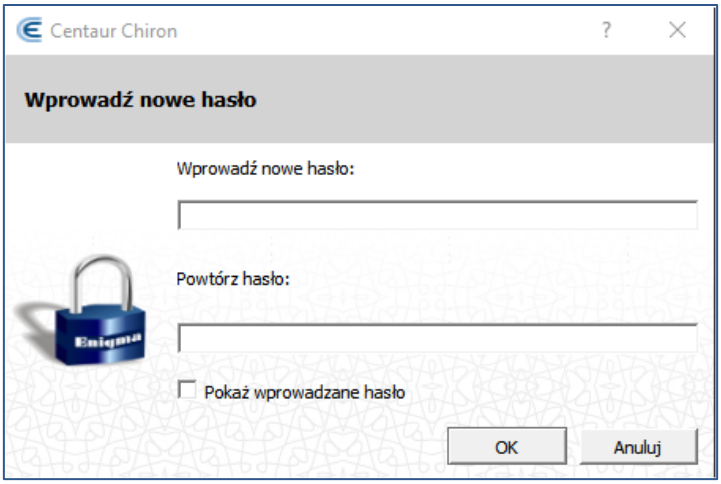
4) Wskazujemy miejsce i nazwę pliku, w którym zapisany zostanie nowy certyfikat z kluczami. Hasło do nowego pliku będzie identyczne z hasłem wpisanym w ppkt 3.

2.5. Wygeneruj certyfikat do pliku na podstawie kodu jednorazowego.

1) Opcja ta umożliwia wygenerowanie nowego certyfikatu na podstawie kodu. Wybranie tej opcji wywoła okno:

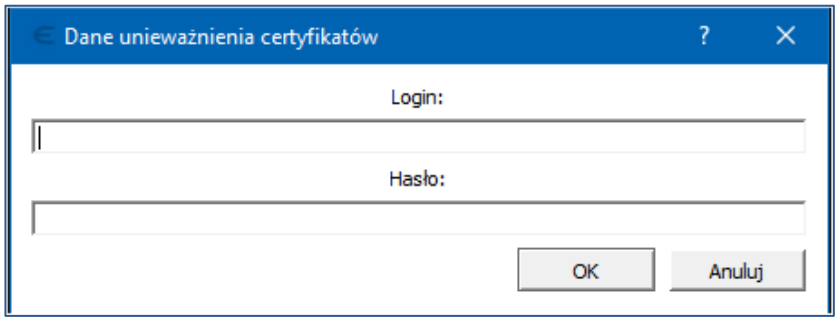


2) Wprowadzamy otrzymany kod *(jednym ciągiem, nie ma znaczenia wielkość znaków)*;
3) Wskazujemy miejsce i nazwę pliku, w którym zapiszemy nowe klucze kryptograficzne i certyfikat;
4) Wprowadzamy hasło, które będzie chronić wygenerowane klucze kryptograficzne i certyfikat *(minimalna długość hasła to 4 znaki)*.

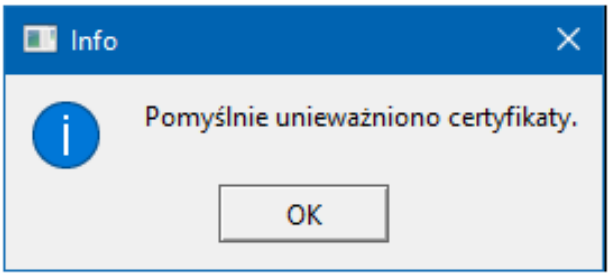


2.6. Unieważnij certyfikat użytkownika.

1) Opcja ta umożliwia unieważnienie wszystkich certyfikatów użytkownika wystawionych w systemie DOCert;
2) **UWAGA: Ta opcja dostępna jest tylko dla wybranych systemów informatycznych i niektórych typów certyfikatów;**
3) W celu unieważnienia certyfikatów wprowadzamy otrzymane w Punkcie Rejestracji Użytkowników dane;



4) Zatwierdzamy klikając OK.



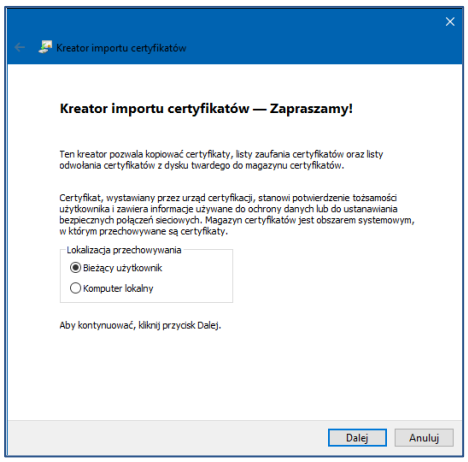
3. Instalacja certyfikatów

Opisana poniżej instalacja certyfikatów, pozwoli na ich wykorzystanie w następujących przeglądarkach internetowych:

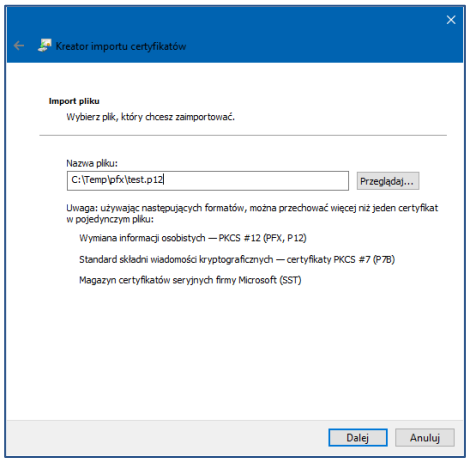
- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Opera

W celu zainstalowania certyfikatu należy:

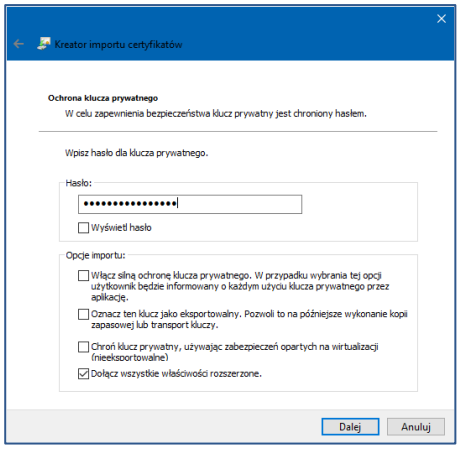
1) Kliknąć dwa razy na pliku zawierającym zestaw kluczy i certyfikatów (rozszerzenie pliku : .p12 lub .pfx);
2) W otwartym oknie „Kreator importu certyfikatów" pozostawiamy domyślną konfigurację (Bieżący użytkownik), klikamy ***Dalej***;



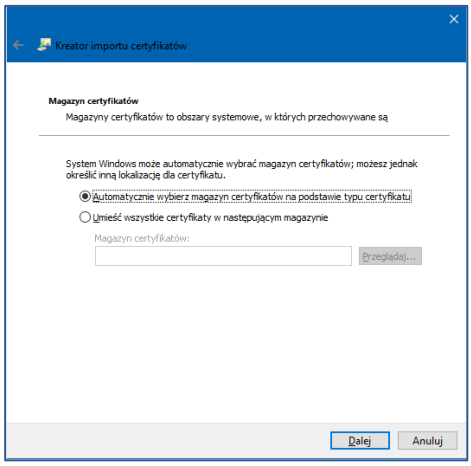
3) Jeśli nazwa pliku nie jest wskazana, przyciskiem *Przeglądaj* wskazujemy plik, jeśli nazwa pliku jest wskazana klikamy ***Dalej***;



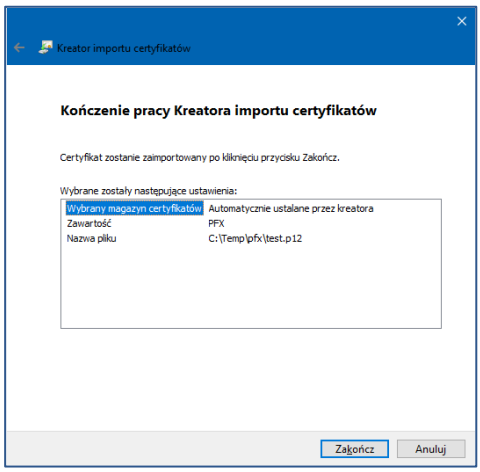
4) Podajemy hasło do pliku z kluczami, następnie klikamy ***Dalej***;



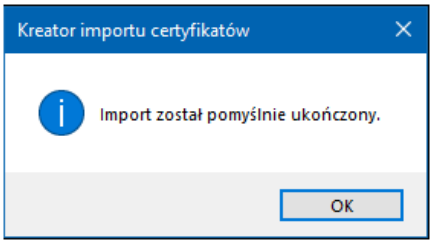
5) W otwartym oknie „Kreator importu certyfikatów" pozostawiamy domyślną konfigurację (Automatycznie wybierz magazyn…), zatwierdzamy klikając ***Dalej***;



6) W podsumowaniu ustawień klikamy ***Zakończ***;

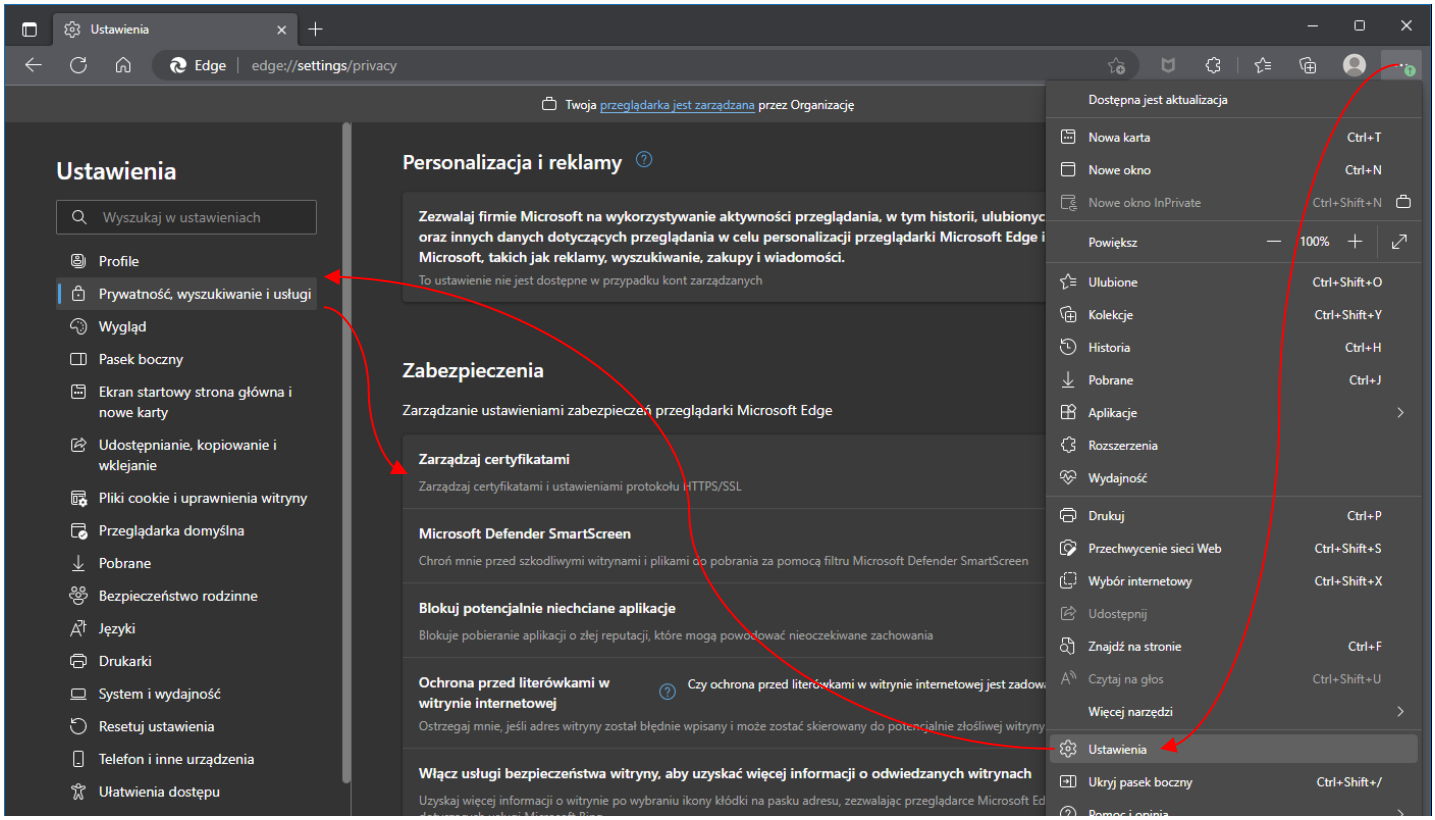


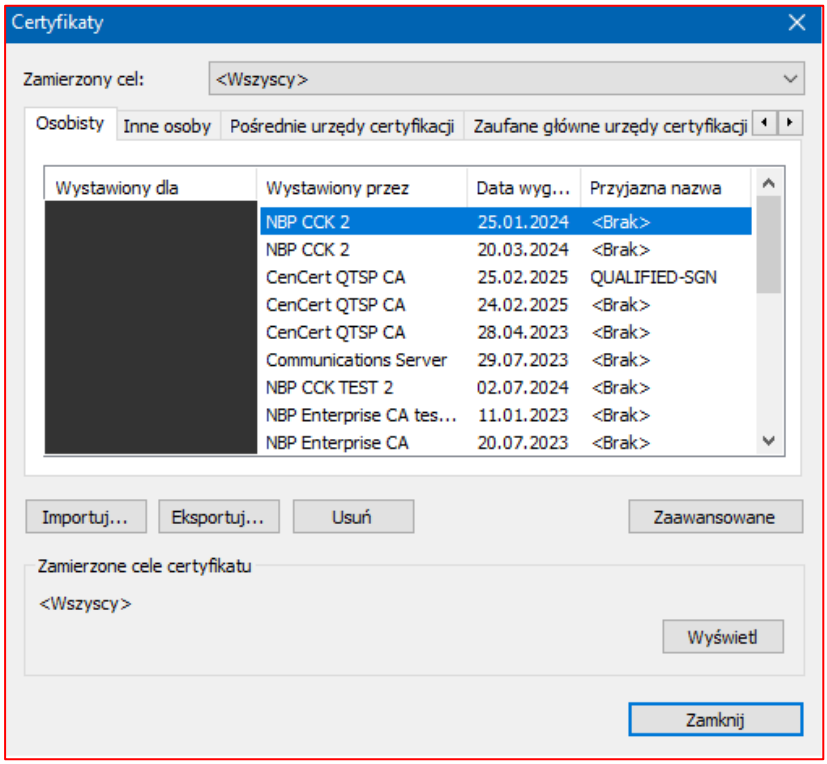
7) Pomyślny import kończy się komunikatem :



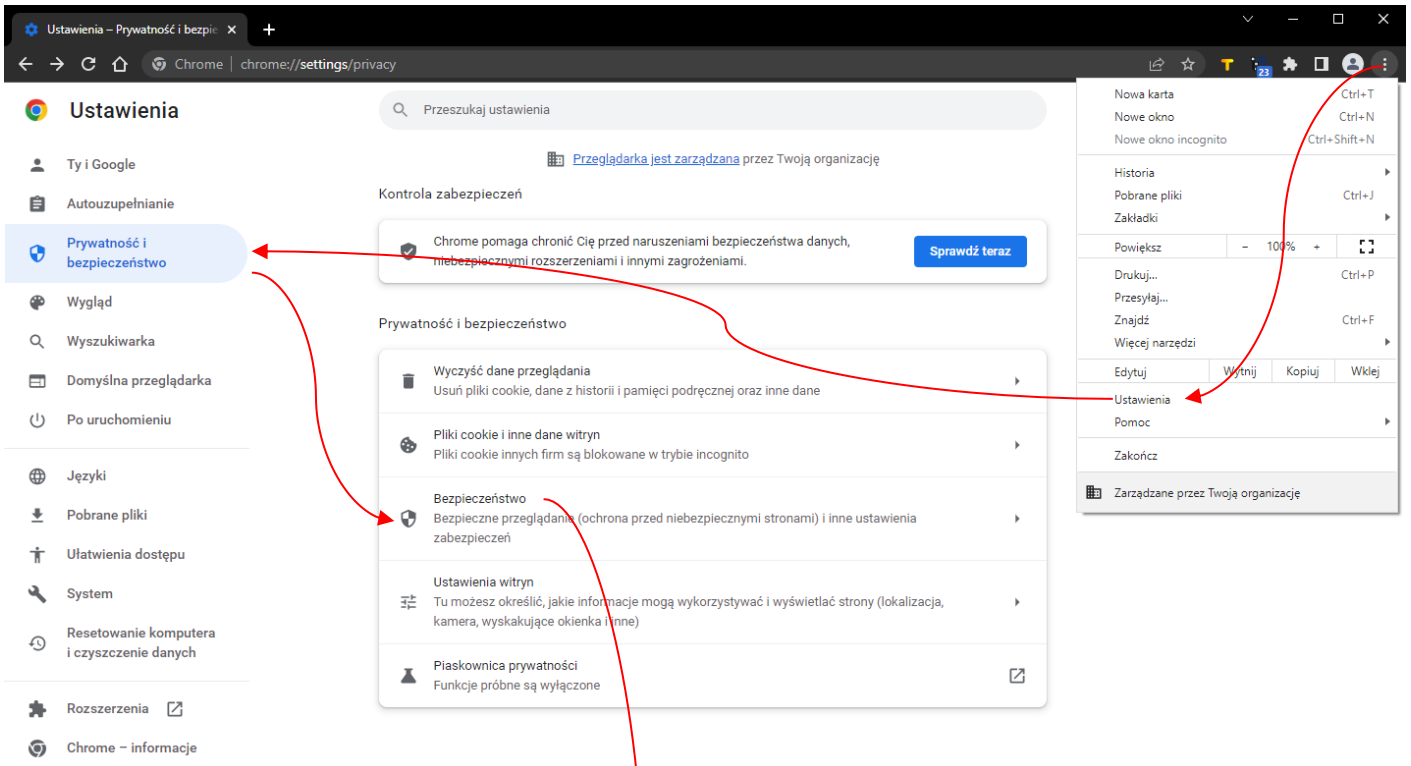
8) Podgląd magazynu certyfikatów dostępny jest z poziomu:

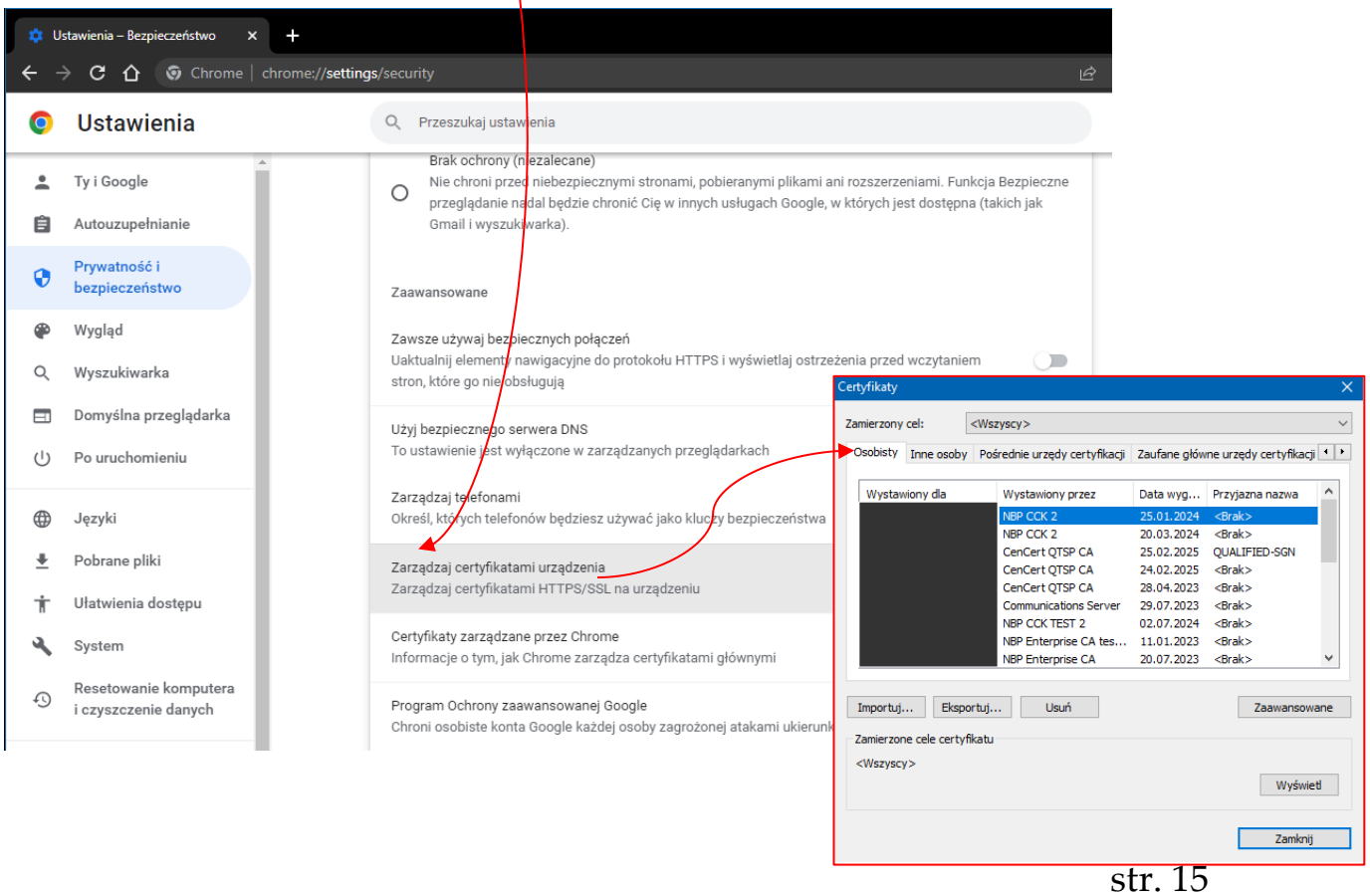
- **Microsoft Edge** → *Ustawienia* → *Prywatność, wyszukiwanie i usługi* → *Zarządzaj certyfikatami;*


Ustawienia
Edge | edge://settings/privacy
Twoja przeglądarka jest zarządzana przez Organizację
Ustawienia
Wyszukaj w ustawieniach
Profile
Prywatność, wyszukiwanie i usługi
Wygląd
Pasek boczny
Ekran startowy strona główna i nowe karty
Udostępnianie, kopiowanie i wklejanie
Pliki cookie i uprawnienia witryny
Przeglądarka domyślna
Pobrane
Bezpieczeństwo rodzinne
Języki
Drukarki
System i wydajność
Resetuj ustawienia
Telefon i inne urządzenia
Ułatwienia dostępu
Personalizacja i reklamy
Zezwalaj firmie Microsoft na wykorzystywanie aktywności przeglądania, w tym historii, ulubionyc
oraz innych danych dotyczących przeglądania w celu personalizacji przeglądarki Microsoft Edge i
Microsoft, takich jak reklamy, wyszukiwanie, zakupy i wiadomości.
To ustawienie nie jest dostępne w przypadku kont zarządzanych
Zabezpieczenia
Zarządzanie ustawieniami zabezpieczeń przeglądarki Microsoft Edge
Zarządzaj certyfikatami
Zarządzaj certyfikatami i ustawieniami protokołu HTTPS/SSL
Microsoft Defender SmartScreen
Chroń mnie przed szkodliwymi witrynami i plikami do pobrania za pomocą filtru Microsoft Defender SmartScreen
Blokuj potencjalnie niechciane aplikacje
Blokuje pobieranie aplikacji o złej reputacji, które mogą powodować nieoczekiwane zachowania
Ochrona przed literówkami w witrynie internetowej
Ostrzegaj mnie, jeśli adres witryny został błędnie wpisany i może zostać skierowany do potencjalnie złośliwej witryny
Włącz usługi bezpieczeństwa witryny, aby uzyskać więcej informacji o odwiedzanych witrynach
Dostępna jest aktualizacja
Nowa karta Ctrl+T
Nowe okno Ctrl+N
Nowe okno InPrivate Ctrl+Shift+N
Powiększ 100%
Ulubione Ctrl+Shift+O
Kolekcje Ctrl+Shift+Y
Historia Ctrl+H
Pobrane Ctrl+J
Aplikacje
Rozszerzenia
Wydajność
Drukuj Ctrl+P
Przechwycenie sieci Web Ctrl+Shift+S
Wybór internetowy Ctrl+Shift+X
Udostępnij
Znajdź na stronie Ctrl+F
Czytaj na głos Ctrl+Shift+U
Więcej narzędzi
Ustawienia
Ukryj pasek boczny Ctrl+Shift+/

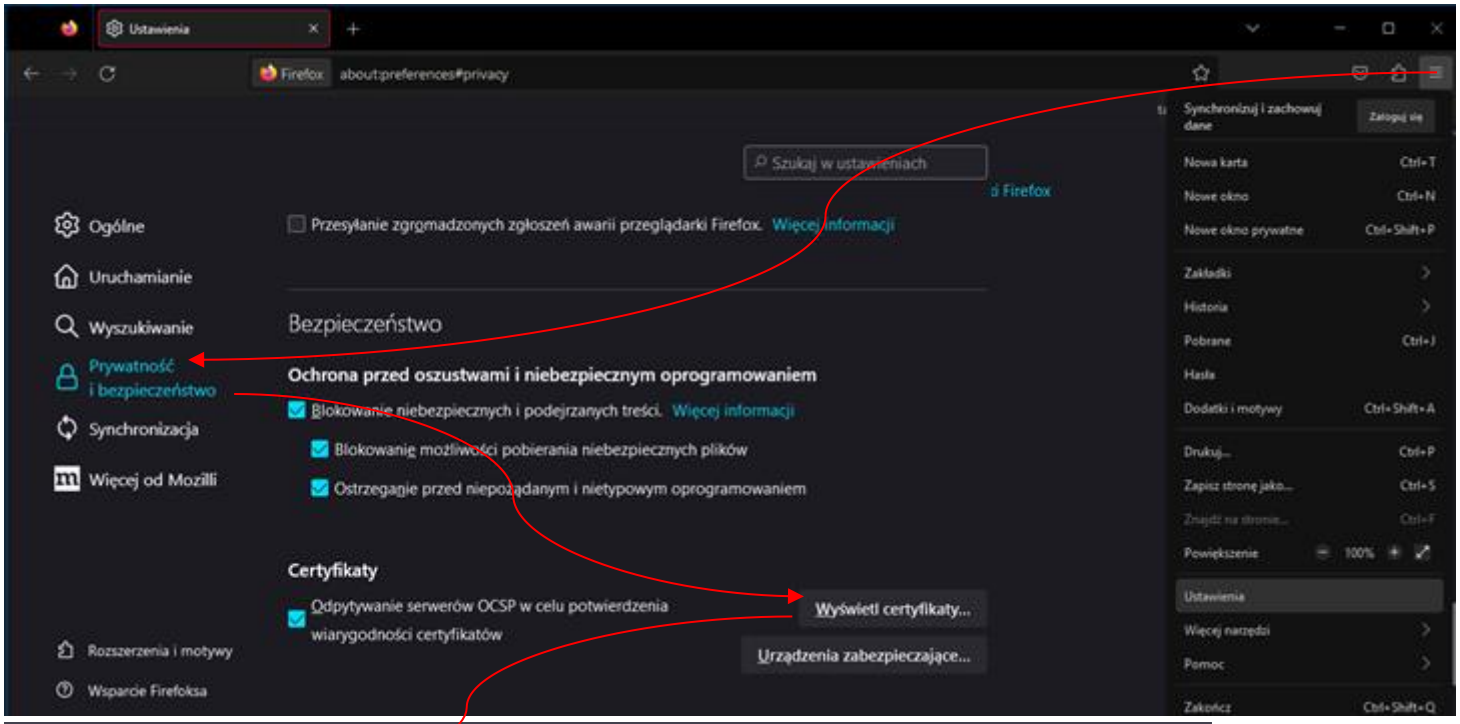

Certyfikaty
Zamierzony cel: <Wszyscy>
Osobisty
Inne osoby
Pośrednie urzędy certyfikacji
Zaufane główne urzędy certyfikacji
Wystawiony dla
Wystawiony przez
Data wyg...
Przyjazna nazwa
NBP CCK 2 25.01.2024 <Brak>
NBP CCK 2 20.03.2024 <Brak>
CenCert QTSP CA 25.02.2025 QUALIFIED-SGN
CenCert QTSP CA 24.02.2025 <Brak>
CenCert QTSP CA 28.04.2023 <Brak>
Communications Server 29.07.2023 <Brak>
NBP CCK TEST 2 02.07.2024 <Brak>
NBP Enterprise CA tes... 11.01.2023 <Brak>
NBP Enterprise CA 20.07.2023 <Brak>
Importuj...
Eksportuj...
Usuń
Zaawansowane
Zamierzone cele certyfikatu
<Wszyscy>
Wyświetl
Zamknij

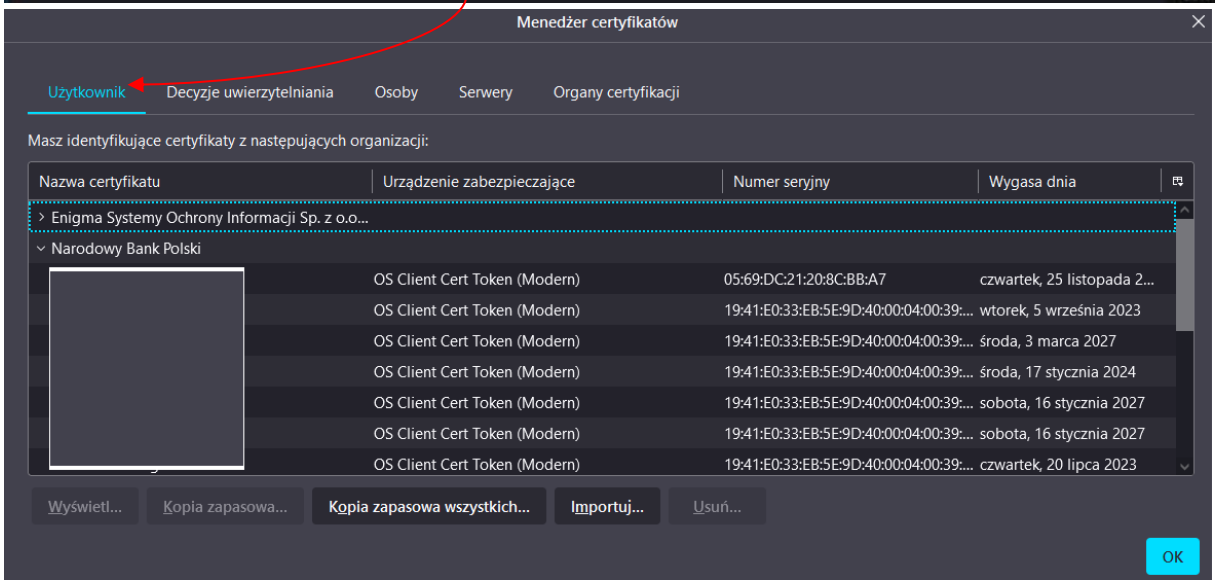
- **Google Chrome** → *Ustawienia* → *Prywatność i bezpieczeństwo* → *Bezpieczeństwo* → *Zarządzaj certyfikatami urządzenia;*



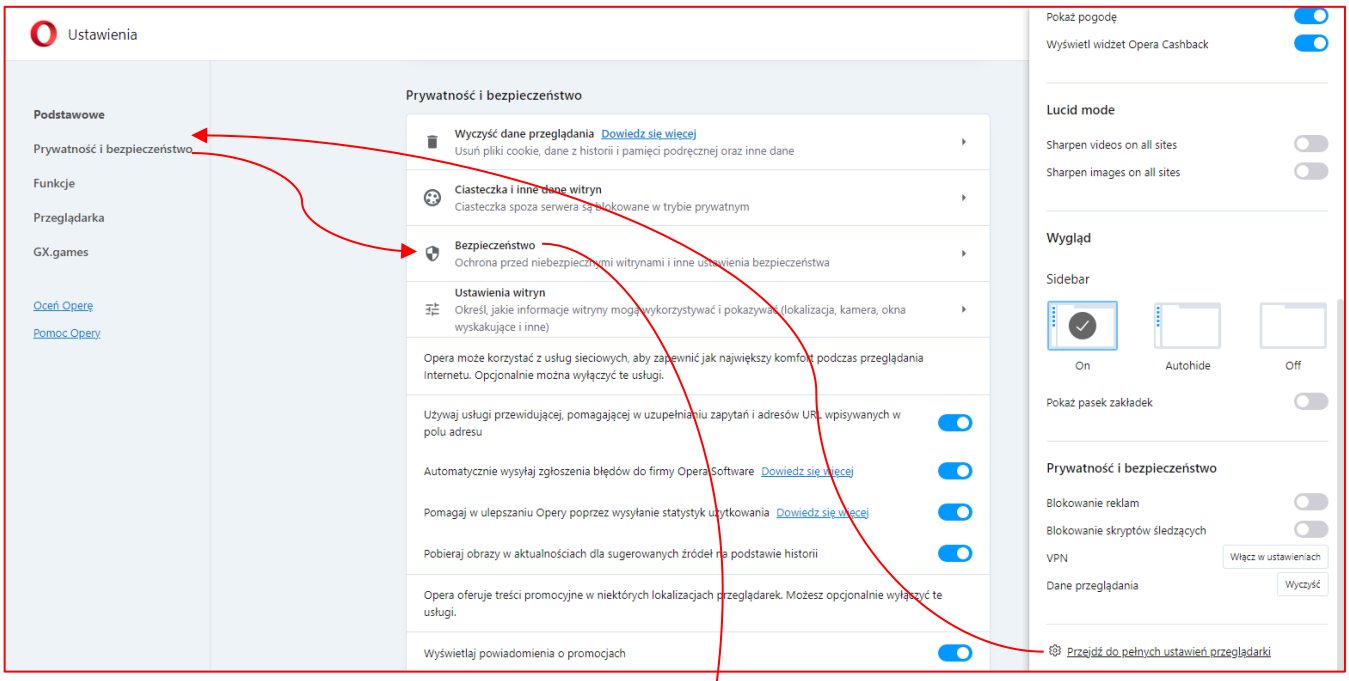


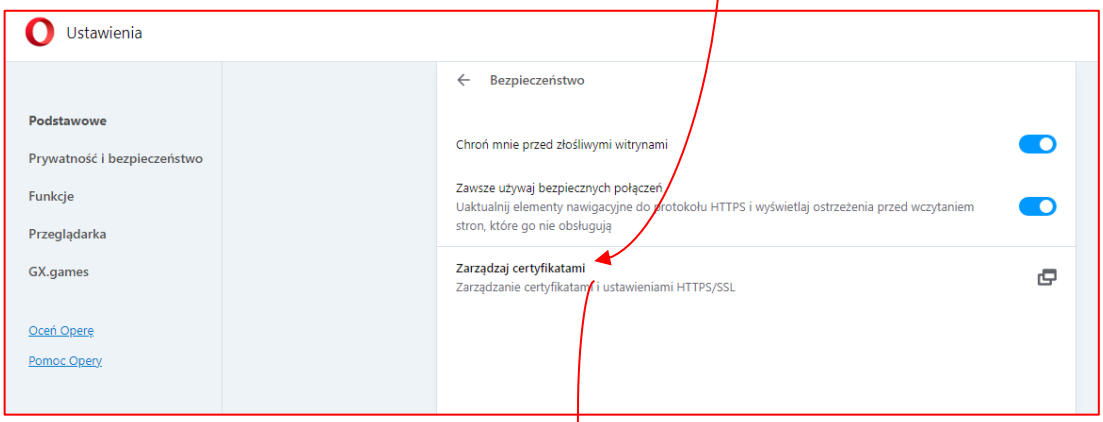
- **Mozilla Firefox** → *Ustawienia* → *Prywatność i bezpieczeństwo* → *Wyświetl certyfikaty;*

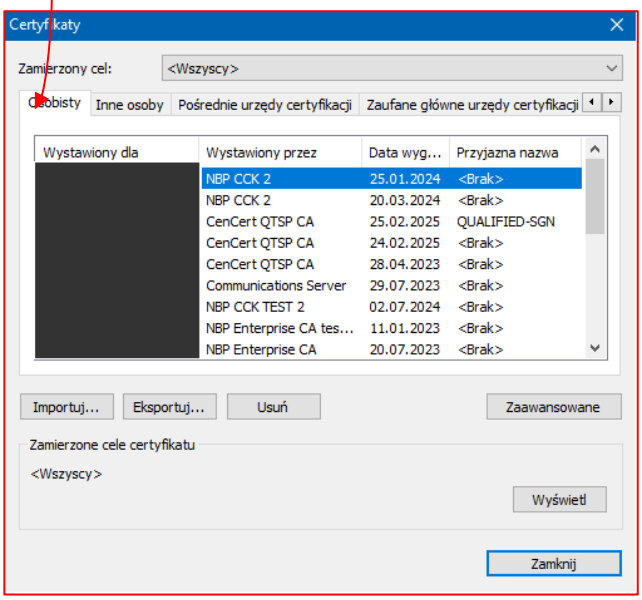




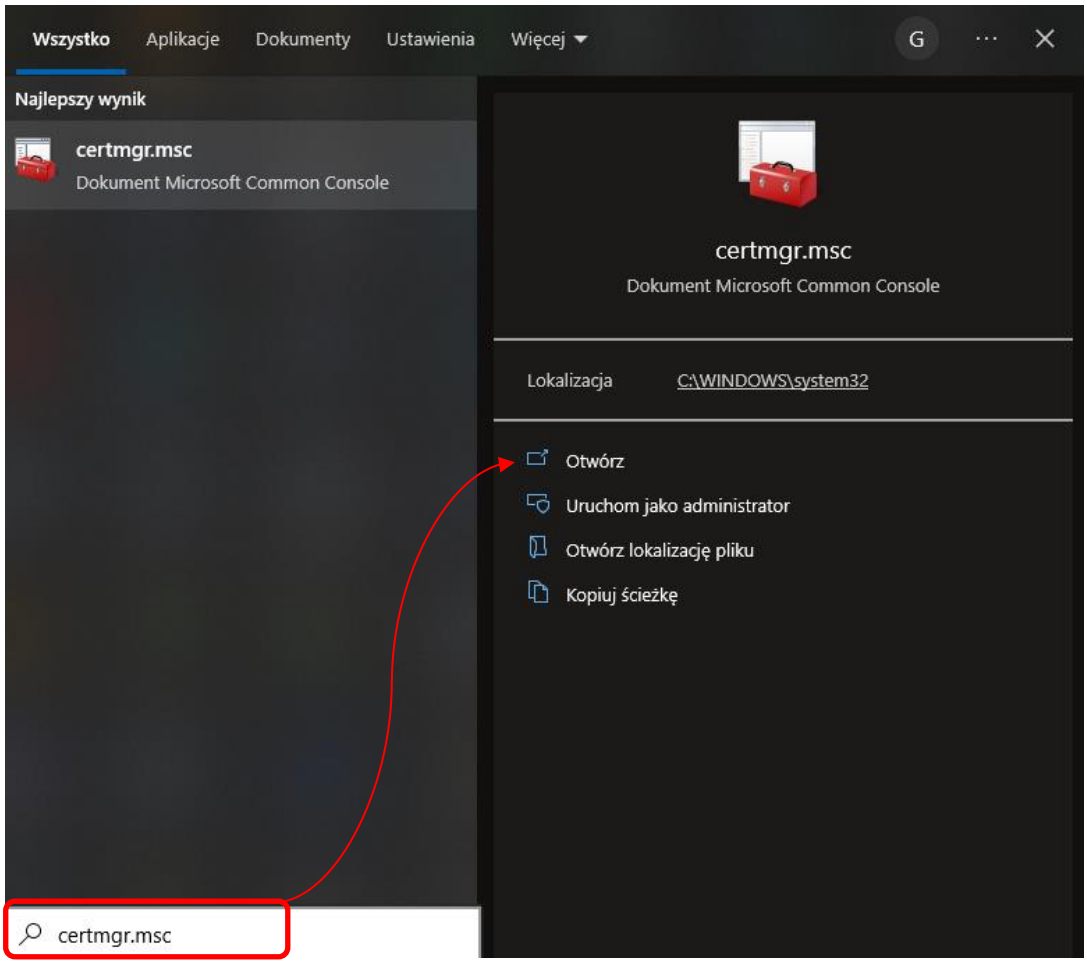
- **Opera** → *Ustawienia* → *Prywatność i bezpieczeństwo* → *Bezpieczeństwo* → *Zarządzaj certyfikatami;*

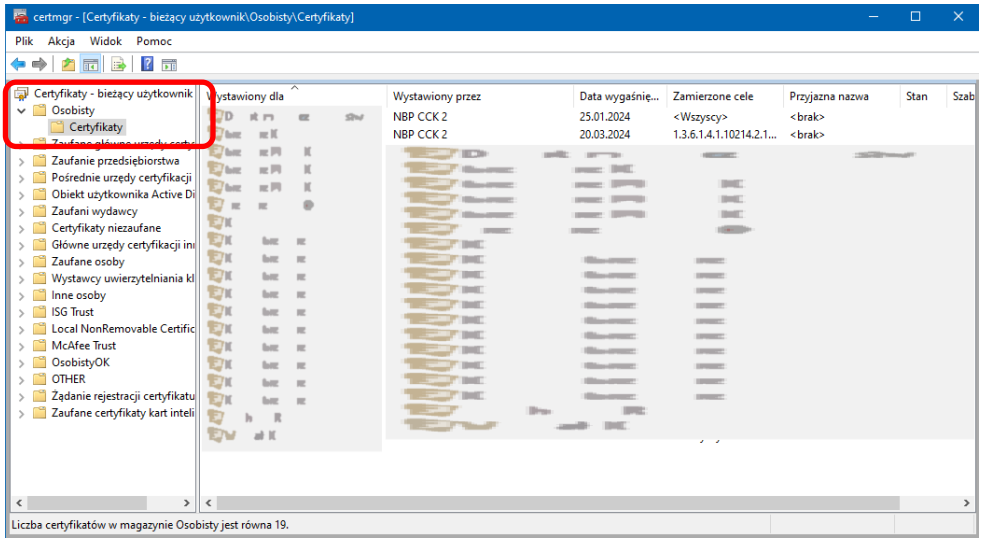






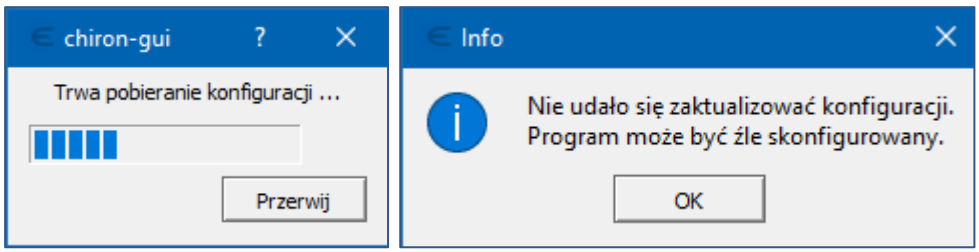
- Wbudowanej w system konsoli Microsoft → należy uruchomić ***certmgr.msc.***





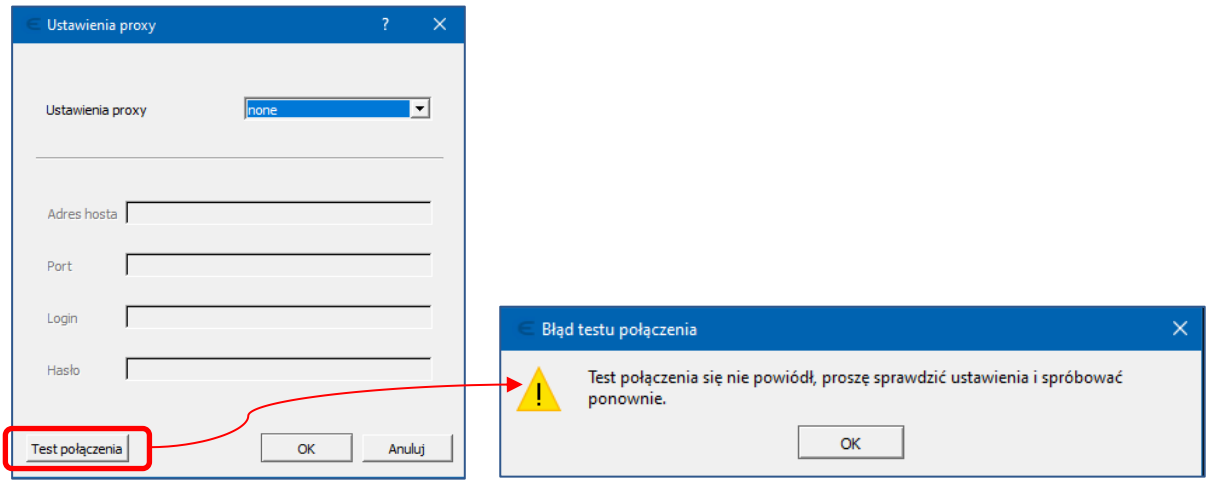
4. Obsługa błędów

1) Po uruchomieniu aplikacji pojawia się komunikat:



Aplikacja nie pobrała aktualnej konfiguracji, należy sprawdzić :

- czy masz połączenie z Internetem,
- czy została wprowadzona konfiguracja Proxy (jeśli dostęp do Internetu tego wymaga), opis konfiguracji Proxy znajduje się w pkt.2.1
- wykonaj „Test połączenia", w okienku Ustawienia proxy, jeżeli mimo prawidłowych ustawień otrzymujesz komunikat :



Zgłoś się do *swojego* administratora sieci, w celu diagnozy braku połączenia.

2) Odnowienie certyfikatów zakończyło się błędem:

2		ENCARD		Błąd zwrócony przez centrum certyfikacji: Token: ENCARD zawiera certyfikaty, które nie mogą zostać odnowione, ponieważ z konfiguracji CCK usunięto schemat certyfikacji wg. którego zostały wystawione

Lub

2		IDProtect#3548000223344D31		Błąd zwrócony przez centrum certyfikacji: Token: IDProtect#3548000223344D31 zawiera certyfikaty, które nie mogą zostać odnowione, ponieważ z konfiguracji CCK usunięto schemat certyfikacji wg. którego zostały wystawione

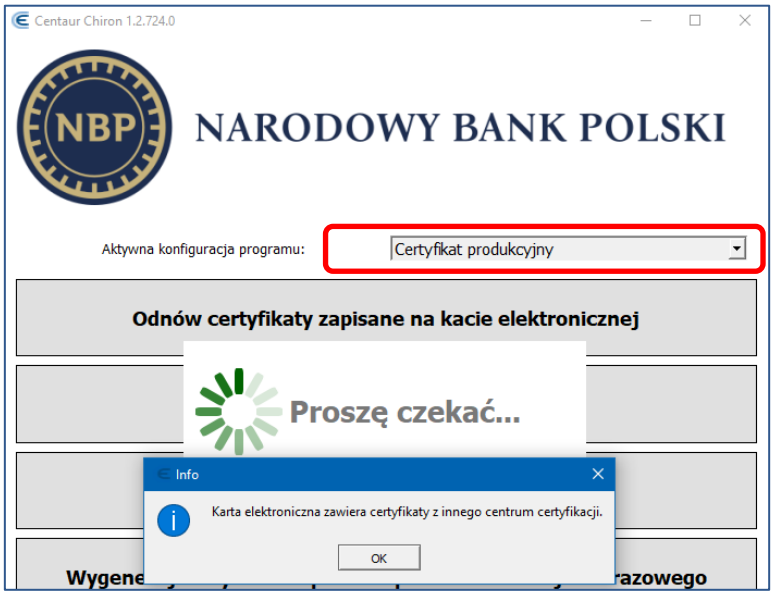
Natomiast pozycja nr 1 prezentuje się w postaci:

	Nazwa certyfikatu	Nazwa tokenu	Schemat recertyfikacji	Status
1	EMAILADDRESS=test@nbp.pl, CN=Wydział - IK, O=Wydział IK, C=PL	IDProtect#3548002521244D31	KARTA jeden klucz	Pomyślnie zaktualizowano certyfikat.

Jeżeli pozycja nr.1, która zawiera informacje o podmiocie odnawiającym certyfikat i status operacji zakończył się powodzeniem, natomiast w pozycjach kolejnych brak jest *Nazwy certyfikatu* i status zakończył się komunikatem jak powyżej – należy zignorować ten błąd.

Wyżej wymieniona sytuacja może mieć miejsce w przypadku gdy na karcie znajdują się certyfikaty klucza publicznego (bez klucza prywatnego), certyfikaty wystawione w szablonach wycofanych z użycia lub certyfikaty wystawione przez obce urzędy certyfikacji.

3) W przypadku komunikatu :



- Sprawdź czy wybrałeś odpowiednią konfigurację programu: (Certyfikat produkcyjny – Certyfikat testowy).

4) W przypadku odnawiania certyfikatów zapisanych w pliku (*.p12 / *.pfx), pojawia się błąd o braku dostępu do pliku:
    a. Należy sprawdzić czy użytkownik posiada pełne uprawnienia do pliku,
    b. Plik powinien znajdować się lokalnie na dysku u użytkownika dokonującego operacji odnowienia, nie zaleca się wskazywania pliku umieszczonego na zasobie sieciowym
5) Operacja zakończyła się poprawnie jednak nie można odnaleźć pliku:

    Przy generowaniu certyfikatów na podstawie kodu jednorazowego, w przypadku nie wskazania ścieżki (zatwierdzono domyślną ścieżkę) w celu odszukania plik należy:

    - przeszukać dyski filtrując pliki *.pfx, *.p12,

    - uruchomić ponownie kreator generowania, przejść do kroku w którym aplikacja prosi o wskazanie nazwy pliku i zweryfikować czy w podanej ścieżce znajduje się plik.