

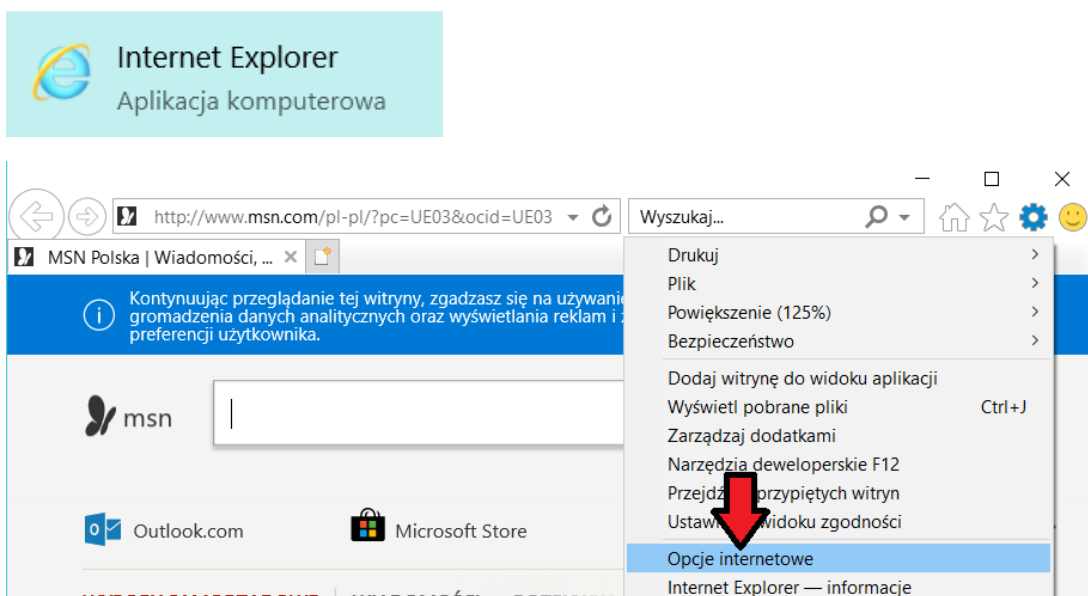
UWAGA!

Instrukcja tylko dla informatyków!

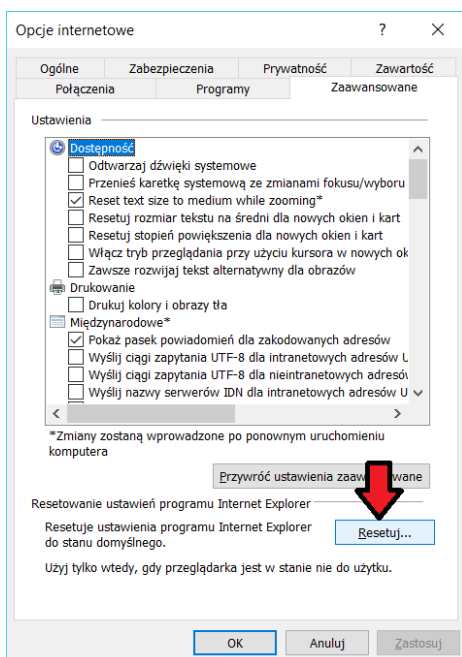
Wprowadzenie zmian na jej podstawie przez osobę nieuprawnioną może doprowadzić do utraty certyfikatów i konieczności pracy bez dostępu do systemu CEPiK 2.0

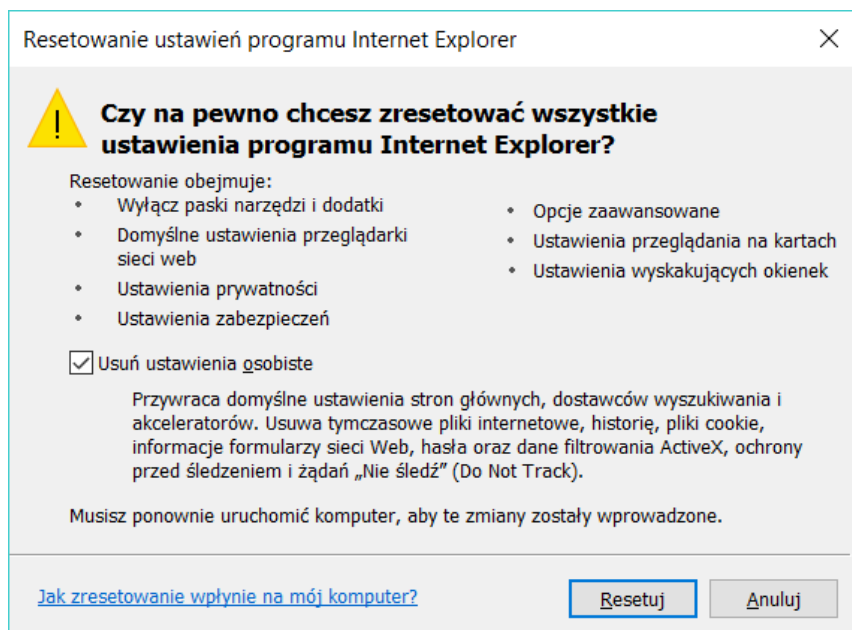
1. Internet Explorer

a) Uruchamiamy przeglądarkę „Internet Explorer” i przechodzimy do ustawień

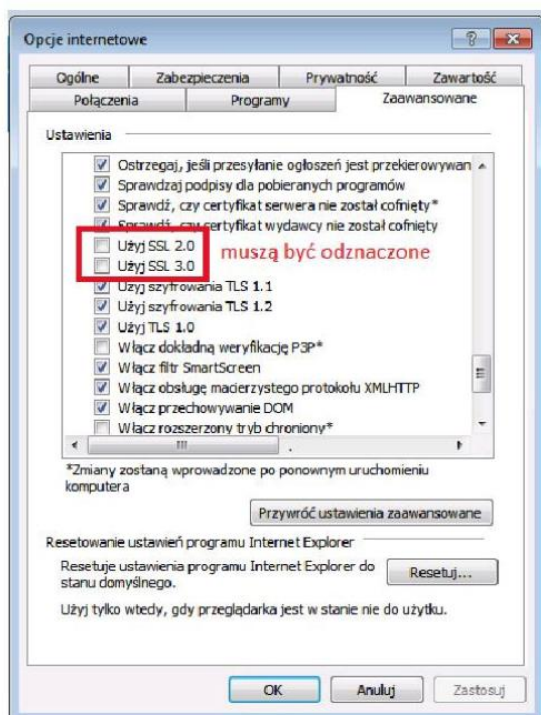


b) Resetujemy ustawienia przeglądarki do ustawień domyślnych

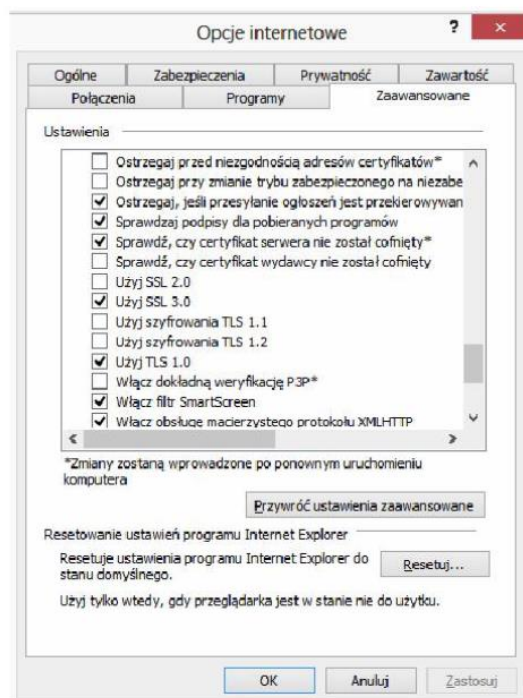




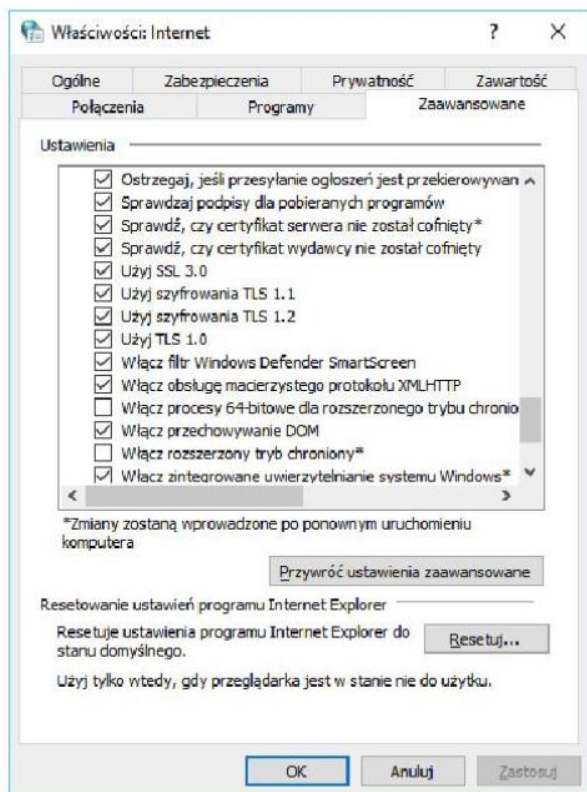
c) Weryfikujemy poprawności ustawień dla obsługi komunikacji z serwerami CEPIK 2.Przy (Windows 7 pamiętamy o usunięciu zaznaczeń w punktach „Użyj SSL 2.0” i „Użyj SSL 3.0”)



Widok ustawień w Windows 7



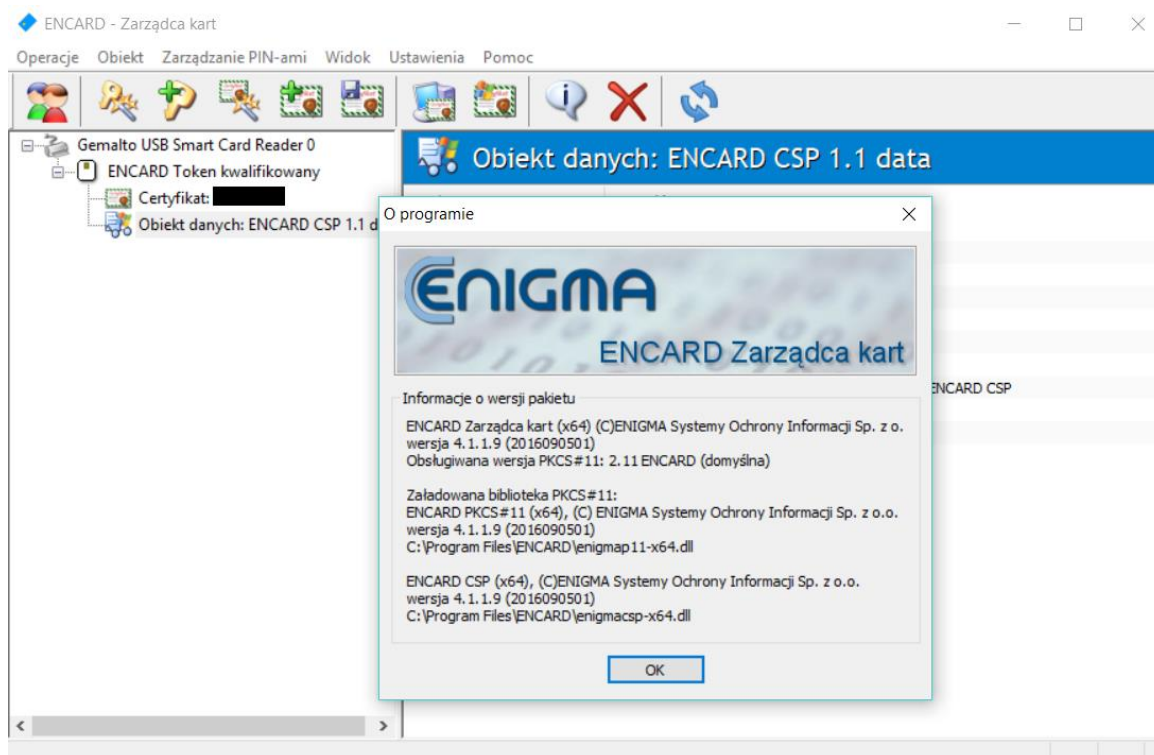
Widok ustawień w Windows 8.1



Widok ustawień w Windows 10

2. Karty ENCARD

a) Uruchamiamy program „ENCARD Zarządca kart” i sprawdzamy wersję



b) Jeśli wersja jest inna niż najnowsza **4.1.1.9** to odinstalowujemy starą wersję

Panel sterowania\Wszystkie elementy Panelu sterowania\Programy i funkcje

« Wszystkie elementy Panelu sterowania » Programy i funkcje

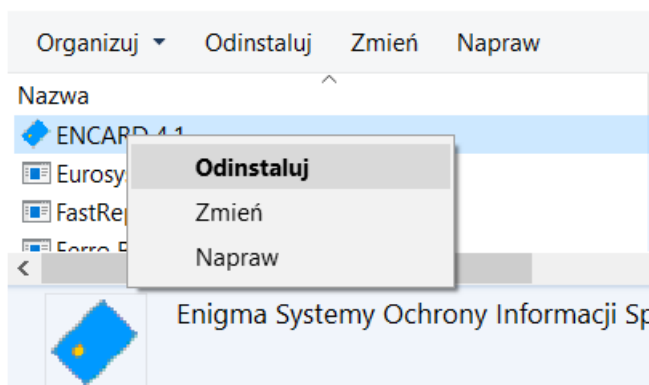
Strona główna Panelu sterowania

Wyświetl zainstalowane aktualizacje

Włącz lub wyłącz funkcje systemu Windows

Odinstaluj lub zmień program

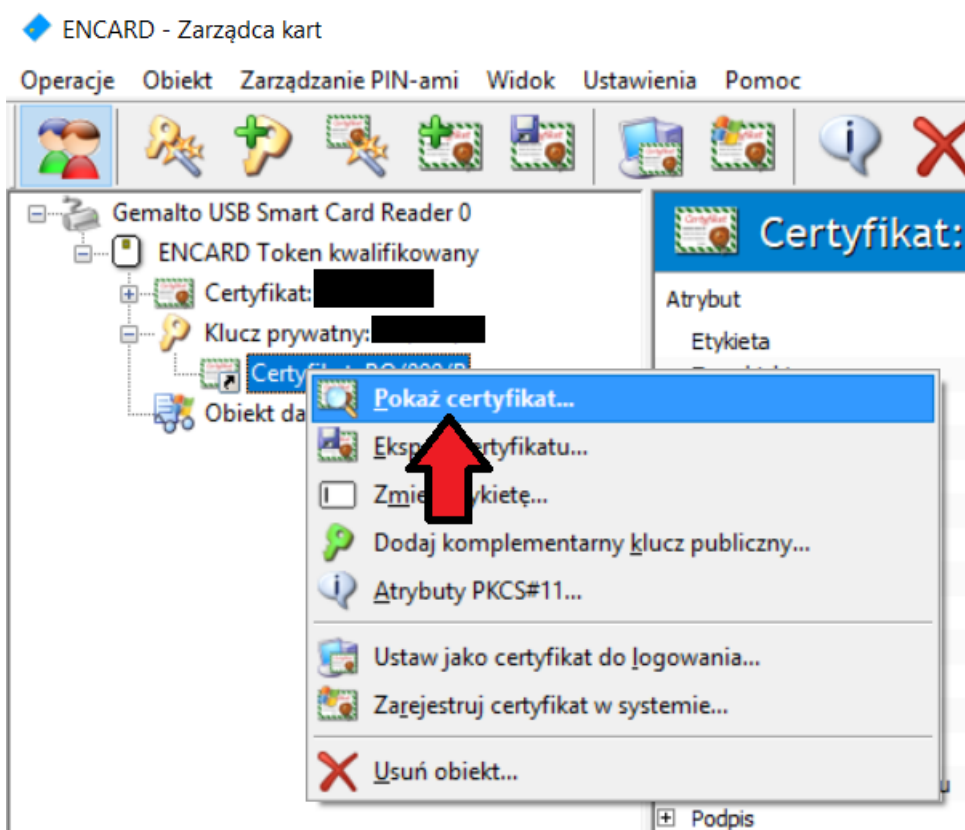
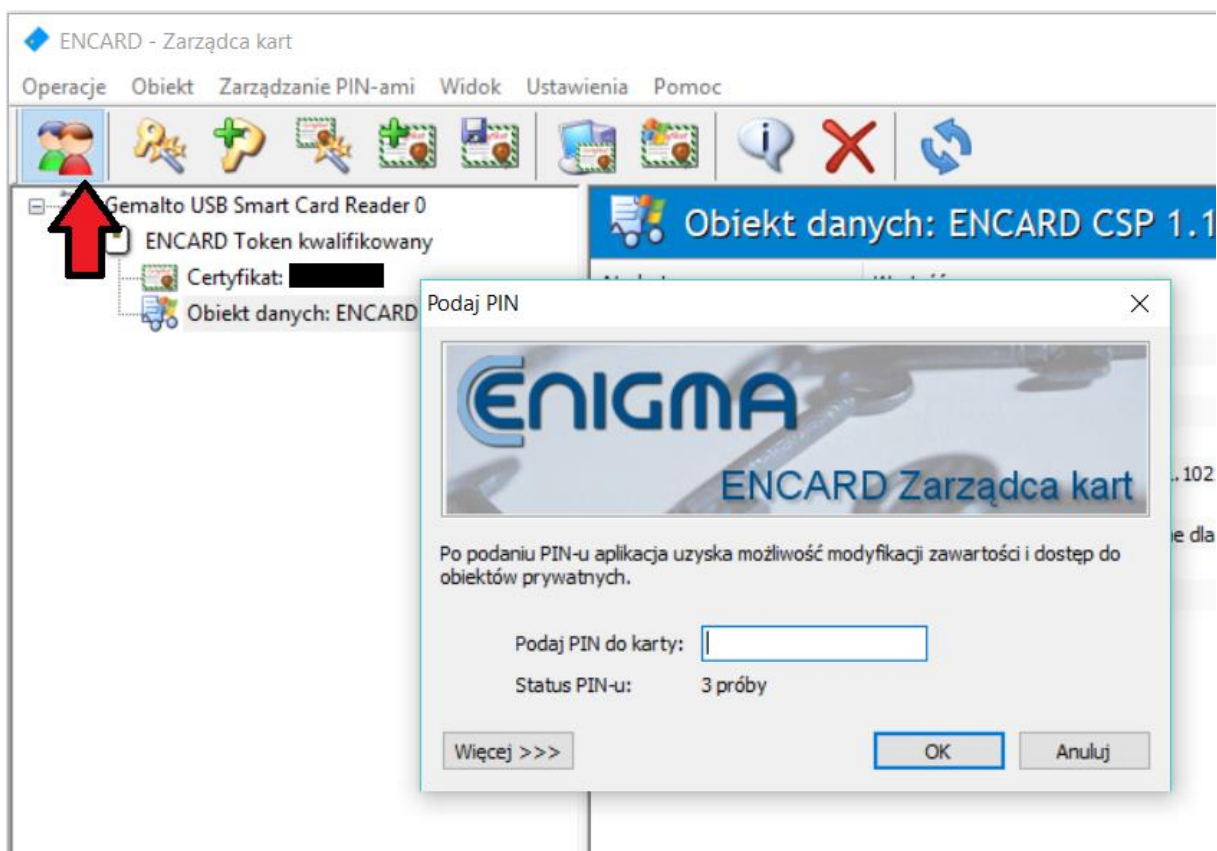
Aby odinstalować program, zaznacz go na liście, a nas Odinstaluj, Zmień lub Napraw.

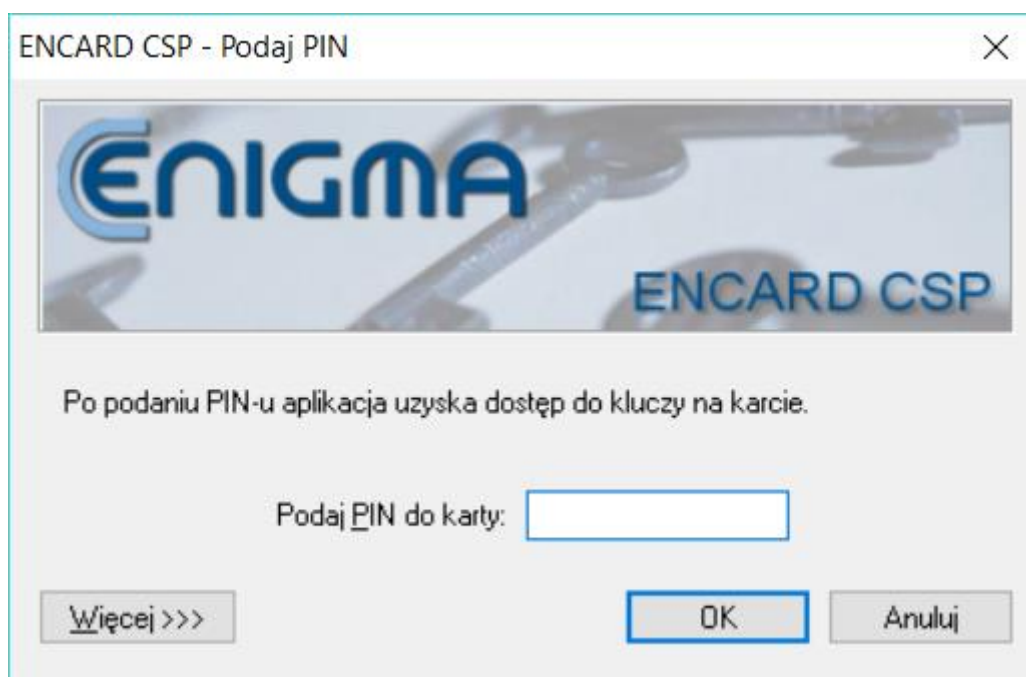
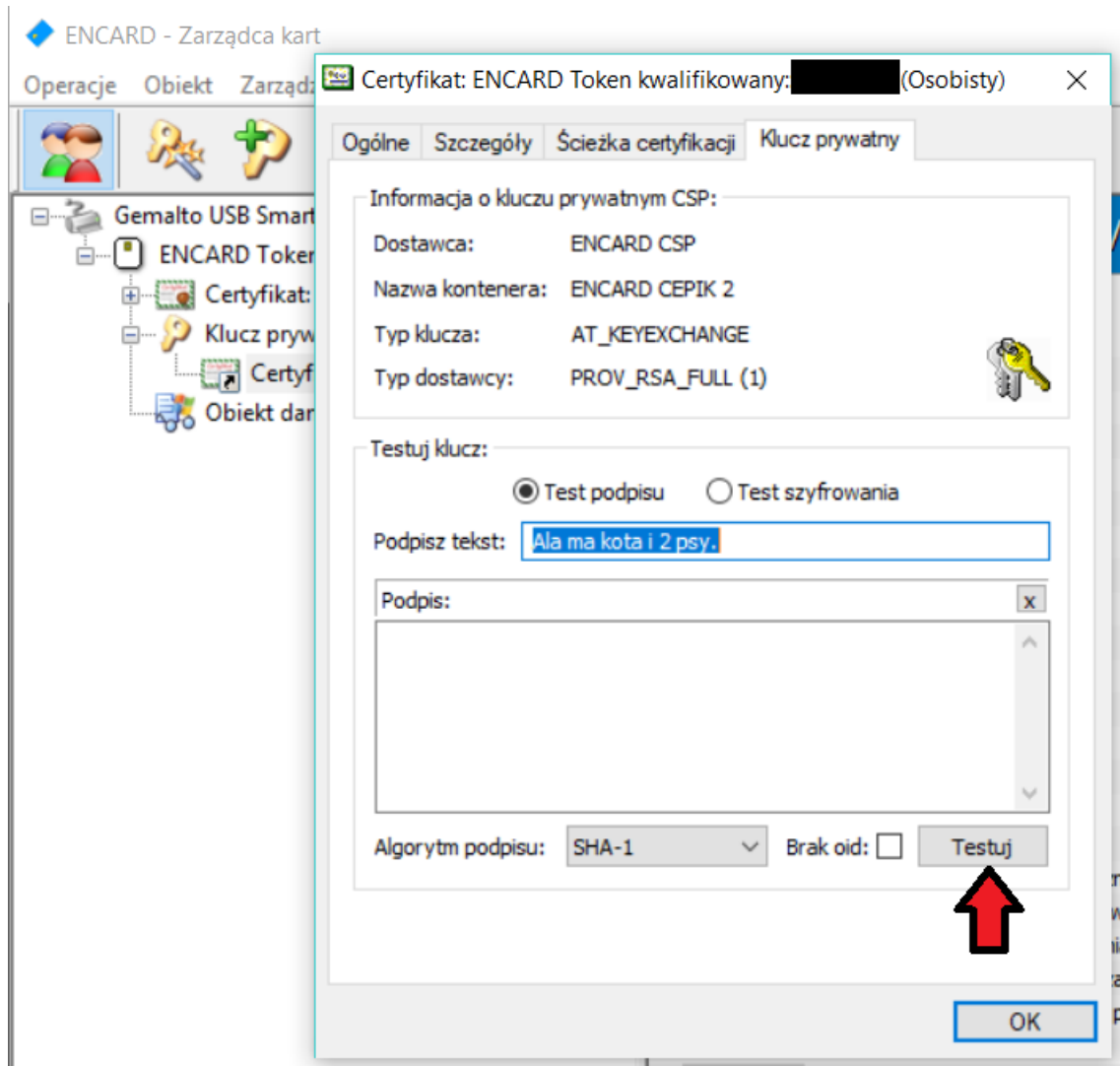


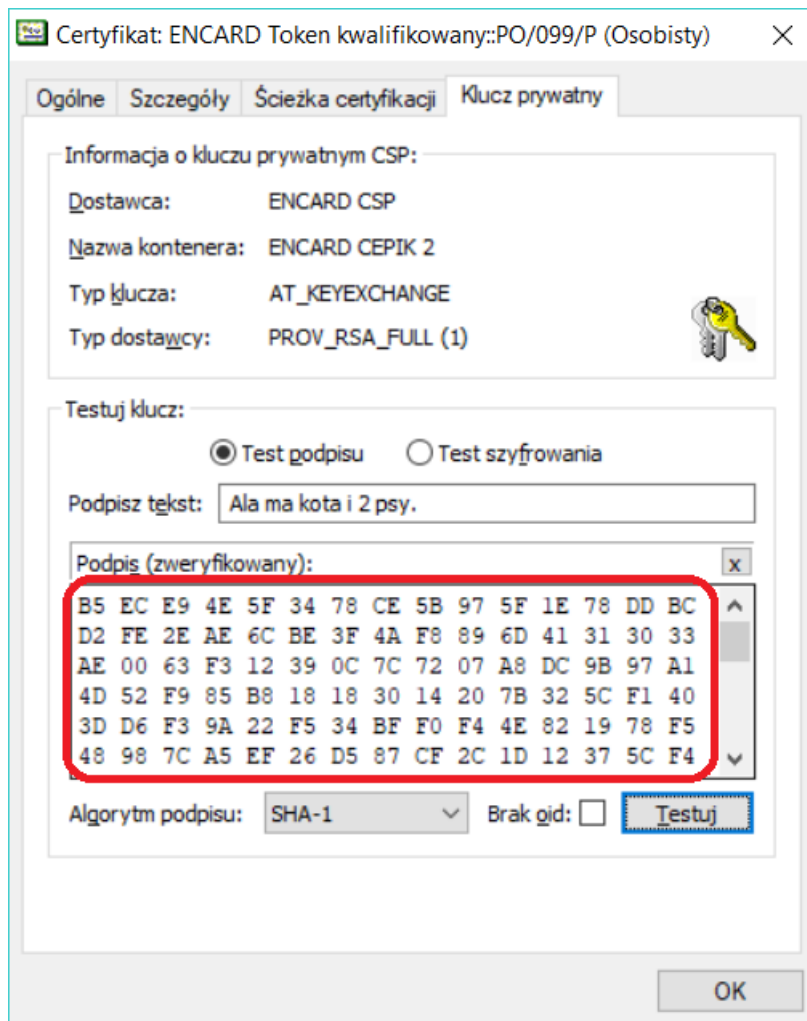
I instalujemy zalecaną wersję pobraną ze strony producenta

<https://www.cencert.pl/Oprogramowanie%20PEMHEART/> w wersji zgodnej z systemem operacyjnym (**32 bity dla 32 bitowego Windowsa a 64 bity dla 64 bitowego Windowsa**)

c) Sprawdzamy poprawność instalacji karty i jej działania w systemie operacyjnym

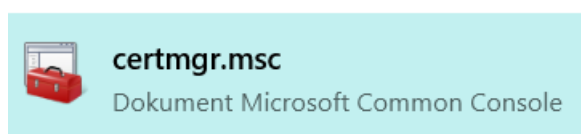






Powyżej poprawny wynik testu (**inny wynik to błąd**)

- d) Jeśli wynik z testu z poprzedniego podpunktu jest niepoprawny, należy wykonać poniższą procedurę



Uruchamiamy przystawkę do obsługi certyfikatów Windows i odszukujemy certyfikat SSL taki jak wyświetlany w oprogramowaniu karty ENCARD (**nazwa certyfikatu, wystawca jak i daty ważności muszą być takie same !**)

certmgr - [Certyfikaty - bieżący użytkownik\Osobisty\Certyfikaty]

Plik Akcja Widok Pomoc

Wystawiony dla	Wystawiony przez	Data wygaśnięcia	Zamierzone cele	Przyjazna nazwa
04016638-C86D-4C1A-AB9B-C5E...	Apple iPhone Device CA	2017-07-28	Uwierzytelnienie serwera, Uwierzytel...	APNS certificate
Infrastruktura	Infrastruktura	2021-05-12	<Wszyscy>	<brak>
	Certum Code Signing CA SHA2	2019-03-09	Podpisywanie kodu, Podpisywanie ...	
	Infrastruktura	2019-10-10	<Wszyscy>	<brak>
	Operatorzy	2019-09-12	Uwierzytelnienie klienta	

ENCARD - Zarządca kart

Operacje Obiekt Zarządzanie PIN-ami Widok Ustawienia Pomoc

Gemalto USB Smart Card Reader 0

ENCARD Token kwalifikowany

Certyfikat: [redacted]

Klucz prywatny: [redacted]

Certyfikat: [redacted]

Obiekt danych: ENCARD CSP 1.1 data

Certyfikat: [redacted]

Atrybut	Wartość
Etykieta	
Typ obiektu	Certyfikat X-509
Dostęp do obiektu	publiczny
Rozmiar obiektu na karcie	1192 bajty
Identyfikator klucza	[redacted]
Numer wersji certyfikatu	3
Numer seryjny	[redacted]
Klucz publiczny	RSA, 2048 bitów
Moduł	[redacted]
Wykładnik publiczny	[redacted]
Zastosowanie klucza do	podpisów, szyfrowania, uzgadniania kluczy
Wystawiony przez	Operatorzy, CEPIK2, CEPIK...
Wystawiony dla	[redacted]
Okres ważności certyfikatu	od 2018-09-12, 9:07 do 2019-09-12, 9:07

certmgr - [Certyfikaty - bieżący użytkownik\Osobisty\Certyfikaty]

Plik Akcja Widok Pomoc

Certyfikaty - bieżący użytkownik

- Osobisty
 - Certyfikaty
 - Zaufane główne urzędy certyfikacji
 - Zaufanie przedsiębiorstwa
 - Pośrednie urzędy certyfikacji
 - Obiekt użytkownika Active Directory
 - Zaufani wydawcy
 - Certyfikaty niezaufane
 - Główne urzędy certyfikacji innych
 - Zaufane osoby
 - Wystawcy uwierzytelniania klientów
 - Inne osoby
 - Local NonRemovable Certificate
 - OTHER
 - Żądanie rejestracji certyfikatu
 - Zaufane certyfikaty kart inteligentnych

Wystawiony dla	Wystawiony przez
04016638-C86D-4C1A-AB9B-C5E...	Apple iPhone Device CA
Infrastruktura	Infrastruktura
[redacted]	Certum Code Signing CA SHA2
[redacted]	Infrastruktura
[redacted]	Operatorzy

Otwórz

Wszystkie zadania

Wytnij

Kopiuj

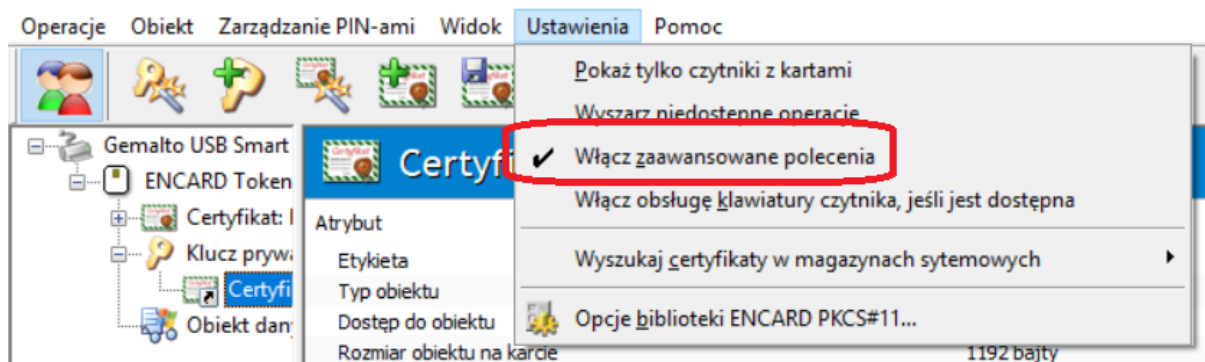
Usuń

Właściwości

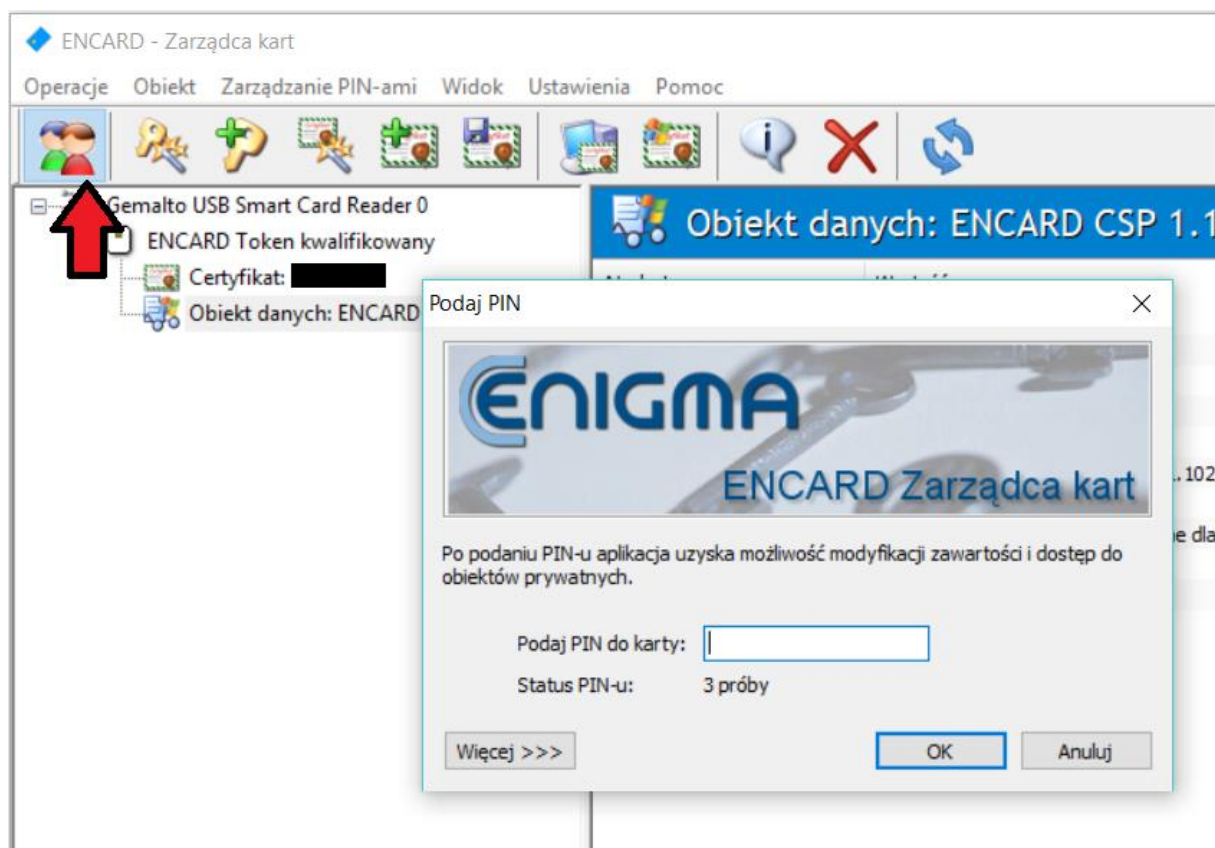
Pomoc

Usuujemy znaleziony certyfikat z przystawki certyfikatów Windows (**UWAGA! przed wykonaniem tego kroku, sprawdzamy 2-3 razy czy wskazujemy odpowiedni certyfikat, przez przypadek możemy usunąć inny bardzo ważny certyfikat np. ten od VPN**)

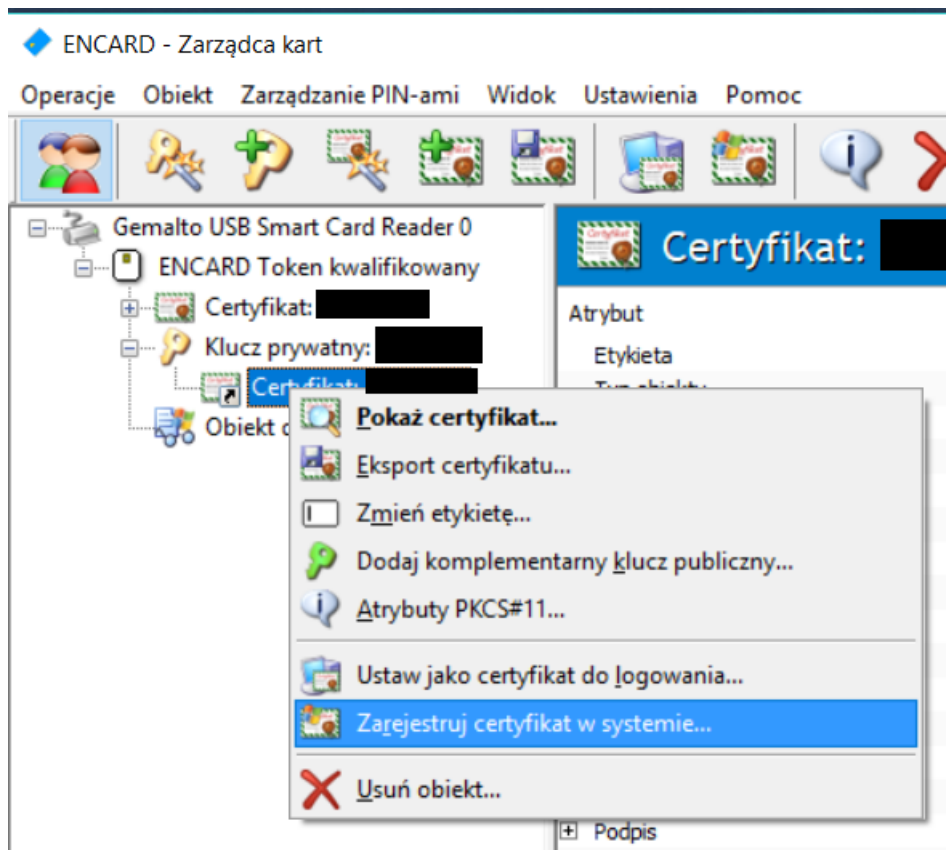
ENCARD - Zarządca kart



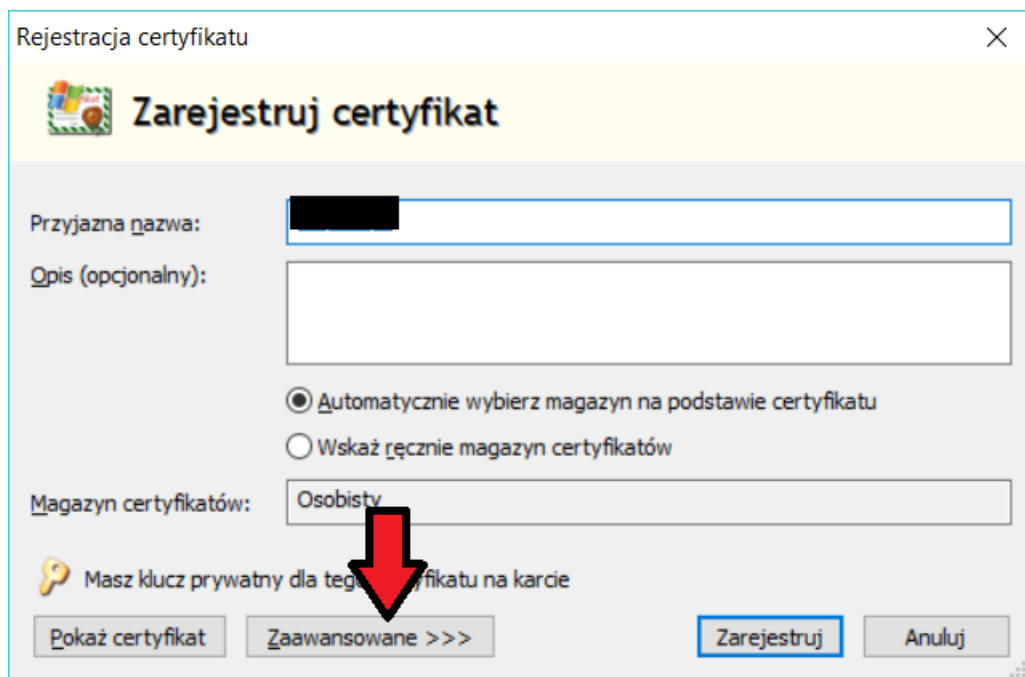
Włączamy zaawansowane polecenia w oprogramowaniu karty ENCARD



Logujemy się do profilu karty



Wybieramy certyfikat i rejestrujemy go w systemie (w trybie zaawansowanym)



Rejestracja certyfikatu


Zarejestruj certyfikat

Przyjazna nazwa:

Opis (opcjonalny):

☒ Automatycznie wybierz magazyn na podstawie certyfikatu
☐ Wskaż ręcznie magazyn certyfikatów

Magazyn certyfikatów:

 Masz klucz prywatny dla tego certyfikatu na karcie

Parametry CSP rejestrowanego klucza

☐ Nie rejestruj klucza prywatnego
☐ Automatyczna nazwa kontenera

Nazwa kontenera:

Typ klucza:

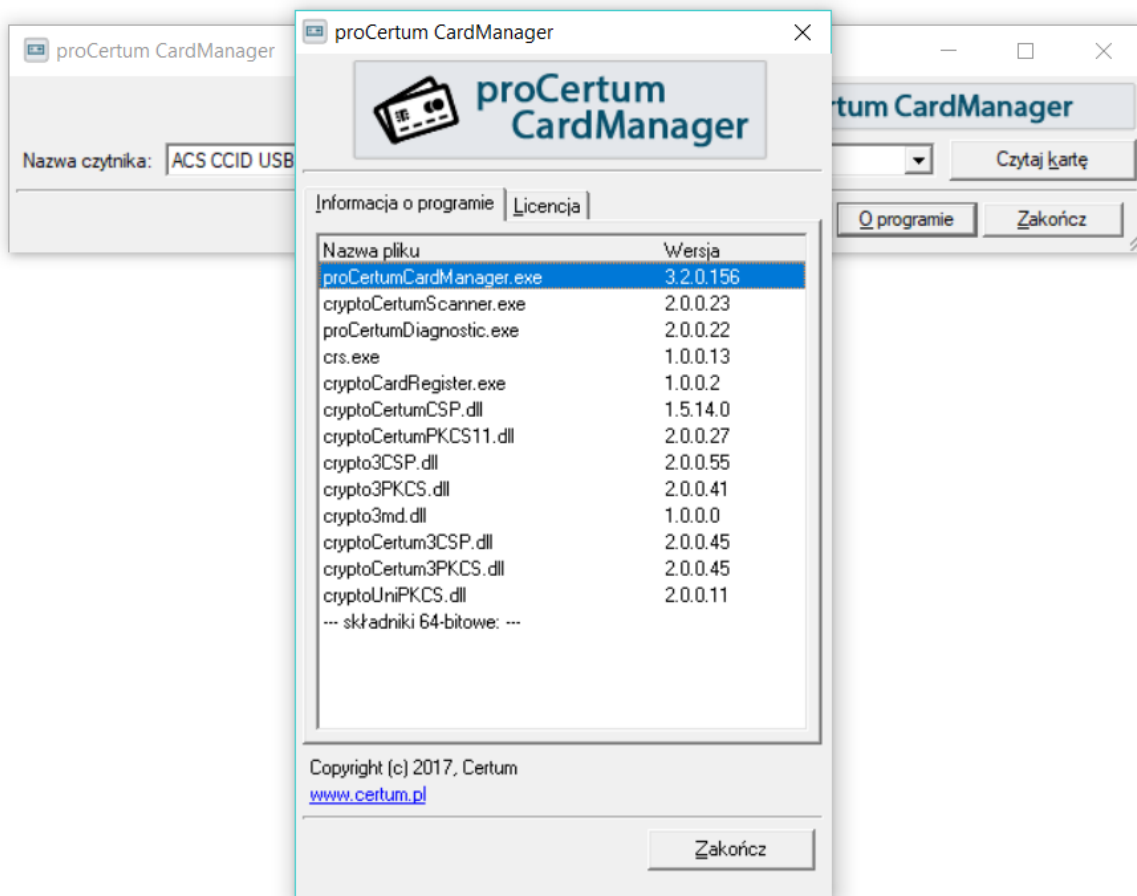
Zarejestruj dla CSP:

Usuujemy zaznaczenie z pola „Automatyczna nazwa kontenera” i zmieniamy nazwę kontenera (**UWAGA! musi być inna niż poprzednia**). Następnie naciskamy przycisk „Zarejestruj”

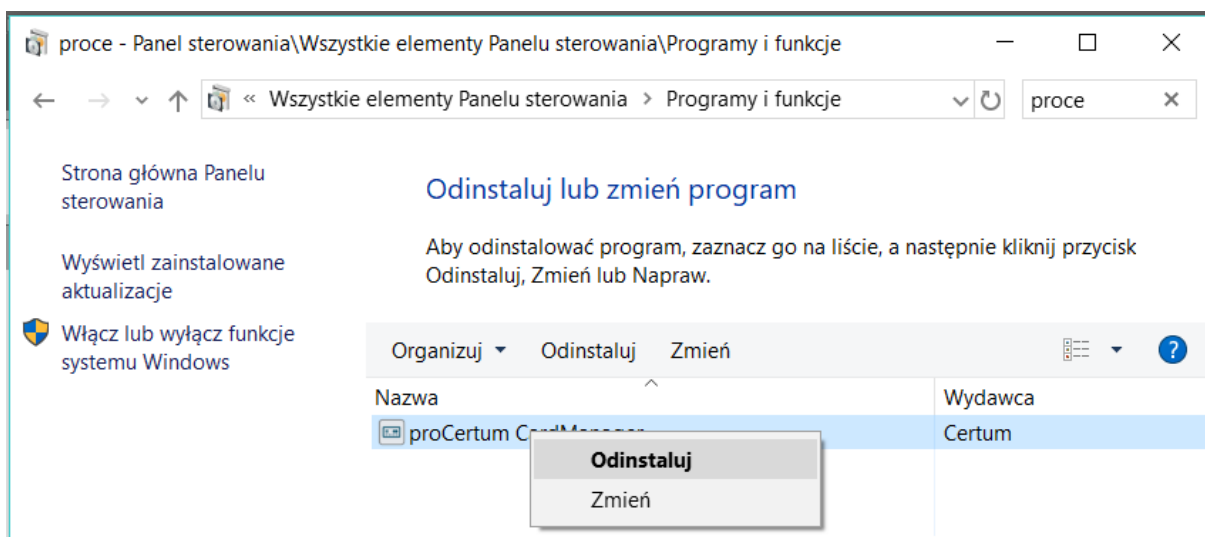
Na koniec wykonujemy sprawdzenie karty, przy pomocy procedury opisanej w punkcie – 1c (test podpisu „ala ma kota”)

3. Karty CERTUM

a) Uruchamiamy program ProCertum CardManager i sprawdzamy jego wersję

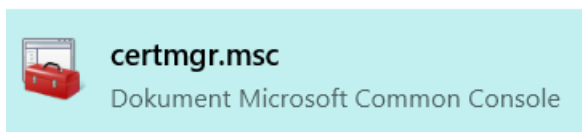


b) Jeśli wersja jest inna niż najnowsza 3.2.0.154 to odinstalowujemy starą wersję i zgodnie z zaleceniami producenta, restartujemy komputer

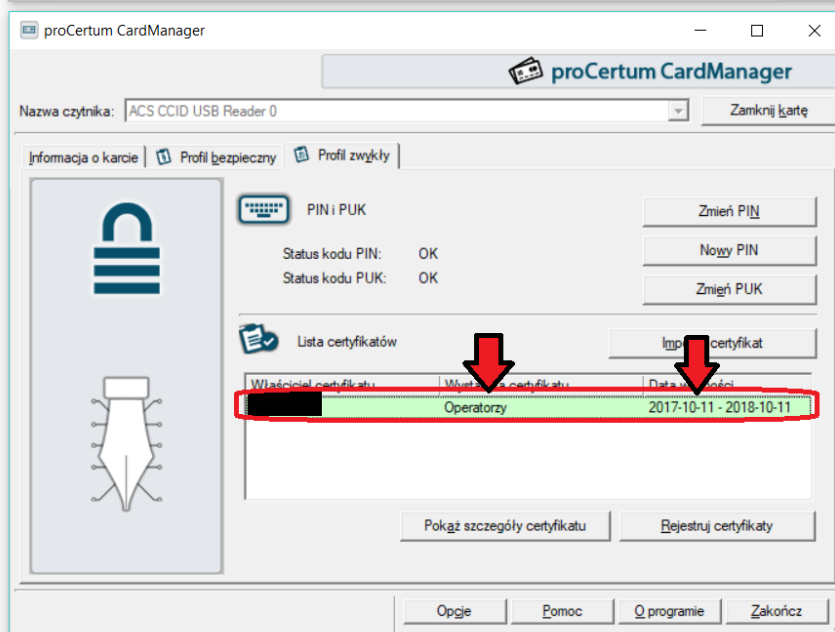
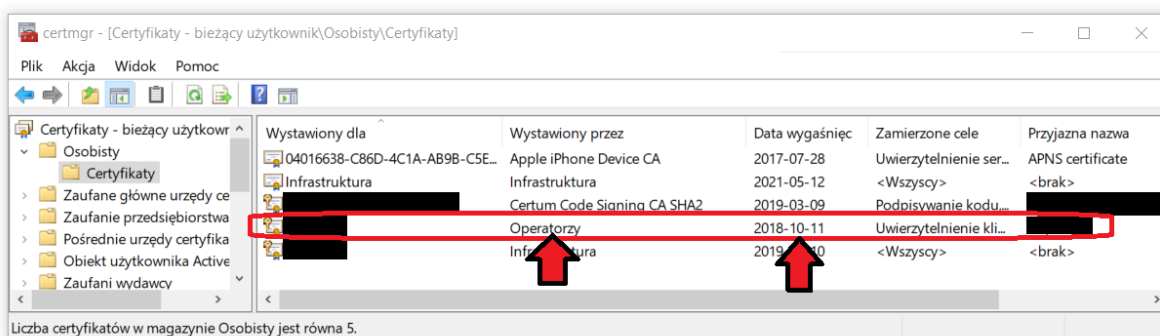


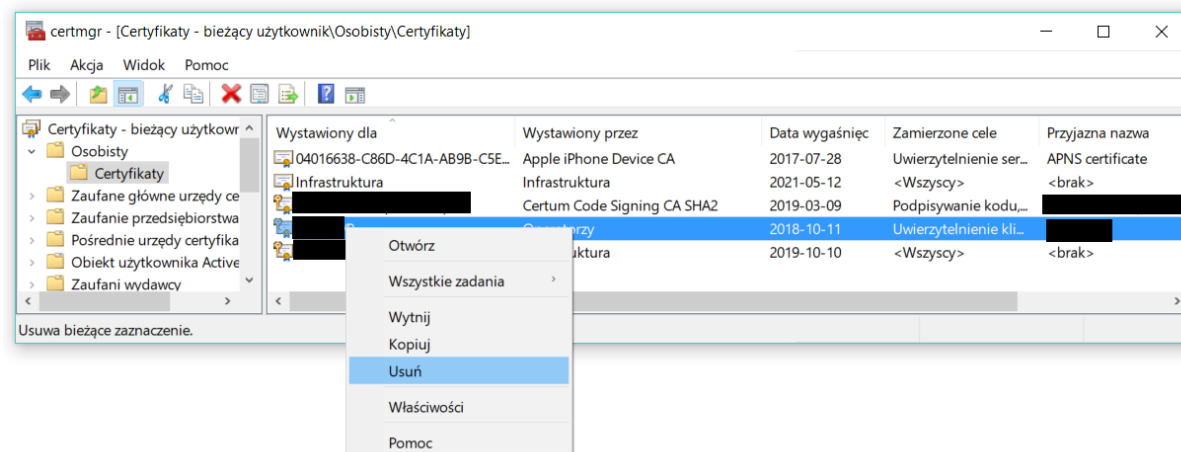
Po restarcie, instalujemy najnowszą wersję programu do obsługi karty, pobraną ze strony producenta https://www.certum.pl/pl/wsparcie/cert_oferta_procertum_cardmanager/ (**zalecana jest wersja 32 bitowa, niezależnie od wersji używanego systemu Windows**).

- c) W przypadku problemów z prawidłowym działaniem karty, wykonujemy ponowną rejestrację certyfikatu w systemie

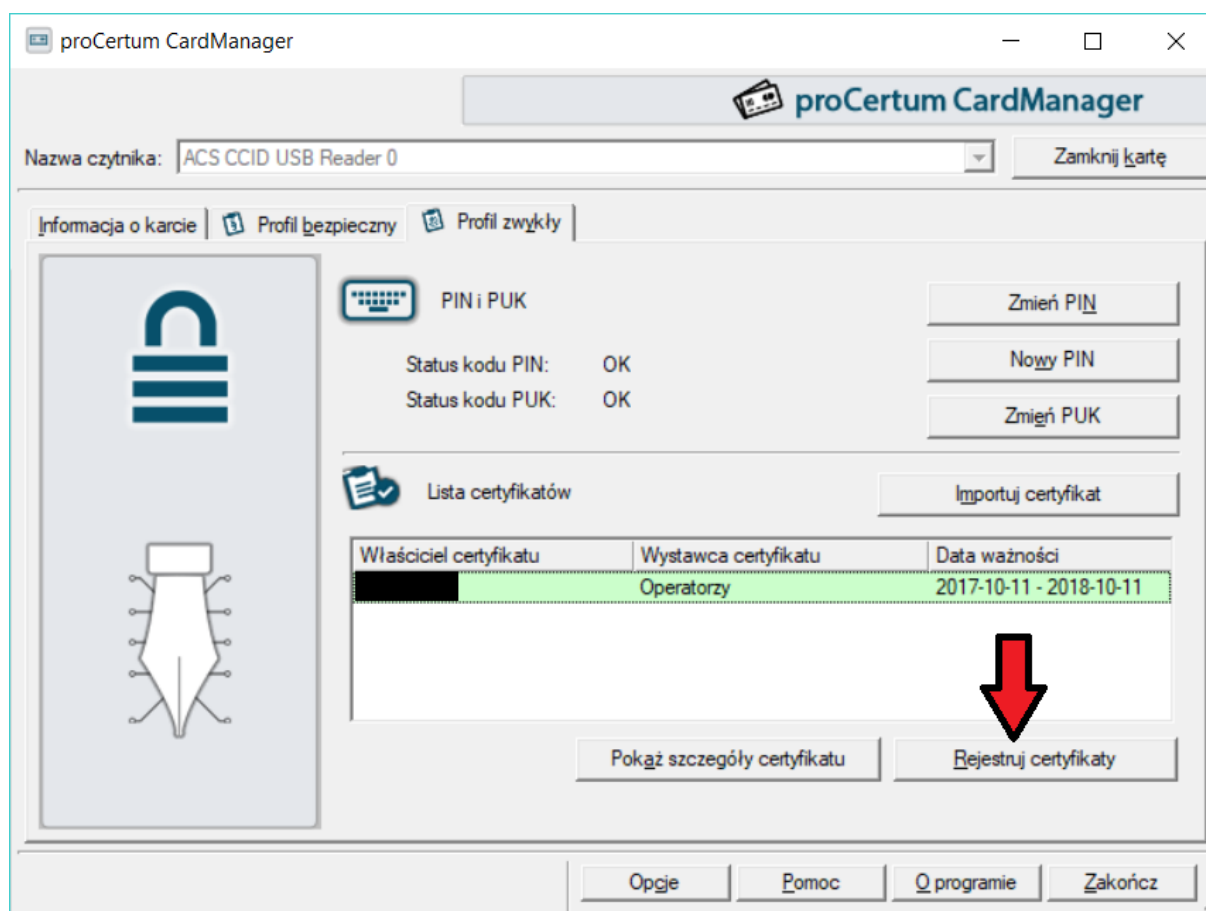


Uruchamiamy przystawkę do obsługi certyfikatów Windows i odszukujemy certyfikat SSL taki jak wyświetlany w oprogramowaniu karty ProCertum (**nazwa certyfikatu, wystawca jak i daty ważności muszą być takie same !**)





Usuujemy znaleziony certyfikat z przystawki certyfikatów Windows (**UWAGA! przed wykonaniem tego kroku, sprawdzamy 2-3 razy czy wskazujemy odpowiedni certyfikat. Przez przypadek możemy usunąć inny bardzo ważny certyfikat np. ten od VPN**)



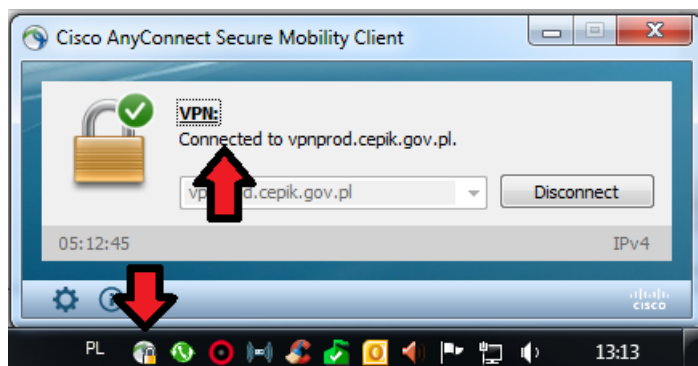
Ponownie rejestrujemy certyfikat w systemie Windows

4. Weryfikacja poprawności działania, poza Stacją.SQL

a) Wymagane jest aktywne połączenie VPN z serwerami CEPIK 2.0

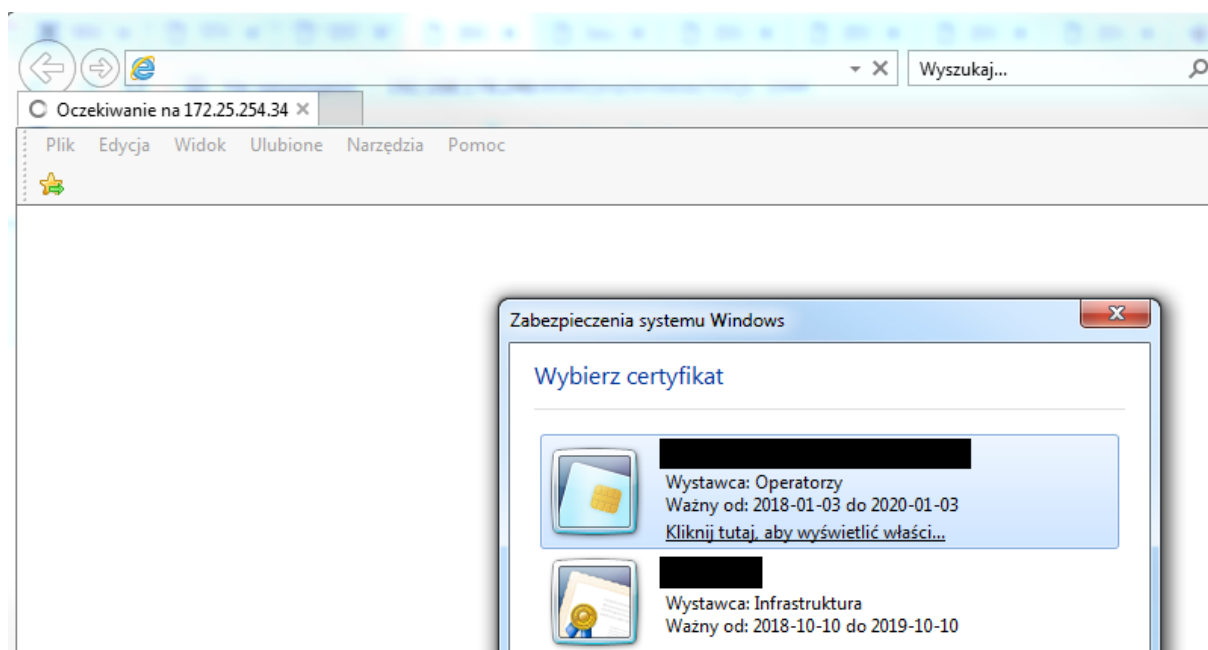
Stosowne oprogramowanie oraz instrukcja konfiguracji dostępne na stronie

<http://www.cepik.gov.pl/web/cepik2-portal/si-cepik-2.0>



b) Otwarcie przeglądarki Internet Explorer na stronie

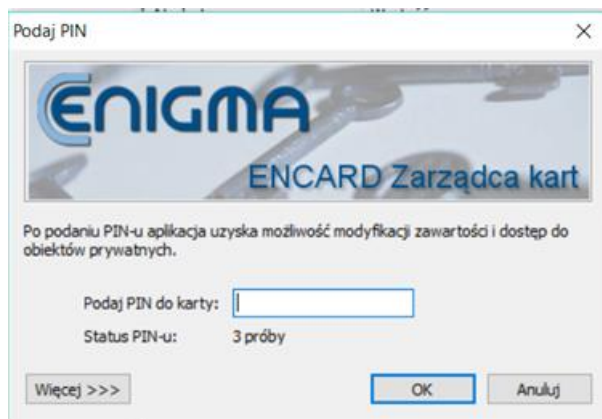
<https://172.25.254.34/cepik/api/skp?wsdl>



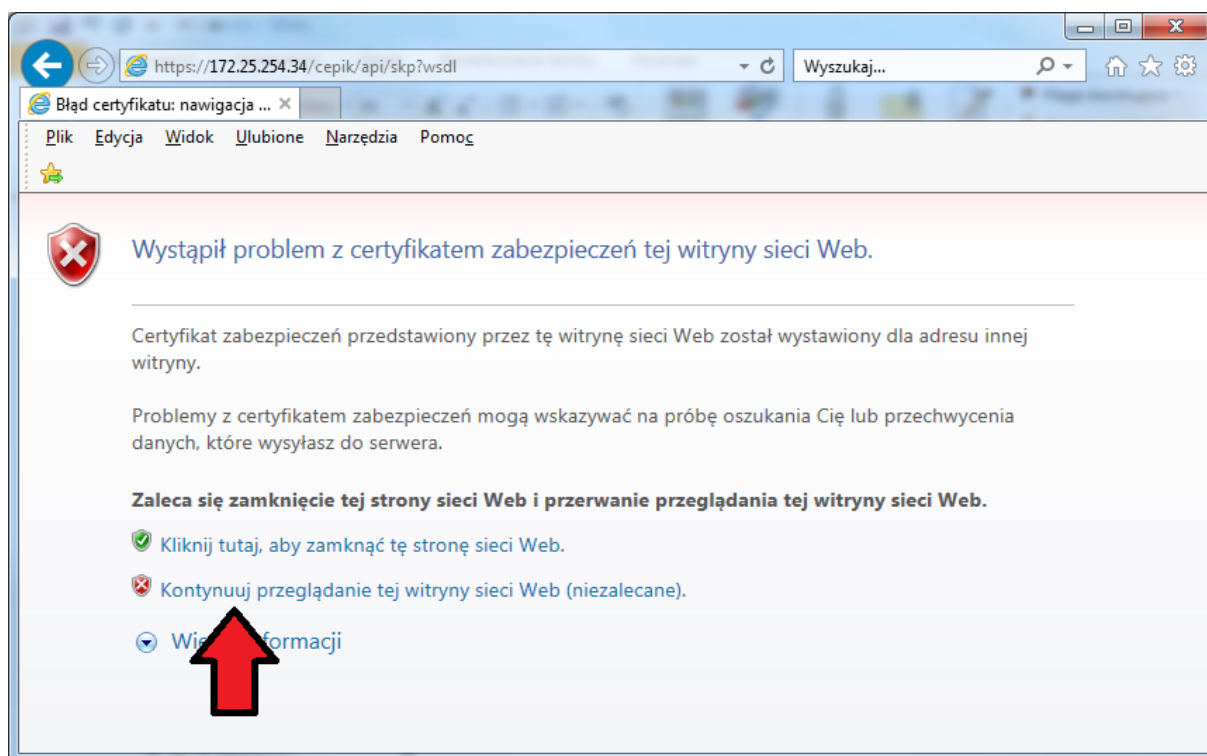
Wybieramy i zatwierdzamy certyfikat karty SSL (wystawca to Operatorzy poprzednio CCK Cepik... oraz data ważności certyfikatu zgodna z tą wyświetlaną w oprogramowaniu karty kryptograficznej

(UWAGA! monit o wybór certyfikatu może pojawić się

w tle któregoś z aktywnych okien-należy na to zwrócić uwagę)

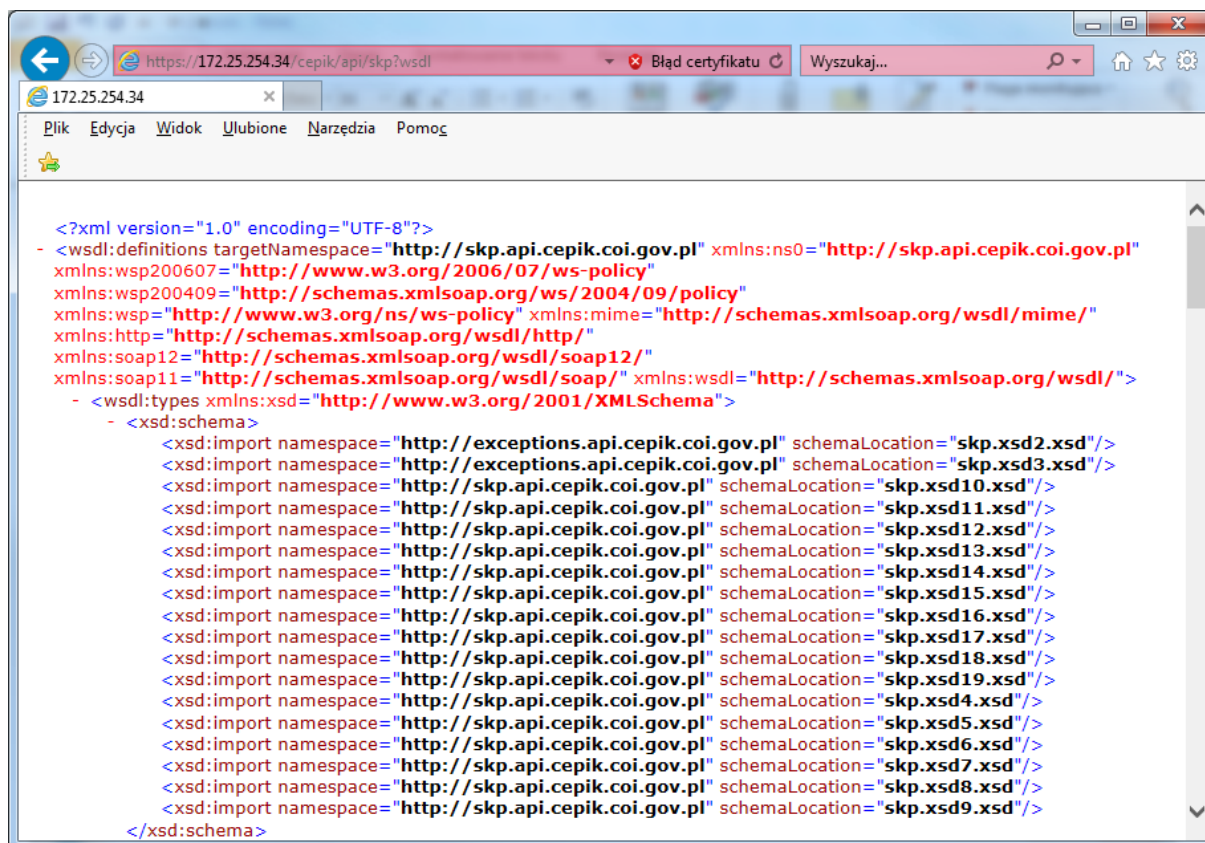


Wprowadzamy poprawny PIN do karty (**UWAGA! monit o wpisanie PIN do karty może pojawić się w tle któregoś z aktywnych okien-należy na to zwrócić uwagę**)



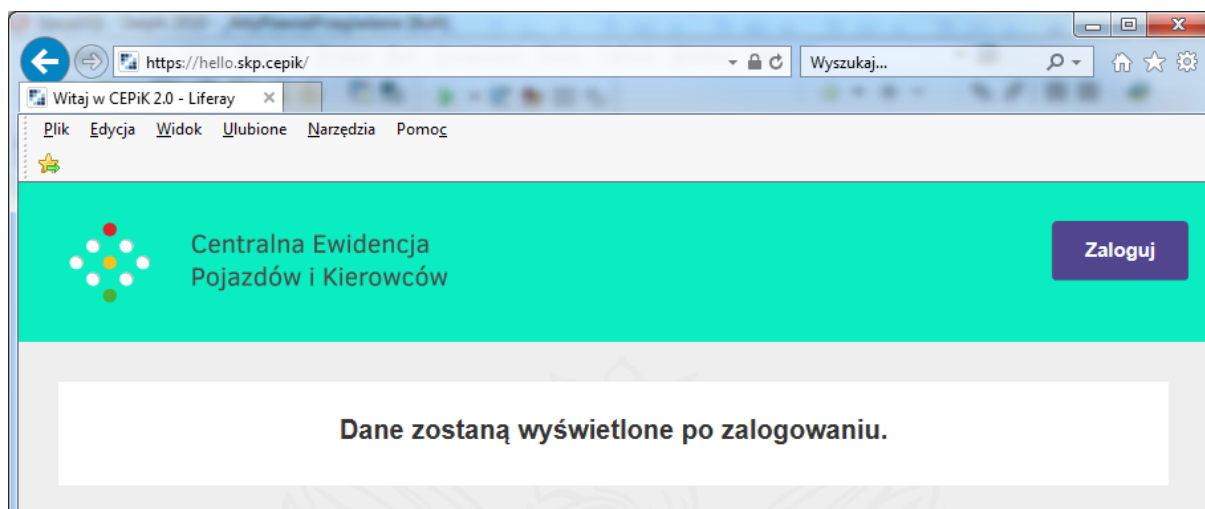
Potwierdzamy wejście na stronę

I ponownie wyświetli się nam wybór certyfikatu i monit o podanie PIN do karty



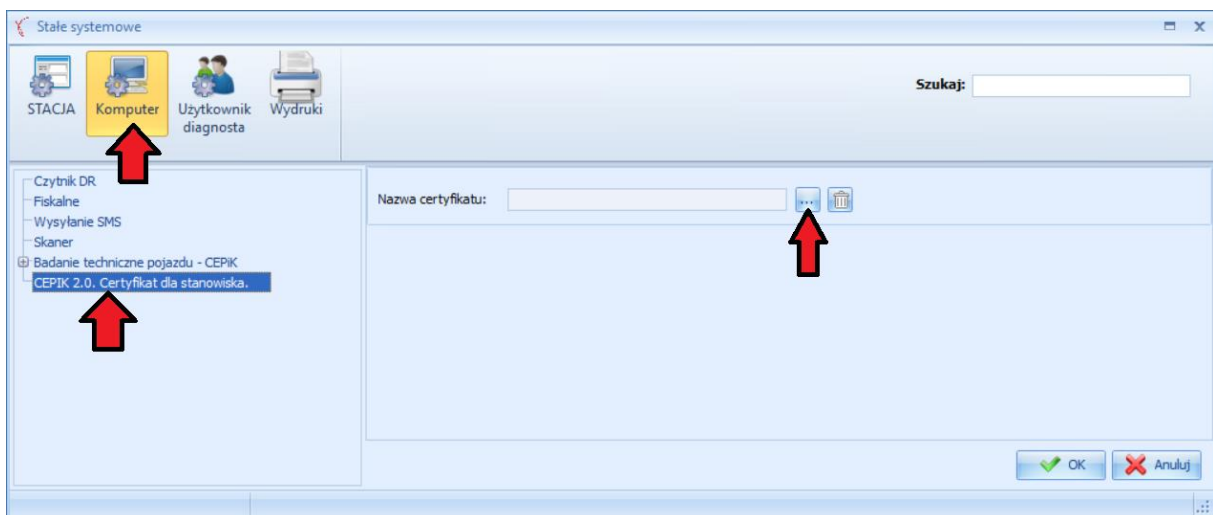
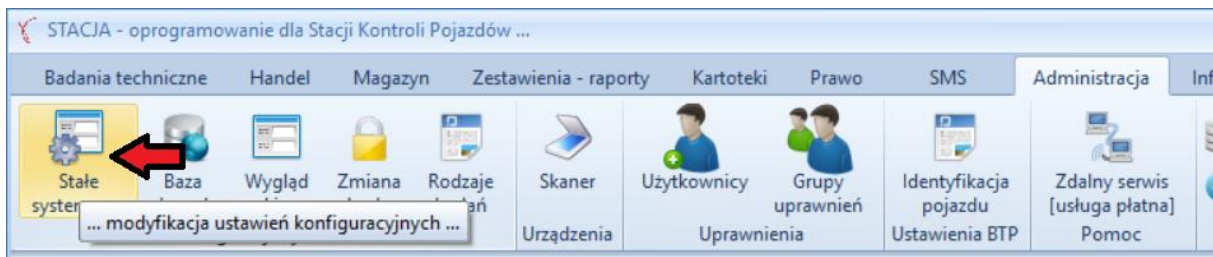
Na koniec tak powinna wyglądać, poprawnie wyświetlana strona (**UWAGA! jeśli wynik jest inny to konieczny może być restart komputera i/lub dodanie wyjątku w programie antywirusowym np. w ESET HIPS – tryb nauki**)

- c) Jako potwierdzenie poprawności działania, można otworzyć przeglądarkę Internet Explorer na stronie <https://hello.skp.cepik/> (tam podobnie jak w poprzednim podpunkcie, także będzie wymagane wskazanie certyfikatu SSL i podanie PIN do karty)

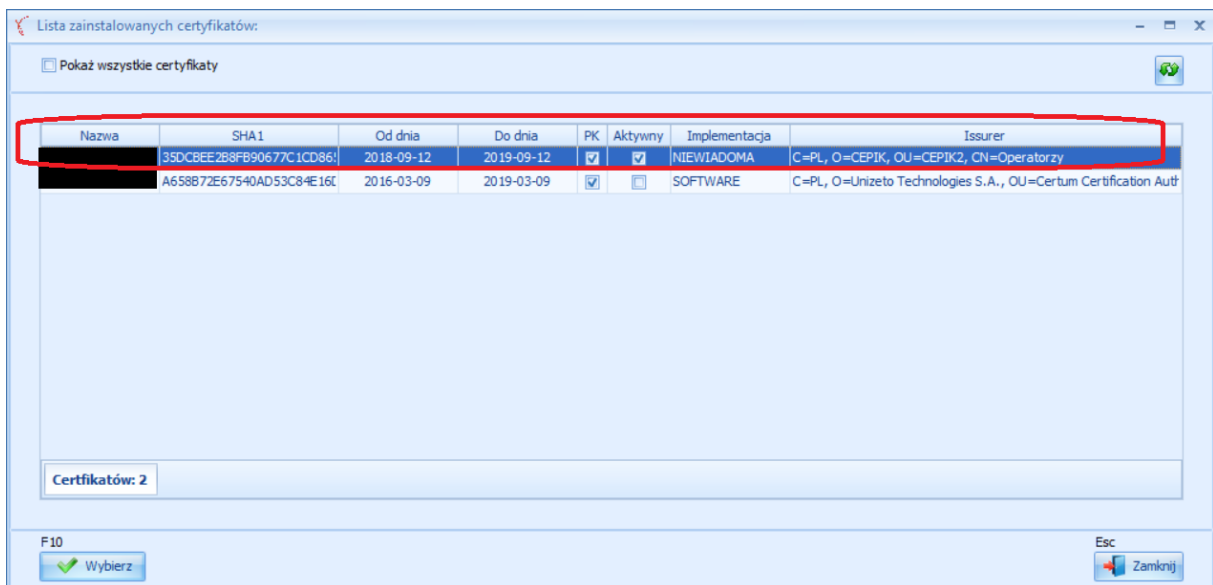


5. Wskazanie i test certyfikatu SSL po stronie Stacji.SQL

- Logujemy się na konta Administratora programu Stacja.SQL
- Ustawiamy ważny certyfikat w stałych systemowych

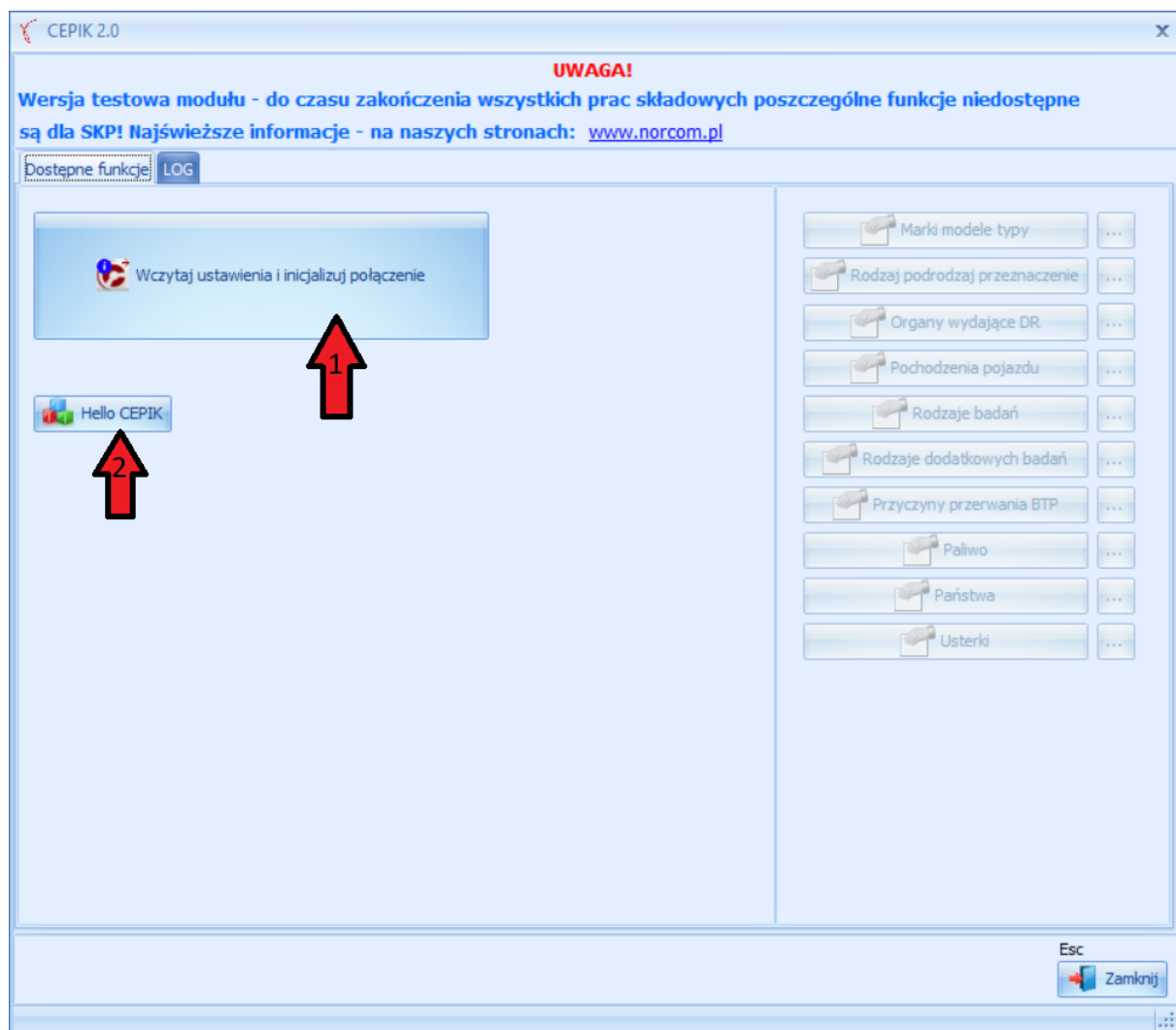
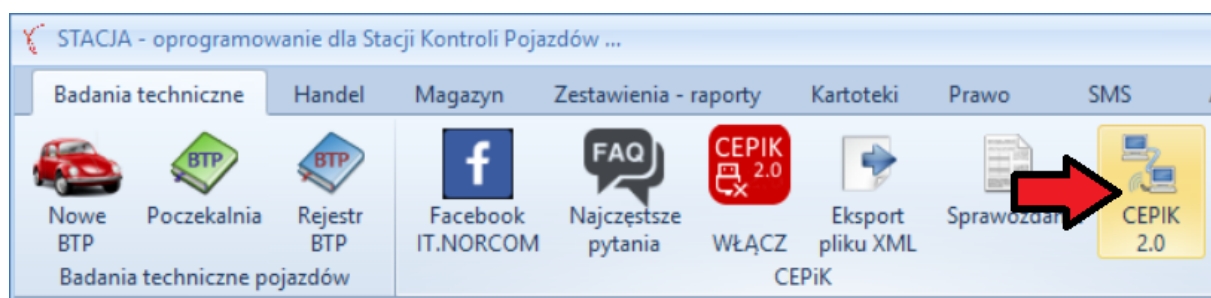


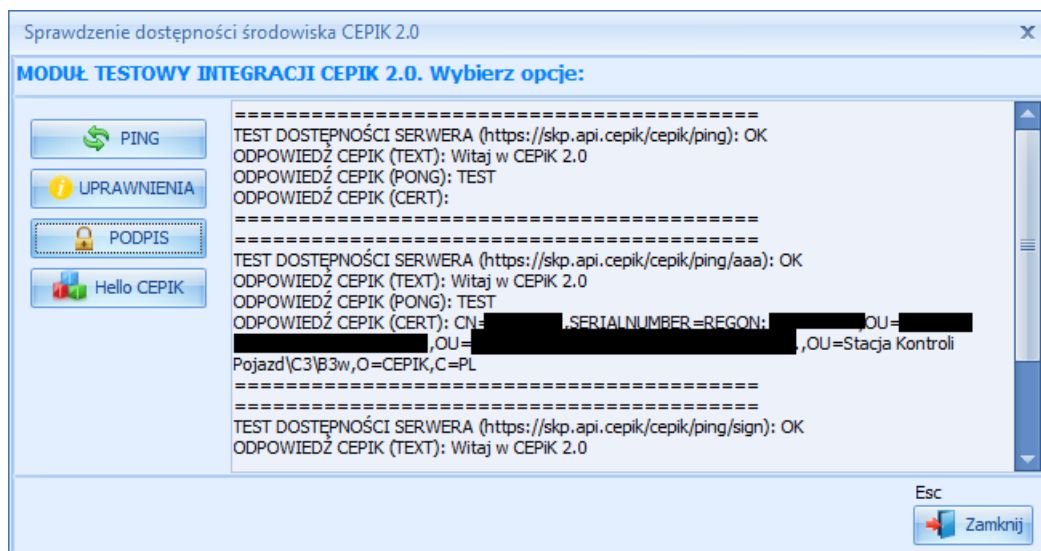
Na zakładce „Komputer” wskazujemy certyfikat SSL, który będzie używany na komputerze na którym aktualnie pracujemy



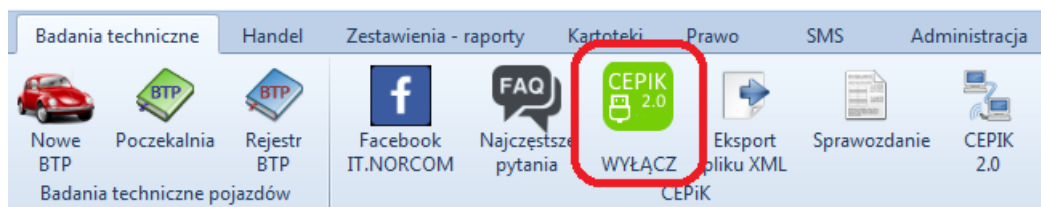
Wskazujemy certyfikat SSL (pola PK i Aktywny powinny być znaczone)

- Wykonujemy testy HelloCepik





Przykłady poprawnych odpowiedzi z testowych modułów



Warto zwrócić też uwagę na to, że ikonka „Cepik 2.0” zmienia kolor na zielony, jeżeli dostępne jest połączenie VPN z CEPIK 2.0