

# Konfiguracja sieci „eduroam” pod systemem Win 10 (22H2) i system Win 11.

Należy upewnić się, że w systemie nie ma utworzonego profilu sieci o nazwie "eduroam", otwieramy wiersza poleceń i wpisujemy komendę „cmd” i wciskamy „Enter”. Sprawdzić listę dostępnych profili sieciowych należy wpisać polecenie:

`netsh wlan show profiles`

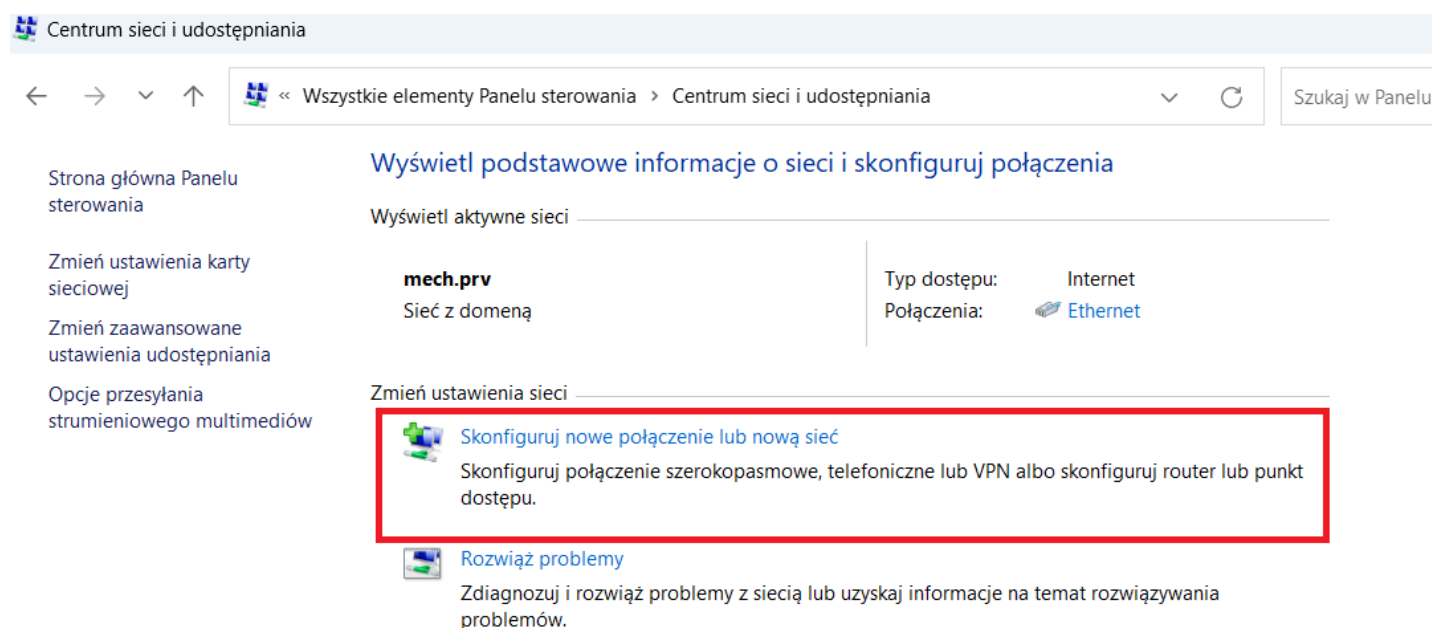
```
User profiles
-----
All User Profile      : eduroam
All User Profile      : PL-28A
```

Jeżeli na liście profili znajduje się „eduroam”, to należy go usunąć komendą:

`netsh wlan delete profile name="eduroam"`

```
C:\Users\piotr>netsh wlan delete profile name="eduroam"
Profile "eduroam" is deleted from interface "Wi-Fi".
```

Następnym krokiem jest przejście do Centrum sieci i udostępniania. W tym celu należy w opcji „Wyszukaj” otworzyć „Panel sterowania” następnie wybrać otworzyć „Centrum sieci i udostępniania” i przejść do „Skonfiguruj nowe połączenie lub nową sieć” oraz „Ręczne nawiązanie połączenia z siecią bezprzewodową”.



Okno Centrum sieci i udostępniania.

Wybierz opcję połączenia.

Połącz z Internetem  
Skonfiguruj połączenie szerokopasmowe lub telefoniczne z Internetem.

Skonfiguruj nową sieć  
Skonfiguruj nowy router lub punkt dostępu.

**Ręczne nawiązywanie połączenia z siecią bezprzewodową**  
Połącz się z siecią ukrytą lub utwórz nowy profil sieci bezprzewodowej.

Połącz z miejscem pracy  
Skonfiguruj połączenie telefoniczne lub połączenie VPN z miejscem pracy.

Dalej

Anuluj

Okno konfiguracji nowego połączenia lub sieci.

Wypełniamy nazwy sieci – „**eduroam**” oraz typ zabezpieczeń – „**WPA2-Enterprise**” i klikamy „**Dalej**”.

Wprowadź informacje o sieci bezprzewodowej, którą chcesz dodać.

Nazwa sieci:

eduroam

Typ zabezpieczeń:

WPA2-Enterprise

Typ szyfrowania:

AES

Klucz zabezpieczeń:

Ukryj znaki

Uruchom to połączenie automatycznie

Połącz, nawet jeśli sieć nie wykonuje emisji

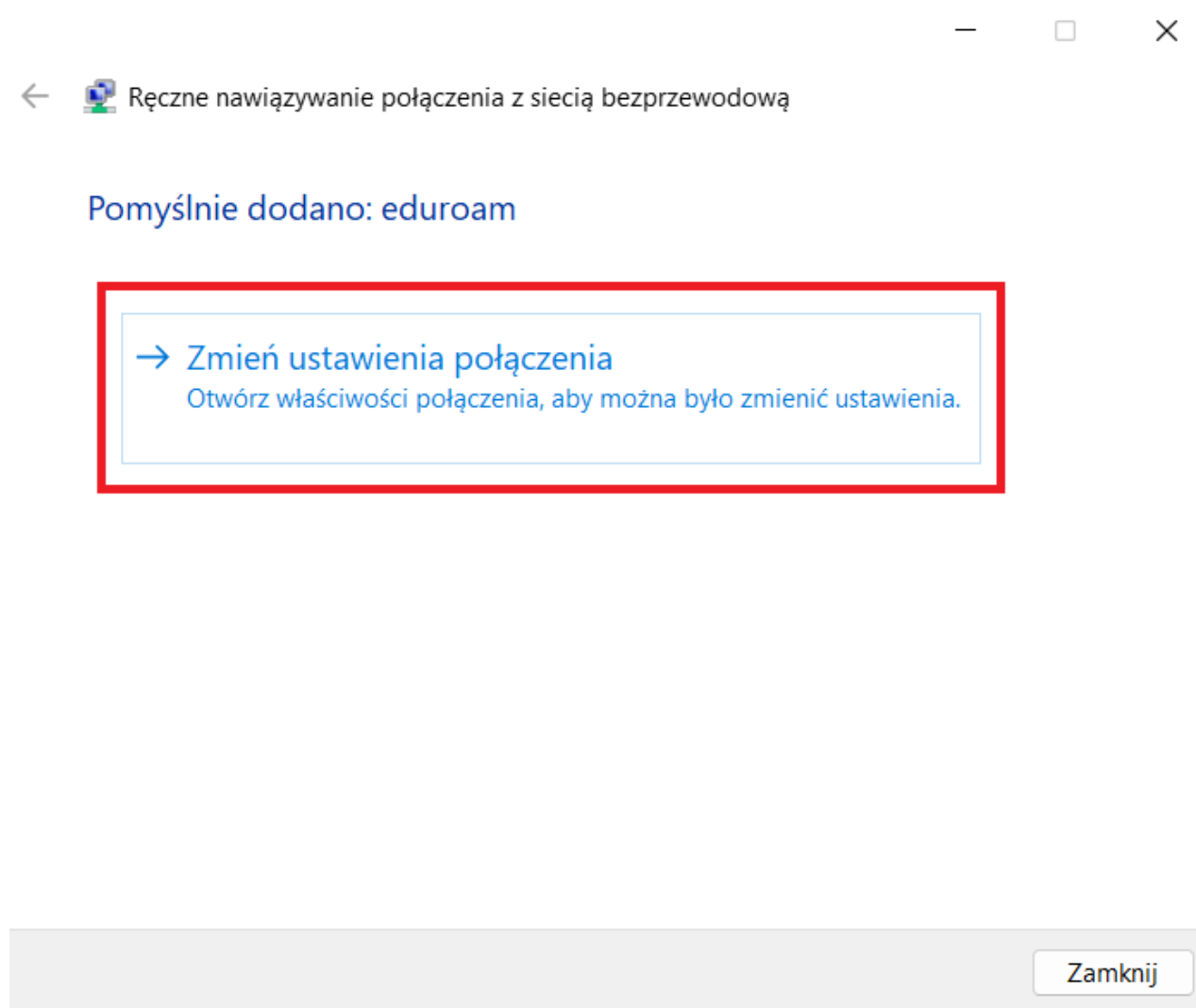
Ostrzeżenie: jeśli wybierzesz tę opcję, może to zagrozić prywatności komputera.

Dalej

Anuluj

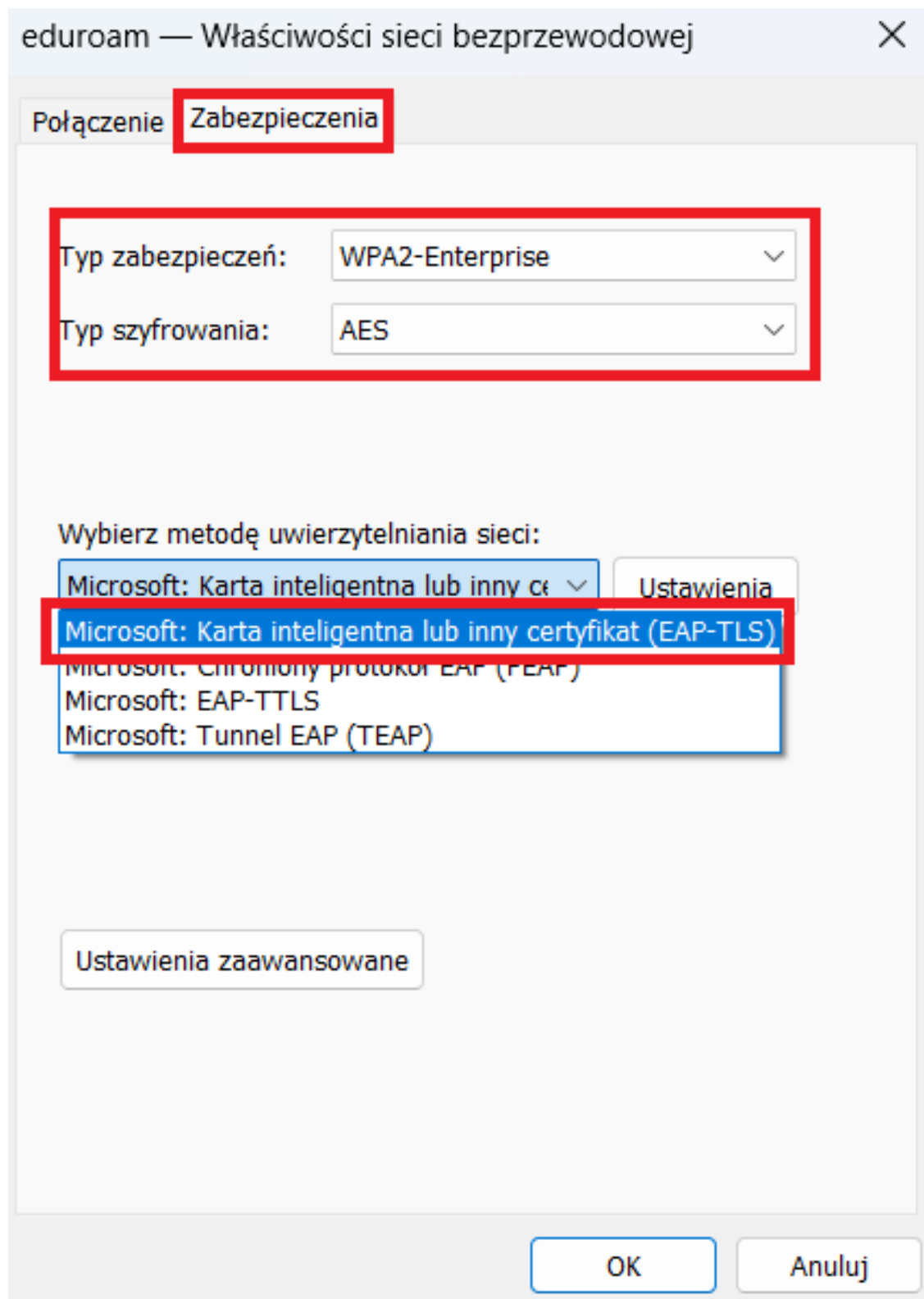
Okno ręcznego nawiązywania połączenia z wypełnionymi danymi.

Przechodzimy do „Zmień ustawienia połączenia”



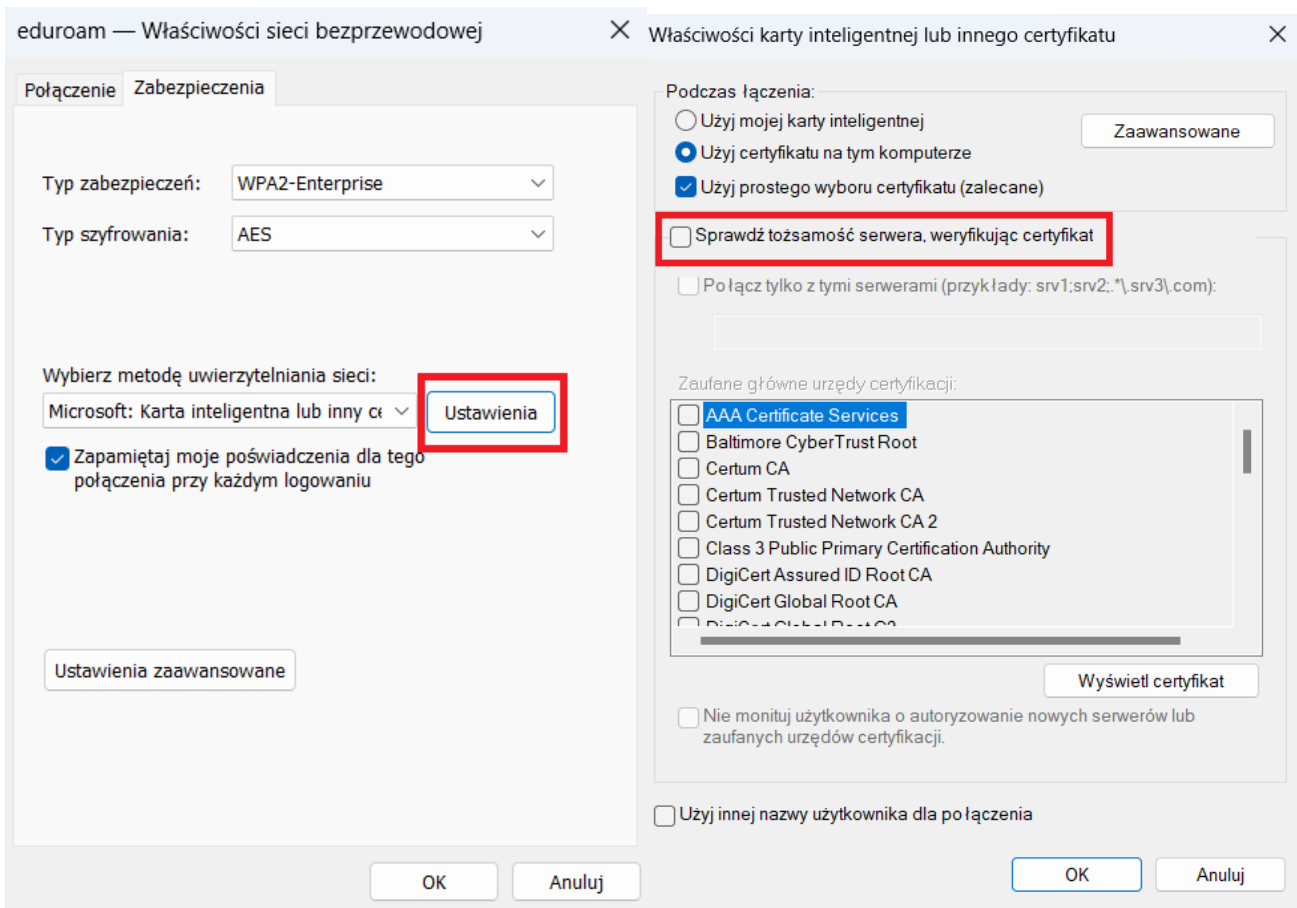
Okno umożliwiające przejście do zaawansowanych ustawień sieci po dodaniu profilu.

W zakładce „**Zabezpieczenia**”, należy wybrać z rozwijalnej listy wyboru uwierzytelniania sieci opcję: **Microsoft: Karta inteligentna lub inny certyfikat**.



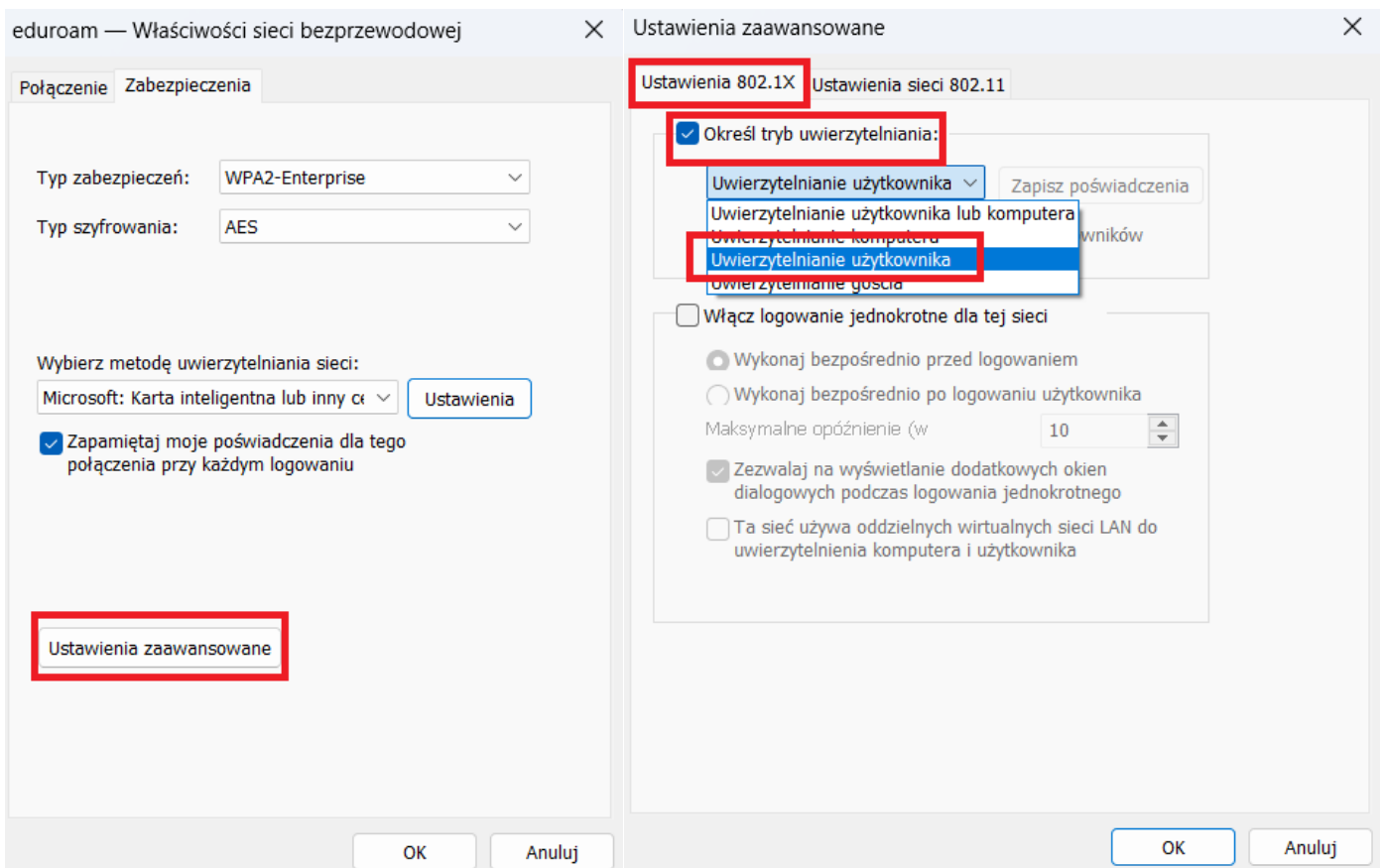
Okno Właściwości sieci bezprzewodowej.

Z poziomu okna dialogowego *Właściwości sieci bezprzewodowej*, należy teraz wykonać dwie równie ważne operacje. Pierwszą z nich jest kliknięcie przycisku **Ustawienia** i **odznaczenie** w nowym oknie pola wyboru: **Sprawdź tożsamość serwera, weryfikując certyfikat**



Przejdźcie do **ustawień** certyfikatu.

**Wyłączenie sprawdzenia tożsamości serwera.**



Przejdźcie do **ustawień zaawansowanych** sieci. Określenie trybu **uwierzytelniania użytkownika**.

Konfiguracja profilu sieci dla typu zabezpieczenia **WPA2-Enterprise** jest zakończona. W tym celu należy ponownie przejść do **wiersza poleceń**, wpisać "cmd", potwierdzić „Enter” i wprowadzić następującą komendę:

`netsh wlan set profileparameter name="eduroam" authentication=wpa2 encryption=tkip`

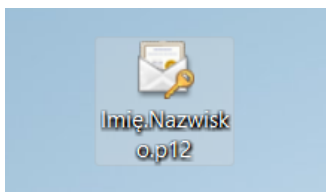
```
Wiersz polecenia
Microsoft Windows [Version 10.0.22621.1344]
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.
C:\Users\piotr>netsh wlan set profileparameter name="eduroam" authentication=wpa2 encryption=tkip
```

połączenie do modyfikacji typu szyfrowania.

```
Wiersz polecenia
Microsoft Windows [Version 10.0.22621.1344]
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.
C:\Users\piotr>netsh wlan set profileparameter name="eduroam" authentication=wpa2 encryption=tkip
Profile "eduroam" on interface "Wi-Fi" updated successfully.
```

Potwierdzenie pomyślnego wprowadzenia zmian w typie szyfrowania sieci na **WPA2**.

Wgrujemy certyfikat osobisty i postępujemy według opisu na zdjęciach j/n.



← Kreator importu certyfikatów

### Kreator importu certyfikatów — Zapraszamy!

Ten kreator pozwala kopiować certyfikaty, listy zaufania certyfikatów oraz listy odwołania certyfikatów z dysku twardego do magazynu certyfikatów.

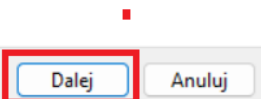
Certyfikat, wystawiany przez urząd certyfikacji, stanowi potwierdzenie tożsamości użytkownika i zawiera informacje używane do ochrony danych lub do ustanawiania bezpiecznych połączeń sieciowych. Magazyn certyfikatów jest obszarem systemowym, w którym przechowywane są certyfikaty.

Lokalizacja przechowywania

Bieżący użytkownik

Komputer lokalny

Aby kontynuować, kliknij przycisk Dalej.





### Ochrona klucza prywatnego

W celu zapewnienia bezpieczeństwa klucz prywatny jest chroniony hasłem.

Wpisz hasło dla klucza prywatnego.

Hasło:

  
 Wyświetl hasło

#### Opcje importu:

- Włącz silną ochronę klucza prywatnego. W przypadku wybrania tej opcji użytkownik będzie informowany o każdym użyciu klucza prywatnego przez aplikację.
- Oznacz ten klucz jako eksportowalny. Pozwoli to na późniejsze wykonanie kopii zapasowej lub transport kluczy.
- Chroń klucz prywatny, używając zabezpieczeń opartych na wirtualizacji (nieeksportowalne)
- Dołącz wszystkie właściwości rozszerzone.

Dalej

Anuluj



### Import pliku

Wybierz plik, który chcesz zaimportować.

Nazwa pliku:

C:\Users\piotr\Desktop\imię.nazwisko.p12

Przełóżaj...

Uwaga: używając następujących formatów, można przechować więcej niż jeden certyfikat w pojedynczym pliku:

- Wymiana informacji osobistych — PKCS #12 (PFX, P12)
- Standard składni wiadomości kryptograficznych — certyfikaty PKCS #7 (P7B)
- Magazyn certyfikatów seryjnych firmy Microsoft (SST)

Dalej

Anuluj



## Kończenie pracy Kreatora importu certyfikatów

Certyfikat zostanie zaimportowany po kliknięciu przycisku Zakończ.

Wybrane zostały następujące ustawienia:

Wybrany magazyn certyfikatów	Automatycznie ustalone przez kreatora
Zawartość	PFX
Nazwa pliku	C:\Users\piotr\Desktop\imię.nazwisko.p12

Zakończ

Anuluj



### Magazyn certyfikatów

Magazyny certyfikatów to obszary systemowe, w których przechowywane są

System Windows może automatycznie wybrać magazyn certyfikatów; możesz jednak określić inną lokalizację dla certyfikatu.

Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu

Umieść wszystkie certyfikaty w następującym magazynie

Magazyn certyfikatów:

Przeglądaj...

Dalej

Anuluj





Import został pomyślnie ukończony.

OK

Otwieramy stronę główną [pk.edu.pl](http://pk.edu.pl) i pobieramy certyfikat na dole strony „ca\_root.crt” [link](#).



Rozpoczynamy instalację według opisu poniżej.

Otwieranie pliku - ostrzeżenie o zabezpieczeniach



**Czy chcesz otworzyć ten plik?**



Nazwa: C:\Users\piotr\Desktop\ca\_root.crt

Wydawca: **Nieznany wydawca**

Typ: Certyfikat zabezpieczenia

Od: C:\Users\piotr\Desktop\ca\_root.crt

Otwórz

Anuluj

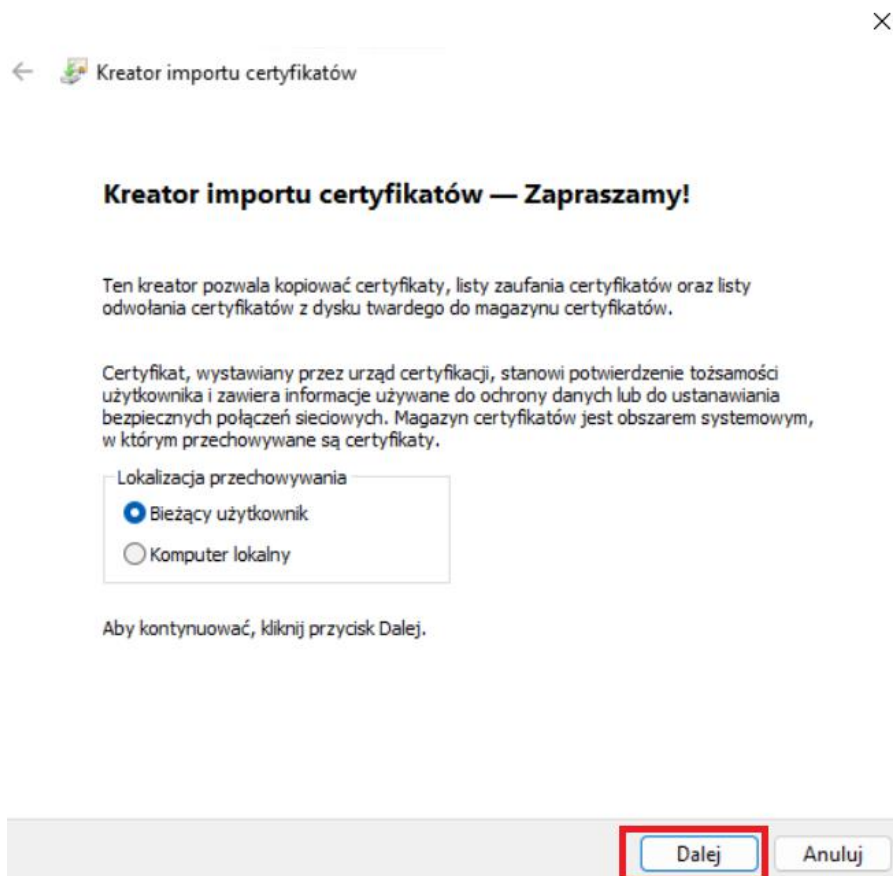
Zawsze pytaj przed otwarciem tego pliku



Pliki pochodzące z Internetu mogą być użyteczne, ale ten typ pliku może być szkodliwy dla komputera. Jeśli nie masz zaufania do źródła, nie otwieraj tego oprogramowania. [Jakie jest zagrożenie?](#)



Przechodzimy do „Zainstaluj certyfikat”.





### Magazyn certyfikatów

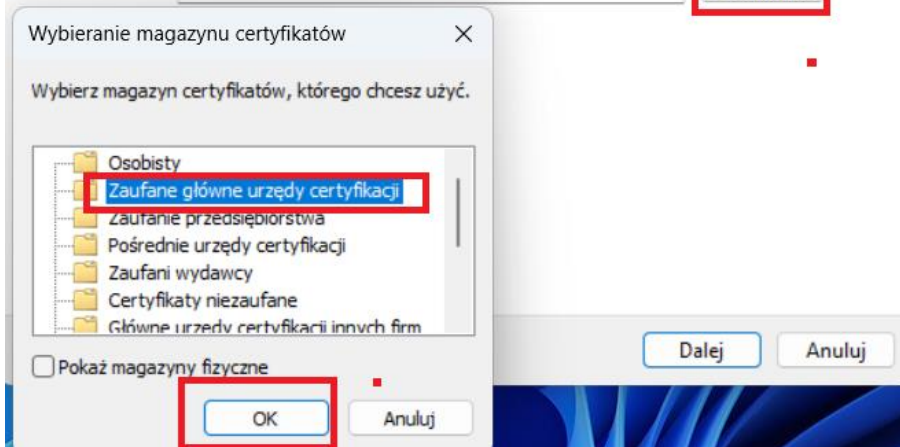
Magazyny certyfikatów to obszary systemowe, w których przechowywane są

System Windows może automatycznie wybrać magazyn certyfikatów; możesz jednak określić inną lokalizację dla certyfikatu.

- Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu
- Umieść wszystkie certyfikaty w następującym magazynie

Magazyn certyfikatów:

Przeglądaj...



### Magazyn certyfikatów

Magazyny certyfikatów to obszary systemowe, w których przechowywane są

System Windows może automatycznie wybrać magazyn certyfikatów; możesz jednak określić inną lokalizację dla certyfikatu.

- Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu
- Umieść wszystkie certyfikaty w następującym magazynie

Magazyn certyfikatów:

Zaufane główne urzędy certyfikacji

Przeglądaj...

Dalej

Anuluj

## Kończenie pracy Kreatora importu certyfikatów

Certyfikat zostanie zaimportowany po kliknięciu przycisku Zakończ.

Wybrane zostały następujące ustawienia:

Magazyn certyfikatów wybrany przez użytkownika	Zaufane główne urzędy certyfikacji
Zawartość	Certyfikat

Zakończ

Anuluj

### Ostrzeżenie o zabezpieczeniach



Za chwilę zostanie zainstalowany certyfikat z urzędu certyfikacji, który rzekomo reprezentuje:

CERTUM PK

System Windows nie może zweryfikować, czy certyfikat rzeczywiście pochodzi od „CERTUM PK”. Należy potwierdzić jego pochodzenie, kontaktując się z „CERTUM PK”. W procesie będzie pomocna następująca liczba:

Odcisk palca (sha1): A4F1C1AB DBE788FE 801D9DE6 D05346B4 ADF1A6B7

Ostrzeżenie:

Jeśli ten certyfikat główny zostanie zainstalowany, system Windows będzie automatycznie ufać każdemu certyfikatowi wystawionemu przez ten urząd certyfikacji. Instalacja certyfikatu z niepotwierdzonym odciskiem palca to potencjalne zagrożenie. Kliknięcie przycisku Tak oznacza, że decydujesz się podjąć to ryzyko.

Czy chcesz zainstalować ten certyfikat?

Tak

Nie

Zatwierdzamy zainstalowanie powyższego certyfikatu „**Tak**”.

Można przejść do listy wyboru aktywnych sieci „**WiFi**”, wskazać sieć „**eduroam**” i po wybraniu połączenia korzystając z odpowiedniego certyfikatu rozpoczynamy pracę w **Internecie**.

\*Test przeprowadzony na systemie **Win 11** z poprawką **22H2**.