Wymagania wstępne

Aby korzystać z sieci eduroam działającej na Politechnice Lubelskiej należy

- 1. posiadać **działający** adres e-mail w domenie *pollub.pl*, który zazwyczaj ma postać <u>i.nazwisko@pollub.pl</u> (w celu uzyskania adresu należy się skontaktować z *Centrum Informatycznym PL*)
- 2. od administratora usługi *eduroam* uzyskać paczkę i.nazwisko.zip zawierającą wszystkie klucze/certyfikaty niezbędne do konfiguracji połączenia (szczegółowy opis: <u>http://eduroam.pollub.pl</u> w sekcji *Rejestracja*)

Przed rozpoczęciem konfiguracji połączenia zaleca się aktualizację sterowników karty bezprzewodowej do najnowszej dostępnej wersji.

UWAGA! W systemie Windows 8.1 sprawdzanie certyfikatu serwera radius nie działa prawidłowo w przypadku wykorzystania uwierzytelniania EAP-TLS [1,2]. Poniższy opis przestawia sposób konfiguracji połączenia z wyłączonym sprawdzaniem certyfikatu serwera. Oznacza to że komputer łącząc się z siecią eduroam nie będzie sprawdzał czy dane uwierzytelniające wysyła do jednego z serwerów eduroam pracujących na Politechnice Lubelskiej. W przypadku systemu Windows 8.1 zalecana jest zmiana uwierzytelniania na EAP-PEAP i wykorzystanie skomplikowanego hasła. EAP-PEAP obsługiwany jest prawidłowo.

1) https://www.mail-archive.com/radiator@open.com.au/msg18424.html

2) http://social.technet.microsoft.com/Forums/windows/en-US/884bd094-de2d-49a0-80bd-

e2e0e8741a50/windows-81-and-eaptls-issue-not-working-after-upgrade?forum=w8itpronetworking

Usuwanie ustawień sieci eduroam

Jeżeli na komputerze była wcześniej konfigurowana sieć *eduroam* należy usunąć zapamiętane ustawienia. W tym celu:

1) włączamy pasek wyszukiwania za pomocą kombinacji Windows+Q i w polu wyszukiwania wpisujemy cmd. Następnie spośród wyników wybieramy *Wiersz polecenia*.



2) w wierszu polecenia wpisujemy polecenie netsh wlan delete profile eduroam i zatwierdzamy przyciskiem *enter*



Importowanie certyfikatu użytkownika

1) Otwieramy plik i.nazwisko.p12 (lub imię.nazwisko.p12), który znajduje się w pliku zip otrzymanym od administratora. Plik p12 zawiera certyfikat i klucz prywatny użytkownika. Uruchamia się *kreator importu certyfikatów*.

Kreator importu certyfi	katów — Zapraszamy!
Ten kreator pozwala kopiować certy odwołania certyfikatów z dysku twar	ikaty, listy zaufania certyfikatów oraz listy dego do magazynu certyfikatów.
Certyfikat, wystawiany przez urząd użytkownika i zawiera informacje uży bezpiecznych połączeń sieciowych. N w którym przechowywane są certyfił	certyfikacji, stanowi potwierdzenie tożsamości wane do ochrony danych lub do ustanawiania łagazyn certyfikatów jest obszarem systemowy katy.
Lokalizacja przechowywania	
Aby kontynuować, kliknij przycisk Da	lej.

2) Zatwierdzamy import wskazanego klucza/certyfikatu.

Imj	port pliku Wybierz plik, który chcesz zaimportować.
	Nazwa pliku:
	C: Users \anonim \Desktop \mie.nazwisko.p12 Przeglądaj
	Uwaga: używając następujących formatów, można przechować więcej niż jeden certyfik w pojedynczym pliku:
	Wymiana informacji osobistych — PKCS #12 (PFX, P12)
	Standard składni wiadomości kryptograficznych — certyfikaty PKCS #7 (P7B)
	Magazyn certyfikatów seryjnych firmy Microsoft (SST)
	Delai

3) Wprowadzamy hasło do własnego klucza prywatnego (hasło znajduje się w wiadomości e-mail od administratora *eduroam*).

)chr	rona klucza prywatnego W celu zapewnienia bezpieczeństwa klucz prywatny jest chroniony hasłem.
	Wpisz hasło dla klucza prywatnego.
	Haslor
	Wyświet 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 kop zapasowej lub transport kluczy.
	✓ Dołącz wszystkie właściwości rozszerzone.

4) Pozwalamy kreatorowi na *automatyczny wybór magazynu*, w którym umieszczony będzie importowany 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
	Dalej Anuluj

5) Potwierdzamy wybrane opcje.

€ ୬	^J Kreator importu certyfika	atów	
	Kończenie pracy Krea	atora importu certyfikatów	
	Certyfikat zostanie zaimportowan	ıy po kliknięciu przycisku Zakończ.	
	Wybrane zostały następujące us	tawienia:	
	Wybrany magazyn certyfikatów	Automatycznie ustalane przez kreatora	
	Zawartość Nazwa oliku	PFX C:\\lsers\anonim\Deskton\imie nazwisko.n12	
		Zakończ	Anuluj

X

Konfiguracja połączenia

1) Przesuwamy kursor myszy do prawego dolnego rogu ekranu. Na pasku wybieramy ustawienia.



2) Na kolejnym pasku wybieramy Panel Sterowania.



3) W Panelu sterowania wybieramy widok Duże ikony a następnie Centrum sieci i udostępniania.



4) W Centrum sieci i udostępniania wybieramy Skonfiguruj nowe połączenie lub nową sieć

¥	Centrum sieci i udostępniania – 🗖 🗙				
🔄 🄄 🔹 🕇 🚆 « Wszystki	e elementy Panel > Centrum sieci i udostępniania v 🖒 Szukaj w Panelu sterowania 🔎				
Strona główna Panelu	Wyświetl podstawowe informacje o sieci i skonfiguruj połączenia				
sterowarna	Wyświetł aktywne sieci W tej chwili nie masz połączenia z żadną siecią.				
Zmień ustawienia karty sieciowej					
Zmień zaawansowane	Zmień ustawienia sieci				
ustawienia udostępniania	📷 Skonfiguruj nowe połączenie lub nową sieć				
	Skonfiguruj połączenie szerokopasmowe, telefoniczne lub VPN albo skonfiguruj router lub punkt dostępu.				
	Rozwiąż problemy				
	Zdiagnozuj i rozwiąż problemy z siecią lub uzyskaj informacje na temat rozwiązywania problemów.				
Zobacz też					
Grupa domowa					
Opcje internetowe					
Zapora systemu Windows					

5) W	kreatorze	wybieramy	Reczne	e nawiązyv	wanie poł	laczenia z	siecia l	bezprzewodow	vą
	,		2 2				2	2		۰.

ybic	
	Połącz z Internetem Skonfiguruj połączenie szerokopasmowe lub telefoniczne z Internetem.
2	Skonfiguruj nową sieć Skonfiguruj nowy router lub punkt dostępu.
2	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.

6) W nowym oknie (a) wpisujemy nazwę sieci *eduroam*, (b) wybieramy typ zabezpieczeń WPA2-Enterprise, (c) opcjonalnie zaznaczamy opcję Uruchom to połączenie automatycznie, (d) następnie klikamy na przycisk Dalej.

📀 🔮 Ręczne nawiązyw	vanie połączenia z siec	cią bezprzewodową	
Wprowadź inform	acje o sieci bezprzewo	odowej, którą chcesz dodać.	
Nazwa sieci:	eduroam		
Typ zabezpieczeń:	WPA2-Enterprise	~	
Typ szyfrowania:	AES	¥	
Klucz zabezpieczeń:		Ukryj znaki	
🗹 Uruchom to połą 🗌 Połącz, nawet jeś	czenie automatycznie li sieć nie wykonuje emisji		
Ostrzeżenie: jeśli	wybierzesz tę opcję, może to	o zagrozić prywatności komputera.	
		Dalej Anuluj	

7) Po otrzymaniu komunikatu o pomyślnym dodaniu sieci *eduroam* wybieramy opcję *zmiany ustawień połączenia.*

Ręczne nawiązywanie połączenia z siecią bezprzewodową	
Pomyślnie dodano: eduroam	
Zmień ustawienia połączenia Otwórz właściwości połączenia, aby można było zmienić ustawienia.	
	Zamknij

8) W nowym oknie przechodzimy na zakładkę *zabezpieczenia*, gdzie sprawdzamy poprawność *Typu zabezpieczeń* oraz *typu szyfrowania* a następnie ustawiamy metodę uwierzytelniania sieci na *Microsoft: Karta inteligentna lub inny certyfikat*. Następnie wybieramy przycisk *Ustawienia*

eduroam — Właściwości sieci bezprzewodowej			
Połączenie Zabezpieczenia			
Typ zabezpieczeń: WPA2-Enterprise	~		
Typ szyfrowania: AES	~		
Wybierz metodę uwierzytelniania sieci: Microsoft: Karta inteligentna lub inny cer 💙 Ustawier I Zapamiętaj moje poświadczenia dla tego połączenia przy każdym logowaniu Ustawienia zaawansowane	ia		
ОК	Anuluj	j	

9) Włączamy użycie certyfikatu zainstalowanego na komputerze oraz prosty wybór certyfikatu, wyłączamy weryfikację certyfikatu serwera. Zatwierdzamy wprowadzone zmiany przyciskiem OK

Właściwości karty inteligentnej lub innego certyfik
Podczas łączenia: O Użyj mojej karty inteligentnej O Użyj certyfikatu na tym komputerze ✓ Użyj prostego wyboru certyfikatu (zalecane)
Sprawdź tożsamość serwera, weryfikując certyfikat
Połącz tylko z tymi serwerami (przykłady: srv1;srv2;.*\srv3\.com):
Zaufane główne urzędy certyfikacji:
Add Trust External CA Root
Baltimore CyberTrust Root
Certum CA
Class 3 Public Primary Certification Authority
DigiCert Assured ID Root CA
< >>
Wyświetl certyfikat
Nie monituj użytkownika o autoryzowanie nowych serwerów lub zaufanych urzędów certyfikacji.
Użyj innej nazwy użytkownika dla połączenia
OK Anuluj

10) Kończymy konfigurację sieci. Komputer powinien automatycznie połączyć się z siecią eduroam.