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)
- 3. posiadać hasło zabezpieczające osobisty certyfikat użytkownika (hasło jest przekazywane użytkownikowi podczas tworzenia konta)

Przed rozpoczęciem konfiguracji połączenia należy z paczki *i.nazwisko.zip* wyodrębnić pliki *i.nazwisko.p12* oraz *plca_cert.crt* i umieścić je w na karcie SD / w pamięci masowej zainstalowanej w telefonie/tablecie.

UWAGA! Ze względu na dużą różnorodność urządzeń z systemem Android przy konfiguracji połączenia na telefonach/tabletach różnych firm lub w różnych wersjach systemu mogą występować rozbieżności w stosunku do niniejszej instrukcji.

Instalowanie certyfikatu CA z karty SD/pamięci masowej (na przykładzie Android 8.0 "Oreo")

Instalacja certyfikatu CA nie jest konieczna, jednak jest zalecana, ponieważ zapewnia bezpieczeństwo danych logowania użytkownika.

Ustawienia Q		÷	Lokalizacja i blokady 🕜	÷	Szyfrowanie i dane logowania 🛛 😢
ø	Wyświetlacz Tapeta, uśpienie, rozmiar czcionki		Prywatność		Szyfrowanie
•	Dźwięk Głoścość wikracie Nie przeszkadzać		Lokalizacja WŁ. / Oszczędzanie baterii		Zaszyfruj telefon Zaszyfrowany
	Pamięć wewnętrzna		Pokazuj hasła Wpisywane znaki są przez chwilę wyświetlane		Magazyn danych logowania
A	Lokalizacja i blokady		Aplikacje do administrowania urządzeniem		Typ pamięci Wspomagana sprzętowo
-	Blokada ekranu, odcisk palca Użytkownicy i konta		3 aktywne aplikacje Blokada karty SIM		Zaufane dane uwierzytelniające Wyświetlaj zaufane certyfikaty CA
	Bieżący użytkownik:	ſ	Szyfrowanie i dane logowania		Dane logowania użytkownika Wyświetlanie i zmiana zapisanych danych logowania
Ť	Czytniki ekranu, wyświetlacz, sterowanie interakcją		Agenty zaufania	[Zainstaluj z nośnika Zainstaluj certyfikaty z nośnika
G	Google Usługi i ustawienia		1 aktywny agent zaufania Przypinanie ekranu		Wyczyść dane o certyfikatach
()	System Języki, kopia zapasowa, aktualizacje		Wył.		usun wszystkie certyfikaty
	Bomoo		Aplikacje monitorujące		

W menu ustawień telefonu wybieramy kolejno *Lokalizacja i blokady*, a następnie *Szyfrowanie i dane logowania* i *Zainstaluj z nośnika*.



Pojawi się wbudowany menadżer plików. Należy odszukać i wybrać zapisany wcześniej plik certyfikatu *plca_cert.crt*. Przed instalacją certyfikatu należy potwierdzić wzór/pin/odcisk palca... (w zależności od używanej metody zabezpieczeń). Jeżeli nie mamy włączonej żadnej metody zabezpieczeń może być konieczne jej włączenie. Następnie wprowadzamy nazwę, która będzie identyfikowała certyfikat CA np. *plca* i wybieramy przeznaczenie danych logowania – w naszym wypadku *Wi-Fi*.

Instalowanie certyfikatu osobistego z karty SD/pamięci masowej (na przykładzie Android 8.0 "Oreo")

Instalacja certyfikatu osobistego jest analogiczna do instalacji certyfikatu CA.

Usta	Ustawienia Q		Lokalizacja i blokady 🛛 🛛 😨		Szyfrowanie i dane logowania 🛛 🕐
Ð	Wyświetlacz Tapeta, uśpienie, rozmiar czcionki		Prywatność		Szyfrowanie
•	Dźwięk Głośność, wibracie, Nie przeszkadzać		Lokalizacja WŁ. / Oszczędzanie baterii		Zaszyfruj telefon Zaszyfrowany
=	Pamięć wewnętrzna		Pokazuj hasła Wpisywane znaki są przez chwilę wyświetlane		Magazyn danych logowania
	23% zajęte – 98,74 GB wolne		Aplikacie do administrowania urządzeniem		Typ pamięci Wspomagana sprzętowo
0	Blokada ekranu, odcisk palca		3 aktywne aplikacje		Zaufane dane uwierzytelniające Wyświetlaj zaufane certyfikaty CA
2	Użytkownicy i konta Bieżący użytkownik:	ſ	Blokada karty SIM Szyfrowanie i dane logowania		Dane logowania użytkownika
Ť	Ułatwienia dostępu Czytniki ekranu, wyświetlacz, sterowanie interakcją	l	Telefon zaszyfrowany	ſ	Zainstalui z nośnika
G	Google Usługi i ustawienia		Agenty zaufania 1 aktywny agent zaufania	L	Zainstaluj certyfikaty z nośnika
()	System Jezyki, kopia zapasowa, aktualizacie		Przypinanie ekranu Wył.		Wyczyść dane o certyfikatach Usuń wszystkie certyfikaty
	Domoc		Aplikacje monitorujące		

W menu ustawień telefonu/tabletu wybieramy kolejno *Lokalizacja i blokady*, a następnie *Szyfrowanie i dane logowania* i *Zainstaluj z nośnika*.

≡ Pixel	Q 🔳	 ← Szyfrowanie i dane logowania 	← Szyfrowanie i dane logowania 🕐
	Nazwa 🔨	Szyfrowanie	Szyfrowanie
	ē	Wyodrębnij certyfikat Wprowadź hasło, aby wyodrębnić certyfikaty.	Zaszyfruj telefon Zaszyfruyany Nadaj certyfikatowi nazwę
i.nazwisko 266 KB 19:00	pica_cert.crt	ANULUJ OK Zaufane dane uwierzytelniające	Przeznaczenie tych danych logowania: Wi-Fi
	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	Wyswietiaj zaufane certytikaty CA Dane logowania użytkownika Wyświetlanie i zmiana zapisanych danych logowania	Pakiet zawiera: jeden klucz użytkownika jeden certyfikat użytkownika
			ANULUJ OK
			Wyczyść dane o certyfikatach Usuń wszystkie certyfikaty

Pojawi się wbudowany menadżer plików. Należy odszukać i wybrać zapisany wcześniej plik certyfikatu *i.nazwisko.p12*. Aby wyodrębnić certyfikat konieczne jest podanie hasła zabezpieczającego certyfikat otrzymanego mailem po utworzeniu konta. Przed instalacją certyfikatu należy potwierdzić wzór/pin/odcisk palca... (w zależności od używanej metody zabezpieczeń). Następnie wprowadzamy nazwę, która będzie identyfikowała certyfikat osobisty np. *mojcert* i wybieramy przeznaczenie danych logowania – w naszym wypadku *Wi-Fi*.

Konfiguracja połączenia (na przykładzie Android 8.0 "Oreo")



W menu ustawień Wi-Fi włączamy łączność przez sieć Wi-Fi i przechodzimy do dodawania nowej sieci wybierając *Dodaj sieć*. Następnie: (1) wprowadzamy nazwę sieci: *eduroam*, (2) wybieramy typ zabezpieczeń: *802.1x EAP*, (3) wybieramy metodę EAP: *TLS*, (4) (opcjonalnie) wybieramy zainstalowany wcześniej certyfikat urzędu certyfikacji: *plca* (jeżeli certyfikat nie został zainstalowany wybieramy *Nie sprawdzaj poprawności*), (5) wybieramy zainstalowany wcześniej certyfikat osobisty *mojcert*, (6) w polu *Tożsamość* wpisujemy adres e-mail w domenie pollub.pl (zazwyczaj i.nazwisko@pollub.pl). Zapisujemy wprowadzoną konfigurację.

Telefon/tablet powinien automatycznie nawiązać połączenie z siecią gdy znajdzie się w zasięgu.