Konfiguracja połączenia

Informacje techniczne dla użytkowników obsługiwanych przez ACK Cyfronet AGH pomocne przy konfigurowaniu połączenia do sieci eduroam

Najszybszą metodą na skonfigurowanie połączenia jest posłużenie się automatycznymi instalatorami dostępnymi pod adresem http://cat.eduroam.org/ .

Po kliknięciu w pasek "użytkownik eduroam: pobierz instalator eduroam" pojawi się okienko z wyborem instytucji. Dla kont pochodzących z Cyfronetu należy wybrac z listy Cyfronet a następnie właściwy system operacyjny.

W indywidualnych przypdakach, np. gdy użytkownik dysponuje systemem nie wspieranym przez automatyczne instalatory, może zaistnieć konieczność wykonania "ręcznej" konfiguracji.

Poniżej przedstawione są wskazówki mogące ułatwić proces konfiguracji:

- W pierwszej kolejności należy zainstalować za pomoca systemowej przeglądarki internetu certyfikat CA ACK CYFRONET dostępny pod adresem http://cyfronet.pl/cyfcacert.der i wybrać akcję "Otwórz", a następnie "Zainstaluj certyfikat". Zostanie uruchomiony Kreator importu certyfikatów. Należy ręcznie wskazać magazyn certyfikatów : "Trusted Root Certification Authorities" i zainstalować certyfikat.
- Następnie można skonfigurować połączenie sieciowe z uwzględnieniem następujących parametrów:
  - SSID: eduoram
  - typ szyfrowania: WPA2-AES
  - uwierzytelnianie typu: EAP(PEAP)/MSCHAP V2
- w ustawieniach EAP/MSCHAP V2 koniecznie wyłączyć automatyczne uwierzytelnienie na podstawie danych podanych przy logowaniu do Windows

Dla systemu operacyjnego typu Linux, na potrzeby uwierzytelniania można stosować oprogramowanie "wpa_supplicant". Przykładowa konfiguracja dla "wpa_supplicant":

```
network={
 ssid="eduroam"
 scan_ssid=1
 key_mgmt=WPA-EAP
 eap=PEAP
 identity="cyf-kr666@cyfronet.pl"
 password="haslo"
 ca_cert="cyfcacert.der"
 phase1="peaplabel=0"
 phase2="auth=MSCHAPV2"
 }
```

UWAGA - bardzo ważny dla bezpieczenstwa jest zainstalowany oraz sprawdzany w trakcie uwierzytelniania certyfikat serwera. Jakiekolwiek problemy z certyfikatem mogą wskazywać na próbę przejęcia procedury uwierzytelniania przez fałszywy serwer i powinny być zgłaszane do administratora sieci.