



Novosti u usluzi eduroam

1. srpanj, 2021.

Dubravko.Penezić@srce.hr



Sadržaj

- eduroam
- CAT
- Obnova RADIUS serverskih certifikata
- eduroam hosting
- Pitanja i odgovori





- " eduroam™ (education roaming) je roaming-usluga zamišljena pod okriljem europske udruge akademskih i istraživačkih mreža (TERENA) i ostvarena kroz međunarodni projekt GÉANT."
- Žičani i bežični pristup mrežnoj opremi
- Sigurna, jednostavna i za krajnjeg korisnika potpuno besplatna usluga pristupa Internetu
- Preko 1.100 pristupnih točaka u Hrvatskoj
- Preko 28.000 pristupnih točaka u svijetu
- <https://www.eduroam.hr/>
- <https://www.eduroam.org/>



eduroam je ...

- Globalna usluga
- Autentikacijski model u funkcionalnoj žičnoj ili bežičnoj mreži za pristup Internetu
- Autentikacija je bazirana na 802.1x skupu standarda, uz mogućnost implementacije 802.1q standarda
- Namijenjen prvenstveno akademskoj i znanstvenoj zajednici
- Za autentikaciju korisnika se koristi RADIUS hijerarhijska ili dinamička infrastruktura bazirana na DNS modelu (realmovi).
- Passpoint , OpenRoaming



installer.eduroam.hr

- Web aplikacija koja olakšava podešavanje korisničkih uređaja za sigurno korištenje usluge eduroam
- Nastala 2011. godine
 - Podržani svi OS-ovi koji su tada podržavali 802.1x autentikaciju
- Konfiguracija korisničkih uređaja definirana je slijedećim parametrima:
 - protokoli: EAP/TTLS - PAP
 - serverski certifikat (root CA)
 - provjera polja *subject* u certifikatu
- Dodatno sučelje za prikupljanje podataka o matičnim ustanovama (logotip, naziv, root CA certifikat)
- FAQ



CAT

- Configuration Assistant Tool (<https://cat.eduroam.org/>)
- Nastao 2013. kako bi zadovoljio globalnu potrebu alatom koji omogućuje jednostavnu i sigurno konfiguraciju korisničkih uređaja
- Podržava različite tipove EAP protokola
- Set OS-ova koji se najviše koriste
- API za kontrolu konfiguracija



Installer <-> CAT

- Installer:
 - + strogo kontrolirana okolina, jednostavnije održavanje
 - + pokrivena većina OS-ova (stariji uređaji)
 - + laka prilagodna našim potrebama
 - + podržan žičani pristup od početka
 - potreba za vlastitim održavanjem svih konfiguracija i implementacija novih OS-ova, uređaja i testiranje istih na fizičkim uređajima
- CAT:
 - + pokriva različite tipove EAP implementacija
 - + preveden na više jezika (ima podršku na hrvatskom)
 - + razvoj i provjera konfiguracija (šira zajednica i tim projekta GEANT)
 - + API
 - + opensource – može i vlastita instalacija
 - nemamo izravnu kontrolu nad razvojem (konfiguracija, podržani OS-ovi)



Installer = CAT

- Tim Srca putem CAT API-ija podešava konfiguracije za sve matične ustanove u RH
- Administratori matičnih ustanova koriste installer kao i do sada
- Korisnici mogu:
 - i dalje koristiti <https://installer.eduroam.hr/> (naša preporuka)
 - izravno pristupati CAT-u (<https://cat.eduroam.org>)
- Podržani OS-ovi:
 - Android 4.4+, Chrome OS, iOS, Mac OS X, Microsoft Windows Vista, 7, 8, 10
 - Pokriveno 99,5 % svih uređaja koji se mogu spojiti na eduroam
- Praćenje novih verzija OS-a, testiranje novih uređaja, te sigurnosne zakrpe obavlja tim CAT-a
- Podržani Passpoint/OpenRoaming, WPA3



Novosti nakon prelaska na CAT

- Drugačije sučelje prilikom konfiguracije/instalacije programske podrške
- Stabilan rad uz najnoviju podršku
- Problemi u snalaženju s novim rješenjima za:
 - Android telefone
 - Windows 10



Android telefoni i CAT

- Promjena načina dohvata nužne programske podrške (nužan dohvat s Google PlayStore-a)
- Promjena načina konfiguriranja (*native vs user app*)
 - Ne brisati aplikaciju s telefona
- Dva programska rješenja - ovisno o verziji Androida (eduroamcat i geteduroam)
- Promjena u Google SDK (provjera naziva servera putem SAN atributa iz certifikata)



Windows 10 i CAT

- Drugačiji postupak uključivanja wired podrške za 802.1x
- Mogućnost postojanja višestrukih profila s istim SSID-om
 - Naša preporuka: obrisi sve prethodne (eduroam) profile



Obnova RADIUS serverskih certifikata

- Serverski RADIUS certifikati svoj naziv drže u *subject* atributu certifikata
Subject: C=HR, ST=Zagreb, L=Zagreb, O=SRCE, CN=freeradius.srce.hr
- Nova implementacija Android SDK provjerava samo vrijednost atributa *SAN (Subject Alternative Name)*
X509v3 Subject Alternative Name:
DNS:freeradius.srce.hr
- SAN je poseban podatak kod kreiranja certifikata i zato je potrebno regeneriranje serverskog certifikata
- Korisnici ne trebaju ništa napraviti
- Pojedine ustanove će trebati obnoviti i root CA (zahtjevniji postupak)



Skripta za generiranje certifikata

- Dostupna na <https://www.eduroam.hr/server-certs>
- Bash skripta sa nekoliko konfiguracijskih datoteka
- Očekuje da su certifikati u fRCerts direktoriju
- Izvršava se pod root ovlastima
- Nakon uspješne regeneracije treba restartati freeradius servis



Instalacija i konfiguriranje

Datoteke iz *radius-cert-admin.tar* datoteke treba raspakirati u direktorij u kojem se nalazi fRcerts direktorij, za Debian te putanje su

```
Lenny      /etc/freeradius/certs
Squeeze    /etc/freeradius/certs
Jessie     /etc/freeradius/certs
Stretch    /etc/freeradius/3.0/certs
```

Datoteka se raspakira s ovlastima root korisnika naredbom

```
# tar xvf radius-cert-admin.tar
```

Po instalaciji u direktoriju će se naći slijedeće nove datoteke:

```
cert-admin - skripta za rad s certifikatima
openssl.cnf - konfiguracija za openssl
README - ova uputa
xpextensions - naputak o ekstenziji za MS Windows
```



Instalacija i konfiguriranje (2)

Potrebno je urediti prvi dio *cert-admin* skripte i to ispravnim popunjavanjem vrijednosti polja:

```
COUNTRY="HR"  
PROVINCE="grad"  
CITY="grad"  
ORGANIZATION="skraceni_naziv_institucije"  
ORG_UNIT=""  
PASSWORD="neki_password"  
DOMAIN="realm_iz_AAI_sustava"
```

Primjer ispravnog popunjavanja:

```
COUNTRY="HR"  
PROVINCE="Zagreb"  
CITY="Zagreb"  
ORGANIZATION="SRCE TEST"  
ORG_UNIT=""  
PASSWORD="PaTh4526"  
DOMAIN="srce-test.hr"
```

Zatim treba podestiti da skripta *cert-admin* bude izvršna, naredbom

```
# chmod 700 cert-admin
```



Pokretanje

Backup postojećeg direktorija s certifikatima

```
# cp -R fRcerts fRcerts.orig
```

Kreiranje novog RADIUS serverskog certifikata

```
# ./cert-admin -newserver
```

Verifikacija RADIUS serverskog certifikata

```
# ./cert-admin -chkservercert
```



eduroam hosting usluga

- eduroam RADIUS poslužitelj za davatelje usluge eduroam koji ne mogu sami održavati svoj RADIUS servis
- <https://hosting.eduroam.hr/>
- Pregled statistika i logova
- Upute za prijavu dostupne na webu



Sekundarni AAI@EduHr servisi

- Usluga sekundarnih servisa u AAI@EduHr-u omogućava privremeno preuzimanje IdP funkcionalnosti matične ustanove u slučaju havarije iste
- <https://www.aaiedu.hr/za-maticne-ustanove/udomljavanje-ldap-imenika/udomljavanje-sekundarnih-servisa-na-posluzitelju-u-srcu>
- Realizirana podrška za višestruke certifikate za potrebe eduroama
- Administrator ustanove (sistemac) mora potpisati certifikat kako bi bio postavljen na našem serveru



Pitanja

- U vezi eduroam-a?
- U vezi AAI@EduHr?
- Prijedlozi tema za webinar?



Hvala!

<eduroam@srce.hr>



www.srce.unizg.hr

Ovo djelo je dano na korištenje pod licencom
Creative Commons *Imenovanje-Nekomercijalno-
Bez prerada* 4.0 međunarodna.

creativecommons.org/licenses/by-nc-nd/4.0/deed.hr

Srce politikom otvorenog pristupa široj javnosti osigurava dostupnost i korištenje svih rezultata rada Srca, a prvenstveno obrazovnih i stručnih informacija i sadržaja nastalih djelovanjem i radom Srca.

www.srce.unizg.hr/otvoreni-pristup

