eduroam radionica

Miroslav Milinović, Dubravko Penezić, Dario Šafar
<admin@eduroam.hr>
Sveučilišni računski centar Sveučilišta u Zagrebu

Osijek, Rijeka, Split, Zagreb, 8.-11. travanj 2013.

srce

eduroam

Sadržaj

- stanje eduroam usluge u Republici Hrvatskoj i svijetu
- uspostava i održavanje eduroam pristupne točke
- eduroam nadzorna sonda
- eduroam installer i sigurnost usluge

Što je eduroam?

(opis i stanje usluge u Hrvatskoj i svijetu)

Mobilnost korisnika → roaming usluga

- zahtjevi:
  - mogućnost jednoznačne identifikacije korisnika na krajevima mreže
  - pristup gostima
  - skalabilnost
    - administracija i autentikacija korisnika
  - lagana uspostava i korištenje
    - minimalni zahtjevi na korisnika i podešavanje njegovog računala
  - otvorenost
  - sigurnost i zaštita privatnosti

Što je eduroam?

- eduroam™: skraćenica od EDUcation ROAMing
- moto: “**Open your laptop and be online**”
- globalna (akademska) roaming usluga
- siguran i jednostavan pristup mreži za krajnje korisnike
  - neovisan o mjestu i vremenu pristupa
  - konzistentan i uniforman
  - čuva privatnost
- povijest:
  - koncept i prototip nastali u okviru TERENA TF-Mobility (2002.)
  - produkcijska usluga je uspostavljena u okviru EU FP6 projekta GÉANT2 (2008.),
  - razvoj i održavanje nastavljeni u okviru EU FP7 projekta GÉANT3

eduroam™

- SSID = eduroam
- korisničke oznake oblika uid@realm (ivo@srce.hr)
- autentikaciju obavlja matična ustanova (IdP; davatelj identiteta), a autorizaciju davatelj usluge (SP, točka pristupa, posjećena ustanova)
- odabrani tehnički standard: 802.1x + EAP
- roaming temelji na hijerarhiji RADIUS poslužitelja
- dostupan na (gotovo) svim platformama/uređajima



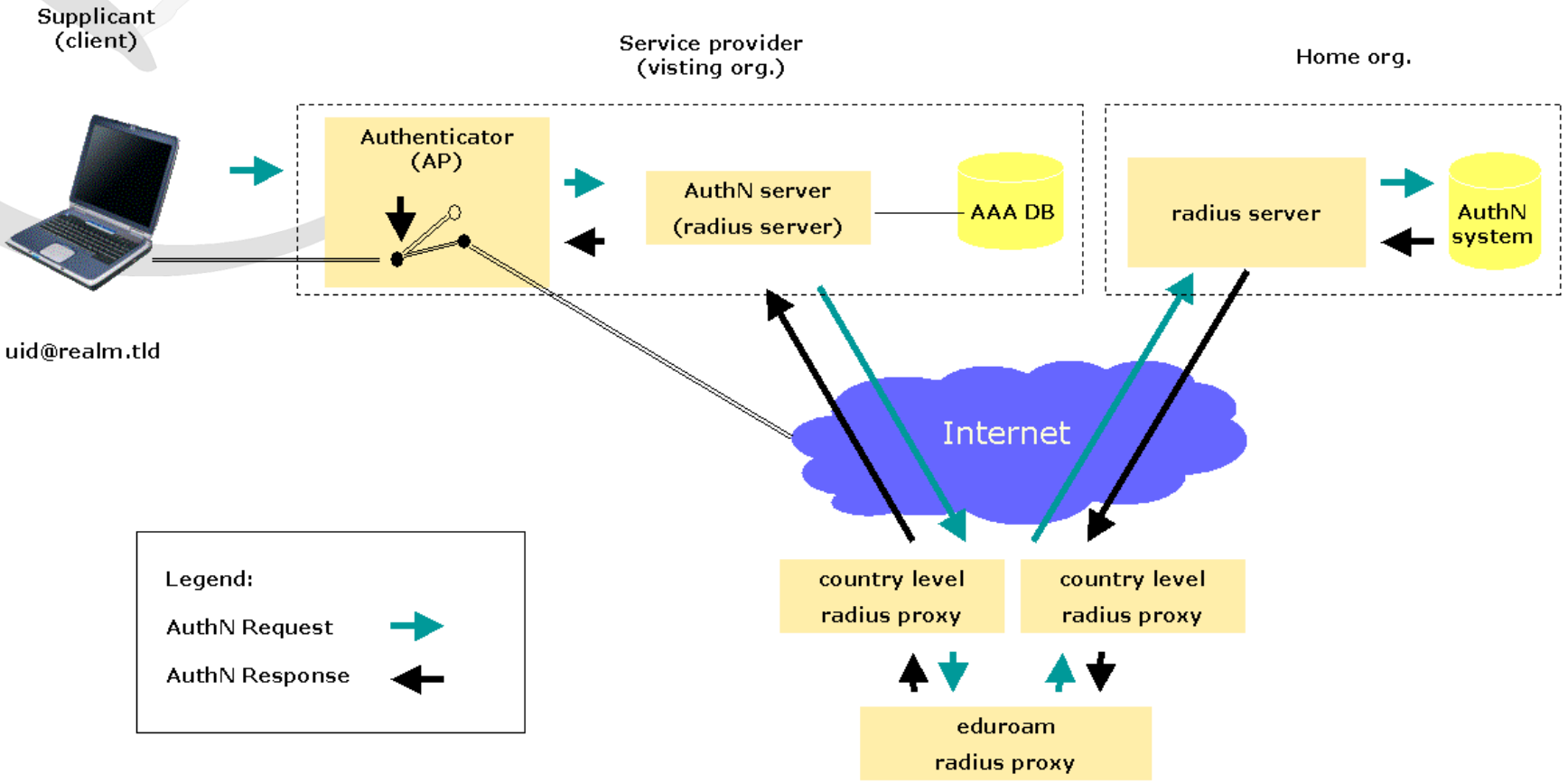
Tehnologija eduroam

- **rabi 802.1X protokol(e)**
  - *layer-2 port-based* standard za (kontrolirani) pristup mreži
  - detektira korisnika na “kraju mreže”
    - port na (aktivnom) pristupnom mrežnom uređaju (NAS)
    - može biti AP ili preklopnik (*switch*)
  - dok se ne potvrdi identitet korisnika moguć je samo promet EAP paketa, ostalo (npr: HTTP ili DHCP) je blokirano na *data link* razini
  - sigurnost: enkripcija podataka korištenjem dinamičkih ključeva (802.11i; WPA/TKIP → WPA2/AES, ...)
  - dodjela VLAN-a pri autorizaciji (802.1q)

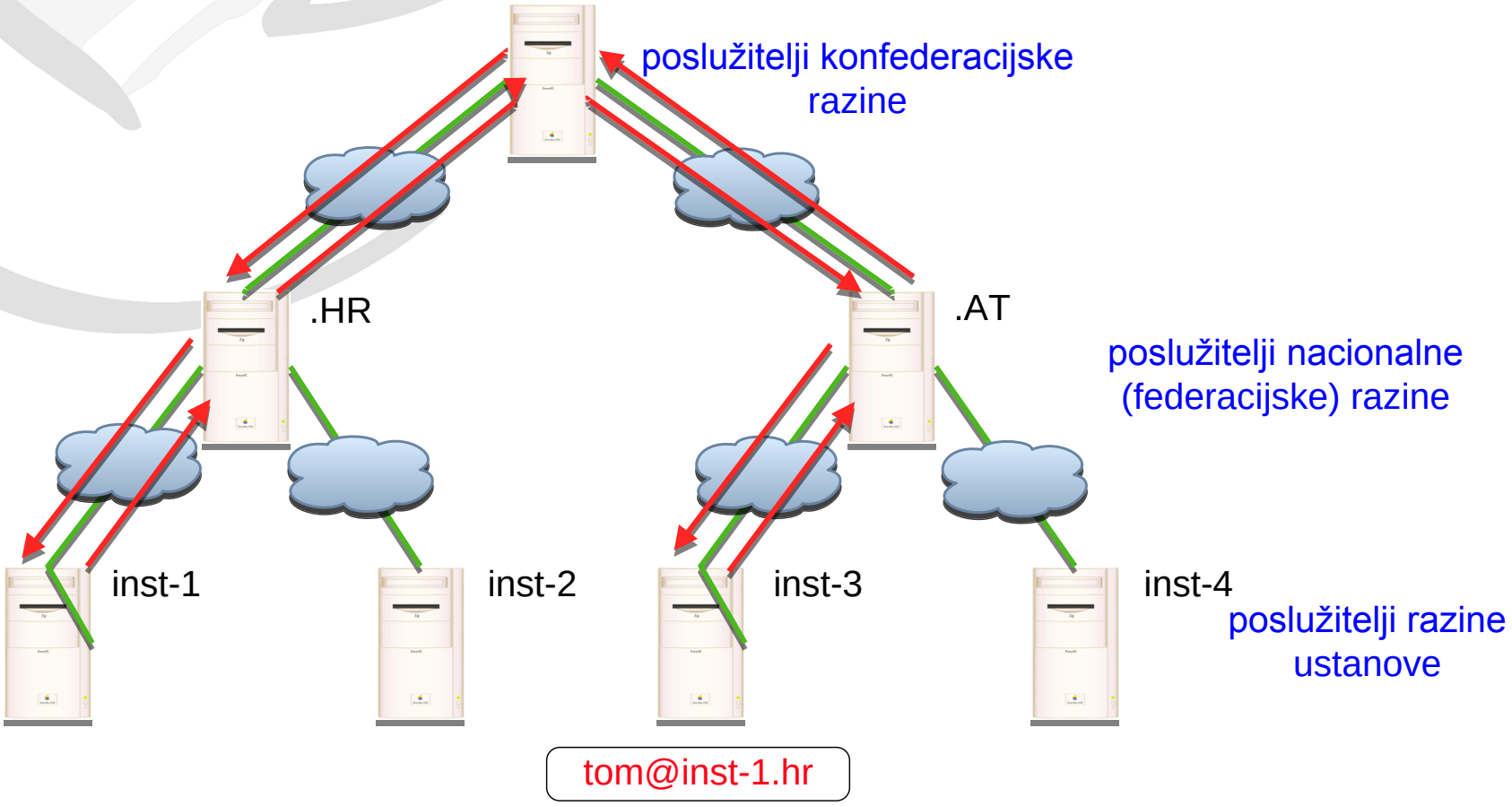
Tehnologija eduroam (2)

- **autentikacija temeljena na uporabi EAP-a**
  - EAP (Extensible Authentication Protocol)
  - omogućuje različite autentikacijske metode EAP/TTLS, EAP/TLS, PEAP, ...
- **RADIUS proxy kao temelj za roaming**
  - RADIUS je transportni protokol za autentikacijske podatke
  - *user names format*: user@realm (npr. ivo@srce.hr)
  - hijerarhija RADIUS poslužitelja (rabe se *shared secrets*) uz *realm-based proxying*
- **povjerenje u sustav (*trust fabric*) temelji na**
  - hijerarhiji RADIUS poslužitelja
  - Pravilniku o ustroju eduroam usluge (*The eduroam policy*)

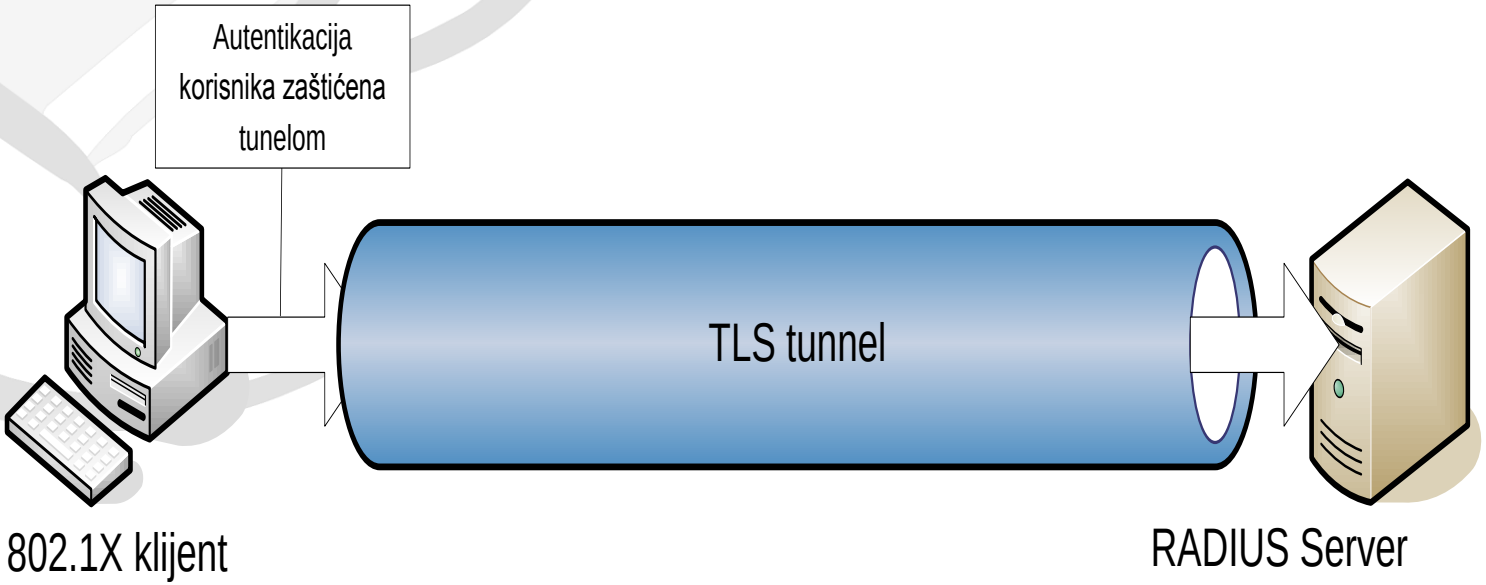
eduroam™

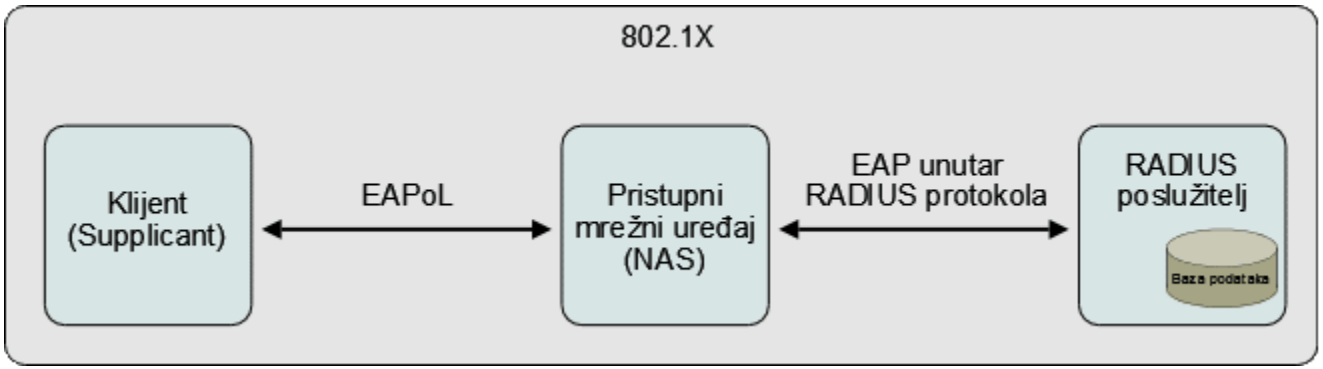

Supplicant
(client)
Service provider
(visting org.)
Home org.
Authenticator
(AP)
AuthN server
(radius server)
AAA DB
radius server
AuthN
system
uid@realm.tld
Internet
country level
radius proxy
country level
radius proxy
eduroam
radius proxy
Legend:
AuthN Request
AuthN Response

Prenošenje podataka o korisniku RADIUS infrastrukturom

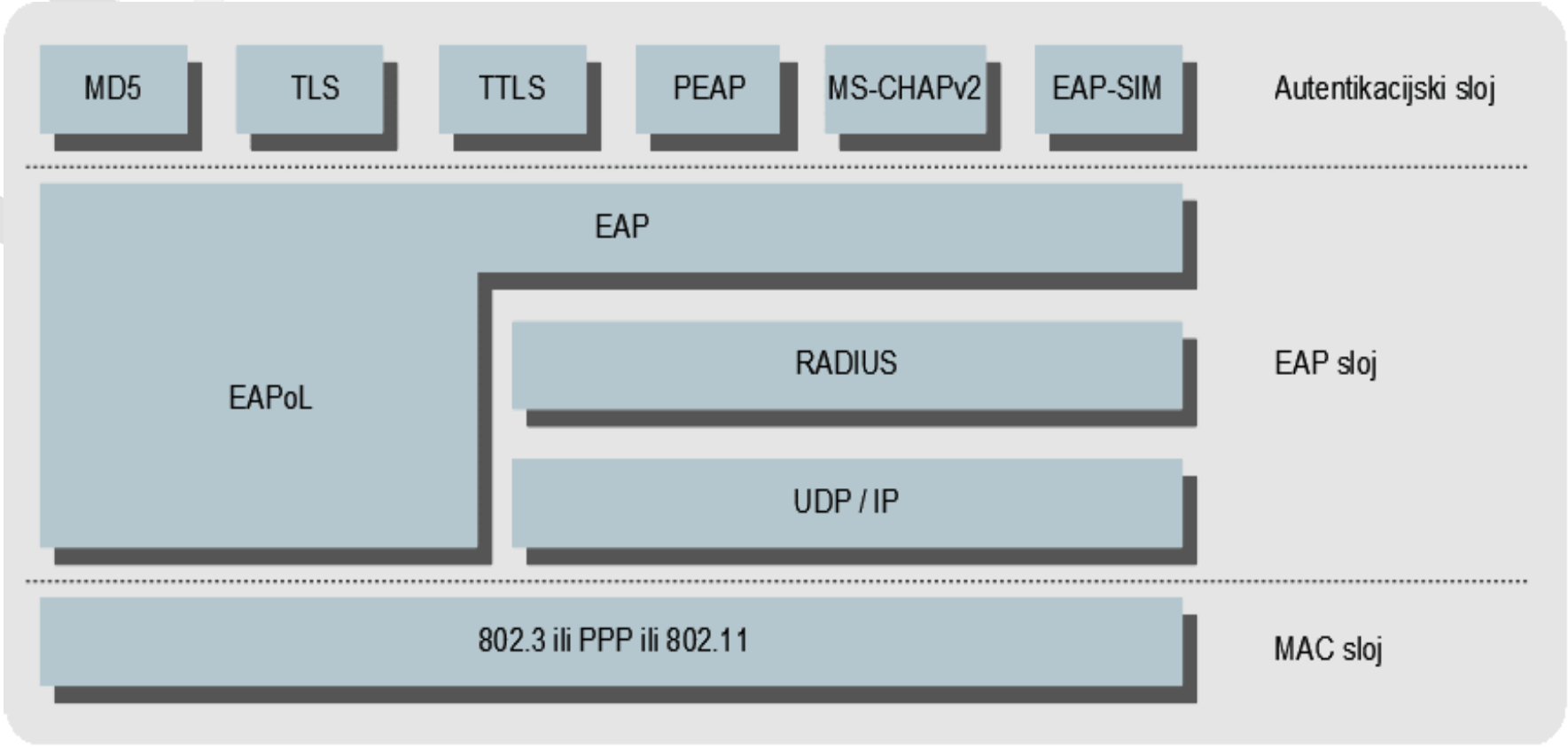


EAP tunel

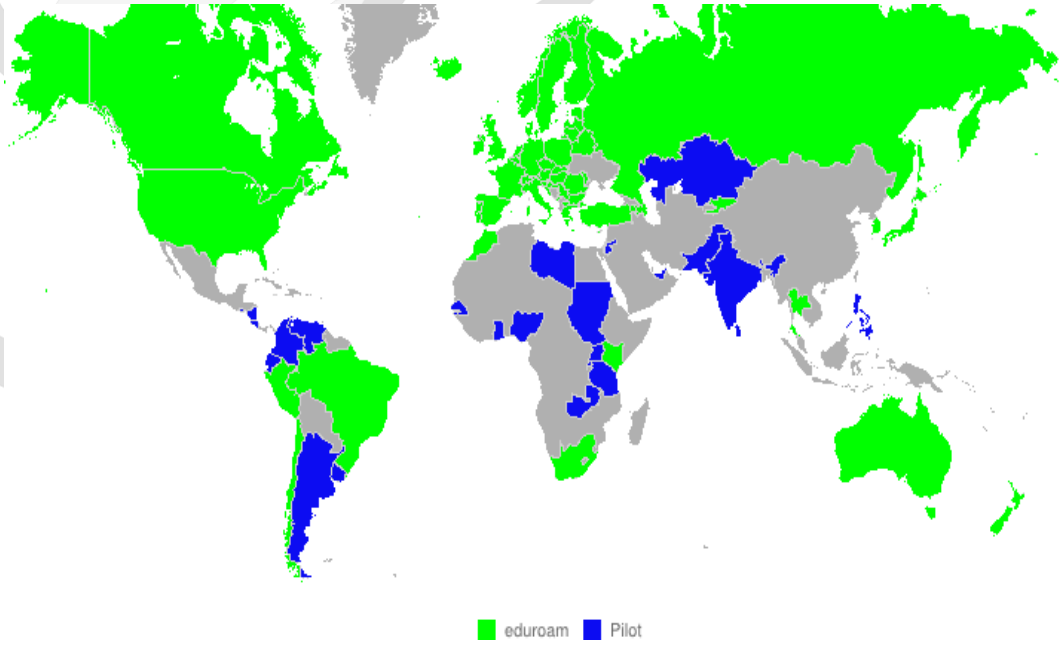

Autentikacija korisnika zaštićena tunelom
TLS tunnel
802.1X klijent
RADIUS Server


802.1X
Klijent (Supplicant)
EAPoL
Pristupni mrežni uređaj (NAS)
EAP unutar RADIUS protokola
RADIUS poslužitelj
Baza podataka

EAP – slojevi protokola



eduroam: globalna usluga

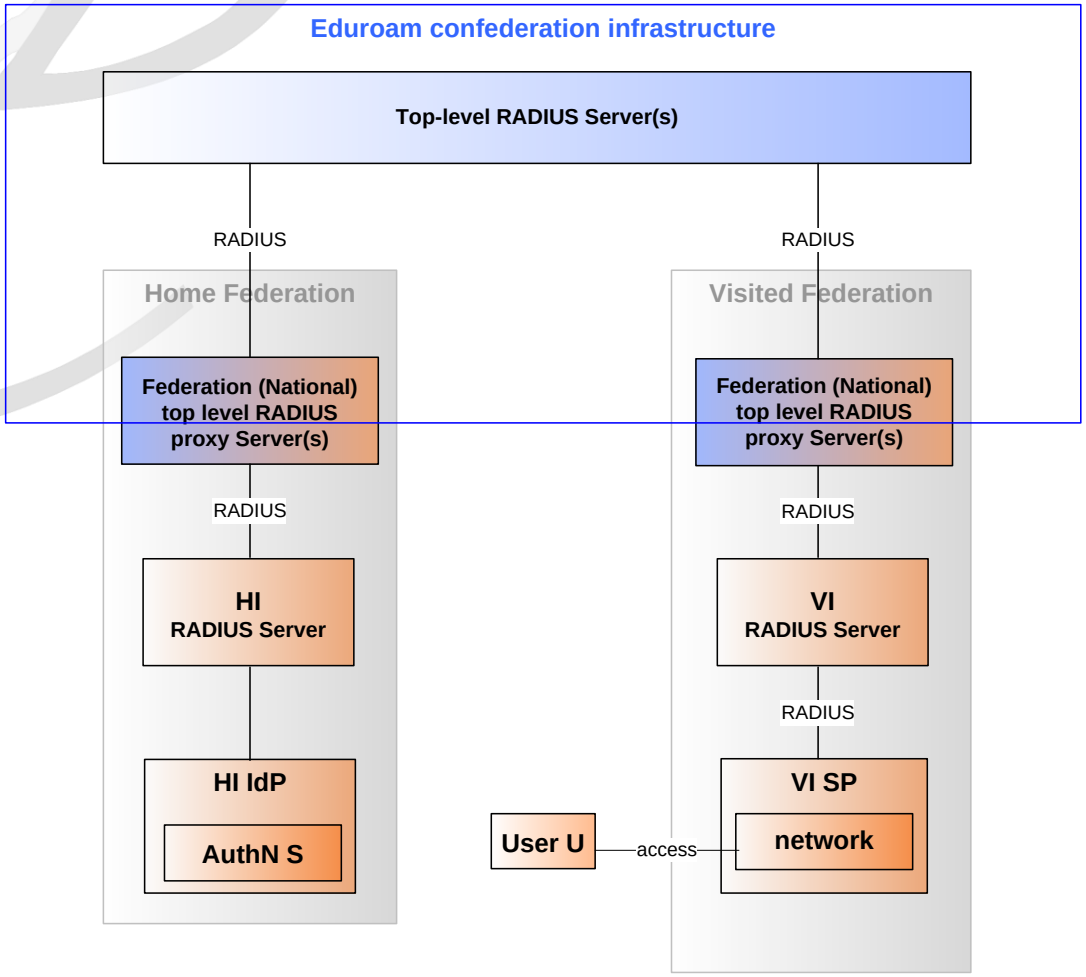


www.eduroam.org

eduroam usluga

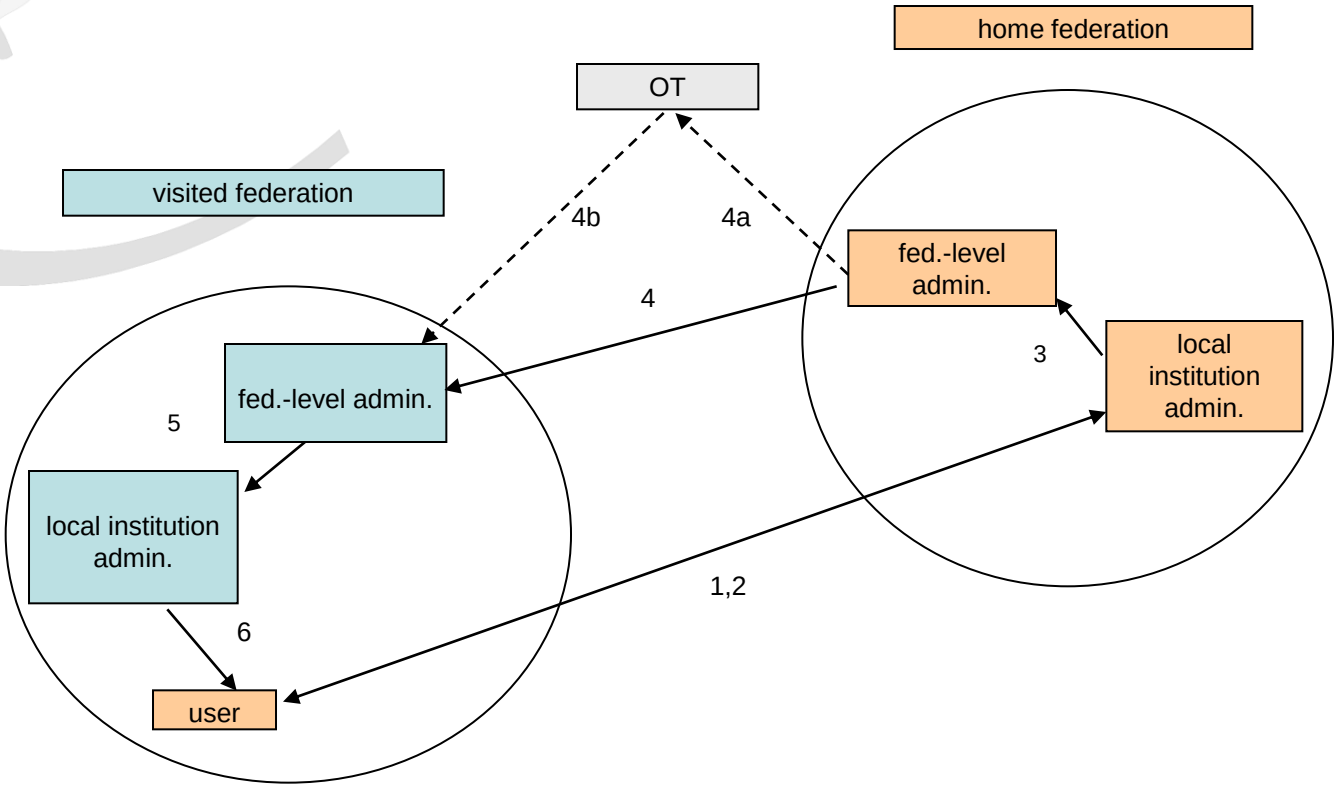
- **globalna usluga**
  - globalna koordinacija – GeGC
  - 60+ zemalja na 6 kontinenata
- **europska eduroam usluga**
  - u okviru GEANT3/GEANT3+ projekta
  - 43 zemlje; Srce koordinator
- **distribuirana organizacija**
  - po federalnom modelu
- **uslugu čine:**
  - **tehnološka infrastruktura**
    - RADIUS infrastruktura, aktivni mrežni elementi
  - **pravila za sve učesnike (*Policy*)**
    - aktualna verzija 2.0
    - https://www.eduroam.org/index.php?p=docs
  - **servisi za podršku korisnicima**
    - informacije o radu sustava i pomoć pri uporabi
    - nadzor, dijagnostika i mjerenje

Međunarodna eduroam infrastruktura

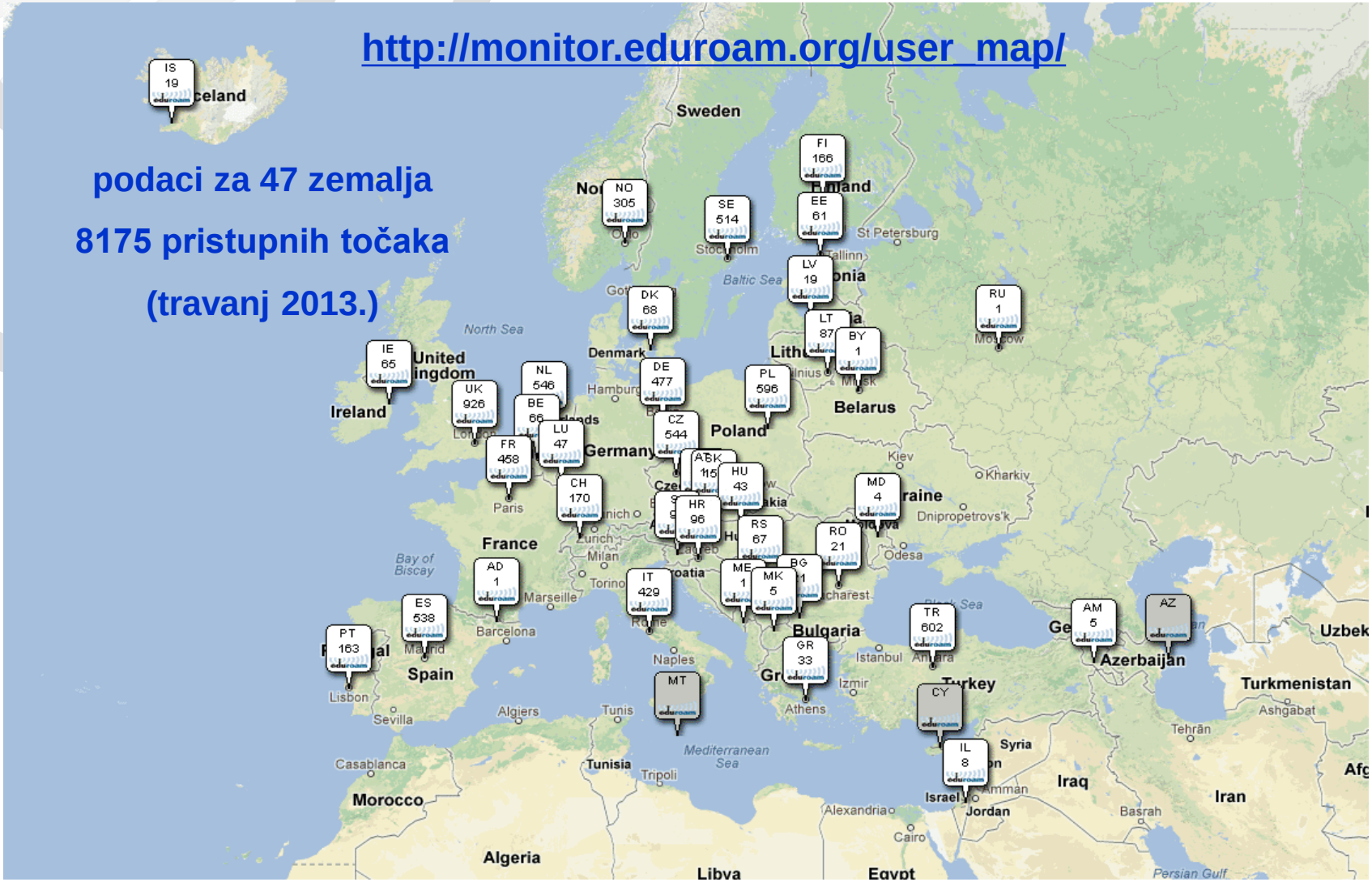


Kategorije korisnika

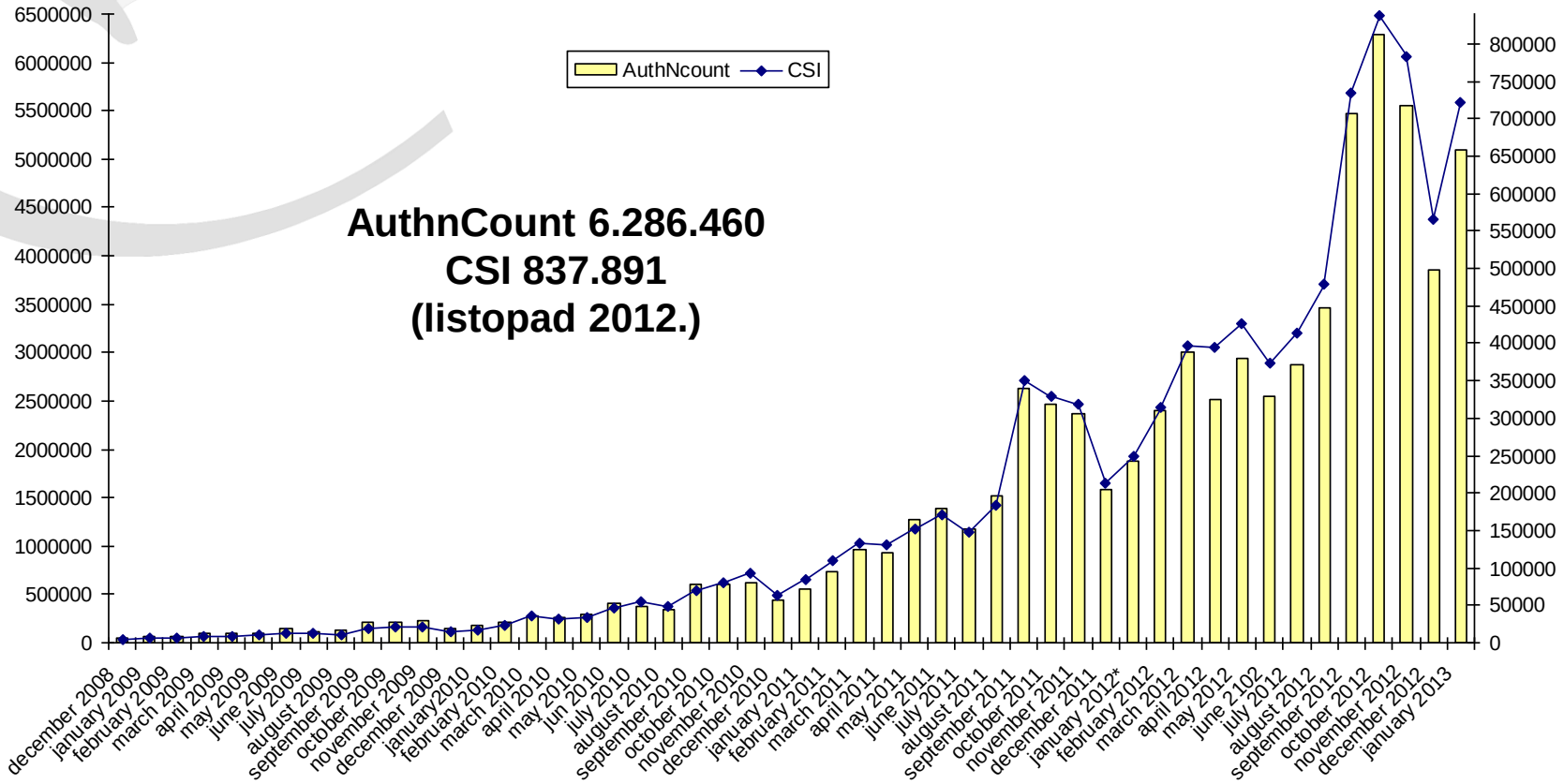
Podrška korisnicima (međunarodni model)



Gdje se može koristiti eduroam?

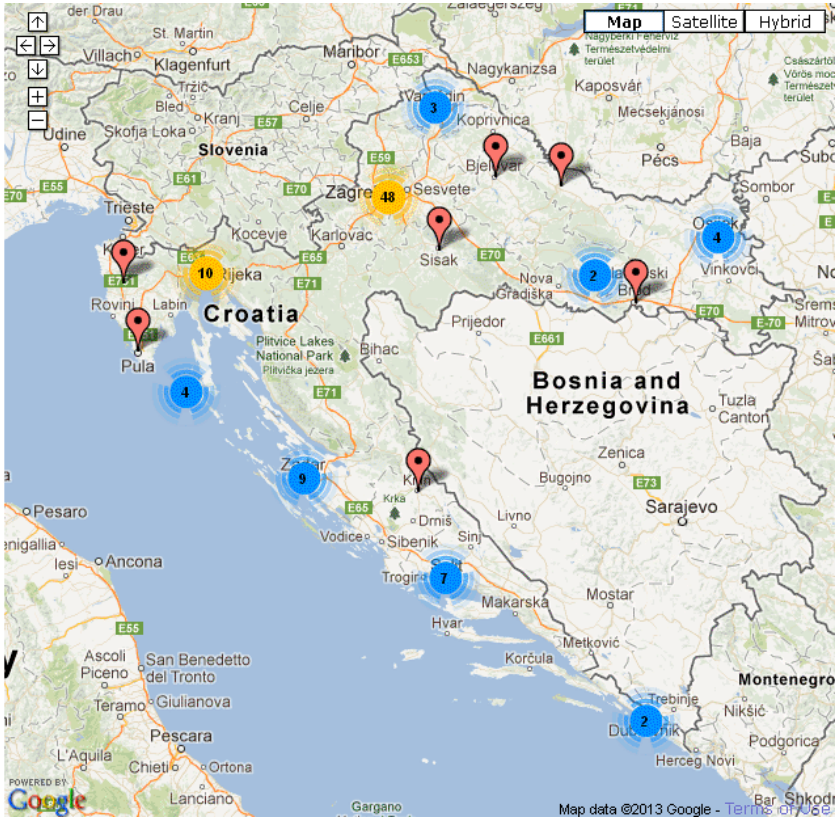


Koliko se eduroam koristi?
(međunarodni promet)



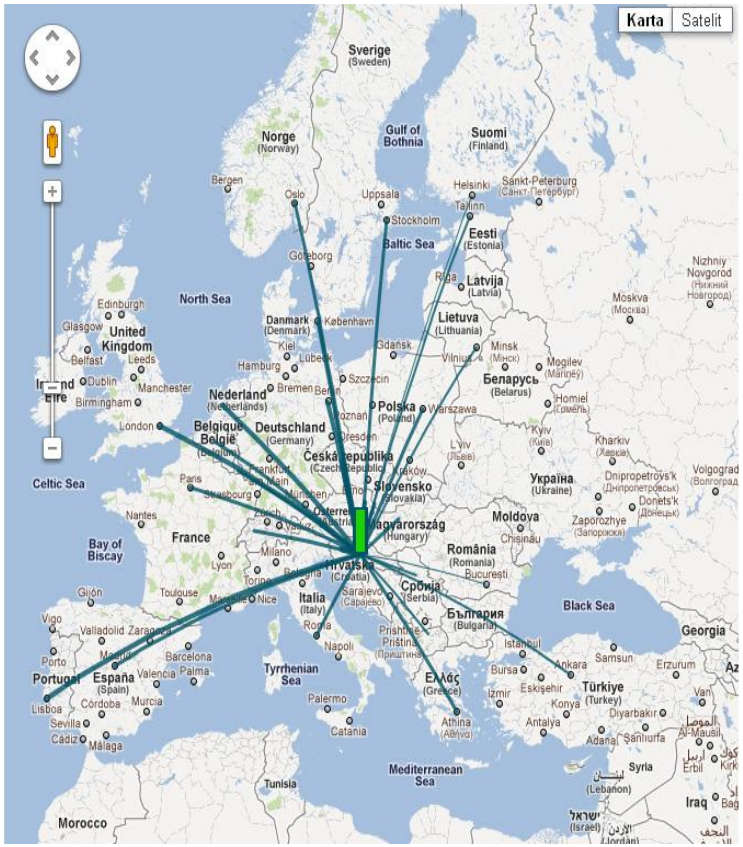
eduroam.hr

- http://www.eduroam.hr
- **elektronički identitet u sustavu AAI@EduHr ≡ mogućnost uporabe eduroam usluge**
- **usluga dostupna (travanj 2013.)**
  - u 20 mjesta/gradova
  - na 96 lokacija
  - i u žičanoj inačici (StuDOM)
- Srce (AAI@EduHr) je uključeno u aktivnosti vezane uz eduroam od samog začetka (2003. godine)



eduroam.hr – međunarodni promet

- http://monitor.eduroam.org/f-ticks/
- (europski) alat za praćenje prometa utemeljen na syslogu
- unapređenja i interna primjena u AAI@EduHr / eduroam.hr tijekom 2013. godine



Kako početi koristiti eduroam?

- potrebno je:
  - posjedovati elektronički identitet u sustavu AAI@EduHr
  - iskonfigurirati uređaj (računalo, pametni telefon, ...) na odgovarajući način
- usluga je za krajnjeg korisnika besplatna bez obzira na točku pristupa (bilo gdje u Hrvatskoj, Europi i svijetu)
- mogući izazov:
  - konfiguriranje uređaja

eduroam installer

- http://installer.eduroam.hr/
- omogućuje krajnjim korisnicima jednostavno i pouzdano konfiguriranje (većine) uređaja
- posebno prilagođen svakoj od matičnih ustanova
  - podatke za aktivaciju treba putem weba dostaviti administrator/sistemac matične ustanove:
    - kratki naziv
    - logo
    - URL adresu web-sjedišta
    - ime RADIUS servera (CN polje u certifikatu)
    - (Root) certfikat poslužitelja (u DER formatu)
  - provjerite popis: http://www.eduroam.hr/installer_status.php
- CAT - globalni alat: https://cat.eduroam.org

Uspostava i održavanje eduroam pristupne točke

(eduroam za davatelje usluge)

Pretpostavke pri uspostavi eduroam pristupne točke

- funkcionalna bežična mreža
- pristupni uređaji podržavaju 802.1x
- korisnici posjeduju odgovarajuće korisničke podatke za autentikaciju
- dostupan je RADIUS server za potrebe autentikacije i pohrane logova

RADIUS poslužitelj

- konfiguracija ovisi o tipu pristupne točke:
  - davatelj pristupa
  - matična ustanova i davatelj pristupa istodobno
- potrebna je ispravna *proxy-eduroam.conf* datoteka
  - zatražite e-mailom na admin@eduroam.hr
- programskim paketima podržan je FreeRADIUS, no mogu se koristiti i druge inačice RADIUS programske podrške

RADIUS konfiguracija – davatelji pristupa

- svi zahtjevi se prosljeđuju (*proxying*)
- svaki davatelj pristupa ima svoju oznaku
- bilježe se logovi (RADIUS *accounting*)
- pristupni uređaji imaju svoj zapis u *clients.conf* datoteci

RADIUS konfiguracija – matična ustanova i davatelj pristupa istodobno

- “lokalni” identiteti se autenticiraju lokalno, a ostali zahtjevi se prosljeđuju (standardna AAI@EduHr konfiguracija)
- svaki davatelj pristupa ima svoju oznaku
- bilježe se logovi (RADIUS *accounting*) i podaci o autentikaciji
- pristupni uređaji imaju svoj zapis u *clients.conf* datoteci

Pristupni uređaji

- različite vrste, različite opcije pri konfiguriranju
- osnovni elementi konfiguracije:
  - SSID – **eduroam** (javno vidljiv)
  - kripto-zaštita bežične mreže – **WPA2** (uobičajno se krije pod nazivom *WPA2 enterprise*)
  - kripto-zaštita bežične komunikacije – **AES**
  - IP adresa lokalnog RADIUS poslužitelja
  - 'secret' iz *clients.conf* datoteke za pristupni uređaj
- ako uređaj podržava podesiti vanjsko logiranje
- moguće je imati više od jednog SSID-a na istom uređaju

Primjer konfiguracije

- Linksys WRT54GS
- FreeRADIUS

WLAN (eduroam) nadzorna sonda

(kako nadzirati rad eduroam usluge)

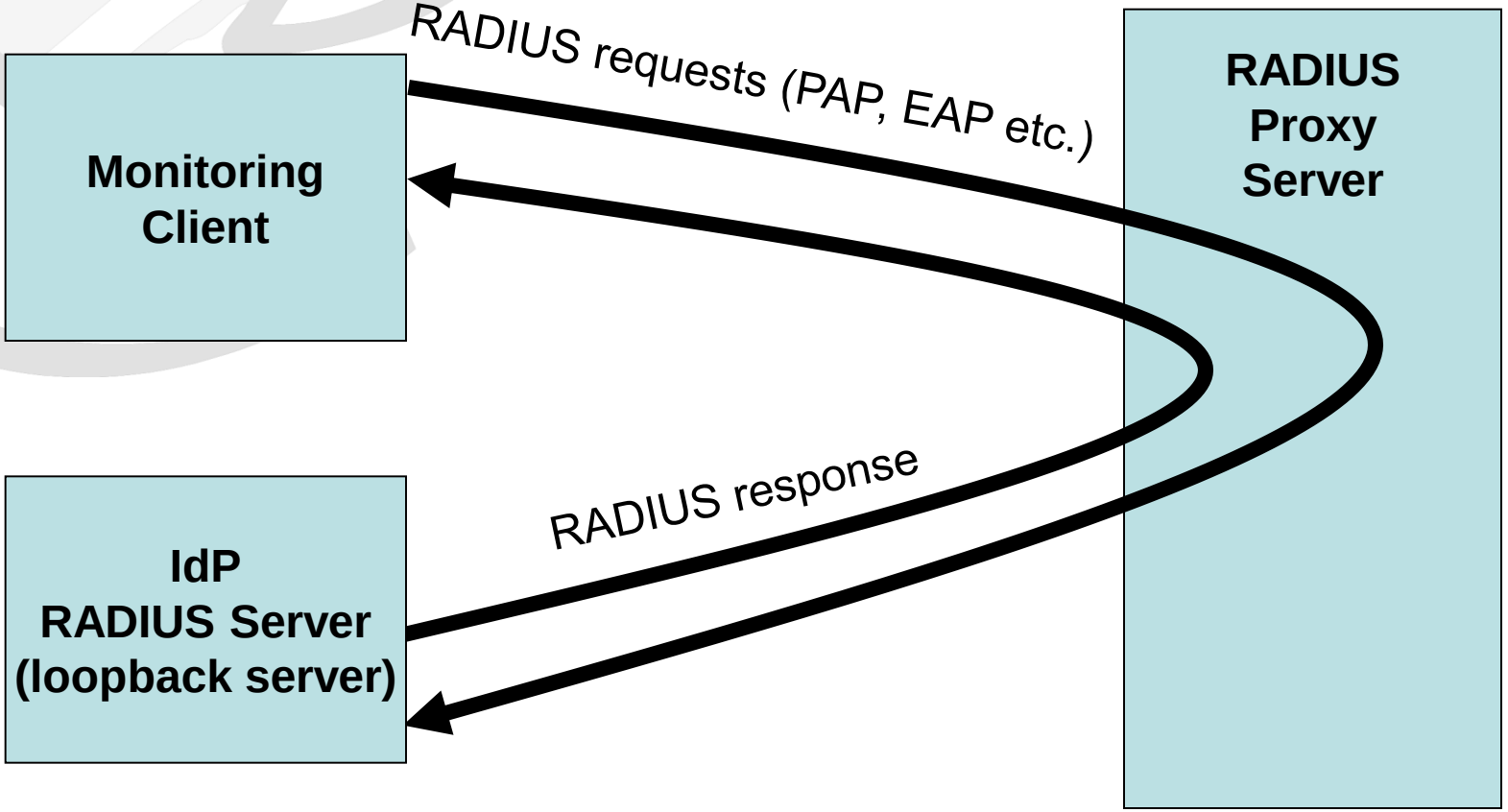
Nadzor eduroam usluge

- Nije dovoljno znati da poslužitelji rade!
- nadzirati se može/treba:
  - poslužitelje/aktivne elemente u sustavu
  - infrastrukturu (put i interakciju između poslužitelja)
  - AA proces (korisničko iskustvo)
- krajnji cilj je potpuni funkcionalni test

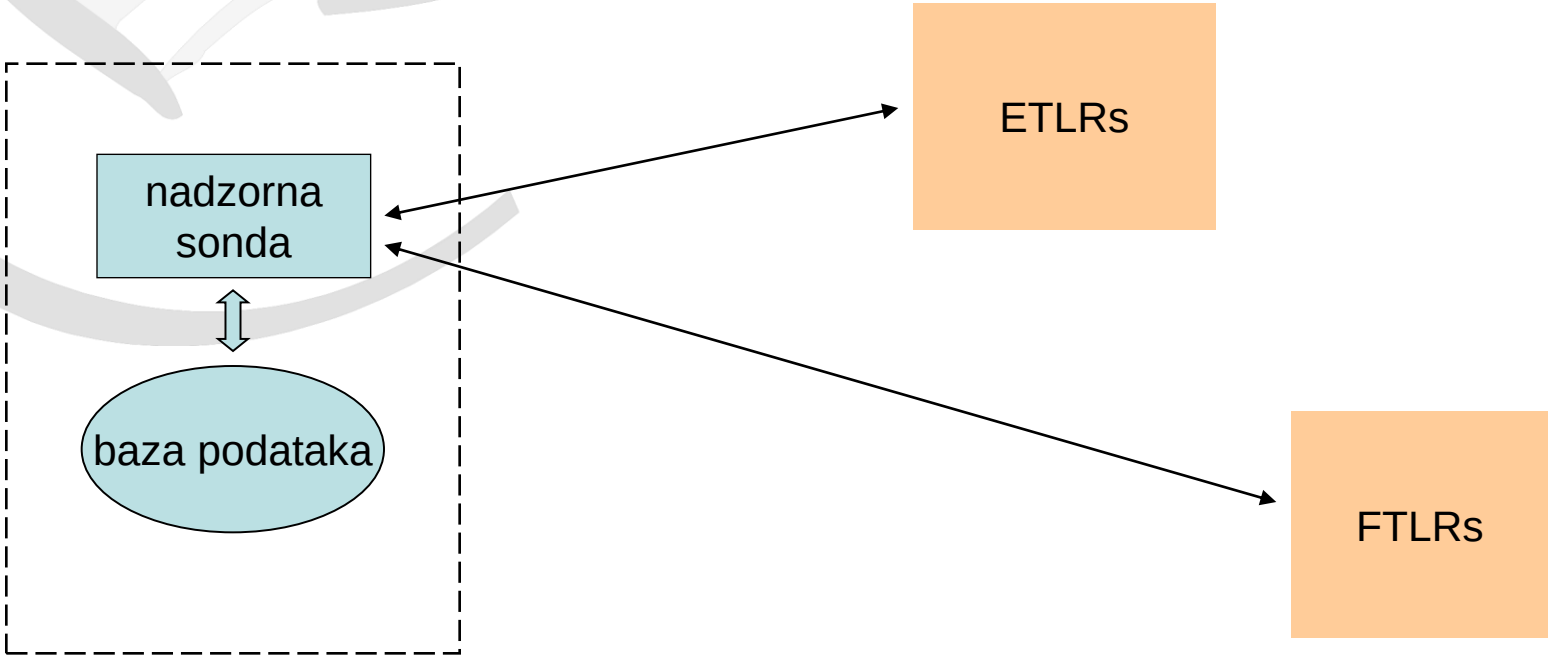
Nadzor eduroam usluge

- http://monitor.eduroam.org
- nadziru se poslužitelji u Europi
- 3 scenarija:
  - nadzor poslužitelja
  - nadzor infrastukture
  - provjera na zahtjev (*testing on demand*)
- nedostaje:
  - "*last mile*" – provjera stanja WLAN-a na koji su korisnik spaja

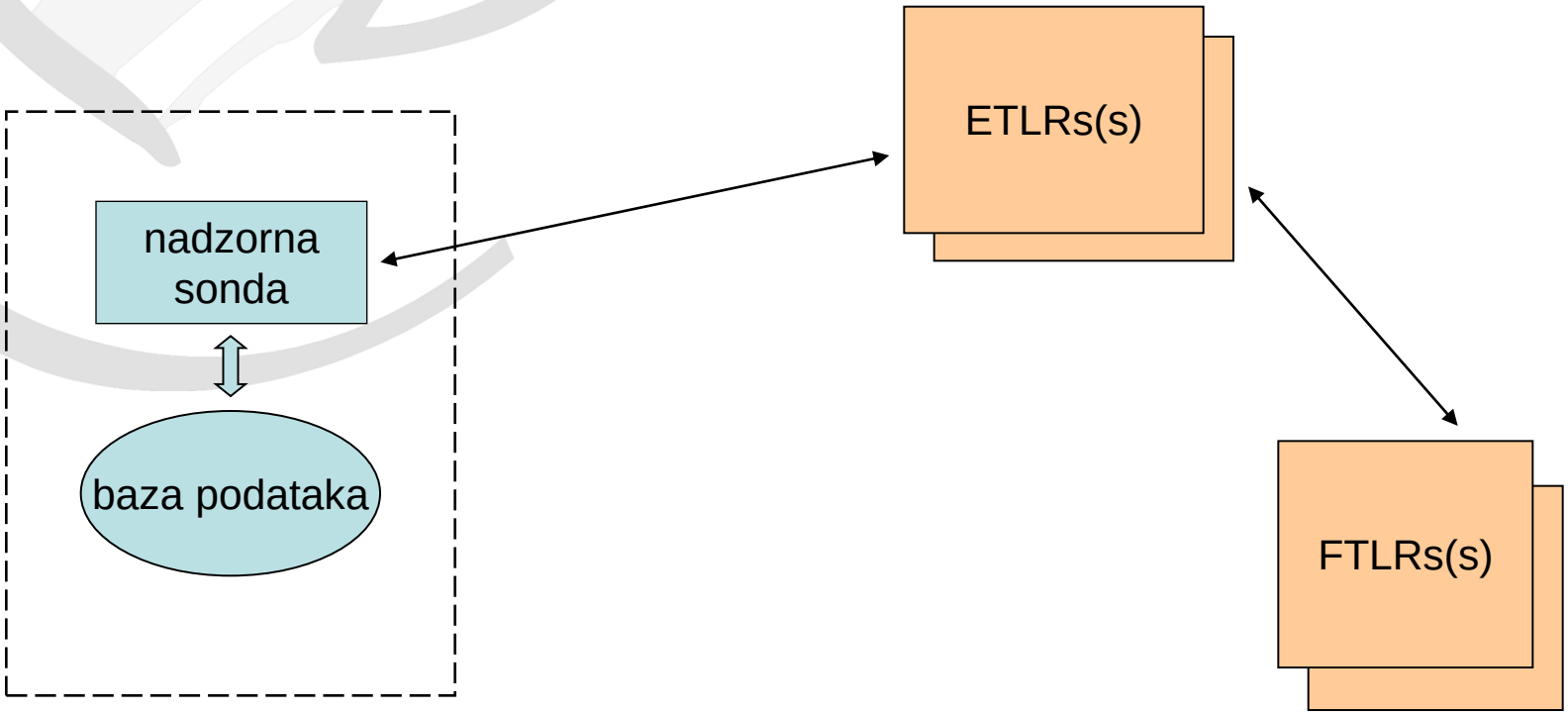
Koncept nadzornog sustava



Nadzor rada poslužitelja



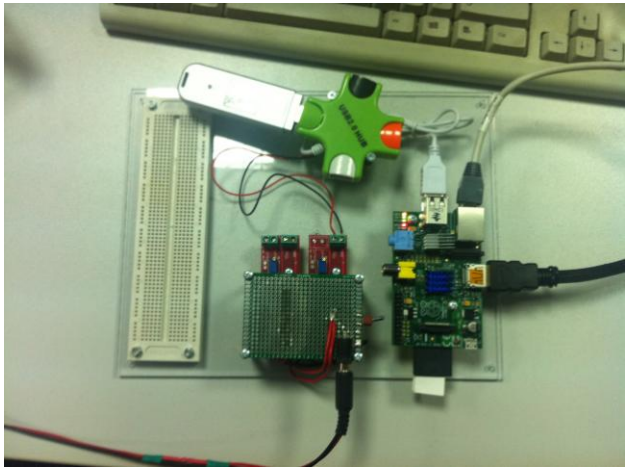
Nadzor rada infrastrukture



Nadzor WLAN-a

- zadatak je napraviti sondu koja će provjeravati stanje WLAN-a / eduroam pristupne točke
- sonda:
  - nadzire dostupne SSID-eve
  - nadzire jačinu/kvalitetu signala
  - nadzire korištene metode autentikacije i kriptiranja
  - testira spajanje na eduroam (autentikacija + provedba akcije)
  - prikuplja podatke koje šalje središnjoj točki radi pohrane i analize
  - ...

Pilot projekt u tijeku



- odabrana platforma
  - Raspberry Pi HW
  - Raspbian Linux
  - Python 2.7.
- trenutni rezultati
  - skeniranje bežičnih signala / SSID-eva
  - rezultati se šalju (korištenjem syslog-a) u bazu podataka za nadzor
  - primjeri mogućih ispisa prikupljenih podataka:
    - http://www.eduroam.hr/sensornet/index.php
    - http://www.eduroam.hr/sensornet/index1.php
    - http://www.eduroam.hr/sensornet/index2.php

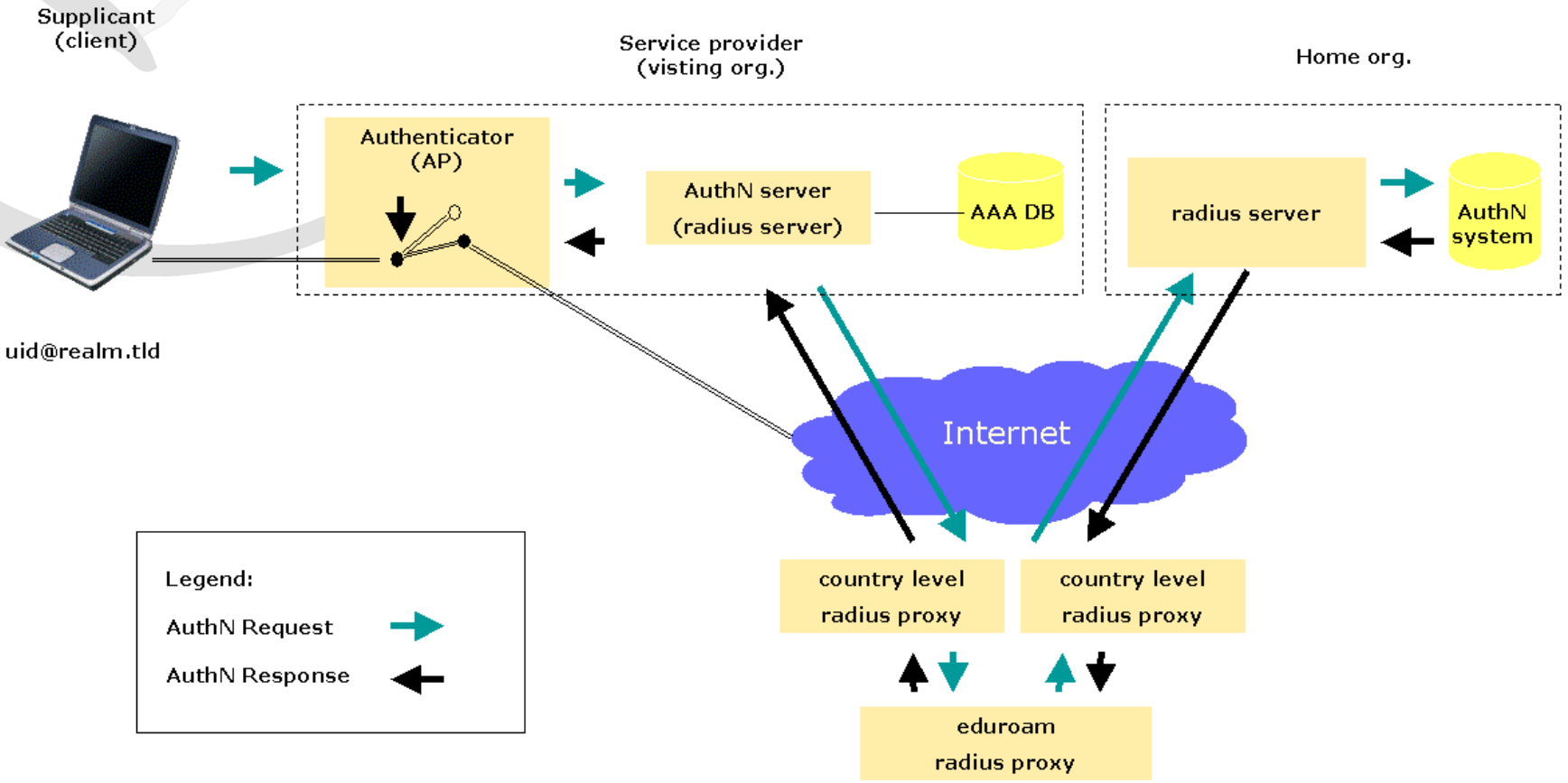
eduroam.hr sonda

Tražimo dobrovoljce koji bi dozvolili instalaciju sonde u svojoj (WLAN) mreži!

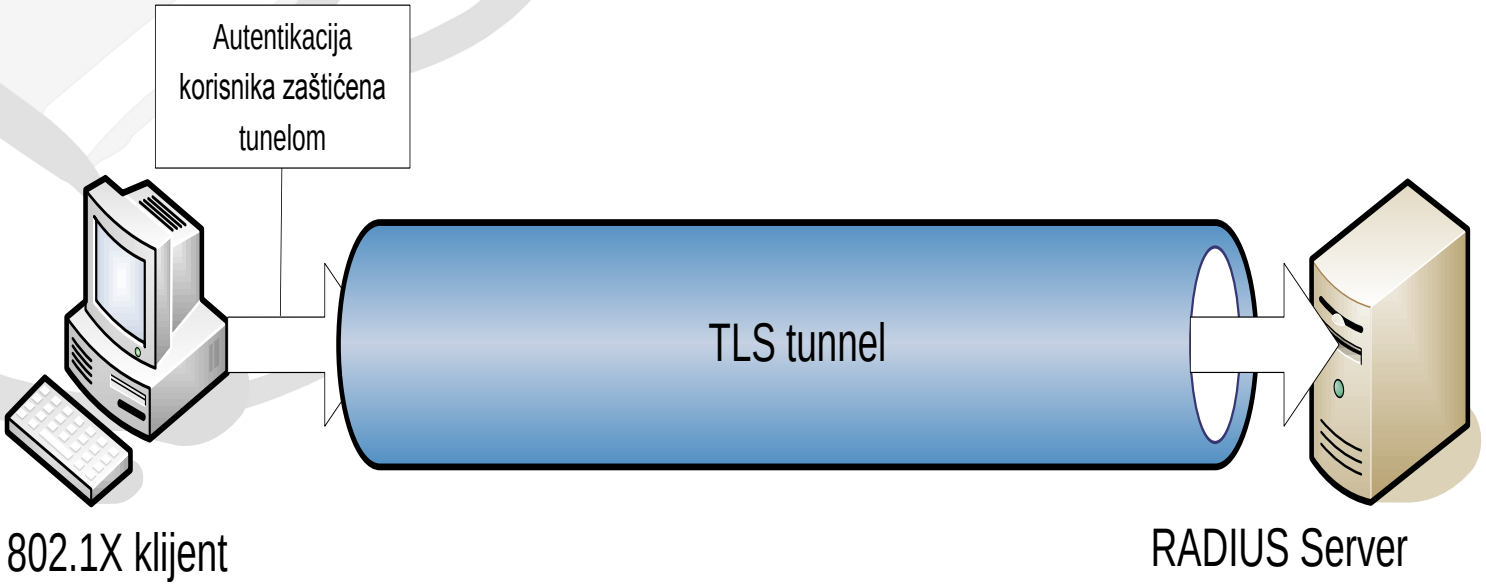
O sigurnosti eduroam usluge

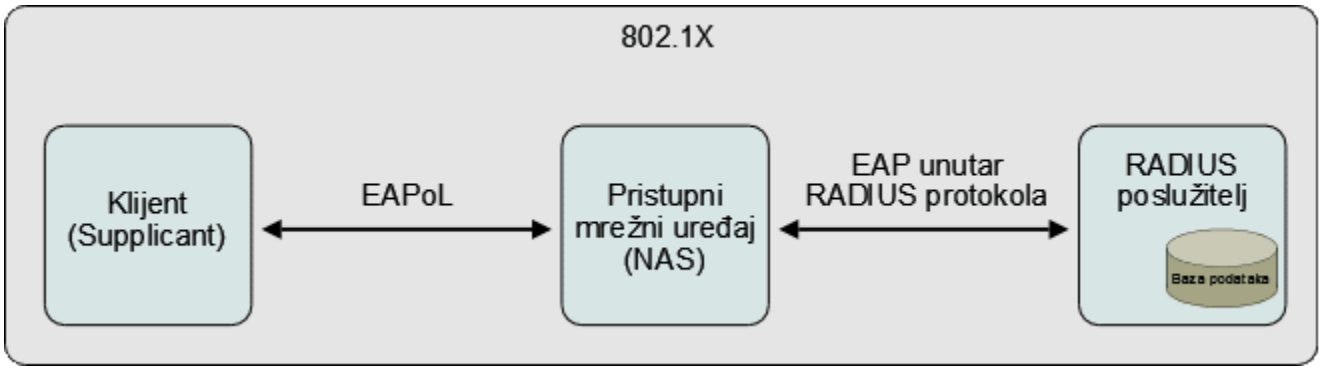
(Zašto je važno koristiti installer?)

eduroam™

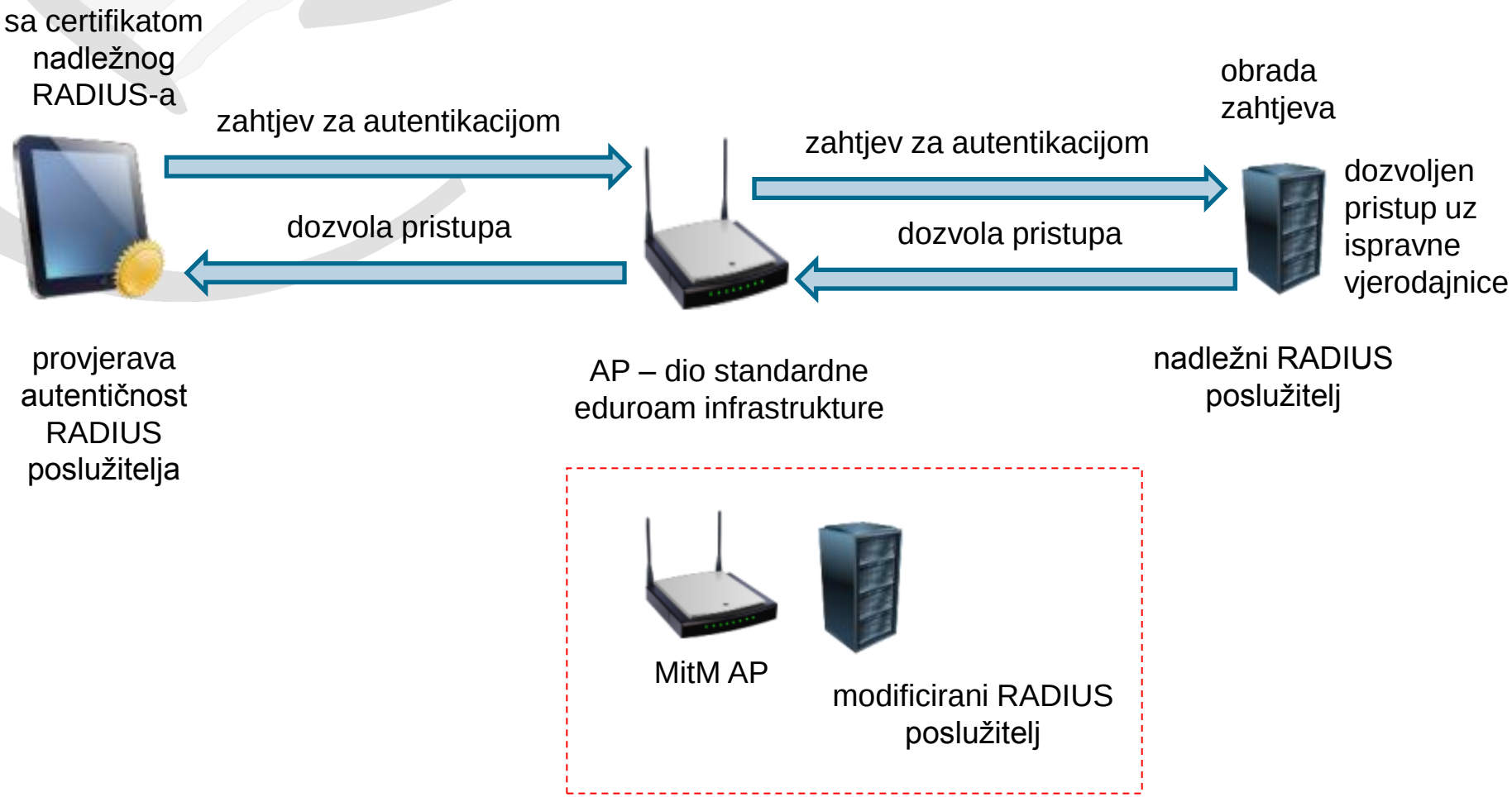

Supplicant
(client)
Service provider
(visting org.)
Home org.
Authenticator
(AP)
AuthN server
(radius server)
AAA DB
radius server
AuthN
system
uid@realm.tld
Internet
country level
radius proxy
country level
radius proxy
eduroam
radius proxy
Legend:
AuthN Request
AuthN Response

EAP tunel

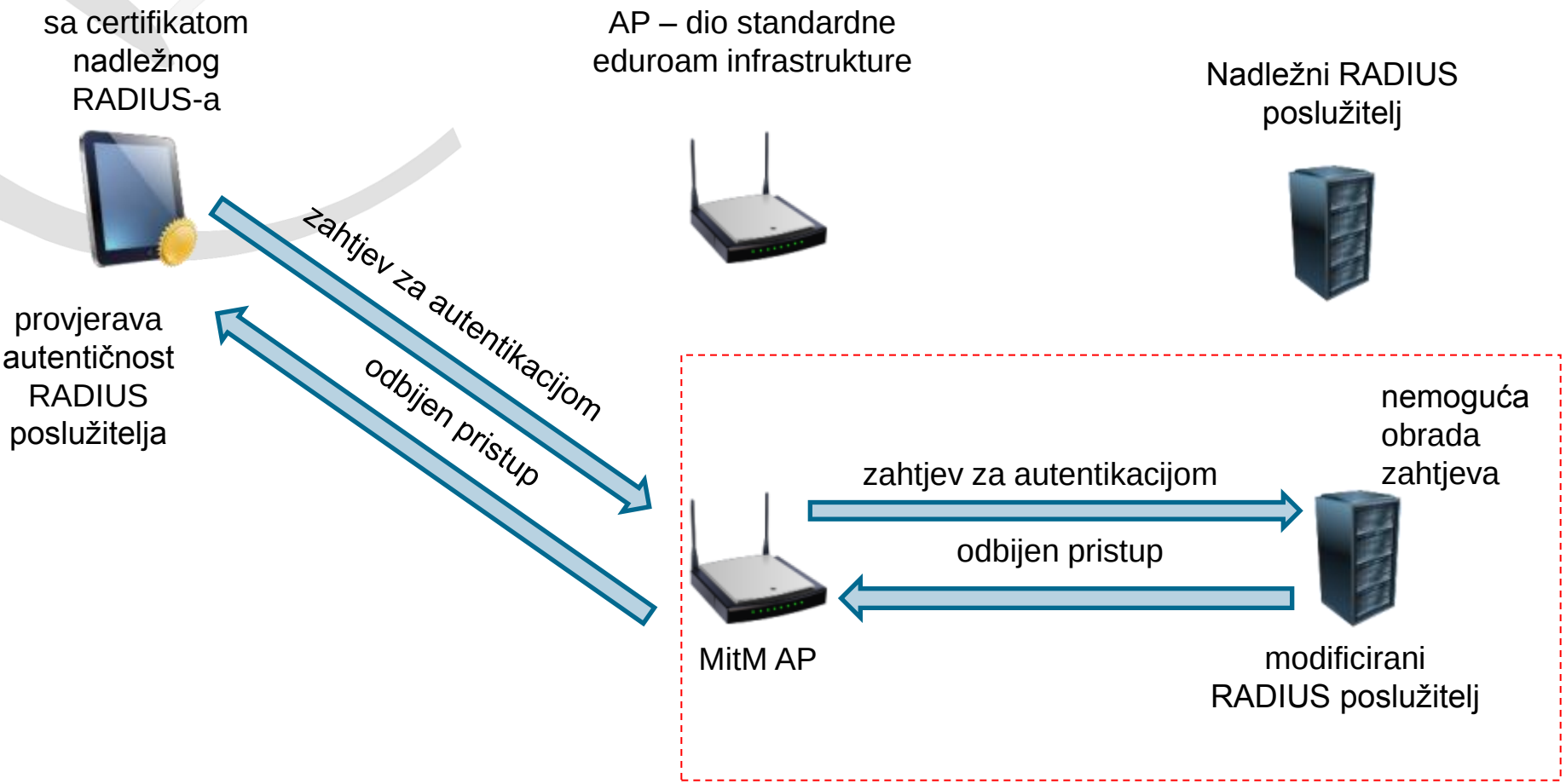

Autentikacija korisnika zaštićena tunelom
TLS tunnel
802.1X klijent
RADIUS Server


802.1X
Klijent (Supplicant)
EAPoL
Pristupni mrežni uređaj (NAS)
EAP unutar RADIUS protokola
RADIUS poslužitelj
Baza podataka

Autentikacija uz korištenje certifikata (putem nadležnog poslužitelja)



Autentikacija uz korištenje certifikata (putem MitM poslužitelja)



Autentikacija bez korištenje certifikata (putem MitM poslužitelja)

AP – dio standardne eduroam infrastrukture

Nadležni RADIUS poslužitelj

bez certifikata nadležnog RADIUS-a

zahtjev za autentikacijom

dozvola pristupa

pristupa mreži, dajući vjerodajnice nepoznatom poslužitelju

MitM AP

zahtjev za autentikacijom

dozvola pristupa

obrađuje zahtjev

raspolaže vjerodajnicama

modificirani RADIUS poslužitelj

Zašto je važno korisititi installer?

- installer omogućuje ispravno konfiguriranje klijenata uz postavljanje provjere certifikata
- svakako tražite od svojih korisnika da obavezno koriste installer i ne mijenjaju postavku koja se odnosi na provjeru certifikata matične ustanove

- u suprotnom se korisnik izlaže MitM napadu ...

... live demo

http://www.eduroam.hr/

admin@eduroam.hr