Prezentacija za administratore eduroam usluge

tjedan 2014.

Autori:
Dario Šafar, Dubravko Penezić, Dubravka Orešković, Miroslav Milinović
admin@eduroam.hr

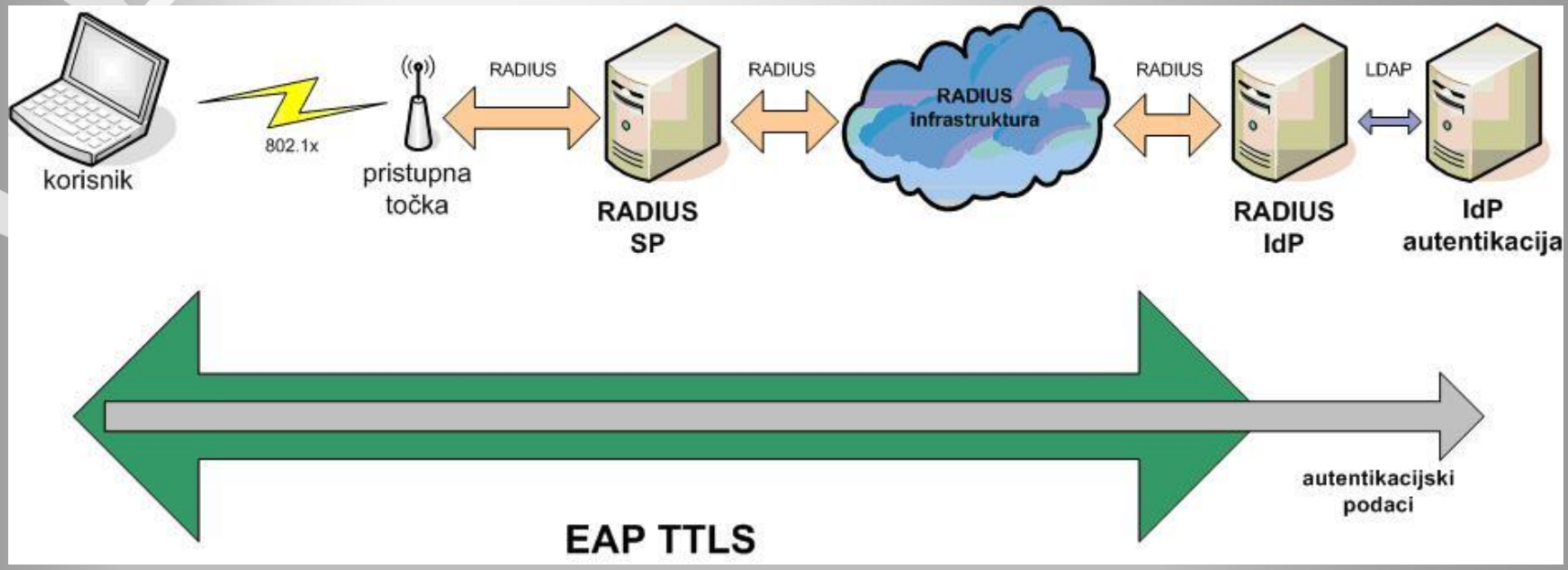
Pregled tema

- Certifikati u sustavu autentikacije eduroam korisnika
- RADIUS atribut CUI
- Certificiranje (auditing) davatelja usluge eduroam
- Statistike i nadzor

Certifikati u sustavu autentikacije eduroam korisnika

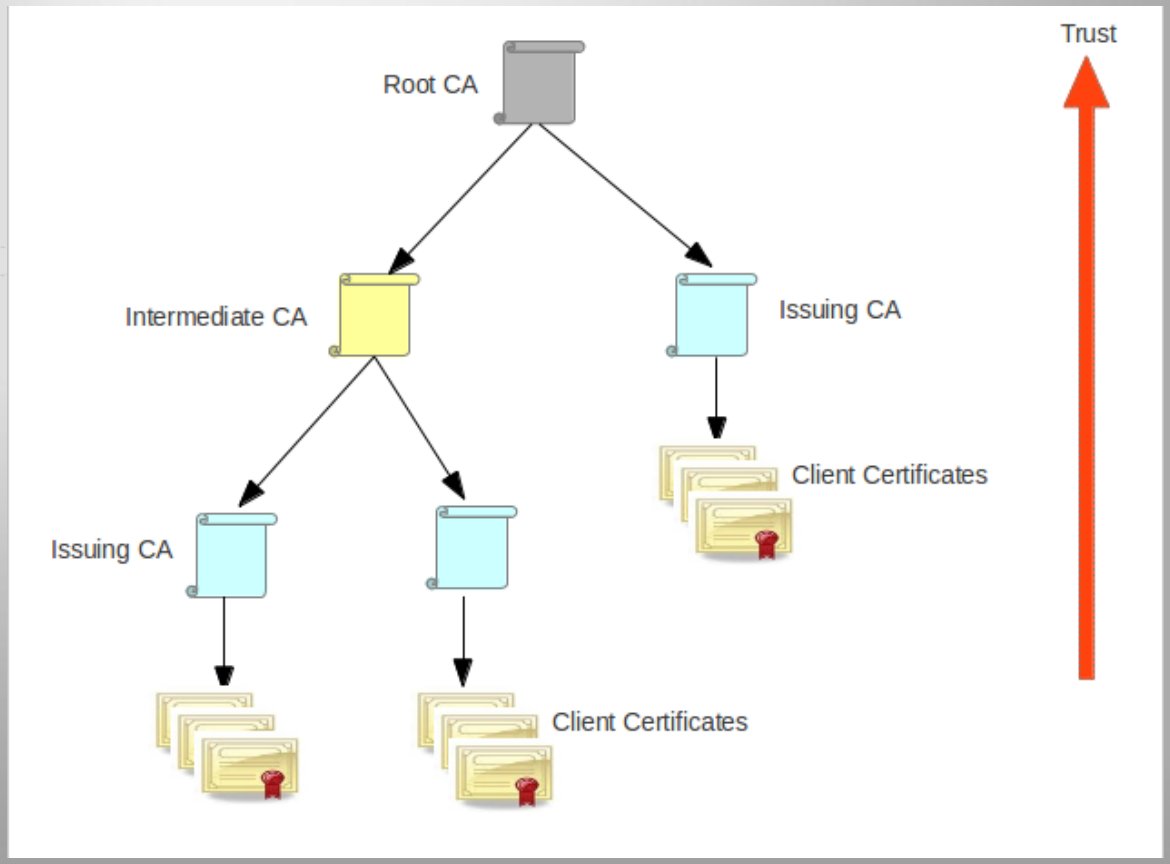
- Zaštita korisničkih podataka pri autentikaciji
- Uspostava TLS tunela
- Visoka razina zaštite

eduroam – EAP TTLS/PAP



- Root CA certifikat
- Serverski certifikat

Hijerarhija certifikata



Root CA

- Vršni autoritet / vršni certifikat
- Autoritet kojem svi vjeruju
- Provjera izdanih certifikata se obavlja putem javnog ključa Root CA

Serverski certifikat

- Certifikat koji je izdan i potvrđen s (nekim) Root CA certifikatom
- Koristi se za predstavljanje servera pri uspostavi sigurne komunikacije (SSL/TTLS/TLS)
- Sadrži CN polje koje se (dodatno) koristi za provjeru jedinstvenosti certifikata

Izrada Root CA certifikata (model samopotpisivanja)

- Jednom u 10 godina
- Mijenja se kada istekne ili sumnjamo u njegovu tajnost
- Skriptom iz komandne linije
  - shell> ./cert-admin -newca
- Certifikat - fRcerts/cacert.der

Izrada serverskog certifikata (model samopotpisivanja)

- Jednom u 10 godina
- Mijenja se po potrebi, no to ne utiče na krajnje korisnike
- Prilikom instalacije (RADIUS) paketa, odnosno njegove reinstalacije
- Postoji i skripta koja se može pokrenuti iz komadne linije
- Privatni ključ: fRcerts/private/server-key.pem
- Javni ključ: fRcerts/server-cert.pem

Održavanje certifikata (model samopotpisivanja)

- Root CA certifikat treba mijenjati u krajnjoj nuždi
  - obavijest korisnicima
  - promjena podataka u installeru
  - reinstalacija eduroam profila na svim korisničkim uređajima
- Serverski certifikat se može mijenjati po potrebi
- Upute za održavanje:
  - http://developer.aaiedu.hr/faq/freeradius-certs.html
  - http://developer.aaiedu.hr/faq/22.html

Podaci za komadno-linijsku skriptu

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

CUI – Chargeable User Identity

- RADIUS atribut
- Definiran u RFC 4372
- Jedinstvena nepromjenjiva oznaka korisnika na nivou pojedinog davatelja pristupa
- Ne sadrži osobne podatke o korisniku

Razlozi za implementaciju

- Jedinstvenost na nivou davatelja usluge
- Omogućuje (efikasni) black-listing
- Depersonalizirana korisnička oznaka

Način generiranja

- Dvije strane u procesu:
  - Davatelj usluge traži CUI
  - Davatelj identiteta izdaje CUI za uspješno autenticiranog korisnika
- Dva RADIUS atributa:
  - ON (Operator-Name) – jedinstvena oznaka davatelja usluge
  - CUI (Chargeable-User-Identity) – jedinstvena oznaka korisnika

Opis procesa (1)

- RADIUS poslužitelj davatelja usluge generira zahtjev za autentikacijom pri čemu taj zahtjev sadrži RADIUS atribute
  - Operator-Name (vrijednost dodjeljuje kordinator)
  - Chargeable-User-Identity s vrijednošću NULL

Opis procesa generiranja (2)

- RADIUS poslužitelj davatelja identiteta na autentikacijski zahtjev odgovara
  - Autentikacija je neuspješna – standardni REJECT
  - Autentikacija je uspješna – standardni ACCEPT uz dodatak CUI atributa čija vrijednost se generira kao MD5 hash od vrijednosti atributa Operator-Name, stvarne korisničke oznake i slučajne vrijednosti (*salt*)
- RADIUS poslužitelj davatelja usluge dohvaća vrijednost CUI atributa i po potrebi obavlja autorizaciju.

Način korištenja

- CUI atribut je obavezan u RH
  (ali ne svuda u svijetu)
- Koristi se pri autorizaciji (black-listing) umjesto User-Name atributa
- Black listing rutinu ne treba mijenjati

Certificiranje davatelja usluge eduroam

- Jedanput godišnje u sklopu certificiranja davatelja usluga u sustavu AAI@EduHr
- Potrebno je zadovoljiti određen broj normi
- Kroz neobavezne norme uvode se nova tehnološka rješenja
- Registar resursa: http://www.aaiedu.hr/aairr

Aktualne norme pri certificiranju davatelja eduroam usluge (1)

- Formalno članstvo
- Poštivanje Pravilnika o ustroju AAI@EduHr
- Zapis u registru resursa:
  - naziv
  - URL adresa
  - opis
  - administrator

Aktualne norme pri certificiranju davatelja eduroam usluge (2)

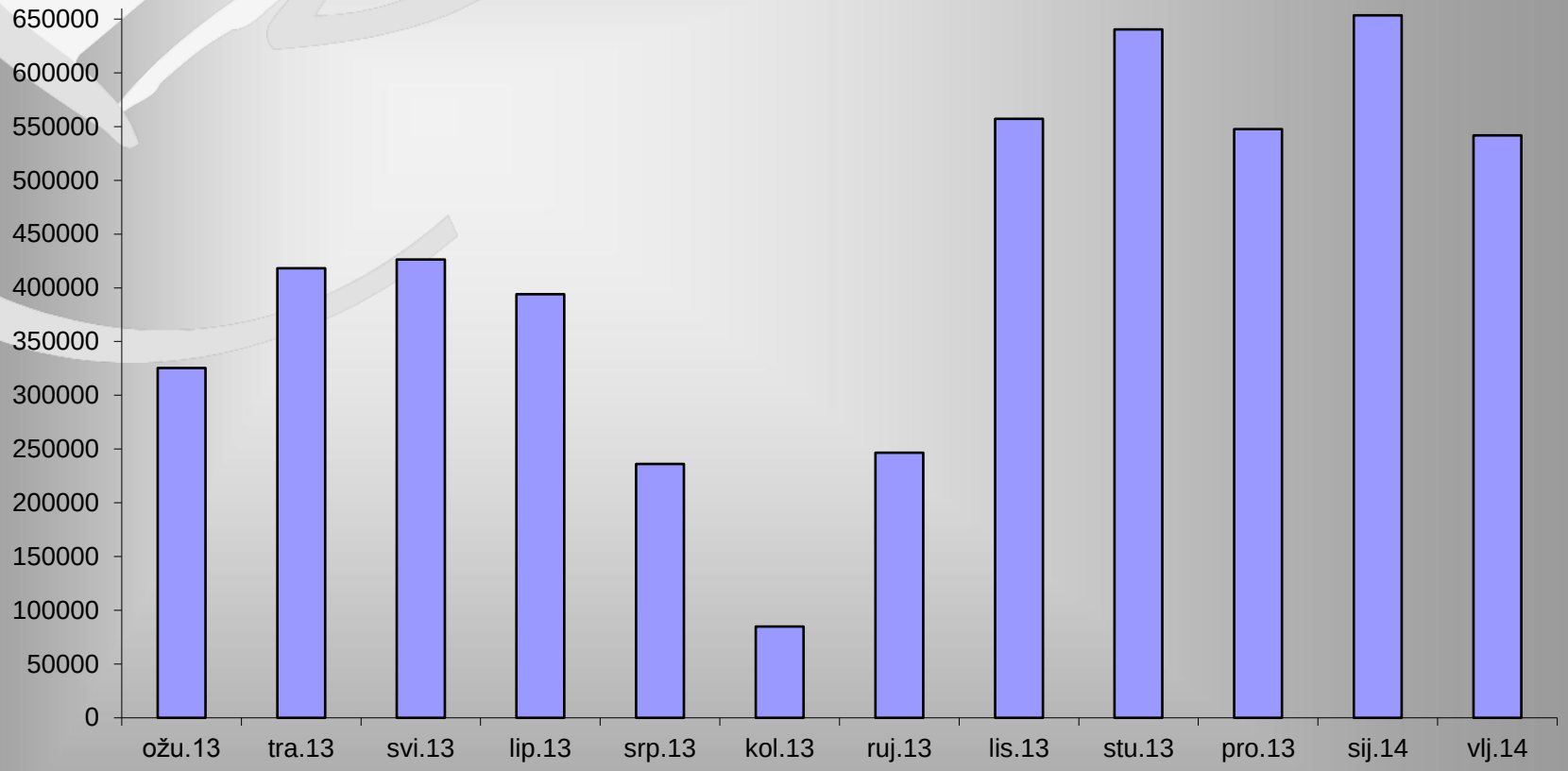
- Korišteni protokol - RADIUS
- RADIUS poslužitelj usluge ispravno prosljeđuje upite središnjim poslužiteljima koristeći EAP protokol
- RADIUS poslužitelj usluge ne modificira atribute koje prosljeđuje središnjim poslužiteljima
- Isporuka atributa *OperatorName*

Koliko se koristi eduroam?

- > 11.000 pristupnih točaka u svijetu (>9300 u 44 zemlje u Europi)
- 160 pristupnih točaka u RH (46 mjesta)
- statistike pristupa:
  - pratimo interinstitucionalne (stvarni roaming)
  - u 2013. u RH je zabilježen 76% porast broja uspješnih autentikacija u odnosu na 2012. godinu
  - na međunarodnoj razini: http://monitor.eduroam.org/f-ticks

Koliko se eduroam koristi? (1)

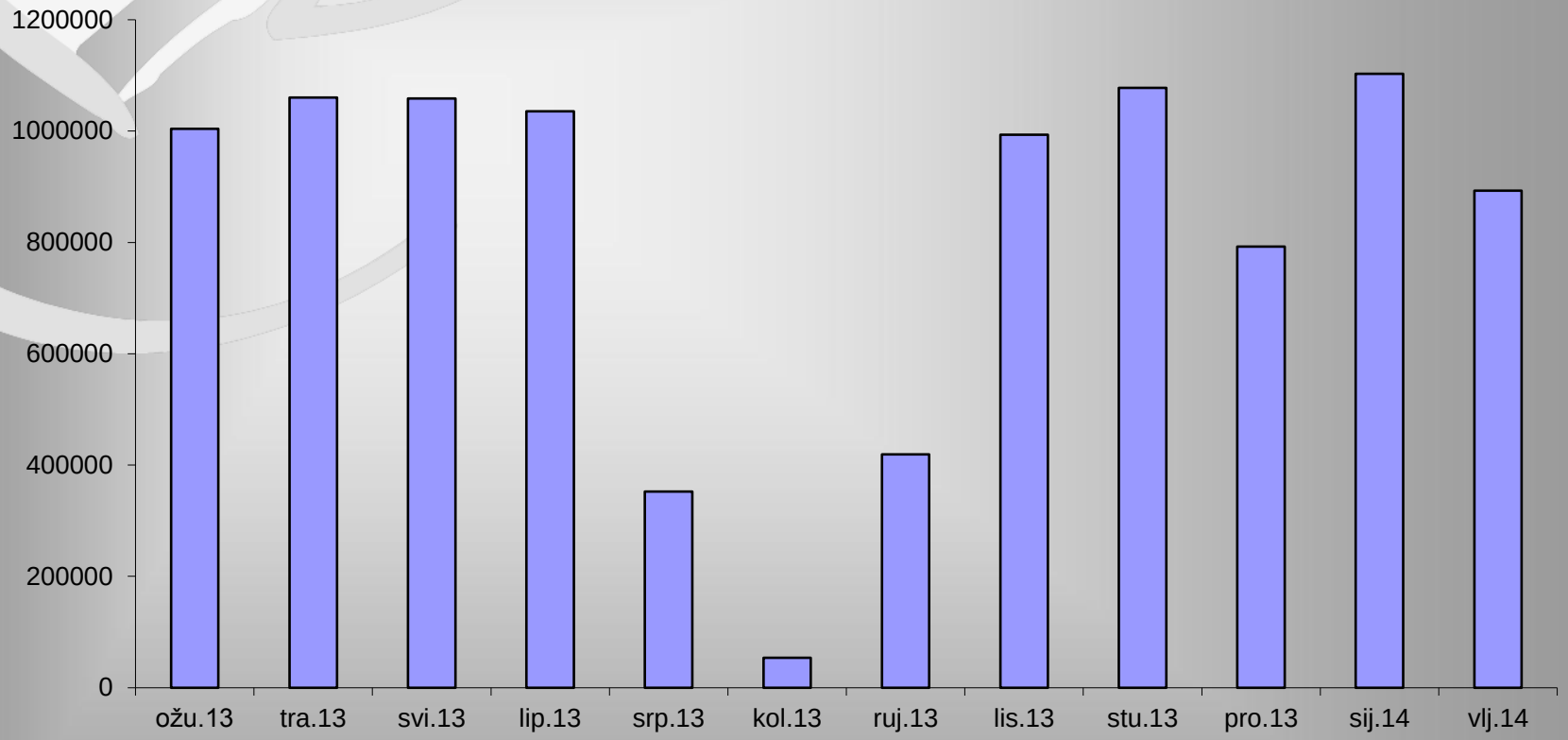
(Interinstitucionalni roaming)



Kretanje broja uspješnih prijava bežičnim putem (*wireless eduroam*)

Koliko se eduroam koristi? (2)

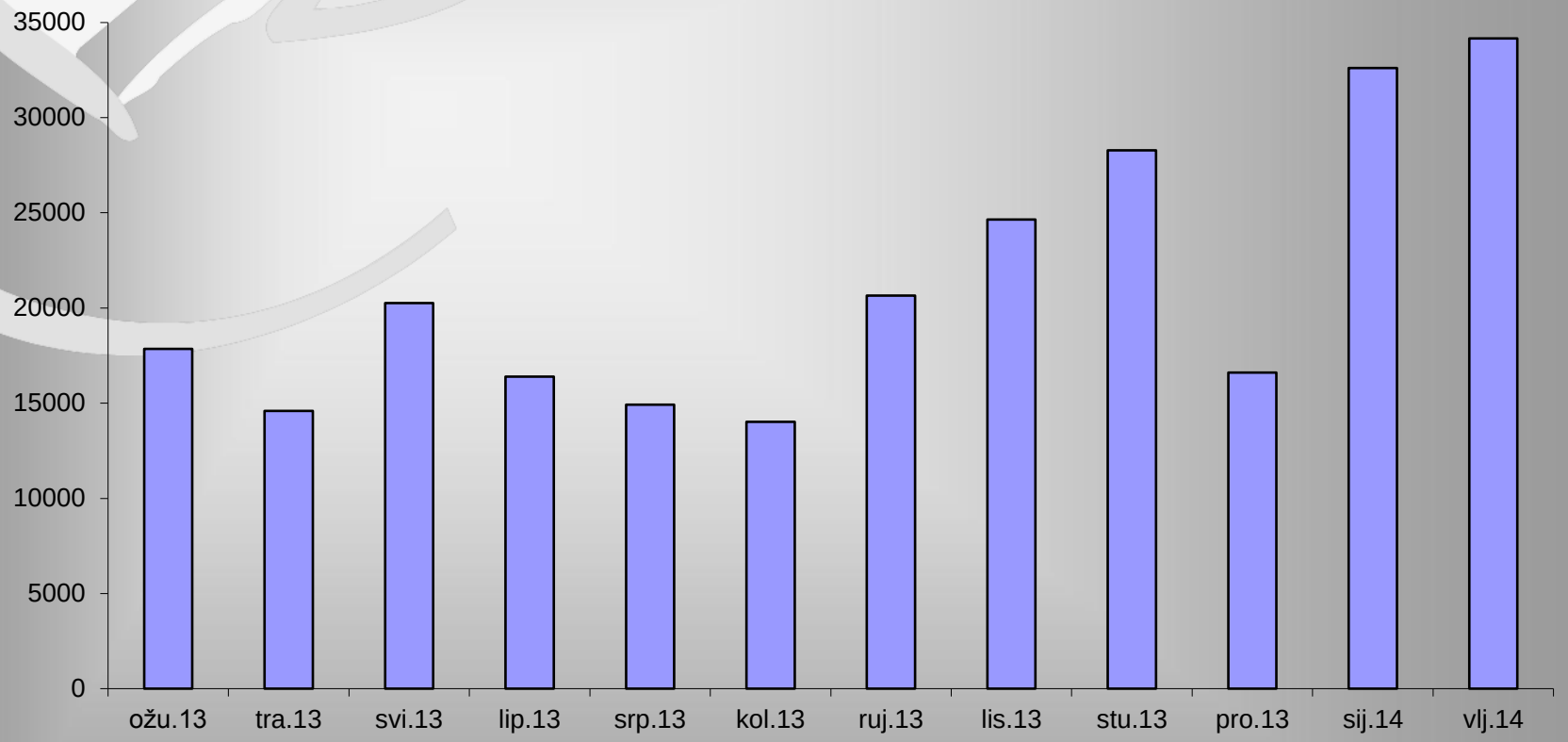
(Interinstitucionalni roaming)



Kretanje broja uspješnih prijava žičanim putem (*wired eduroam*)

Koliko se eduroam koristi? (1)

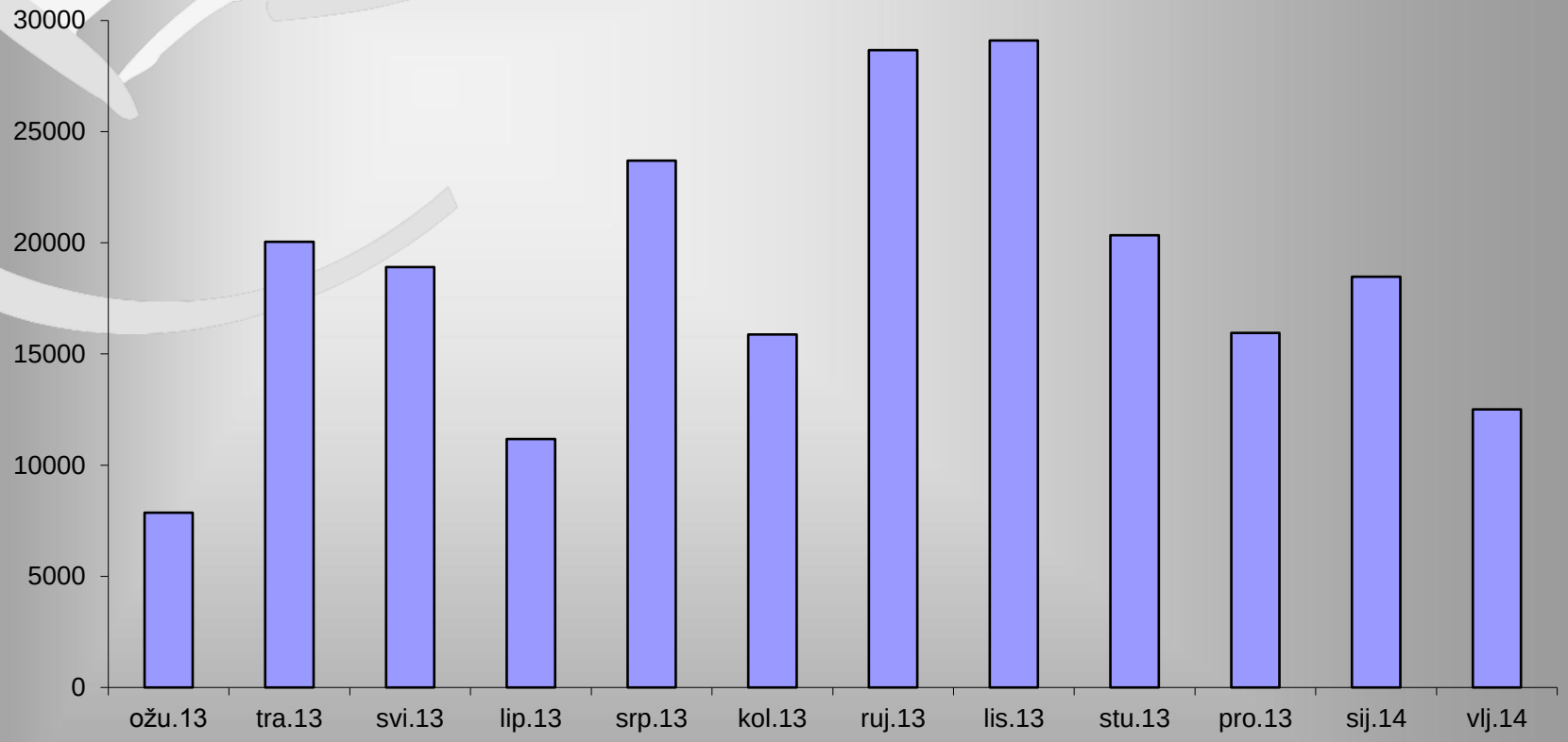
(Međunarodni roaming)



Kretanje broja uspješnih prijava hrvatskih korisnika u inozemstvu

Koliko se eduroam koristi? (2)

(Međunarodni roaming)



Kretanje broja uspješnih prijava inozemnih korisnika u Hrvatskoj

Dodatne informacije

- eduroam u Republici Hrvatskoj http://www.eduroam.hr
- eduroam installer: http://installer.eduroam.hr
- globalna usluga: http://www.eduroam.org

Pitanja i prijedlozi

http://www.eduroam.hr

admin@eduroam.hr