Centar Informacijske Sigurnosti

Eduroam

CIS-DOC-2011-02-005

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. UVOD 4

2. ŠTO JE EDUROAM 5

3. NAČIN RADA EDUROAMA 6

3.1. TEHNOLOGIJE PRIMIJENJENE U EDUROAM SERVISU 6

3.1.1. IEEE 802.1X 7

3.1.2. RADIUS poslužitelji 9

3.1.3. Mrežna infrastruktura i korisnički program za pristup eduroam servisu 10

3.2. REALIZACIJA EDUROAM SERVISA 10

3.2.1. RADIUS poslužitelji konfederacijskog nivoa 10

3.2.2. RADIUS poslužitelji federacijskog nivoa 11

3.2.3. Matični i udaljeni institucionalni RADIUS poslužitelji 11

3.3. PRINCIP RADA EDUROAMA 11

4. EDUROAM U HRVATSKOJ - AAI@EDUHR 14

4.1. IMENIČKE SHEME I UPRAVLJANJE ELEKTRONIČKIM IDENTITETIMA 14

4.2. AAI@EDUHR ARHITEKTURA 15

5. AUTENTIKACIJSKI MEHANIZMI U EDUROAMU 16

5.1. EAP AUTENTIKACIJSKI MEHANIZMI U EDUROAMU 17

5.1.1. EAP-TTLS 17

5.1.2. EAP-TTLS/EAP-GTC 18

6. BUDUĆNOST EDUROAMA 19

7. ZAKLJUČAK 20

8. REFERENCE 21

1. Uvod

U novije doba, kada su korisnici Interneta sve više i više mobilni, a podaci koje putem Interneta prenose osjetljiviji, javila se potreba za sigurnim pristupom Internetu s bilo kojeg mjesta. Prvotne usluge pristupa Internetu mobilnim korisnicima omogućavale su relativno visoku kvalitetu usluge, ali bez ikakvog oblika zaštite podataka koji se prenose. Kako bi se riješio ovaj problem za korisnike akademske zajednice, 2003. godine nekoliko europskih zemalja (uključujući i Hrvatsku) krenulo je u realizaciju novog sustava za pristup Internetu – Eduroam.

U ovom dokumentu bit će detaljno objašnjeno što je to Eduroam, a govorit će se o povijesnim, tehničkim i organizacijskim aspektima te budućem razvoju Eduroam-a. Pri tome će se i posebno izdvojiti način funkcioniranja i organizacije Eduroam usluge u Hrvatskoj (AAI@Edu.hr).

Što je eduroam

Eduroam (*educational roaming)* je *roaming* usluga koju omogućuje konfederacija nacionalnih *roaming* operatera i koja je zamišljena pod okriljem europske udruge akademskih i istraživačkih mreža (TERENA, eng. *Trans-European Research and Education Networking Association*). Eduroam *roaming* usluga je ostvarena kroz međunarodni projekt GÉANT (projekt europske multi-gigabitne akademske računalne mreže). Usluga eduroam, odnosno eduroam *roaming* je usmjerena na omogućavanje bežičnoga, ali i tzv. *wired* (žicom, kroz LAN) pristupa Internetu bilo gdje u svijetu.

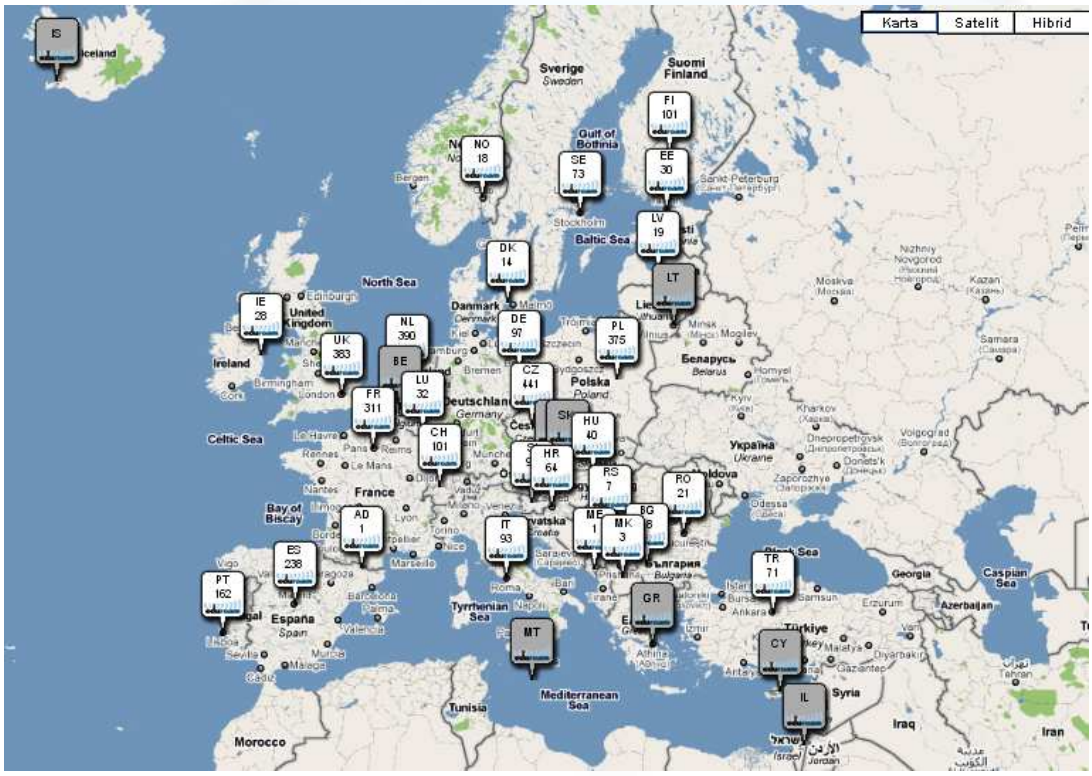
Slika 1. Logo eduroama
Izvor: eduroam.org

Hrvatska je od samoga početka, zahvaljujući projektu AAI@EduHr, aktivna u izgradnji i pružanju usluge eduroam. Usluga eduroam je sigurna, jednostavna i za krajnjeg korisnika potpuno besplatna usluga pristupa Internetu**.** Trenutno je dostupna na brojnim lokacijama u Hrvatskoj te u 36 europskih zemalja, Kanadi, Australiji, SAD, Japanu i brzo se širi. Eduroam inicijativa je započela 2003. godine pod okriljem već spomenute organizacije TERENA i cilj joj je bio kombinirati infrastrukturu baziranu na RADIUS-u s IEEE 802.1X tehnologijom. RADIUS (eng. *Remote Authentication Dial In User Service*) je mrežni protokol koji omogućuje centraliziranu autentikaciju, autorizaciju i dodjelu prava korisnicima (AAA, eng. *Authentication, Authorization, and Accounting*) s ciljem spajanja računala na mrežne servise. IEEE 802.1X je dio obitelji standarda koji čine lokalne i gradske (eng. *local/metropolitan*) mreže. Početna provjera je provedena između 5 institucija smještenih u Nizozemskoj, Finskoj, Portugalu, Engleskoj i Hrvatskoj. Hrvatska institucija koja je vezana uz same početke eduroama je Srce (Sveučilišni računski centar). Kasnije su ostale Europske zemlje počele prihvaćati ideju i postepeno su se priključile toj inicijativi te je tako nastao eduroam. Ubrzo se eduroam proširio i izvan europskih granica. Prva neeuropska zemlja koja se priključila eduroamu je Australija (u prosincu 2004. godine). Sada se eduroam dijeli na četiri veće skupine članica. Te skupine su eduroam Europe, eduroam Canada, eduroam USA i eduroam Asia-Pacific (APAN). Eduroam Europa i eduroam Asia-Pacific su konfederacije, dakle okupljaju više zemalja, dok su eduroam Canada i eduroam USA federacije vezane za te zemlje.

Slika 2. Trenutna podjela eduroama sa zemljama koje obuhvaća
Izvor: eduroam.org

2. Način rada eduroama

Eduroam omogućuje korisnicima članica eduroam zajednice zaštićen Internet pristup u instituciji članici eduroam zajednice u kojoj se trenutno nalaze. Sam princip eduroama je sličan *roamingu* u mobilnoj telefoniji, gdje se koriste resursi institucije u kojoj se korisnik trenutno nalazi, dok se autentikacija obavlja na poslužiteljima u instituciji iz koje korisnik potječe. Ukratko, suštinu eduroama najbolje opisuje njen slogan „Otvorite prijenosnik i budite *online*“ (eng. *Open your laptop and be online*). Naravno, ovo ovisi o broju i rasprostranjenosti *hotspotova* (mjesta s pristupom mreži) koje članice postave. Međutim, da bi ovo bilo moguće, neophodna je usklađenost i koordinacija između institucija. Za razliku od mobilnog *roaminga* koji je također zasnovan na korištenju infrastrukture druge mreže, kod eduroama ne postoji komercijalna dobit od korištenja ove usluge. Samim time je i teže stvoriti zajednicu koja će biti u potpunosti u duhu slogana eduroama, odnosno zajednicu rasprostranjenu po cijelom svijetu. Jedino što veže organizacije je stvaranje globalne eduroam zajednice za benefit članova akademskih institucija širom Europe i svijeta. Samo korištenje eduroama je ograničeno na zatvoreno društvo koje čine Nacionalne mreže za istraživanje i edukaciju – NREN (eng. *National Research and Education Network*). Članovi Europske eduroam zajednice su organizacije odgovorne za operaciju nacionalnog *roaming* servisa. Ove organizacije (NRO, eng. *National Roaming Operator*) su u najvećem broju slučajeva i sami NREN-ovi. U nekim državama (zbog tehničkih i/ili organizacijskih ograničenja) postoji slučaj da NRO nije i NREN, ali tada taj NRO mora imati precizno definiran odnos s NREN-om. To znači da NRO koji pruža uslugu *roaminga* mora poštovati pravila koja određuje NREN.



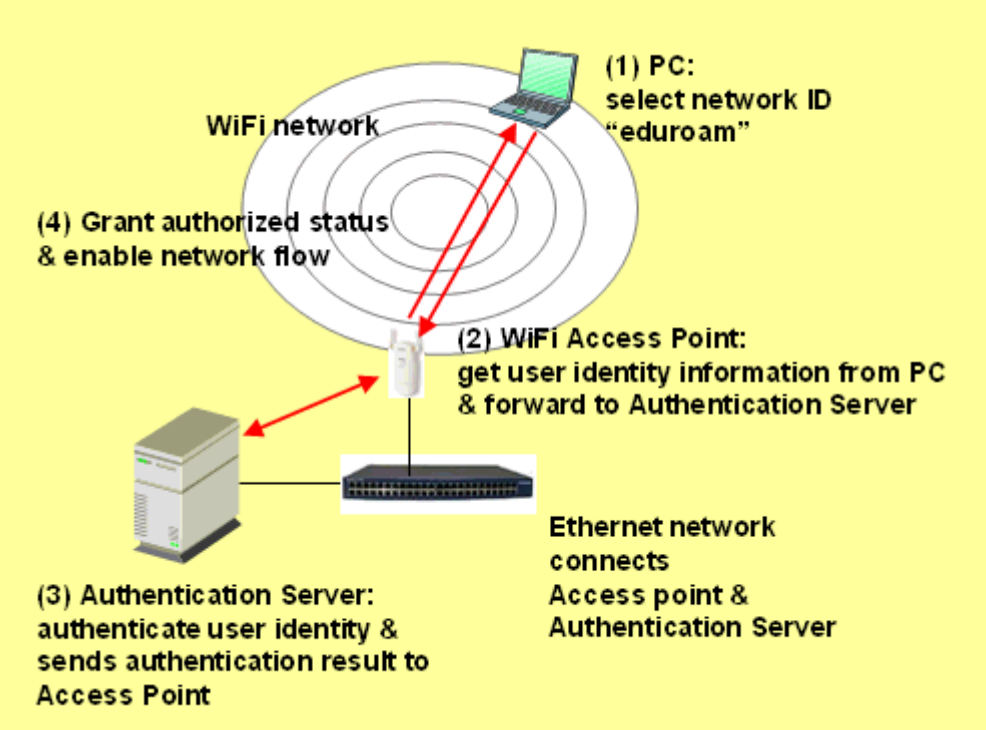
Slika 3. Eduroam pristupna mjesta u Europi
Izvor: eduroam.org

2.1. Tehnologije primijenjene u eduroam servisu

Eduroam koristi sljedeće komponente kako bi realizirao svoj servis:

- ***Network Access Server*** (NAS) – preklopnik (*wireless access point*) koji klijentima pruža pristup lokalnoj mreži,
- **Klijent** (eng. *Supplicant*) –program koji omogućuje korisničku autentikaciju na mreži. *Supplicant* je program koji je ugrađen u operacijski sustav ili je zasebna aplikacija,

- **Autentikacijski poslužitelj** (AS) – za autentikaciju i autorizaciju korisnika te dinamičku konfiguraciju poslužitelja za pristup mreži. AS posjeduje bazu koja sadrži korisničke podatke za autentikaciju. Nekoliko protokola se može koristiti za prijenos korisničkih podataka. Najpoznatiji su TACACS+, RADIUS i *Diameter*. RADIUS poslužitelji imaju do sada najveću primjenu i veliki broj dostupnih implementacija.
- **IEEE 802.1X** – standard za kontrolu pristupa mreži te
- **IEEE 802.1Q** – standard za VLAN dodjeljivanje (eng. *Virtual Local Area Network*).



Slika 4. Realizacija eduroam servisa
Izvor: hku.hk

Korisnik eduroam servisa se na lokalnu mrežu spaja preko NAS-a (eng. *Network Access Server*). Korisničku atentikaciju, odnosno upis korisničkih podataka za pristup eduroamu, korisnik obavlja putem klijenta (eng. *Supplicant*). Korisnički podaci se tada šalju AS-u (eng. *Authentication server*) koji te podatke provjerava. Ako su pristupni podaci korektni, AS prosljeđuje potvrdu pristupa mreži na pristupno mjesto (NAS) i korisnik je slobodan za korištenje eduroam servisa. Protokol IEEE802.1X služi za kontrolu pristupa mreži, odnosno za siguran prijenos korisničkih podataka od korisnika do AS-a i natrag. IEEE802.1Q protokol služi za virtualno dodjeljivanje (VLAN, eng. *Virtual Local Area Network*) prostora na mreži. Pomoću ovog protokola svakom se korisniku virtualno dodjeljuje prostor na mreži na korištenje i time se optimizira brzina pristupa mreži svakom korisniku.

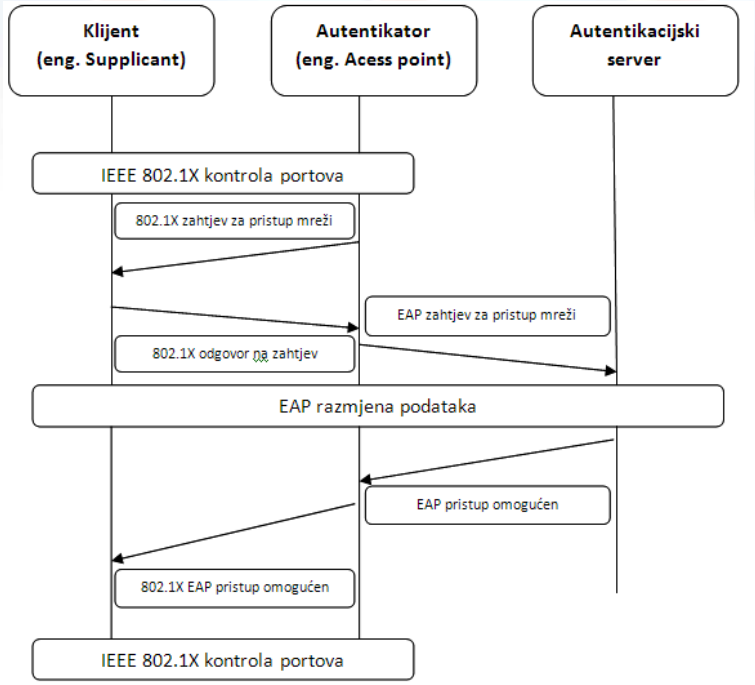
2.1.1. IEEE 802.1X

IEEE 802.1X je standard za kontrolu pristupa računalnoj mreži. Korisnik preko mrežnog sučelja fizički povezuje svoje računalo na računalnu mrežu (na neki priključak mrežnog preklopnika). Mrežni uređaj koji podržava 802.1X protokol može kontrolirati svoje priključke na računalnu mrežu tako da je korisnicima dozvoljena komunikacija samo preko njih ukoliko se poklapaju kriteriji autentikacije i autorizacije. Takvi mrežni uređaji mogu biti preklopnici ili rjeđe WAP uređaji (eng. *Wireless Access Point*). Tri komponente uključene u IEEE 802.1X autentikacijski proces su:

- *Supplicant* - korisnički program koji šalje zahtjev kroz priključak,
- Autentikator - mrežni uređaj, odnosno NAS, te
- Autentikacijski poslužitelj (AS) (u većini slučajeva RADIUS poslužitelj).

Korisnička autentifikacija putem 802.1X zahtjeva korištenje EAP protokola (eng. *Extensible Authentication Protocol*). EAP protokol prenosi autentikacijske podatke preko LAN-a (EAPOL) u okviru RADIUS protokola (koji će biti kasnije detaljnije objašnjen). Podaci se LAN-om prenose do AS-a (eng. *Authentification Server*), a potvrda korisničkih podataka se istim putem vraća do korisnika i omogućuje mu pristup mreži. Autentikator je nadležan za dodjeljivanje resursa, kao i potvrdu povezanosti *Supplicanta,* odnosno povezivanja korisnika na mrežu.

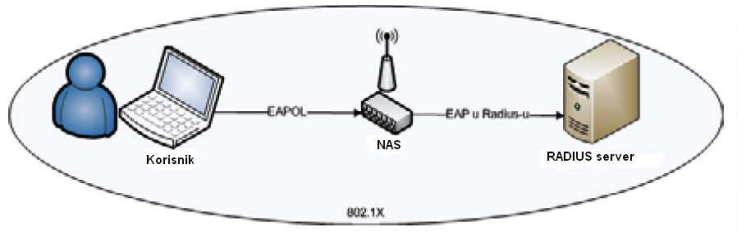
Drugi aspekt standarda 802.1X, koji ga čini svestranim, je veliki broj različitih autentikacijskih metoda koje se mogu koristiti u okviru EAP protokola. Neki od primjera su EAP-MD5, EAP s *One-Time Password* (EAP-OTP) autentikacijom, *Generic Token Card* (EAP-GTC) i EAP-SIM. Kako bi se što bolje zaštitila mrežna komunikacija, posebno u bežičnim mrežama, koriste se metode koje omogućuju uzajamnu autentikaciju (i poslužitelj autentificira klijenta), pri čemu korištenje tih metoda nije nužno. Važno je da *Supplicant* zna može li vjerovati autentikacijskom poslužitelju prije nego što provjeri osjetljive informacije kao što su korisničko ime i lozinka. Primjeri pogodnih autentikacijskih metoda su EAP-TLS, EAP-TTLS i EAP-PEAP. Ove autentikacijske metode su pogodne jer u svakoj od njih RADIUS poslužitelj prvo korisniku šalje svoje certifikate koji sadrže javni ključ. Korisnik može provjeriti ovaj certifikat na osnovu instalirane kopije *Certificate Authority* (CA) javnog ključa i moguće instalirane *Certificate Revocation* liste (CRL) prije nego što se autentikacijski proces nastavi. CRL je lista svih digitalnih certifikata u kojoj se nalazi i certifikat za EAP autentikacijsku metodu i, ako se koristi CA provjera, ona ne mora nužno biti instalirana za provjeru certifikata. Važno je napomenuti da enkripcija (šifriranje) autentikacijskog procesa ne znači i enkripciju podataka od korisnika ili prema korisniku nakon uspješne autentikacije. Svi podaci, osim korisničkih koje on sam razmjenjuje s drugim korisnicima, poslužiteljima i slično nisu zaštićeni enkripcijom i ukoliko se radi o povjerljivim podacima potrebno ih je posebno enkriptirati ili zaštititi na neki drugi način. Unatoč tome, standard 802.1X zajedno s odgovarajućom autentifikacijskom metodom je siguran za distribuciju enkripcijskih ključeva koje klijenti mogu koristiti za svoj promet. Za bežične mreže, metode enkripcije su WEP (40 ili 104 bita) sa rotacijskim ključevima, TKIP ili AES. Korištenje 802.1X autentifikacije sa AES enkripcijom je poznato pod nazivom WPA2, koji je ekvivalentan s IEEE 802.11i standardom.



Slika 5. IEEE 802.1X standard s EAP protokolom

2.1.2. RADIUS poslužitelji

RADIUS je akronim za "*Remote Authentication Dial In User Service*" i definiran je s IETF RFC 2865 i RFC 2866 [3]. Korištenjem RADIUS protokola komuniciraju NAS (eng. *Network Access Server*) i AS. Potrebno je razlikovati RADIUS protokol i RADIUS poslužitelj. RADIUS protokol je EAP protokol prilagođen RADIUS poslužiteljima. EAP protokol u okviru RADIUS protokola prenosi autentikacijske, autorizacijske, konfiguracijske i obračunske podatke od NAS-a do RADIUS poslužitelja. IEEE 802.1X EAP protokol koji se koristi između klijenta i NAS-a je EAPOL (eng. *Extensible Authentication Protocol Over LAN).* NAS enkapsulira EAP sadržaj i transportira autentikacijske poruke do RADIUS poslužitelja (Slika 6). Enkapsulacija na podatak dodaje dodatne informacije važne protokolu da bi taj podatak mogao uspješno i u cijelosti doći do odredišnog računala ili mreže (u ovom slučaju do RADIUS poslužitelja). RADIUS poslužitelj obavlja autentikaciju i prihvaća ili odbija zahtjev. Na temelju odgovora RADIUS poslužitelja NAS korisniku odobrava i zabranjuje pristup mreži. Odgovor od AS-a može sadržati konfiguracijske elemente koje utječu na to kako će korisnik koristiti servis. Nekoliko NAS uređaja se na RADIUS poslužitelj možgu povezati na ekvivalentan način kao nekolicina korisnika na AS.

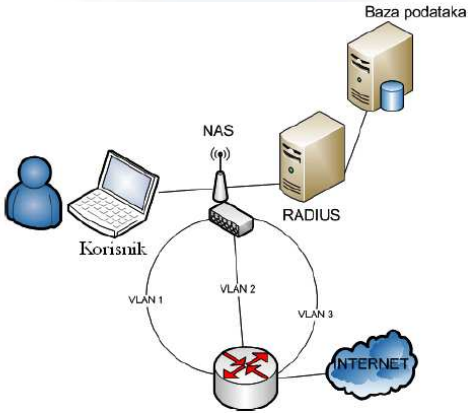


Slika 6. Povezivanje korisnika i RADIUS poslužitelja

RADIUS AS surađuje s ostalim AS-ovima kroz pozadinsku - *backbone* autentikacijsku mrežu gdje jedan AS služi kao posrednik (eng. proxy) za drugi AS. Jednom kada korisnički podaci dođu do AS-a, on uspoređuje podatke sa svojim izvorom. Ukoliko ne može pronaći te podatke u svojem izvoru, AS- preko *backbone* mreže prosljeđuje podatke do drugog AS-a dok se ne pronađe AS koji posjeduje informacije o traženom korisniku ili dok se ne prođe cijela *backbone* mreža.

AS može podržati veliki broj autentikacijskih metoda, a to ovisi o implementaciji. *Unix login*, tekstualne datoteke, SQL baza podataka, *Certification Authority* i LDAP baza su neke od primjera izvora podataka koje AS može koristiti kako bi provjerio korisnički identitet. Također je moguće da se koriste neke metode u kombinaciji s ostalim kriterijima autentikacije, a ti kriteriji su prefiks i sufiks korisničkom imenu, identitet zahtjeva NAS-a, itd.

U slučaju uspješne autentikacije, lokalni RADIUS poslužitelj šalje konfiguracijske opcije do NAS-a kako bi kontrolirao kojem VLAN-u je klijent dodijeljen, odnosno kakve ovlasti korištenja računalne mreže posjeduje. Različiti VLAN-ovi mogu imati različita prava pristupa i mogu biti povezani na različite dijelove mreže, što znači da različiti korisnici na različitim pristupnim mjestima mogu imati različita dopuštenja na mreži (Slika 7).



Slika 7. Struktura lokalne mreže i VLAN podjela

2.1.3. Mrežna infrastruktura i korisnički program za pristup eduroam servisu

Eduroam ne uvjetuje karakteristike sklopovlja neophodne za pristup mreži. Korisnici eduroama mogu pristupiti eduroam servisu bilo preko bežične ili žičane veze. Međutim, zbog specifične konfiguracije, korisnici moraju imati određeni softver kojim se šalju zahtjevi za pristup eduroam mreži. Naime, po propoziciji eduroama, *Access point* -i ili preklopnici moraju podržavati IEEE 802.1X standard koji obuhvaća korištenje EAP protokola (*Extensible Authentication Protocol*) za autentikaciju korisničkih podataka. Korištenjem odgovarajuće EAP metode izvodi se jedna od dvije moguće opcije, ovisno o načinu autentikacije. Prva je uspostavljanje osiguranog tunela od korisničkog računala do poslužitelja matične institucije kojim se obavlja razmjena autentikacijskih informacija (EAP-TTLS ili PEAP). Druga opcija je međusobna autentikacija putem javnih X.509 certifikata (EAP-TLS). Tri prethodno spomenute autentikacijske metode uspostavljaju sigurni TLS (eng. *Transport Layer Security*) tunel od klijentskog računala do poslužitelja matične institucije i korisnički podaci ne mogu biti prisluškivani na svom putu. Također, poželjno je da mrežni uređaji mogu korisnika dodijeliti određenom dijelu mreže (određenom VLAN-u) na osnovu informacija koje su dobili od RADIUS poslužitelja. Program koji koristi 802.1X za slanje zahtjeva za pristup eduroam mreži putem EAP-a obično je ugrađen u operacijski sustav, kao što je slučaj kod operacijskog sustava Windows XP, a može biti i odvojena aplikacija kao što je to primjerice SecureW2. Korisnici moraju podesiti spomenuti program na osnovu zahtjeva eduroam mreže. Ovako podešen program se može koristiti bilo gdje u okviru eduroam zajednice. EAP-TTLS se smatra najlakšim načinom da se eduroam implementira u velikim institucijama. Nažalost, Microsoft Windows nema ugrađenu podršku za EAP-TTLS tako da je u tom slučaju neophodno korištenje dodatnog programa koji podržava EAP-TTLS (npr.već spomenuti SecureW2).

2.2. Realizacija eduroam servisa

Europski eduroam servis je konfederacijski servis (servis kojim se služi više zemalja) kreiran hijerarhijski na distribuiranom sustavu AAA poslužitelja. AAA (eng. *Authentification, Authorization, Accounting*) poslužitelji su poslužitelji za rukovanje korisničkog pristupa mrežnim resursima i osiguravaju autentikacijske i autorizacijske podatke te podatke o računu korisnika. Na vrhu eduroam servisa se nalazi servis konfederacijskog nivoa (eng. *Top level service*). Njegova primarna namjena je pružanje neophodne infrastrukture kako bi se dozvolio mrežni pristup svim članicama u svakom trenutku. Ovaj konfederacijski servis je iznad federacijskih (nacionalni) *roaming* servisa, za koje su nadležni federacijski *roaming* operatori. Federacijski *roaming* operatori su nadležni za eduroam servis na nacionalnom nivou. Ovisno o slučaju, ispod nacionalnih *roaming* operatora mogu biti ostale organizacije akademskog tipa, kao što su sveučilišta, edukacijske ustanove i slično. Trenutna implementacija koristi RADIUS kao AAA poslužitelj. On je implementiran kao hijerarhijski sustav poslužitelja kako bi se prenosili autentikacijski zahtjevi korisnika iz druge institucije do matične institucije, kao i vraćanje odgovarajućeg odgovora natrag. Hijerarhija RADIUS poslužitelja opisana je u nastavku teksta (Slika 9).

2.2.1. RADIUS poslužitelji konfederacijskog nivoa

RADIUS poslužitelji konfederacijskog nivoa (TLRS, eng. *Top level radius server*) služe kako bi usmjeravali AAA (eng. *Authentification, Authorization, Accounting*) zahtjeve ka odgovarajućim institucionalnim ili federacijskim RADIUS poslužiteljima. Trenutno za Europsku konfederaciju postoji nekoliko TLR poslužitelja, i svaki od njih je nadležan za određenu grupu federacijskih poslužitelja. Ukoliko nekom od njih dođe zahtjev za federacijski poslužitelj za koji nisu nadležni, taj TLRS će proslijediti zahtjev TLRS-u koji je nadležan za spomenuti federacijski poslužitelj. Osim Europske eduroam konfederacije, postoje eduroam konfederacije/federacije i u ostalim dijelovima svijeta, kao što je već rečeno. Ovi učesnici su također povezani s Europskom eduroam konfederacijom, ali njihovi NREN-ovi nisu članovi Europske konfederacije.

2.2.2. RADIUS poslužitelji federacijskog nivoa

Federacijski RADIUS poslužitelj (FLRS, eng. *Federation Level Radius Servers*) sadrži listu povezanih institucionalnih poslužitelja i odgovarajućih domena. Oni primaju zahtjeve od konfederacijskih poslužitelja i institucija povezanih na njih te ih prosljeđuju odgovarajućoj instituciji. Federacijski RADIUS poslužitelj može služiti i kao institucionalni RADIUS poslužitelj. Akademska ustanova unutar eduroam mreže, ukoliko nema svoj RADIUS poslužitelj, koristiti federacijski kao bazu korisničkih podataka svojih korisnika.

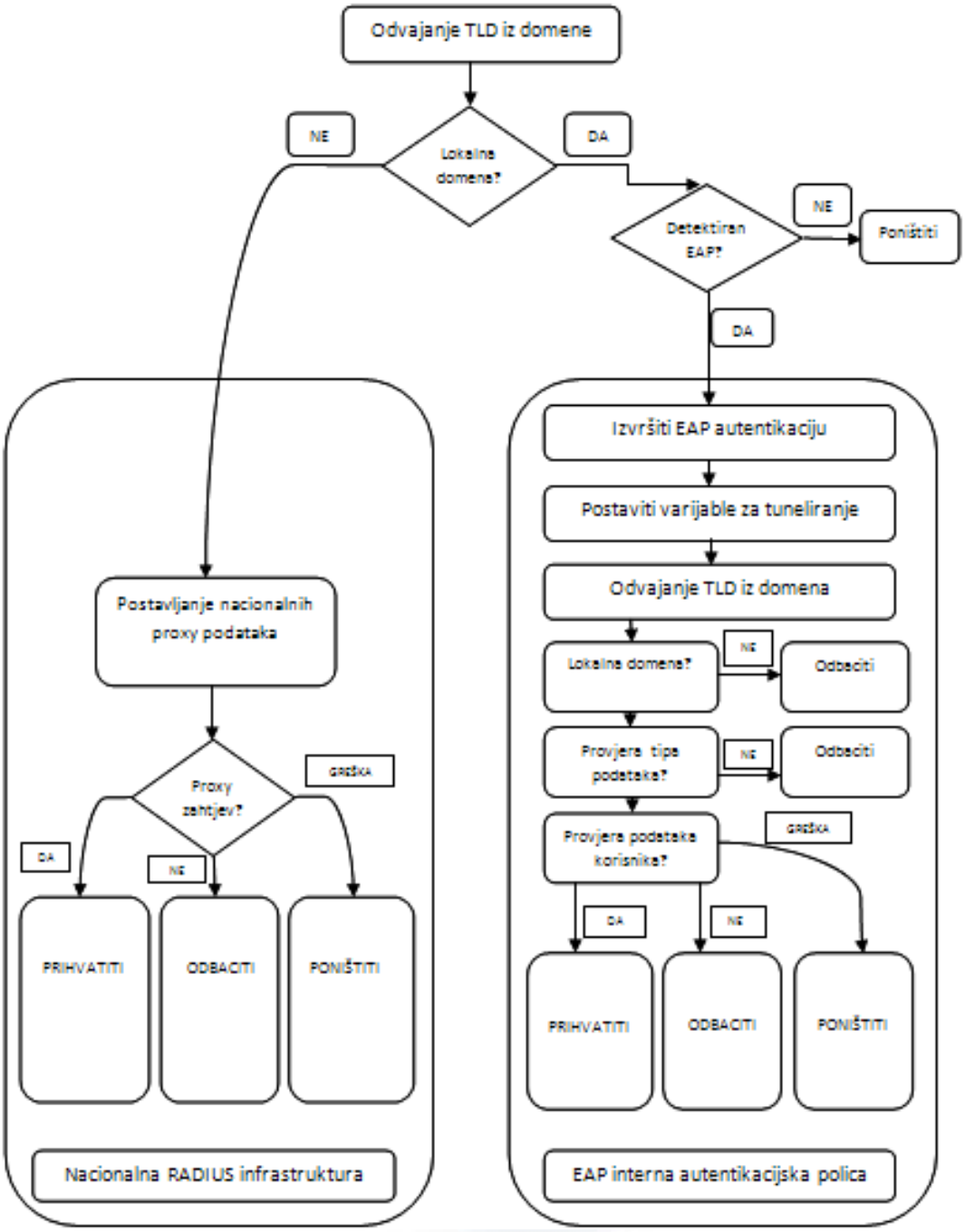
2.2.3. Matični i udaljeni institucionalni RADIUS poslužitelji

Institucionalni RADIUS poslužitelji (eng. *Institutional Radius*) su nadležni za autentikaciju svojih korisnika, bilo da su u matičnoj (eng. *Home Institutional Radius*) ili u udaljenoj mreži (eng. *Remote Institutional Radius*). Osim ove uloge, institucionalni RADIUS poslužitelji do federacijskog poslužitelja prosljeđuju zahtjeve stranih korisnika za pristup mreži institucije. Za razliku od navedena dva tipa RADIUS poslužitelja (konfederacijski i federacijski), koji su u suštini posrednički poslužitelji (eng. proxy) koji samo prosljeđuju zahtjeve, institucionalni poslužitelji su mnogo kompleksniji. Ovi poslužitelji, osim što su i sami u jednom dijelu proxy poslužitelji, također obrađuju zahtjeve i samim time kompletiraju EAP zahtjeve i pretražuju bazu korisničkih podataka.

2.3. Princip rada eduroama

RADIUS poslužitelji formiraju osnovnu strukturu eduroam servisa. Posebno važnu ulogu imaju kada se koriste kao proxy poslužitelji za autentikacijske zahtjeve. Svaki NREN (eng. *National Research and Education Network*) koji sudjeluje u eduroamu koristi jedan RADIUS poslužitelj federacijskog nivoa s makar još jednim RADIUS poslužiteljem federacijskog nivoa postavljenim na drugu lokaciju radi povezanosti makar dviju federacija, odnosno *roaminga*. Poslužitelji federacijskog nivoa imaju kompletnu listu podređenih eduroam poslužitelja institucija u toj federaciji, od kojih je svaka odgovorna za autentikaciju svojih korisnika. Svaki RADIUS poslužitelj institucijskog nivoa treba imati samo informaciju o svom RADIUS poslužitelju federacijskog nivoa. RADIUS poslužitelj federacijskog nivoa je također konfiguriran i kao RADIUS proxy korisnik za eduroam RADIUS poslužitelje konfederacijskog nivoa. Obzirom da RADIUS poslužitelji također funkcioniraju kao proxy poslužitelji za ostale poslužitelje, oni omogućuju gostujućem korisniku da se identificira za pristup mreži s korisničkim podacima koje koristi u svojoj matičnoj instituciji. Ovo je moguće jer lokalni RADIUS poslužitelji jednostavno prosljeđuju autentikacijske poruke do korisnikove matične institucije bez potrebe za daljnjom analizom zahtjeva. Bitno je jedino da lokalni NAS prihvati ili odbije korisnički zahtjev za pristup na osnovu ishoda autentikacijskog zahtjeva matičnoj instituciji.

Ranije u dokumentu je spomenuto da AS može koristiti različite autentikacijske metode u kombinaciji s ostalim kriterijima. Upravo je ova mogućnost iskorištena kako bi se na fleksibilan način osigurala identifikacija matične institucije korisnika i adekvatno prosljeđivanje. Kada korisnik uputi zahtjev za autentikaciju, poslužitelji zaduženi za korisničku domenu odlučuju gdje će se zahtjev poslati. Domena je sufiks korisničkog imena, odvojena znakom „@“ (npr. *@fer.hr*) i izvedena je iz institucionalnog DNS (eng. *Domain Name System*) domenskog prefiksa. Kada korisnik pošalje zahtjev za autentikaciju, prvi institucionalni poslužitelj razdvaja korisničku domenu iz korisničkog imena i obavlja algoritamsku provjeru domena kao što prikazuje Slika 8. Razdvojena korisnička domena naziva se TLD (eng. *Top-Level Domain*).

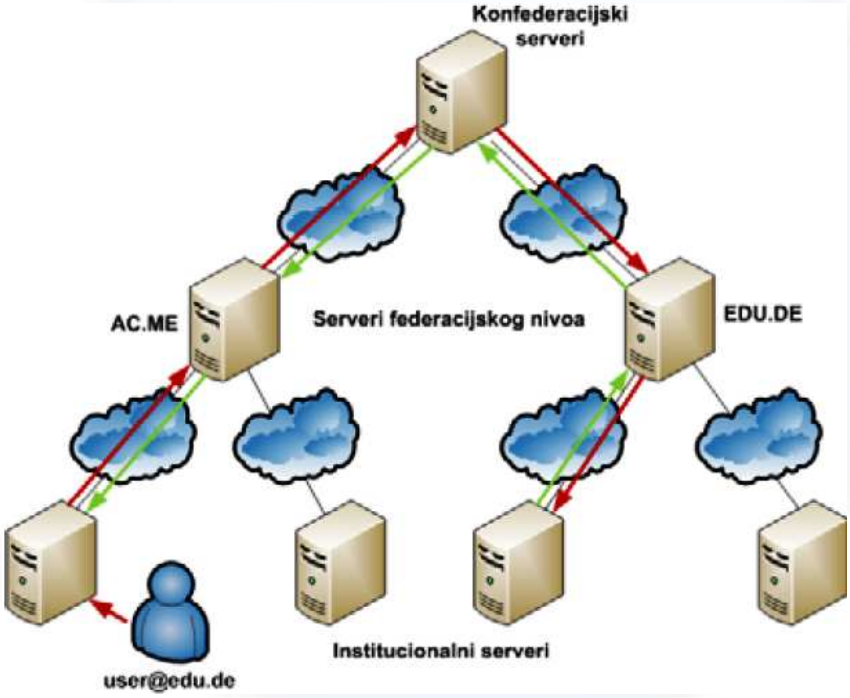


Slika 8. Dijagram toka podataka u okviru institucionalnog RADIUS poslužitelja

Ukoliko je u pitanju lokalna domena, sljedeći korak nakon razdvajanja TLD-a je detektiranje EAP-a, a zatim i korisničkih podataka. Ukoliko je korisnička domena iz iste federacije, federacijski RADIUS poslužitelj prosljeđuje zahtjev do nadležnog institucionalnog poslužitelja, koji će nastaviti provjeru podataka. Ukoliko je domena iz različite federacije, federacijski RADIUS poslužitelj će proslijediti zahtjev na konfederacijski nivo, a zatim će se zahtjev proslijediti do nadležnog institucionalnog poslužitelja u matičnoj federaciji korisnika (Slika 9). Nakon obrade podataka, RADIUS poslužitelj će NAS-u vratiti informaciju o valjanosti korisničkih podataka, uz moguće konfiguracijske opcije. Međutim, mora se uzeti u obzir da postoje značajne razlike između organizacija u okviru eduroam konfederacije koje se dotiču autentikacijskih i enkripcijskih shema koje su izabrali za svoje mreže. Tako na primjer konfiguracije ne moraju biti jednake u svim državama (npr. SAD i Hrvatska nemaju istu konfiguraciju za pristup mreži), kao niti

parametri spajanja (npr. postojanje programske podrške za EAP protokol) i sklopovska/programska ograničenjima u pristupnim uređajima i/ili u RADIUS poslužiteljima. . Kriptirani korisnički autorizacijski podaci su proslijeđeni od strane RADIUS proxy poslužitelja do korisničke matične organizacije i oni se obrađuju kao da je korisnik u matičnoj organizaciji. Moguće je da korisnik mora adaptirati enkripcijsku shemu na osnovu konfiguracije institucije u kojoj se nalazi, odnosno mora je prilagoditi za prijenos preko te institucije. Većina organizacija posjeduje pristupne točke (eng. *access point*) koji podržavaju više enkripcijskih metoda što znači da postoji velika mogućnost da korisnik već koristi matičnu enkripcijsku metodu. U drugom slučaju, on mora izabrati metodu koja je implementirana u toj instituciji. Primjer prosljeđivanja zahtjeva prikazuje slika Slika 9. Autorizacija se koristi na sljedeći način:

1. korisnik kojem je matična domena *@edu.de* pristupa eduroam servisu iz institucije s domenom *@ac.me*.;
2. njegov zahtjev se s institucionalnog poslužitelja preko federacijskog poslužitelja prenosi do konfederacijskog poslužitelja;
3. konfederacijski poslužitelj prosljeđuje zahtjev do federacijskog poslužitelja s domenom *@edu.de;*
4. konfederacijski poslužitelj u svim institucionalnim poslužiteljima koji su povezani na njega pretražuje korisničke podatke. Ukoliko ih pronađe, vraća potvrdu zahtjeva za pristup eduroamu istim putem sve do korisnika.

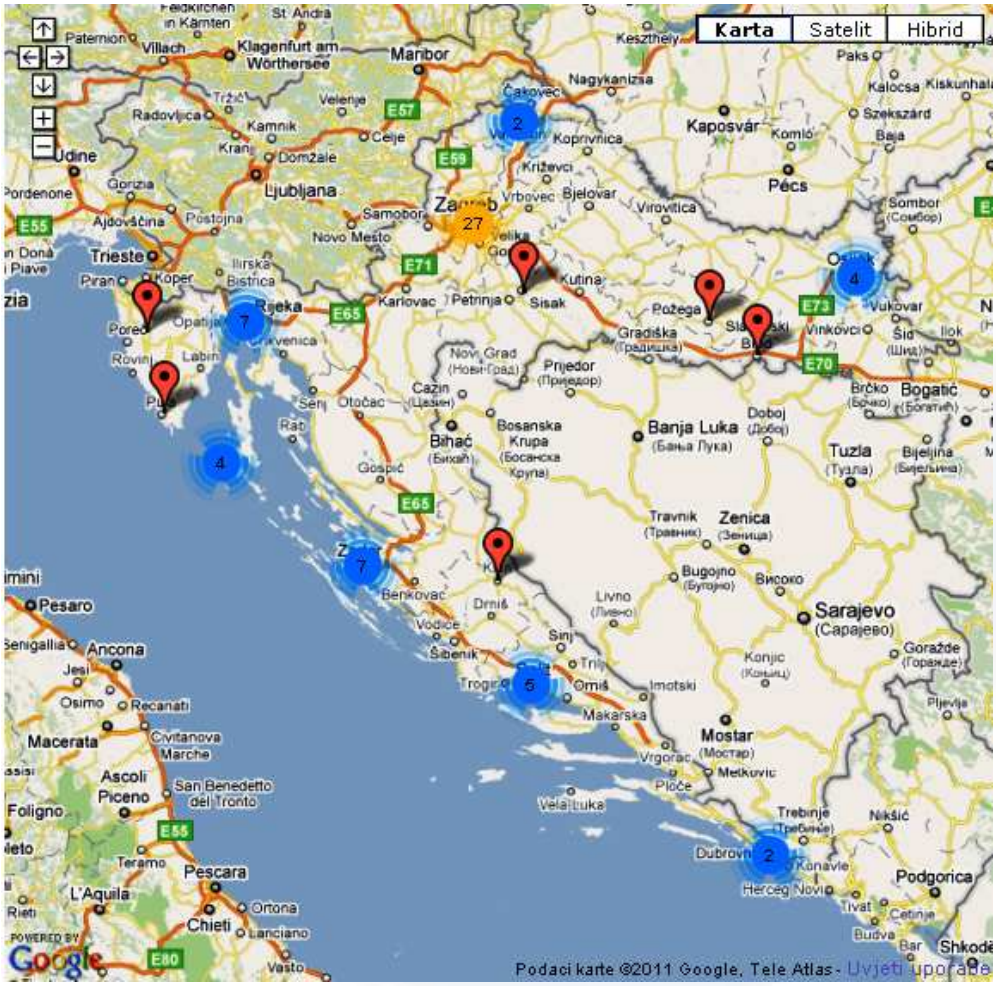


Slika 9. Prosljeđivanje zahtjeva prema matičnoj instituciji
Izvor: sistemac.srce.hr

.

3. Eduroam u Hrvatskoj - AAI@EduHr

Hrvatska je zahvaljujući projektu AAI@EduHr od samoga početka aktivna članica eduroam zajednice koja se danas već proširila i izvan Europe. Kao što je prije rečeno, eduroam je zamišljen kao Europski (kasnije i svjetski) *roaming* sustav i u Hrvatskoj se on odvija u sklopu projekta AAI@EduHr (Slika 8). AAI@EduHr je autentikacijska i autorizacijska infrastruktura sustava znanosti i visokog obrazovanja u Republici Hrvatskoj. Sustav AAI@EduHr tehnički je realiziran uporabom distribuiranih LDAP (eng. *Lightweight Directory Access Protocol*) imenika. Svaka ustanova iz sustava MZOŠ, koja je uključena u sustav AAI@EduHr, ima vlastiti LDAP imenik u kojem su pohranjeni elektronički identiteti korisnika iz te ustanove. AAI@EduHr u punom je pogonu od 1. ožujka 2006. godine.



Slika 10. Eduroam pristupna mjesta u Hrvatskoj
Izvor: eduroam.hr

3.1. Imeničke sheme i upravljanje elektroničkim identitetima

Osnova svake AAI (eng. *Auditing, Accounting, Inter-institutional*) strukture jest sustav upravljanja elektroničkim identitetima. Kao što je već rečeno, AAI@EduHr se temelji na sustavu distribuiranih LDAP imenika, stoga su temelj AAI@EduHr odgovarajuće imeničke sheme zajedno s uvjetima za uspostavu imenika te organizacijskim i proceduralnim okvirima i pravilima za informacijsku potpunost, konzistentnost i vjerodostojnost sadržaja imenika. Dokumentom pod nazivom „Definicija hrEdu imeničkih shema“ definirane su dvije sheme: hrEduPerson kojom se opisuju osobe i hrEduOrg kojom se opisuju ustanove u sustavu AAI@EduHr. Dokument je moguće preuzeti s poveznice:

http://www.aaiedu.hr/docs/AAI@EduHr-hrEduSheme-2010-v1.3.1.pdf

HrEdu sheme razlikuju se od ranije prakse udaljenog pristupa mreži preko modema i ISDN uređaja (utemeljene na sustavu CMU- CARNet modemski ulazi). One su usklađene s aktualnom europskom i svjetskom praksom, posebno što se tiče jednoznačne identifikacije korisnika koja sada predstavlja svojevrsni oblik elektroničke adrese. Tako atribut hrEduPersonUniqueID mora imati vrijednost oblika userid@id_ustanove.hr. Novi oblik identifikatora osobe omogućuje između ostalog i uporabu elektroničkog identiteta u okviru sustava eduroam. Hrvatska je u eduroam spojena u okviru aktivnosti na projektu AAI@EduHr.

Imeničke sheme mogu se i moraju mijenjati. Stoga je uz početnu verziju sheme odmah ustrojen i središnji registar koji osim detaljnih informacija o shemama te svim atributima i šifarnicima nudi korisnicima i mogućnost predlaganja izmjena u shemama (odnosno šifarnicima), kao i registraciju eventualnih lokalno izvedenih dodataka na **hrEdu** sheme. Središnji registar će po potrebi izdavati nove verzije shema hrEduPeson i hrEduOrg kao i upute za njihovu primjenu.

Definiciju imeničkih shema slijedi odgovarajuća dokumentacija i programski paketi: LDAP, RADIUS te AOSI (Aplikacija za Održavanje Sadržaja Imenika). AOSI omogućuje neposredno održavanje imenika, ali je realizirana tako da omogući, u situaciji kada je to izvedivo ili potrebno, povezivanje AAI@EduHr sa sustavima ISSP (Informacijski sustav studentske prehrane) i ISVU (Informacijski sustav visokih učilišta). Time se osigurava kako informacijska potpunost, konzistentnost i vjerodostojnost sadržaja imenika tako i izbjegavanje višestrukog unosa istih ili sličnih podataka na različitim mjestima u ustanovi. AOSI ujedno služi kao veza sa središnjim servisima AAI@EduHr.

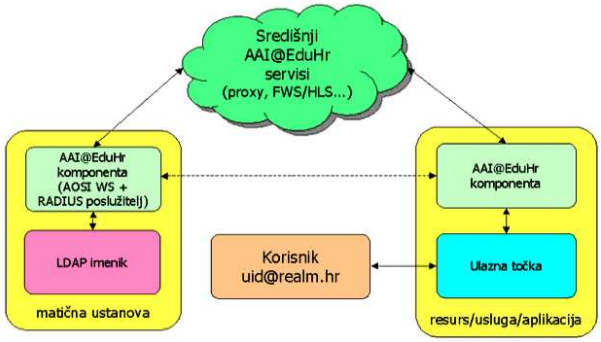
3.2. AAI@EduHr arhitektura

AAI komponentu na matičnoj ustanovi čine LDAP i RADIUS poslužitelji te AOSI web servis. Po izboru ustanove za održavanje sadržaja imenika može se koristiti AOSI klijent (web sučelje). Izgrađena hijerarhija RADIUS poslužitelja vezanih uz LDAP imenike u ustanovama, uz odgovarajuće središnje tzv. proxy RADIUS poslužitelje, standardno se koristi kao temelj autenticiranog i autoriziranog pristupa mreži. Ova hijerarhija se ne odnosi samo za sustav CMU, kojeg sigurno treba smatrati prvim resursom u sustavu AAI@EduHr. Hijerarhija se odnosi i na sustav StuDOM (Internet u studentskim domovima) i ona je generičko rješenje žičnog (eng. *wired*) i bežičnog (eng. *wireless*) pristupa mreži po 802.1x standardu koje se rabi u više ustanova članica CARNeta. Glede pristupa aplikacijama, RADIUS hijerarhija uspješno se rabi i za pristup pojedinim Web sjedištima i uslugama, a tu se mogu izdvojiti *e-learning* alati Moodle i WebCT. Popis svih aplikacija i usluga, kao i upute za pristup istima, može se naći na Internetskim stranicama AAI@EduHr.

http://www.aaiedu.hr/faq_sso_aplikacije.html

Slika 11 prikazuje primjer pristupanja aplikaciji ili usluzi koja koristi sustav AII@EduHr:

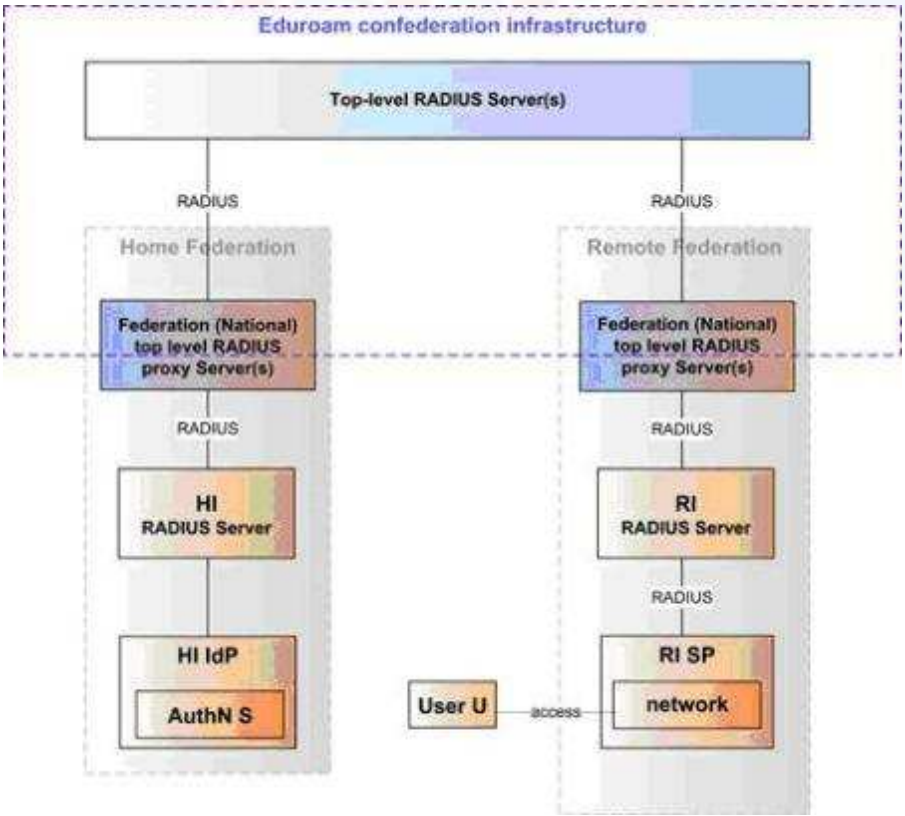
1. orisnik šalje zahtjev za pristup određenoj aplikaciji:
2. AAI@EduHr komponenta (RADIUS poslužitelj) aplikacije prosljeđuje zahtjev do središnjeg servisa;
3. središnji servis šalje zahtjev za pristup do RADIUS poslužitelja u matičnoj ustanovi (u Hrvatskoj je to Srce);
4. u LDAP imenicima matične ustanove provjeravaju se korisnički podaci;
5. potvrda ili odbijanje pristupa istim se putem vraća do korisnika aplikacije.



Slika 11. Pojednostavljena arhitektura AAI@EduHr
Izvor: aaiedu.hr

4. Autentikacijski mehanizmi u eduroamu

802.1x je IEEE protokol za autentikaciju mrežnih pristupnih priključaka koji se bazira na EAP skupu autentikacijskih protokola te omogućuje dodatnu konfiguraciju mrežnog pristupa. Eduroam infrastruktura za autentikaciju se sastoji od hijerarhijskog stabla RADIUS proxy poslužitelja. Ti RADIUS poslužitelji prosljeđuju autentikacijski zahtjev, korištenjem RADIUS EAP zahtjeva, od davatelja pristupa, tj. pristupnog uređaja (SP) do autentikacijskog poslužitelja matične ustanove korisnika koja autentificira korisnika. Po obavljenom postupku autentikacije, informacija o prihvaćanju ili odbijanju se prosljeđuje davatelju pristupa, koji temeljem svojeg sustava autorizacije odobrava ili ne odobrava korisniku pristup mreži.



Slika 12. Eduroam infrastruktura za autentikaciju
Izvor: sistemac.srce.hr

U eduroam sustavu se koriste EAP autentikacijski mehanizmi koji imaju definiran zajednički jedinstveni način komunikacije između davatelja pristupa (SP) i matične ustanove korisnika (IdP)

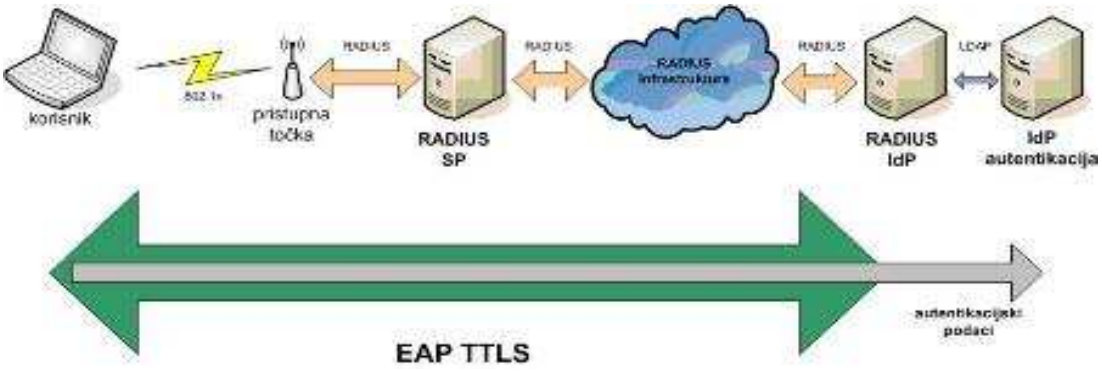
(Slika 12). Nadogradnja komunikacijskog nivoa očituje se u mogućnosti kreiranja različitih autentikacijskih mehanizama Autentikacijski mehanizmi mogu se razlikovati u načinu enkripcije i enkapsulacije podataka, načinu provjere valjanosti korisničkih podataka i slično. Autentikacijski mehanizmi koji koriste definiranu EAP komunikaciju u svom imenu sadrže EAP, npr. EAP-MD5, EAP-TTLS i dr.

4.1. EAP autentikacijski mehanizmi u eduroamu

U sustavu eduroam moguća je uporaba bilo kojeg EAP autentikacijskog mehanizma. Sustav prijenosa ne utječe na izabrani, tj. korišteni EAP autentikacijski mehanizam te je moguće da različiti korisnici koriste različite autentikacijske mehanizme, odnosno da isti korisnik koristi različite autentikacijske mehanizme ovisno o uređaju koji koristi za spajanje. Korisnik može koristiti samo one EAP autentikacijske mehanizme koje podržava matična ustanova korisnika te tada na računalu mora imati instaliranu odgovarajuću korisničku podršku (*supplicant*). Uobičajeno se unutar eduroam sustava susreću EAP-TTLS/PAP, EAP-TTLS/EAP-GTC, EAP-TLS i EAP-PEAP autentikacijski mehanizmi. U hrvatskom eduroamu preporuka je korištenje EAP-TTLS/PAP ili EAP-TTLS/EAP-GTC autentikacijskog mehanizma koje je jednostavno upotrijebiti s AAI@EduHr autentikacijskom infrastrukturom. AAI@EduHr autentikacijska infrastruktura se od svojih početaka zasnivala na EAP-TTLS/PAP i EAP-TTLS/EAP-GTC autentikacijskim mehanizmima. Ti autentikacijski mehanizmi su zato vremenom u Hrvatskoj usavršeni i u potpunosti usklađeni s autentikacijskom strukturom AAI@EduHr te zato preporuča njihova upotreba.

4.1.1. EAP-TTLS

EAP-TTLS je nadogradnja EAP komunikacijskog mehanizma kojom se omogućuje uspostava sigurnog TLS komunikacijskog kanala između korisnika i njegove matične ustanove. Na ovaj način su svi podaci koji se odnose na autentikaciju, a prenose se EAP-TTLS-om, zaštićeni na cijelom svom putu kroz mrežni infrastrukturu, a sam rezultat autentikacije je dostupan pristupnom uređaju davatelja usluge. Ovaj mehanizam omogućuje korisniku zaštitu privatnosti, a infrastrukturi jednostavan način autentikacije. Pri uspostavi EAP-TTLS tunela, poslužitelj matične ustanove korisnika koristi jedinstveni certifikat koji korisnik kod sebe može provjeriti korištenjem certifikata ustanove koja je izdala certifikat s kojim se koristi poslužitelj matične ustanove, čime se dodatno povećava sigurnost uspostavljenog tunela. EAP-TTLS/PAP autentikacijski protokol je kombinacija EAP-TTLS i EAP-PAP autentikacijskih protokola. EAP-TTLS/PAP služi za zaštitu korisničkih podataka u obliku tunela i standardnog PAP (eng. *Password Authentication Protocol*) RADIUS protokola. Standardnim PAP RADIUS protokolom se prenose korisnička oznaka i lozinka za autentikaciju korisnika. Kombinacijom ova dva protokola omogućuje se potpuna privatnost korisnika, a ipak se u uspostavi EAP-TTLS tunela prenosi dovoljna količina podataka da se ostvari veza između korisnika i njegove matične ustanove (*outer identity*). Podatak koji se koristi za pronalaženje matične ustanove korisnika, kao što je već spomenuto, je dio korisničke oznake iza znaka @ i naziva se *realm* (npr. *@fer.hr, @sczg.hr, @srce.hr*). Prednost ove kombinacije protokola je u činjenici da omogućuje korisniku jednostavnu uporabu i automatsko spajanje, dok matičnoj ustanovi daje mogućnost da korisnika autentificira putem različitih lokalnih autentikacijskih mehanizama.



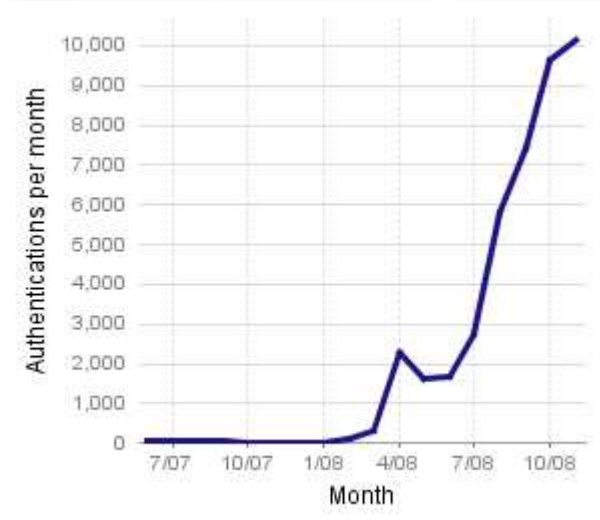
Slika 13. Eduroam autentikacija putem EAP-TTLS protokola
Izvor: sistemac.srce.hr

4.1.2. EAP-TTLS/EAP-GTC

EAP-TTLS/EAP-GTC autentikacijski protokol je kombinacija EAP-TTLS autentikacijskog protokola koji služi za zaštitu korisničkih podataka u obliku tunela i standardnog EAP-GTC (*Generic Token Card*) RADIUS protokola kojim se prenose podaci prilikom korištenja jednostrukih lozinki. Kombinacija ova dva protokola je korisna u slučajevima kada klijent nema podršku za EAP-TTLS/PAP (npr. mobiteli Nokia), a i dalje želi koristiti istu autentikacijsku infrastrukturu. Jedini nedostatak navedene kombinacije autentikacijskih protokola leži u činjenici da se korisnička lozinka mora unijeti prilikom svakog zahtjeva za autentikaciju.

5. Budućnost eduroama

Budućnost eduroama je u širenju po cijelom svijetu i daljnje povećavanje broja korisnika. Najavljeno je veliko širenje eduroama na području Azije u skorijoj budućnosti. Također, eduroam najavljuje dodatno proširivanje broja *hotspot*-ova u Europi. Jedan od ciljeva eduroama je napraviti najpoznatiju akademsku mrežu, odnosno od eduroama napraviti proizvod prepoznatljiv u cijelome svijetu. Već i sada eduroamu se vrlo jednostavno može pristupiti preko Mac OS X operacijskog sustava, a najavljuje se dodatno usavršavanje pristupa preko Android uređaja. U Hrvatskoj je eduroam poprilično raširen (Slika 10), ali postoji mogućnost uvođenja eduroam *hot spot*-ova u još nekim gradovima, primjerice u Šibeniku. Jedini problem za eduroam predstavlja prije spomenuta činjenica da je on nekomercijalan i svako daljnje proširenje i plan za budućnost ovisi o entuzijazmu njegovih članova, a to su studenti, profesori i drugi članovi akademskih zajednica. Eduroam uskoro planira riješiti problem različitih mogućnosti pristupa na različitim mjestima. Primjerice, postavke vatrozida korisnika u posjećenom mjestu mogu biti drugačije od onih korištenih u matičnom mjestu i postoji mogućnost pristupa manjem broju servisa nego u matičnom mjestu. Ovim planom uklonit će se takav tip problema. Krajnji cilj eduroama je izgradnja zajednice u kojoj će svakom njenom članu biti omogućen pristup Internetu gdje god se on u svijetu našao. Tome u prilog ide i eduroamov moto i misao vodilja: „*Open your laptop and be online*“.



Slika 14. Porast broja korisnika eduroama u 2008. godini.
Izvor: wiki.bc.net

6. Zaključak

Eduroam je do sada već postao svjetski *roaming* servis za akademske ustanove. Eduroam omogućuje korisnicima članica eduroam zajednice zaštićen Internet pristup u instituciji članici eduroam zajednice u kojoj se trenutno nalaze. Eduram je baziran na najsigurnijim enkripcijskim i autentikacijskim standardima koji trenutno postoje, a informacijska sigurnost eduroama uvelike nadilazi tipične komercijalne *roaming* servise. Infrastrukturna mreža eduroama je hijerarhijski sastavljena. Sačinjavaju je konfederacijski, federacijski i federacijski poslužitelji. Ti poslužitelji su najčešće RADIUS poslužitelji. Korisnik se na eduroam mrežu spaja preko NAP (eng. *Network Access Point*) uređaja. Zahtjev za pristup mreži se od korisnika preko AP-a šalje do autentikacijskog poslužitelja koji u svojim bazama provjerava korisničke podatke i vraća korisniku dozvolu pristupa. Protokol kojim se korisnički podaci i potvrda pristupa šalju preko mreže zove EAP (protokol protokol IEEE 802.1X standarda za kontrolu pristupa mreži). Eduroam je stigao u Hrvatsku zahvaljujući AAI@EduHr projektu. Za realizaciju eduroam servisa u Hrvatskoj koriste se imeničke sheme i LDAP imenici. LDAP imenici sadrže elektroničke identitete korisnika eduroama iz određene institucije. U Hrvatskoj eduroam pristupnih mjesta (eng. *Access Point*) ima već mnogo, a planira se i daljnje širenje eduroam mreže. Autentikacijski mehanizmi temelje se na EAP protokolu, a u Hrvatskoj se preporuča upotreba TTLS/PAP ili EAP-TTLS/EAP-GTC autentikacijskog mehanizma.

7. Reference

[1] Srce: Autentikacijska i autorizacijska infrastruktura AAI@EduHr, http://www.srce.hr/it-strucnjaci/aaieduhr/, siječanj 2011.

[2] Eduroam: What is eduroam, http://www.eduroam.org/, veljača 2011.

[3] C. Rigney: RADIUS Accounting, https://datatracker.ietf.org/doc/rfc2866/, lipanj 2000.

[4] AAI@EduHr: Što nudi AAI@EduHr (zašto je važna)?, http://www.aaiedu.hr/, siječanj 2010.

[5] Eduroam: Za korisnike, http://www.aaiedu.hr/docs/2009-09-eduroam%20-%20korisnici.pdf, kolovoz 2007.

[6] Miroslav Kiš: Informatički rječnik, Zagreb 2002.