Stanje AAI@EduHr i planovi za 2016. godinu

Miroslav Milinović, Srce

aai@srce.hr

Dan AAI@EduHr

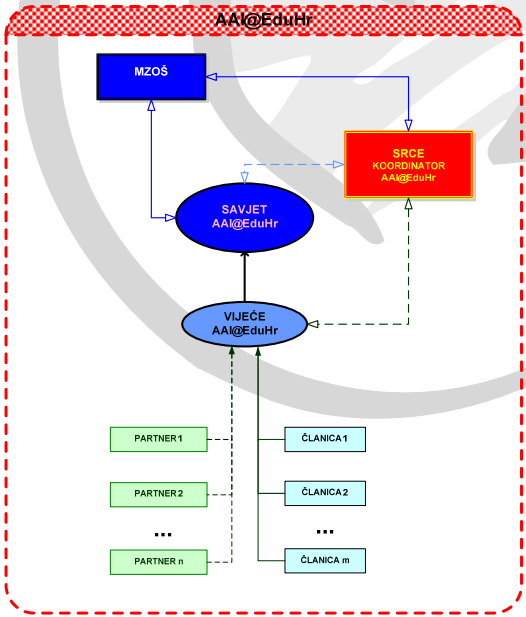
Zagreb, 25. studenog 2015.

srce

Sveučilište u Zagrebu
Sveučilišni računski centar

AAI@EduHr

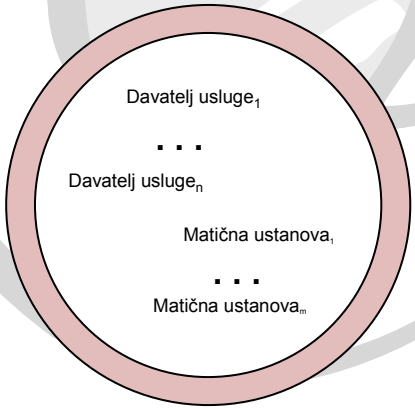
- **Autentikacijska i autorizacijska infrastruktura znanosti i (visokog) obrazovanja u RH**
- **u produkciji od 1. ožujka 2006.**
- ***hub-and-spoke* arhitektura**
- **31. listopada 2015. godine:**
  - 228 matičnih ustanova (imenika)
  - 845.530 elektroničkih identiteta
  - 454 usluge (resursa)
  - sastavnice (svi subjekti) http://www.aaiedu.hr/sastavnice/
  - povezana u globalne sustave eduroam i eduGAIN
- **web: http://www.aaiedu.hr**
- **e-mail: aai@srce.hr**
- **Pravilnik o ustroju, ver.1.3.1.** (http://www.aaiedu.hr/docs/AAI@EduHr-pravilnik-ver1.3.1.pdf)



Sigurnost i zaštita privatnosti

- zaštita kroz 3 vrste mjera:
  - organizacijske
  - informacijske
  - tehničke (tehnološke)

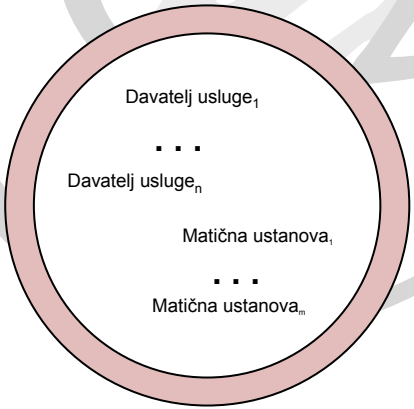
- osnovni elementi:
  - Pravilnik o ustroju
  - sustav certificiranja subjekata (matičnih ustanova i usluga)
  - arhitektura (i korišteni protokoli) sustava AAI@EduHr
  - registri matičnih ustanova i usluga u sustavu AAI@EduHr



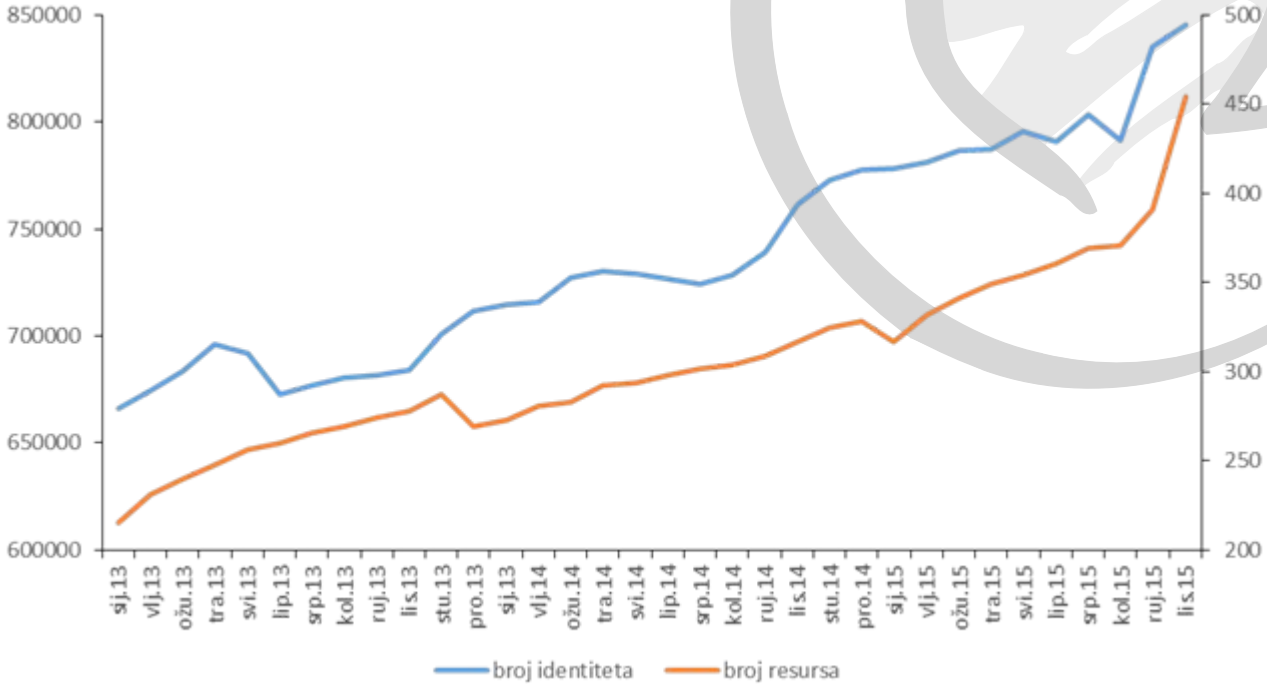
- **iznimno je važno da se matične ustanove pridržavaju normi i svojim postupcima ne ugrožavaju privatnost i sigurnost e-identiteta**

Sustav certificiranja

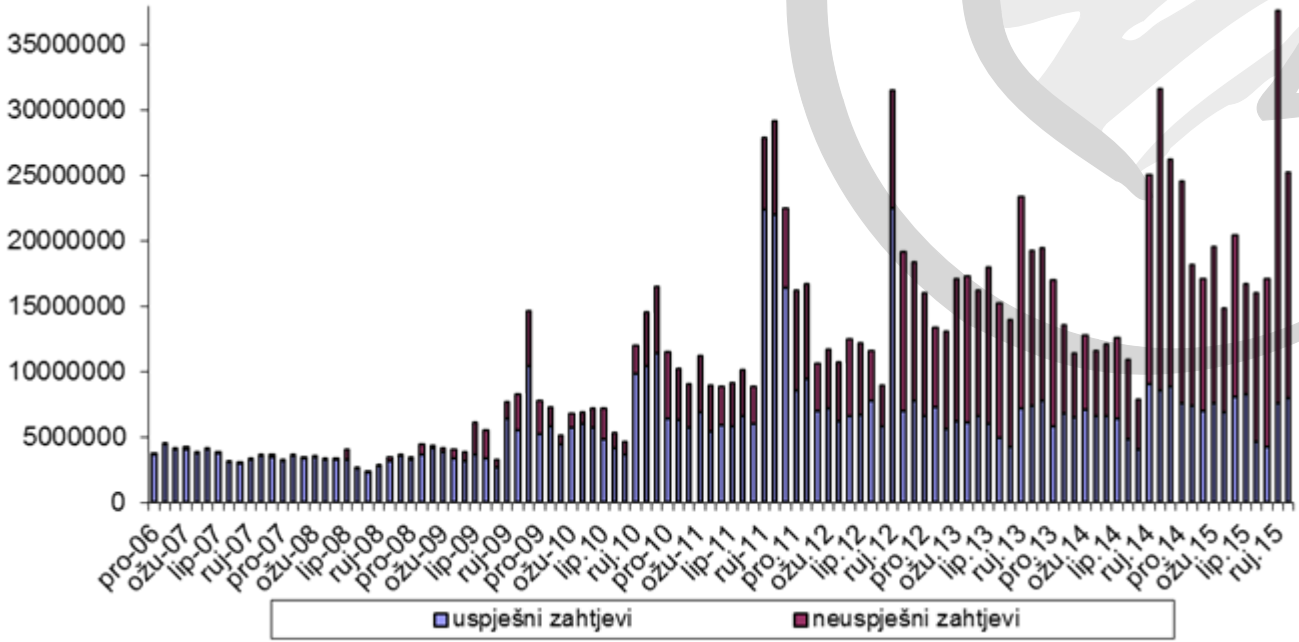
- subjekt certificiranja = matična ustanova ili usluga
- certificiranje = provjera usklađenosti subjekta s normama koje su:
  - organizacijske
  - informacijske
  - tehničke (tehnološke)
- provjere provodi:
  - subjekt (samoprovjerom)
  - Srce - Koordinator AAI@EduHr (neposrednim uvidom ili korištenjem nadzornih/testnih programa/uređaja)
- http://www.aaiedu.hr/certificiranje/



AAI@EduHr u brojkama
(kretanje broja identiteta i registriranih resursa)

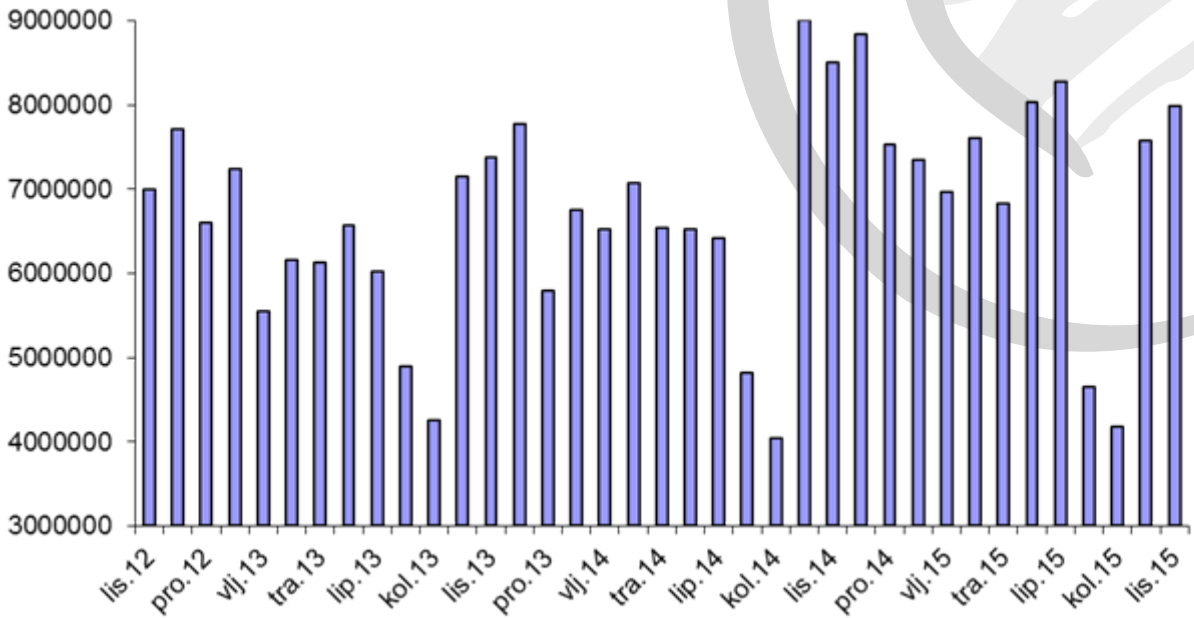


AAI@EduHr u brojkama
(promet na središnjim RADIUS poslužiteljima)



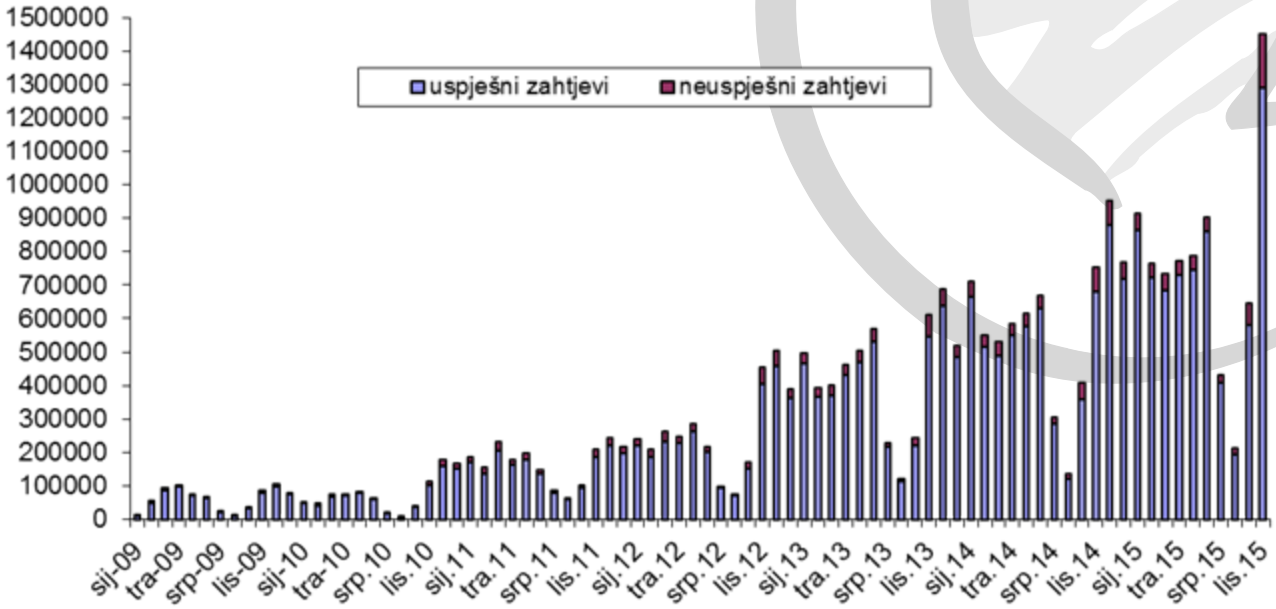
7.377.796 (10.2013.) : 8.509.311 (10.2014.) : 7.987.728 (10.2015.) uspješnih zahtjeva

Kretanje broja uspješnih autentikacija na središnjim RADIUS poslužiteljima



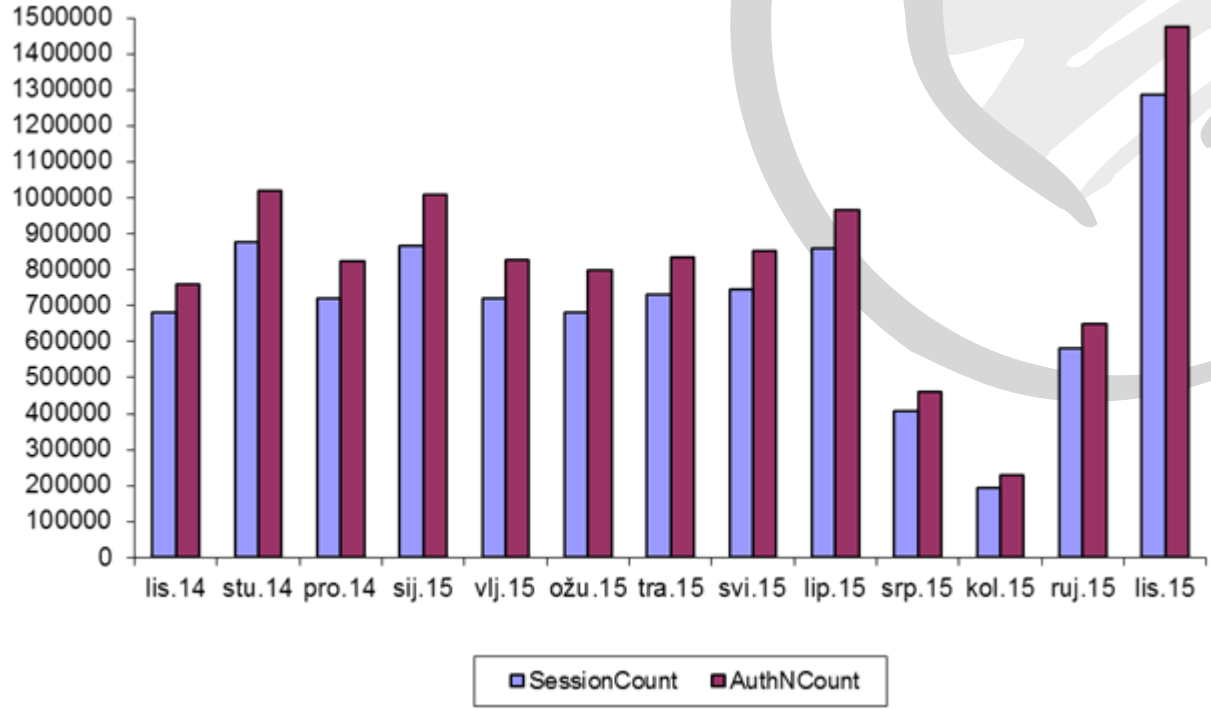
7.377.796 (10.2013.) : 8.509.311 (10.2014.) : 7.987.728 (10.2015.) uspješnih zahtjeva

AAI@EduHr u brojkama
(promet na središnjim SSO/login poslužiteljima)

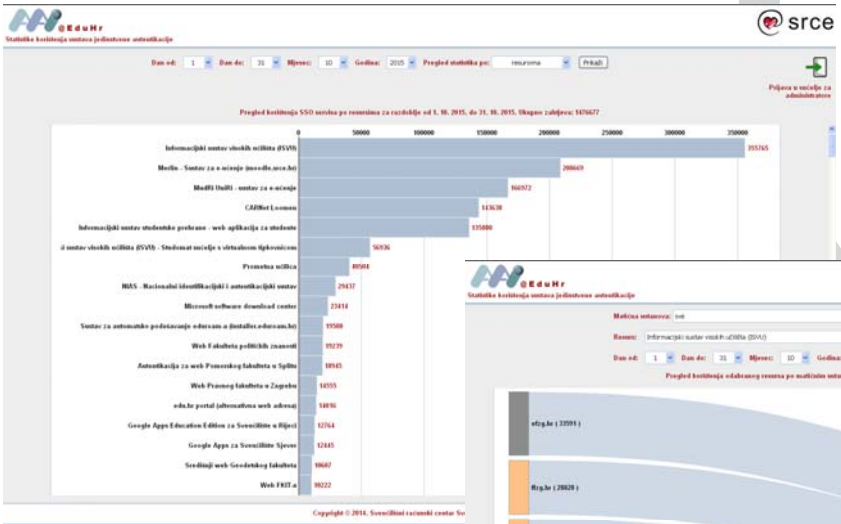


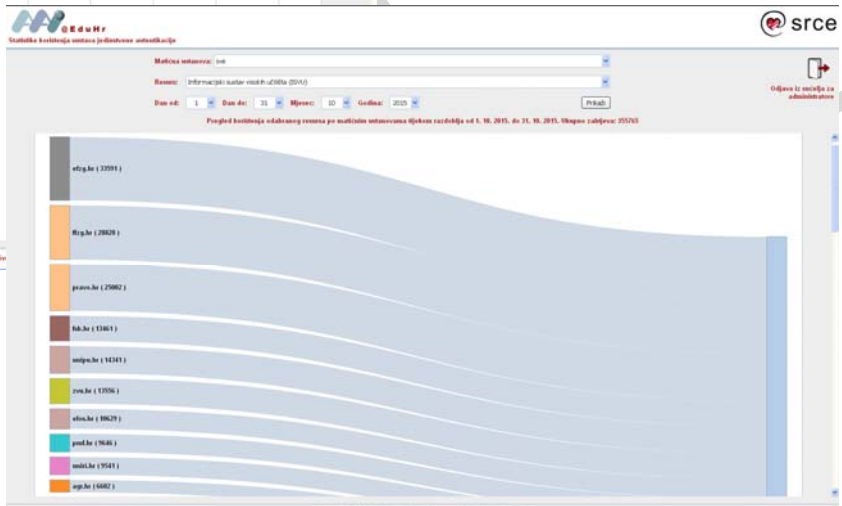
546.751 (10.2013.) : 680.314 (10.2014.) : 1.287.701 (10.2015.) uspješnih zahtjeva

Kretanje broja uspješnih autentikacija na središnjim SSO poslužiteljima

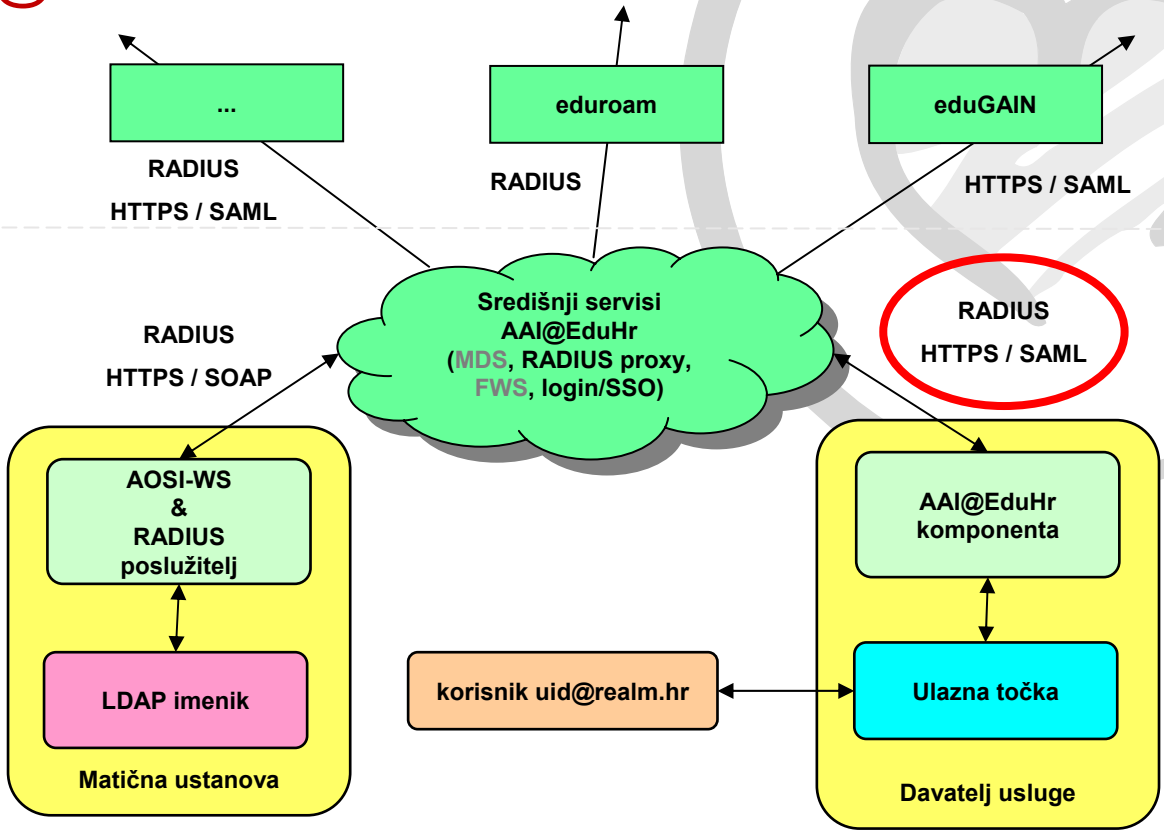


AAI@EduHr u brojkama (http://f-ticks.aaiedu.hr/statistike/)

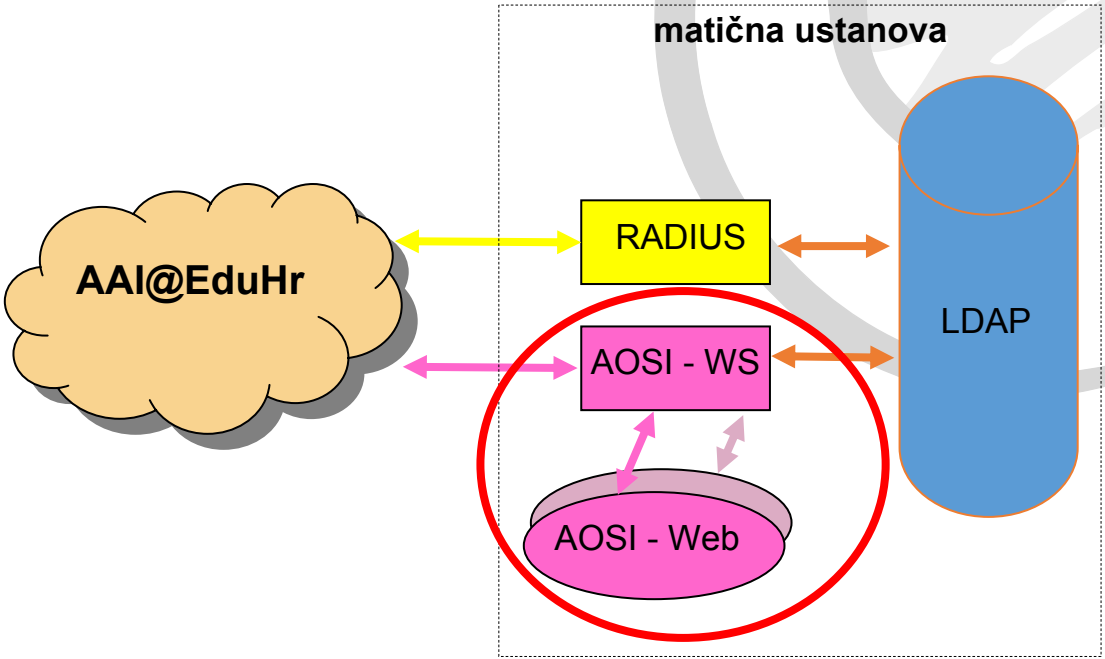




AAI@EduHr - arhitektura



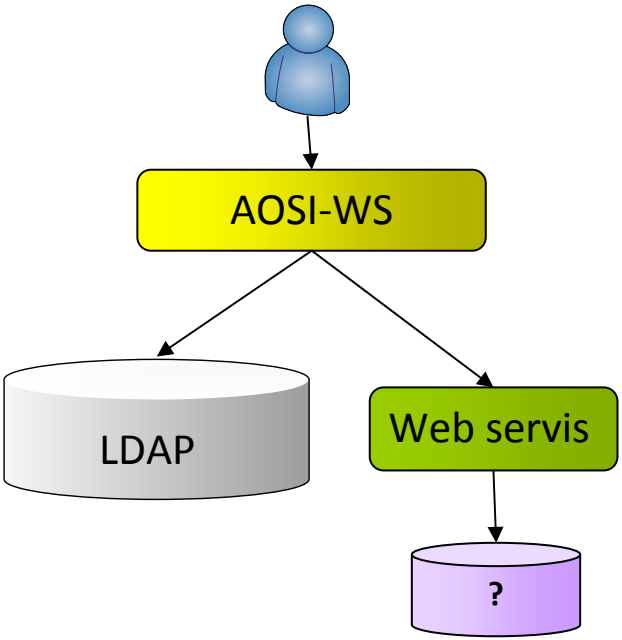
AAI@EduHr: IdM



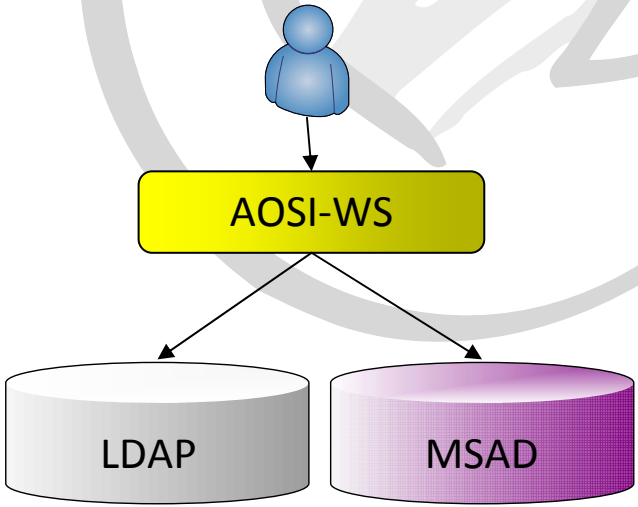
AOSI sustav plug-inova

- okidaju se akcije:
  - **`beforeAddUser`** - prije pokušaja dodavanja e-identiteta u LDAP
  - **`afterAddUser`** - nakon pokušaja dodavanja e-identiteta u LDAP
  - **`beforeDeleteUser`** - prije pokušaja brisanja e-identiteta iz LDAP-a
  - **`afterDeleteUser`** - nakon pokušaja brisanja e-identiteta iz LDAP-a
  - **`beforeChangeAttribute`** - prije pokušaja promjene e-identiteta u LDAP-u
  - **`afterChangeAttribute`** - nakon pokušaja promjene e-identiteta u LDAP-u
- **`before*`** akcije mogu otkazati izvođenje plug-inova ili slijedeće osnovne funkcije
- **`before*`** akcije mogu proslijediti poruke **`after*`** akcijama
- moguće je aktivirati više plug-inova koji se izvršavaju slijedno
- dokumentacija na webu (http://www.aailedu.hr / http://developer.aaiedu.hr)

AOSI plug-inovi: primjeri

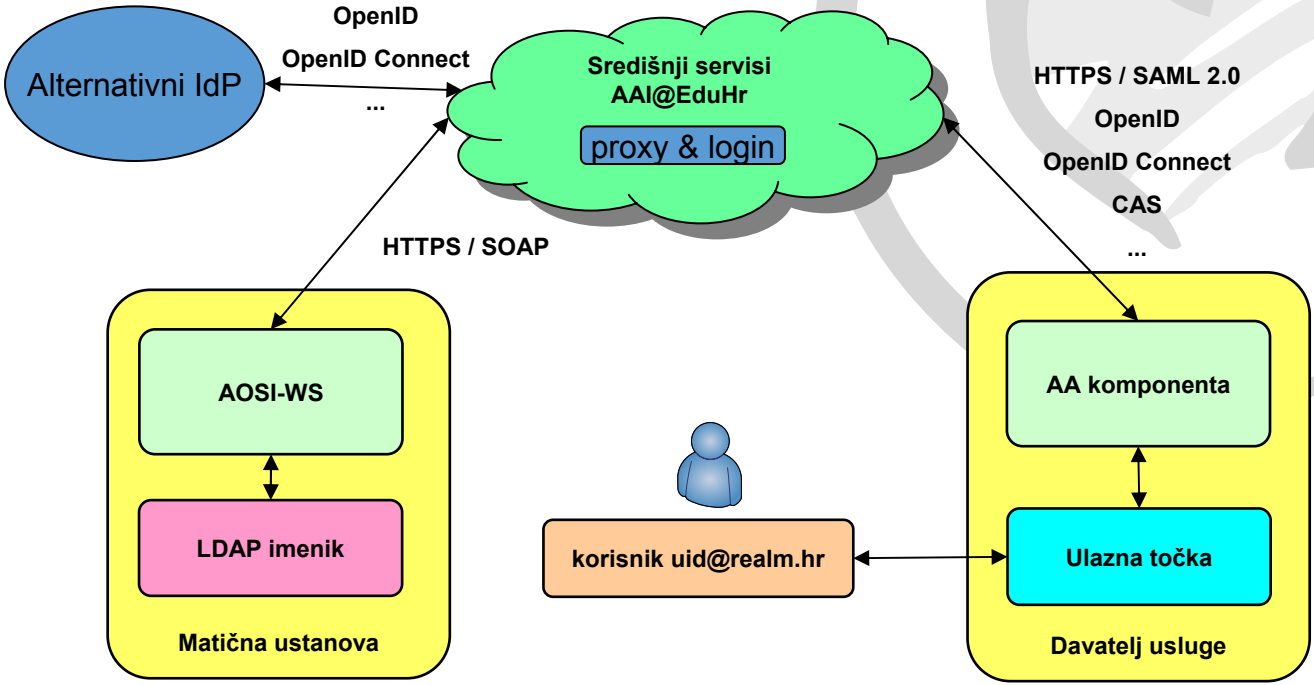


Web service plug-in

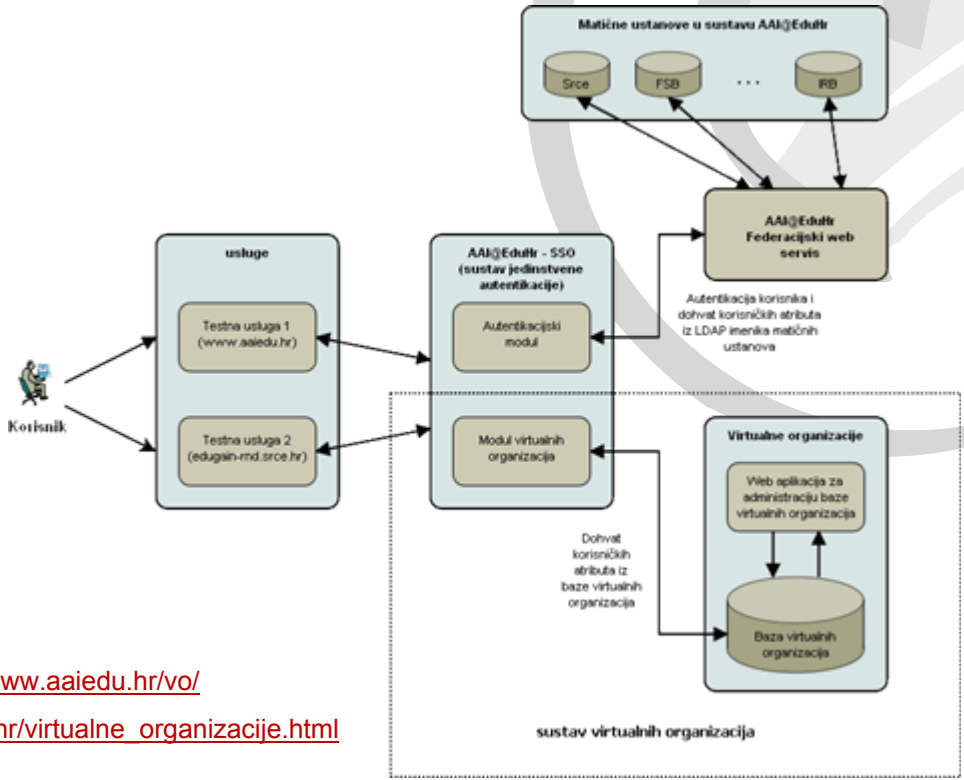


MS Active Directory plug-in

Alternativni protokoli



Upravljanje grupama (VO) u sustavu AAI@EduHr



http://www.aaiedu.hr/vo/

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

Sustav eduGAIN

- Inter-federacijska usluga razvijena u okviru projekta GÉANT
- povezuje federacije e-identiteta (AAI infrastrukture)
  - primarno nacionalne znanstvene i obrazovne AAI
- temeljni cilj: olakšati međunarodnu suradnju i razmjenu informacija kroz povezivanje nacionalnih AAI
- ključno je osigurati povjerenje među svim čimbenicima (federacije, IdP-ovi, SP-ovi)
  - jasno definirana pravila i norme (*Policy Framework*)
  - sigurna i pouzdana tehnička rješenja

AAI@EduHr u eduGAIN-u

- AAI@EduHr je punopravna članica eduGAIN-a
- Srce kao koordinator/operator zastupa AAI@EduHr u tijelima eduGAIN-a

- model koji primjenjujemo:
  - sve matične ustanove su uključene samim povezivanjem AAI@EduHr u eduGAIN
    - isporuka atributa prema preporuci eduGAIN Attribute Profile
    - moguće je zatražiti isključivanje (opt-out)
  - usluge ulaze isključivo na vlastiti zahtjev (opt-in)
    - moraju ispuniti potrebne tehničke i organizacijske uvijete

- više informacija o eduGAIN-u
  - http://www.edugain.org

Kako uslugu povezati u eduGAIN?

- obavijestiti Srce (koordinatora federacije) o namjeri
  - Srce pruža potrebnu tehničku i organizacijsku potporu
- prilagoditi pravila usluge
  - Privacy policy / CoCo
- provesti potrebne tehničke prilagodbe vezane uz
  - upravljanje atributima i pravima pristupa
  - prilagodbu WAYF / login sučelja
  - publiciranje i dohvat metapodataka
  - provjeru tehničke ispravnosti svih komponenti (uključivo i certifikat poslužitelja)
- Srce obavlja prijavu usluge i publiciranje odgovarajućih metapodataka u eduGAIN MDS

AAI@EduHr Lab

- okruženje za testiranje i razvoj novih aplikacija
- tehnološki identično produkcijskom sustavu, ali bez mogućnosti korištenja produkcijskih središnjih servisa i podataka (tj. e-identiteta)
- na raspolaganju svim (potencijalnim) davateljima usluga
- usluge koje su u registru resursa označene kao testne mogu rabiti samo AAI@EduHr Lab okruženje
- http://fed-lab.aaiedu.hr/

Izdvojeno (2015.)

- **unaprijeđena redundancija središnjih servisa**

- **politika promjene početne lozinke**
  - mehanizam*: LDAP pasword policy overlay*
  - novi paketi za matične ustanove bit će raspoloživi u prosincu 2015.
  - prilagodba središnjeg SSO/login servisa

- **podrška davateljima usluga**
  - **ISVU** u potpunosti koristi autentikaciju putem AAI@EduHr
  - podrška za **Office 365** (osiguran automatski *provisioning*)
  - unaprijeđene upute, podrška za dodatne alate i platforme
  - broj resursa se znatno povećao u proteklih godinu dana (317 → 454)

- **novi Web** (objava u prosincu)

- **certifikati za RADIUS i AOSI-WS poslužitelje matičnih ustanova**

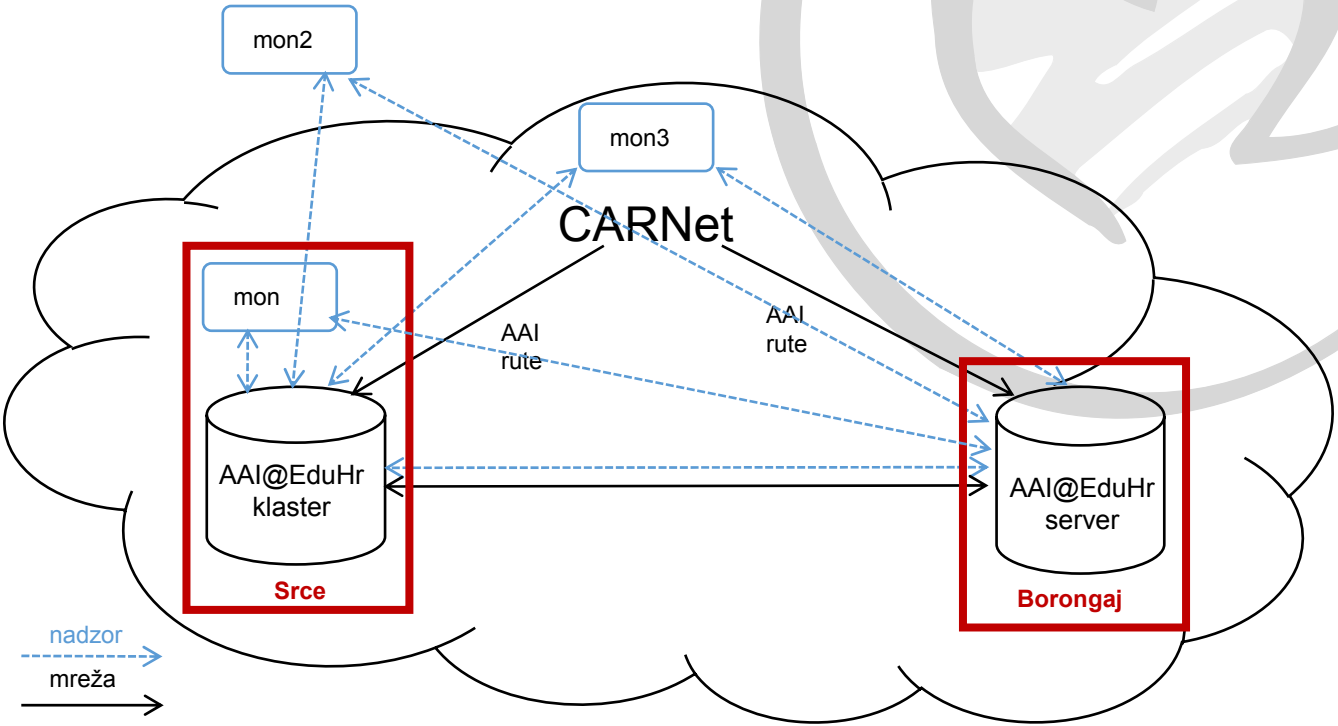
Redundancija u sustavu AAI@EduHr (1)

- središnji servisi sustava AAI@EduHr smješteni su na računalnim klasteru koji se sastoji od tri poslužitelja
- u slučaju ispada bilo kojeg čvora, ostali čvorovi preuzimaju njegove servise
- Što u slučaju mrežnog ispada hale u Srcu, havarije, nestanka struje?
  - RADIUS klijenti se mogu podesiti tako da im sekundarni RADIUS poslužitelj bude bilo gdje.
  - poseban izazov: (web) klijenti koji rabe SSO/login sustav
- **novo rješenje**: poslužitelj na izdvojenoj lokaciji (novi podatkovni centar Srca na kampusu Borongaj) koji po potrebi automatski preuzima funkcije poslužitelja u zgradi Srca

Redundancija u sustavu AAI@EduHr (2)

- **novo rješenje: u punoj produkciji od rujna 2015.**
- na poslužitelju na izdvojenoj lokaciji
  - stalno su aktivni RADIUS i FWS servisi koji rade kao sekundarni poslužitelji za sve usluge koje koriste te protokole
  - održava se funkcionalna replika MDS baze
- tri nadzorna sustava nadziru rad SSO servisa
  - jedan iz mreže Srca
  - jedan iz CARNet mreže
  - jedan van CARNet mreže
- u slučaju da bar dva nadzorna sustava zaključe da SSO nije dostupan (a nijedan od njih ne tvrdi suprotno) SSO servis se seli na poslužitelj na izdvojenoj lokaciji
- seljenje je potpuno automatsko i neprimjetno za korisnike

Redundancija u sustavu AAI@EduHr (3)



Politika promjene zaporke u sustavu AAI@EduHr

- preporuka: korisnici trebaju obavezno promijeniti zaporku po otvaranju elektroničkog identiteta ili nakon što im administrator promijeni zaporku
- u praksi korisnici zanemaruju preporuku i sve se vrijeme koriste zaporkom koja im je inicijalno dodijeljena
- uvođenjem politike promjene zaporke podiže se razina sigurnosti sustava
  - realizirana je uporabom modula *ppolicy overlay* na razini LDAP imenika
  - zahtjeva promjene u (skoro) svim komponentama sustava

Nova pravila (Što se mijenja?)

- Svi će korisnici po otvaranju elektroničkog identiteta ili nakon što im administrator promijeni zaporku, biti **obavezni promijeniti svoju zaporku** u sljedećih 48 sati.
- Ako u tom roku ne promijene zaporku, po isteku roka imat će pravo prijaviti se svojim elektroničkim identitetom još pet (?) puta, a zatim će im se elektronički identitet zaključati.
- Zaključane elektroničke identitete moći će otključati samo administrator, a korisnici će po otključavanju opet morati promijeniti zaporku.
- Da bi se korisnicima olakšala promjena zaporke uvodimo središnje sučelja za promjenu zaporke.
- Korisnik koji mora promijeniti zaporku, nakon što se autenticira putem SSO, preusmjerava se na središnje sučelje za promjenu zaporke, a po uspješnoj promjeni zaporke dalje na uslugu kojoj je pokušao pristupiti.

Kako i kada započeti s primjenom politike promjene zaporke?

- potrebno je nadograditi sve *–aai pakete*
- upute i dokumentacija bit će objavljeni na webu AAI@EduHr (12/2015.)
- krajnji rok za migraciju → certificiranje matičnih ustanova za 2016.

- potencijalni problem: korisnici koji se autenticiraju isključivo RADIUS protokolom ne vide tekst upozorenja da moraju promijeniti zaporku
- otključavanje: putem web sučelja za ažuriranje sadržaja imenika

Plan i iskoraci u 2016.

- izrada nove vezije AOSI-WS
  (povećana pouzdanost i robustnost, upravljanje certifikatima)
- povezivanje sa sustavom ORCID
- revizija središnje baze MDS i usklađivanje s (novim) eduGAIN preporukama
- uspostava središnjeg IdP po načelu *"home for homeless"*
- unaprijeđena primjena certifikata za sve subjekte u sustavu AAI@EduHr
- implementacija višestupanjske autentikacije na odabranim uslugama u sustavu AAI@EduHr
- izrada nove verzije Pravilnika o ustroju sustava AAI@EduHr

- daljnje unapređenje redundantnosti i robustnosti središnjih servisa
- redovita certificiranja matičnih ustanova i usluga

Kako dalje?

- javite nam se ukoliko:
  - želite koristiti
    - VO u sustavu AAI@EduHr
    - alternativne načine autentikacije (npr. društvene mreže)
  - želite svoju aplikaciju učiniti dostupnom putem eduGAIN-a
  - vaša aplikacija/sustav zahtjeva posebne metode ili protokole

- predložite:
  - aplikaciju ili platformu čiju prilagodbu želite provesti
  - promjenu/nadogradnju nekog segmenta sustava AAI@EduHr

http://www.aaiedu.hr/

aai@srce.hr

srce
Sveučilište u Zagrebu
Sveučilišni računski centar

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

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

www.srce.unizg.hr/otvoreni-pristup

srce
otvoreni pristup