

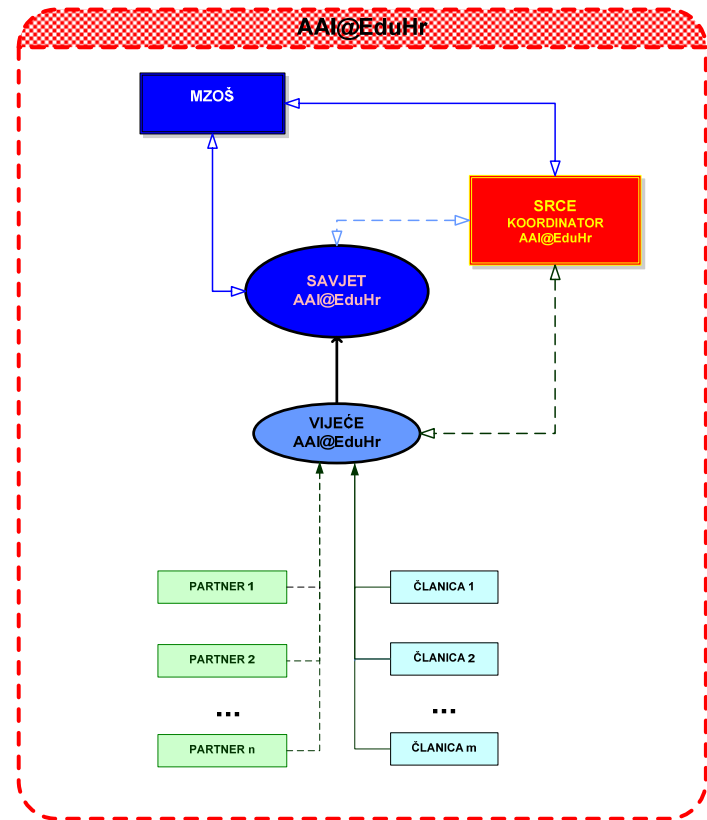


Stanje AAI@EduHr i planovi za 2014. godinu

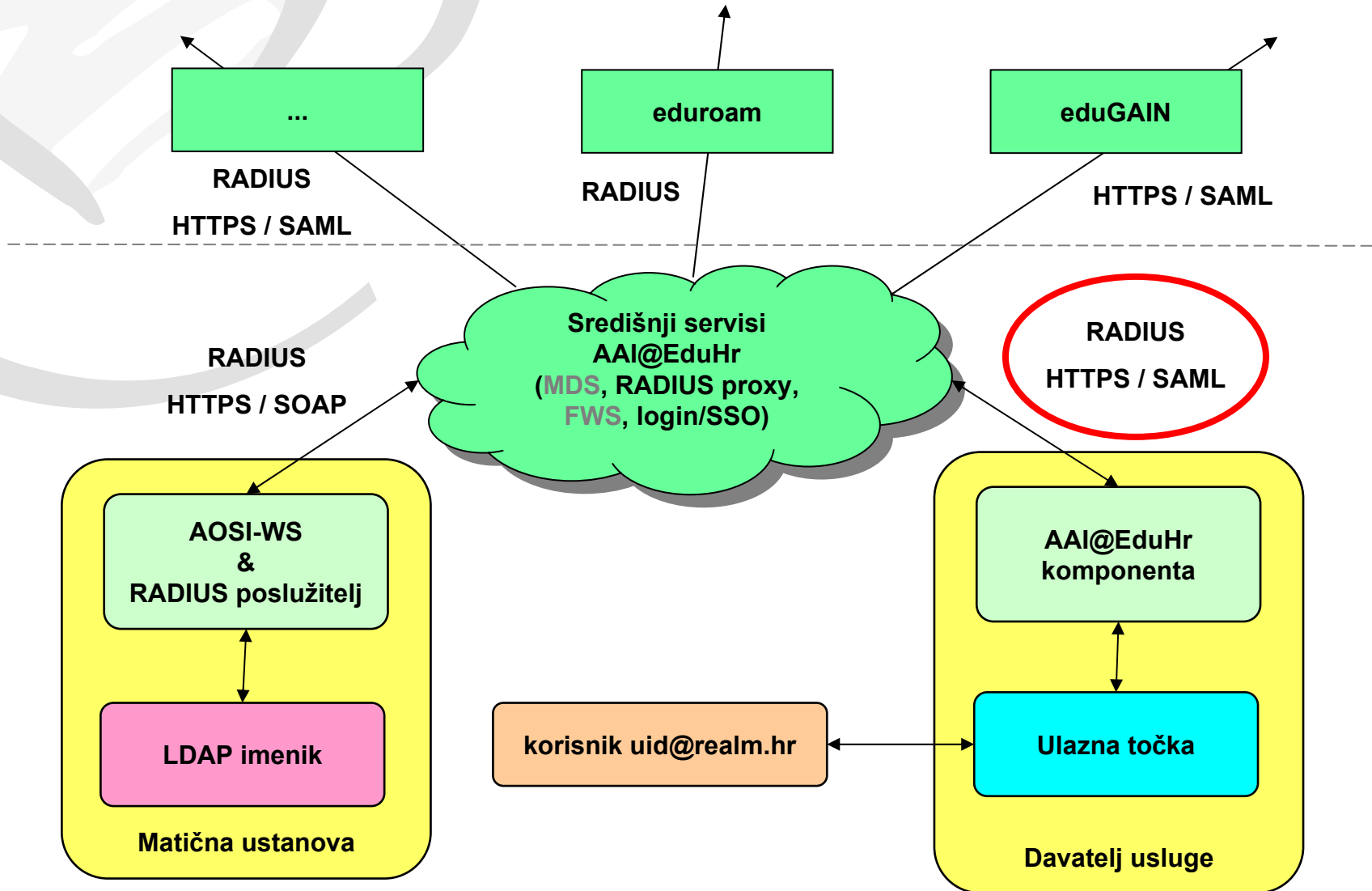
mr.sc. Miroslav Milinović, Srce
<team@aaiedu.hr>

AAI@EduHr

- ❖ Autentikacijska i autorizacijska infrastruktura znanosti i (visokog) obrazovanja u RH
- ❖ u produkciji od 1. ožujka 2006.
- ❖ *hub-and-spoke* arhitektura
- ❖ 30. studenog 2013. godine:
 - ♦ 226 matičnih ustanova (imenika)
 - ♦ 700.948 elektroničkih identiteta
 - ♦ 287 usluga (resursa)
 - ♦ povezana u globalne sustave eduroam i eduGAIN
- ❖ web: <http://www.aaiedu.hr>
- ❖ e-mail: team@aaiedu.hr
- ❖ Pravilnik o ustroju, ver.1.3.1.
(<http://www.aaiedu.hr/docs/AAI@EduHr-pravilnik-ver1.3.1.pdf>)

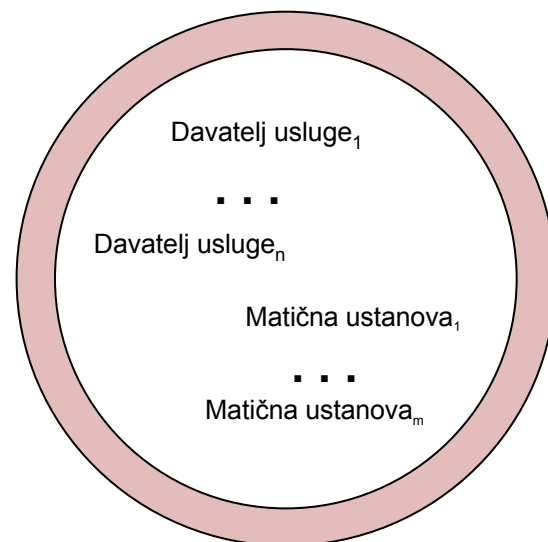


AAI@EduHr



Registri sustava AAI@EduHr

- ❖ registar matičnih ustanova
 - ♦ http://www.aaiedu.hr/aa_i_status.php
- ❖ registar partnera
 - ♦ http://www.aaiedu.hr/partneri_federacije.php
- ❖ registar usluga
 - ♦ <http://www.aaiedu.hr/aairr/>
 - ♦ javni popisi usluga:
 - http://www.aaiedu.hr/usluge_pristupa_mrezi.php
 - http://www.aaiedu.hr/usluge_pristupa_aplikacijama.php
- ❖ sastavnice (svi subjekti)
 - ♦ <http://www.aaiedu.hr/sastavnice/>

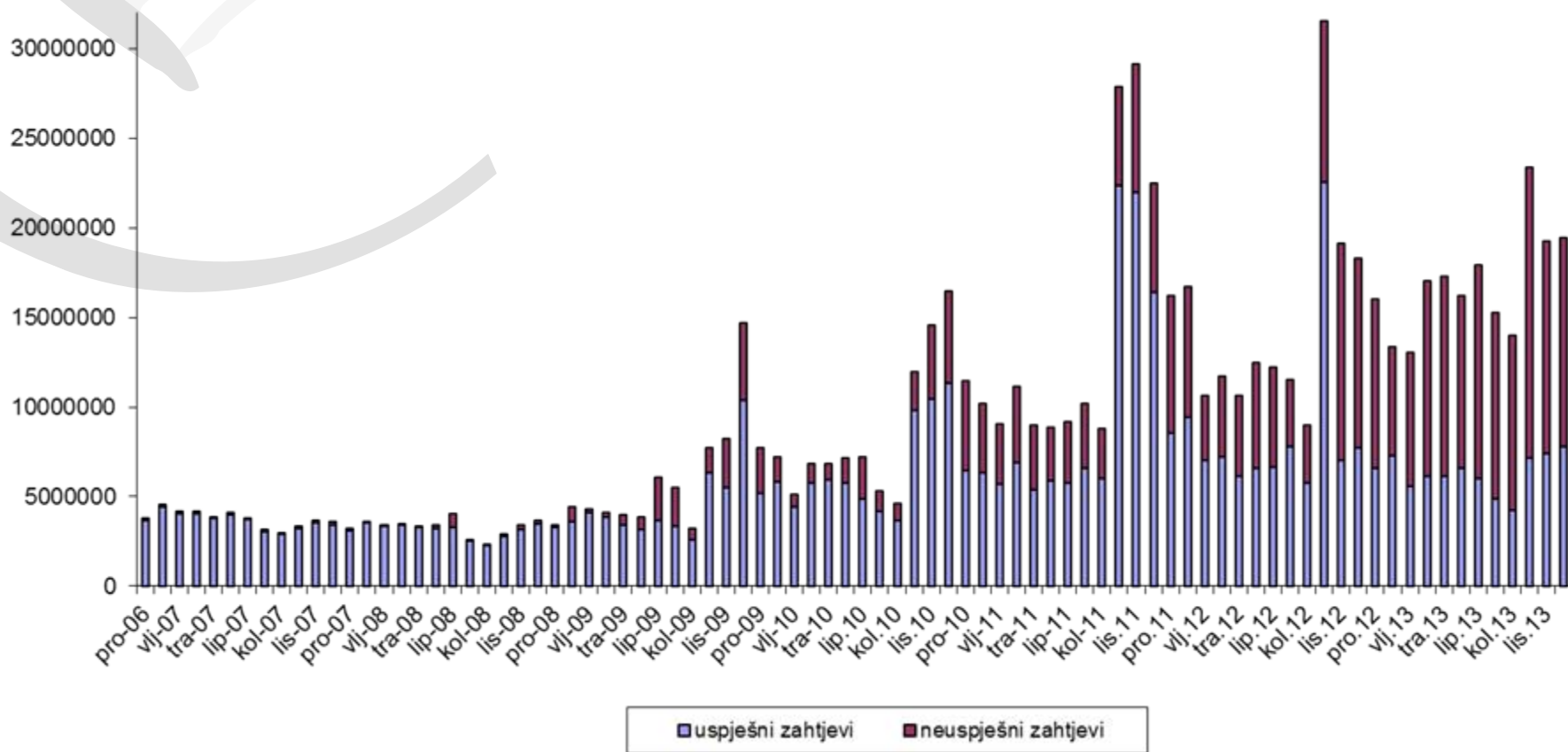


Sustav certificiranja

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

AAI@EduHr u brojkama

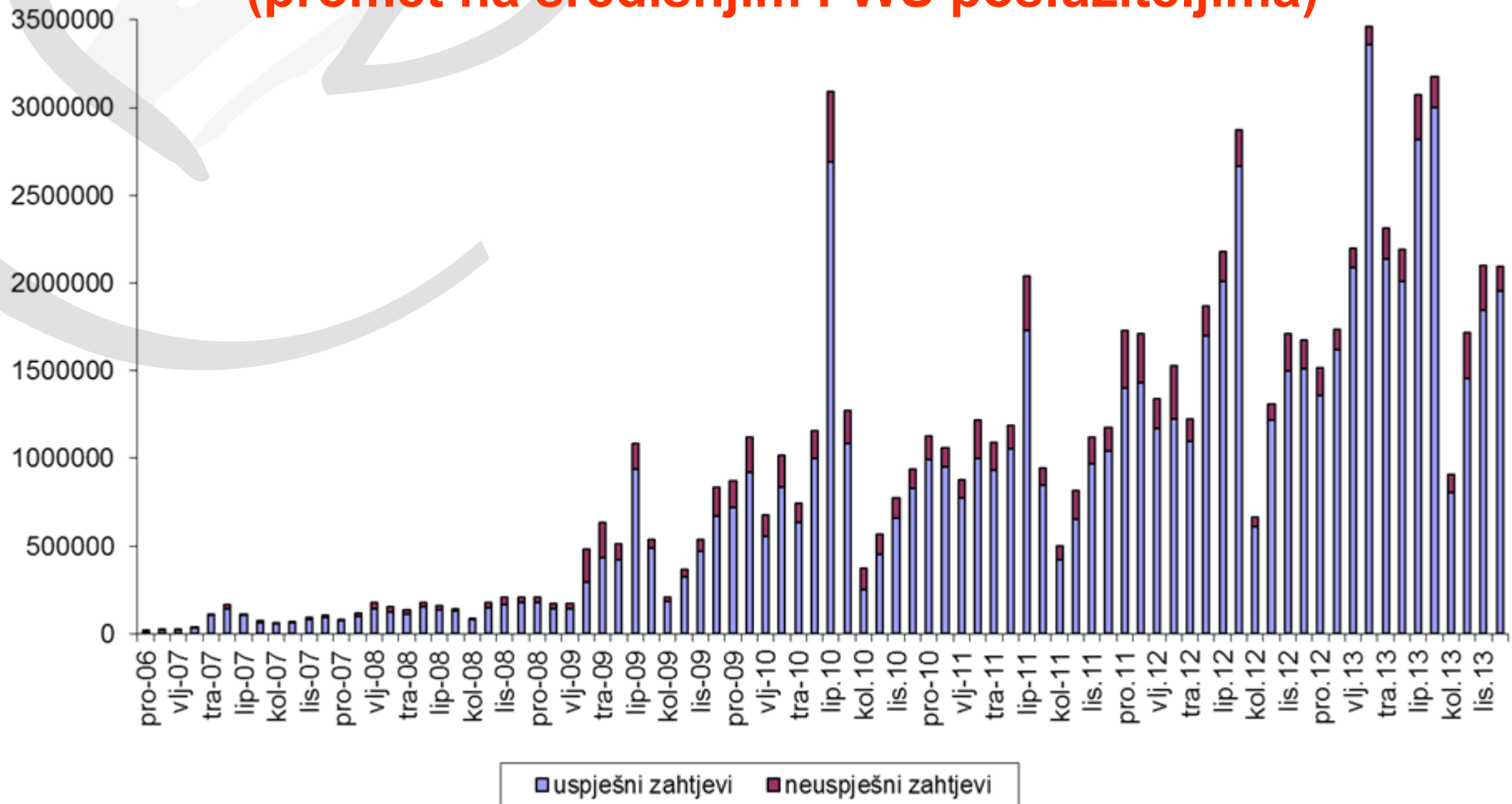
(promet na središnjim RADIUS poslužiteljima)



18.316.207 (11.2012.) : 19.438.350 (11.2013.) obrađenih zahtjeva

AAI@EduHr u brojkama

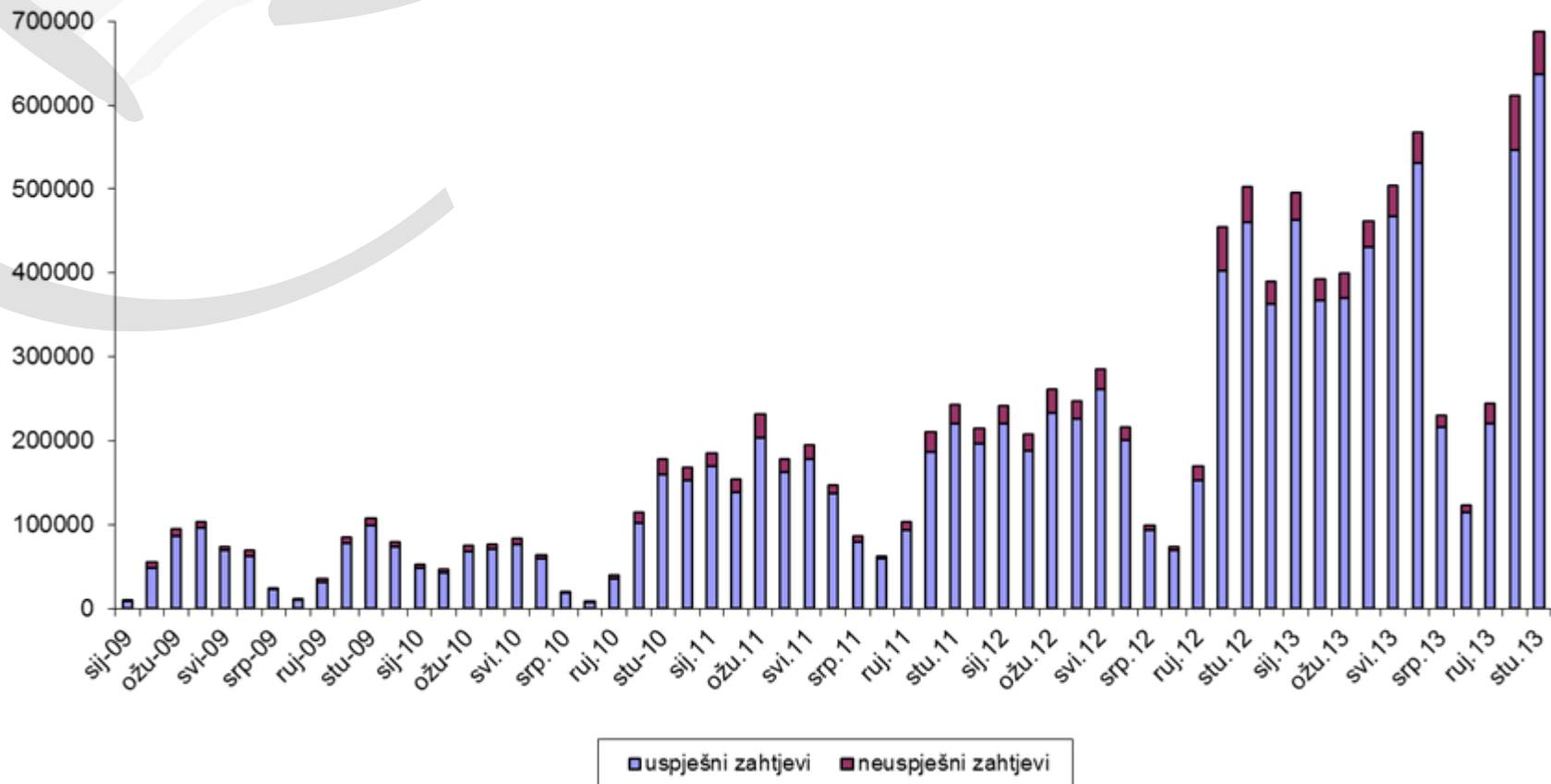
(promet na središnjim FWS poslužiteljima)



1.672.821 (11.2012.) : 2.095.999 (11.2013.) obrađenih zahtjeva

AAI@EduHr u brojkama

(promet na središnjim SSO/login poslužiteljima)



502.373 (11.2012.) : 687.564 (11.2013.) obrađenih zahtjeva

Izdvojeno (2013.)

- ❖ **AAI@EduHr Lab u produkciji**
- ❖ **nadogradnje središnjih servisa**
 - ♦ MDS, SSO login, nadzor
- ❖ **certificiranje subjekata**
 - ♦ unaprijeđen postupak certificiranja matičnih ustanova
 - ♦ unaprijeđena kvaliteta podataka o uslugama
- ❖ **povezivanje sustava AAI@EduHr sa srodnim sustavima**
 - ♦ eduroam, eduGAIN, **NIAS**, ...
- ❖ **programski paketi**
 - ♦ Debian Wheezy
 - ♦ AOSI WS plugins, SPONA
- ❖ **podrška davateljima usluga**
 - ♦ alternativni mehanizmi autentikacije
 - ♦ unaprijeđene upute, podrška za dodatne alate i platforme

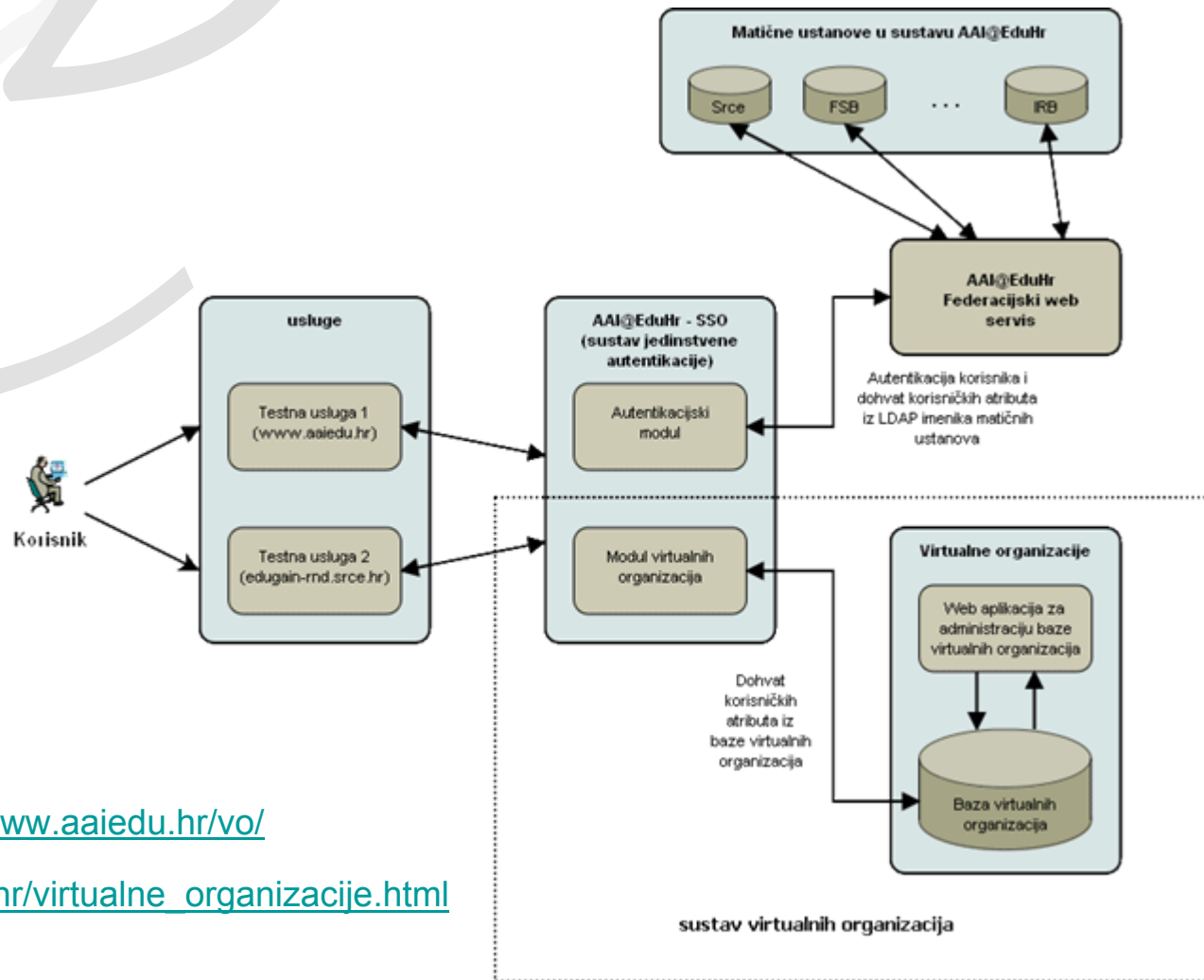
AAI@EduHr Lab

- ❖ 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/>

Izazovi za usluge ...

- ❖ SAML WebSSO profil zahtjeva uporabu web preglednika
- ❖ aplikacije koje ne koriste web preglednik /HTTP(s) protokol
- ❖ korisnici koji nemaju odgovarajući e-identitet
- ❖ aplikacije koje nije (lako) moguće prilagoditi uporabi SAML-a
- ❖ (složene) usluge koje zahtjevaju višestruku autentikaciju (npr. webmail)
- ❖ usluge koje zahtjevaju autentikaciju u više koraka (npr. username/password + PIN)
- ❖ potreba povezivanja različitih federacija e-identiteta (koje nužno ne koriste iste metode i protokole)
- ❖ aplikacije koje trebaju podatke o korisniku iz više izvora (VO)
- ❖ uSSO

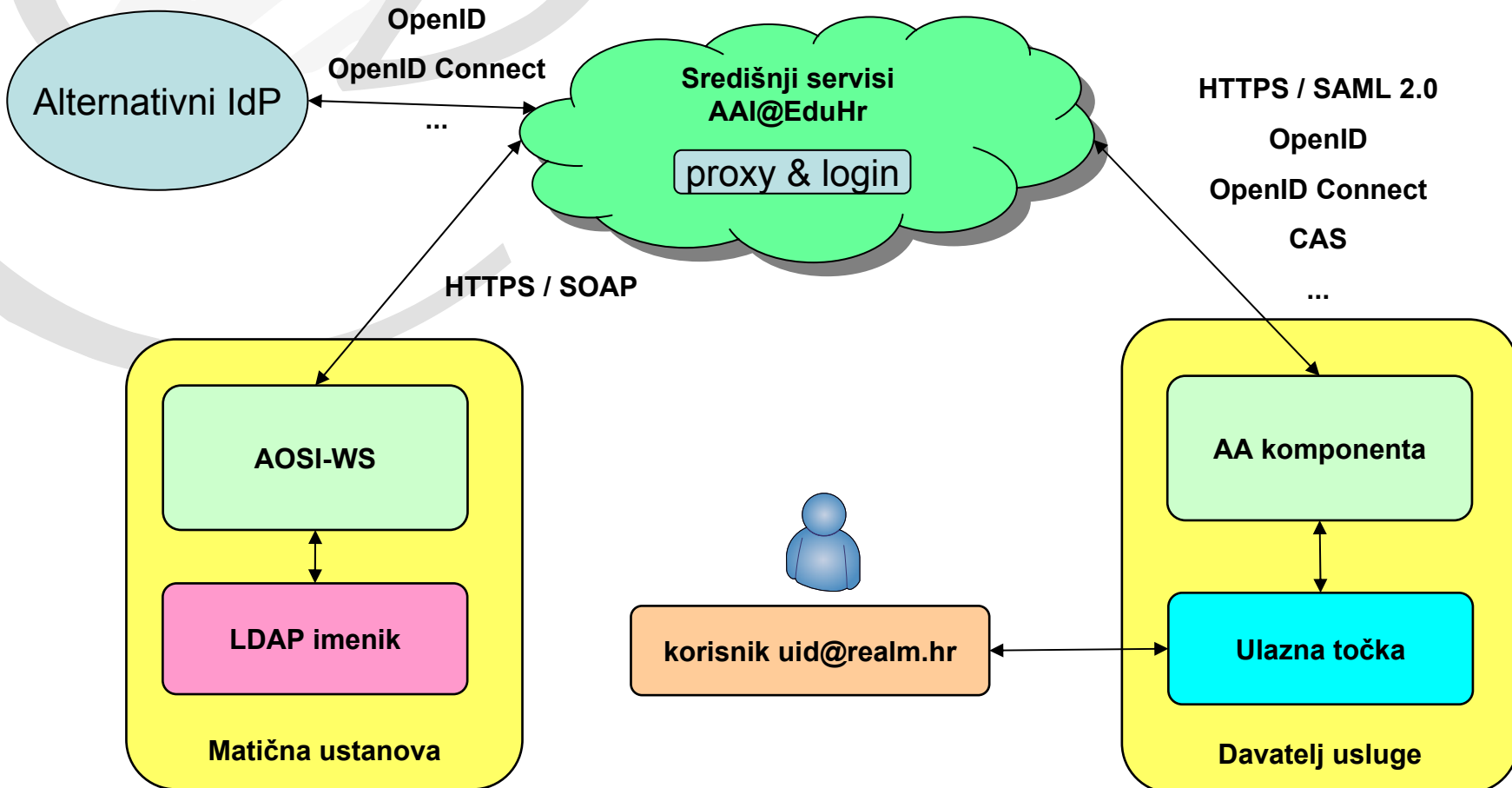
VO u sustavu AAI@EduHr



<http://www.aiedu.hr/vo/>

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

Alternativni protokoli



AAI@EduHr i društvene mreže

Odaberite autentifikacijski servis - Mozilla Firefox

File Edit View History Bookmarks Tools Help

AAI

Back Forward <https://login.aai.edu.hr/proxy/module.php/discopower/disco.php?entityID=https%3A%2F%2Flogin.aai.edu.hr%2Fproxy%2Fmodule.php%2Fsam%2Fsp%2Fmetadata.php%2Fdefault-sp&return=https%3A%2F...> Reload Stop Google Home

Most Visited Customize Links Free Hotmail Windows Marketplace Windows Media Windows Mature Blonde Sucks ...

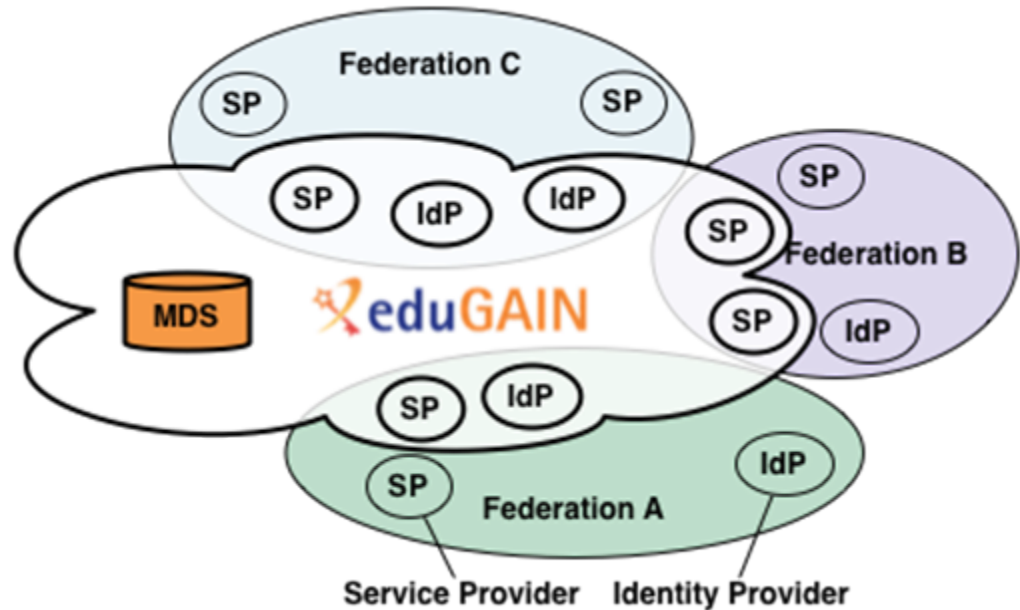
Odaberite servis preko kojeg se želite autentificirati

Incremental search...

- AAI@EduHr
- Facebook
- Google
- LinkedIn
- Twitter

<http://www.unizg.hr/authdemo/>

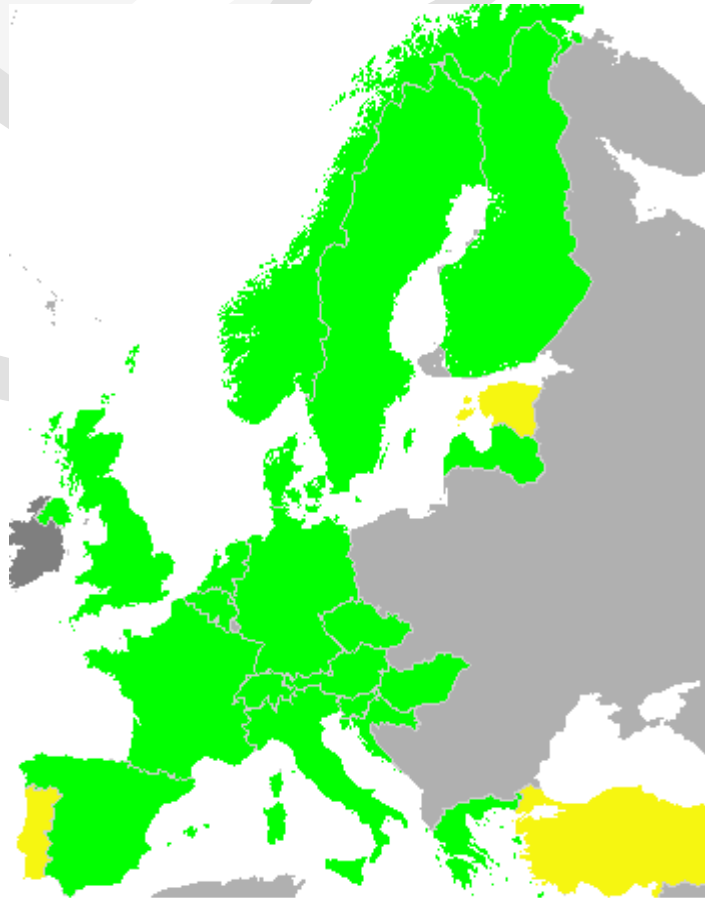
Što je eduGAIN?



- ❖ **educational Global Authentication Infrastructure**
- ❖ **dvije temeljne komponente:**
 - ◆ pravila i norme: eduGAIN Policy Framework
 - ◆ tehnički sustav: MDS (Metadata Distribution Service)

Koliko je eduGAIN raširen?

(studeni 2013.)



■ eduGAIN ■ Joining ■ Candidate



■ eduGAIN ■ Joining ■ Candidate

- ❖ u produkciji od 2011. godine
- ❖ 22 federacije članice
- ❖ 8 federacija u postupku pristupanja
- ❖ www.edugain.org

AAI@EduHr u eduGAIN-u

- ❖ AAI@EduHr je punopravna članica eduGAIN-a
- ❖ Srce kao koordinator/operator zastupa AAI@EduHr u tijelima eduGAIN-a
- ❖ *opt-in* model koji primjenjujemo:
 - ♦ sve matične ustanove su uključene samim povezivanjem AAI@EduHr u eduGAIN
 - isporuka atributa prema preporuci [eduGAIN Attribute Profile](#)
 - ♦ usluge ulaze isključivo na vlastiti zahtjev
 - moraju ispuniti potrebne tehničke uvijete

Kako uslugu povezati u eduGAIN

- ❖ obavijestiti Srce (koordinatora federacije) o namjeri
 - ♦ Srce pruža potrebnu tehničku i organizacijsku potporu
- ❖ prilagoditi pravila usluge
 - ♦ Privacy policy / CoC
- ❖ 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

Aplikacije koje ne koriste Web

- ❖ nove tehnologije, stalne izmjene/nadogradnje
- ❖ OpenID Connect 1.0 / OAuth 2.0
- ❖ Shibboleth ECP (Enhanced Client or Proxy)
 - ◆ koristi SOAP
 - ◆ za aplikacije koje ne koriste Web preglednike
- ❖ Moonshot (<https://community.ja.net/groups/moonshot>)

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 specifične metode ili protokole

- ❖ kontakt: team@aaiedu.hr

Plan i iskoraci u 2014.

- ❖ „*Enabling AAI@EduHr users*”
- ❖ nova inačica sustava FWS i AOSI (WS i WWW sučelje)
- ❖ primjena poslužiteljskih certifikata
- ❖ ispitivanje i pilot-uporaba alternativnih metoda i protokola za autentikaciju (CAS, OAuth, OpenId Connect, moonshot, autentikacija u više koraka)
- ❖ sigurnost i zaštita privatnosti (*consent*)
- ❖ unapređenje sustava nadzora i mjerenja prometa (*F-Ticks*)
- ❖ novo web sjedište (www.aaiedu.hr)
- ❖ revizija Pravilnika o ustroju AAI@EduHr sustava
- ❖ redovita certificiranja matičnih ustanova i usluga
- ❖ održavanje radionica i Dana AAI@EduHr

Enabling AAI@EduHr users

- ❖ **Pozivamo na suradnju!**
- ❖ Javite nam se sa svojim konkretnim prijedlogom za suradnju ili problemom koji ne znate riješiti
- ❖ Objavit ćemo kriterije po kojima ćemo odabrati prijedloge koje ćemo realizirati (sukladno raspoloživim resursima)
- ❖ Rješenja stavljamo na raspolaganje cjelokupnoj zajednici
- ❖ Što možete predložiti?
 - ◆ izradu podrške za neku programsku platformu (npr. Java)
 - ◆ *domestifikaciju* neke konkretne aplikacije/primjene
 - ◆ uvođenje novih AA metoda ili protokola
 - ◆ nove funkcije nekog od središnjih servisa (npr. modula VO)
 - ◆ osiguravanje/unapređenje podrške za neku grupu korisnika
 - ◆ ...



<http://www.aaiedu.hr/>
<http://developer.aaiedu.hr/>

team@aaiedu.hr