AAI@EduHr
radionica za matične ustanove i davatelje usluga

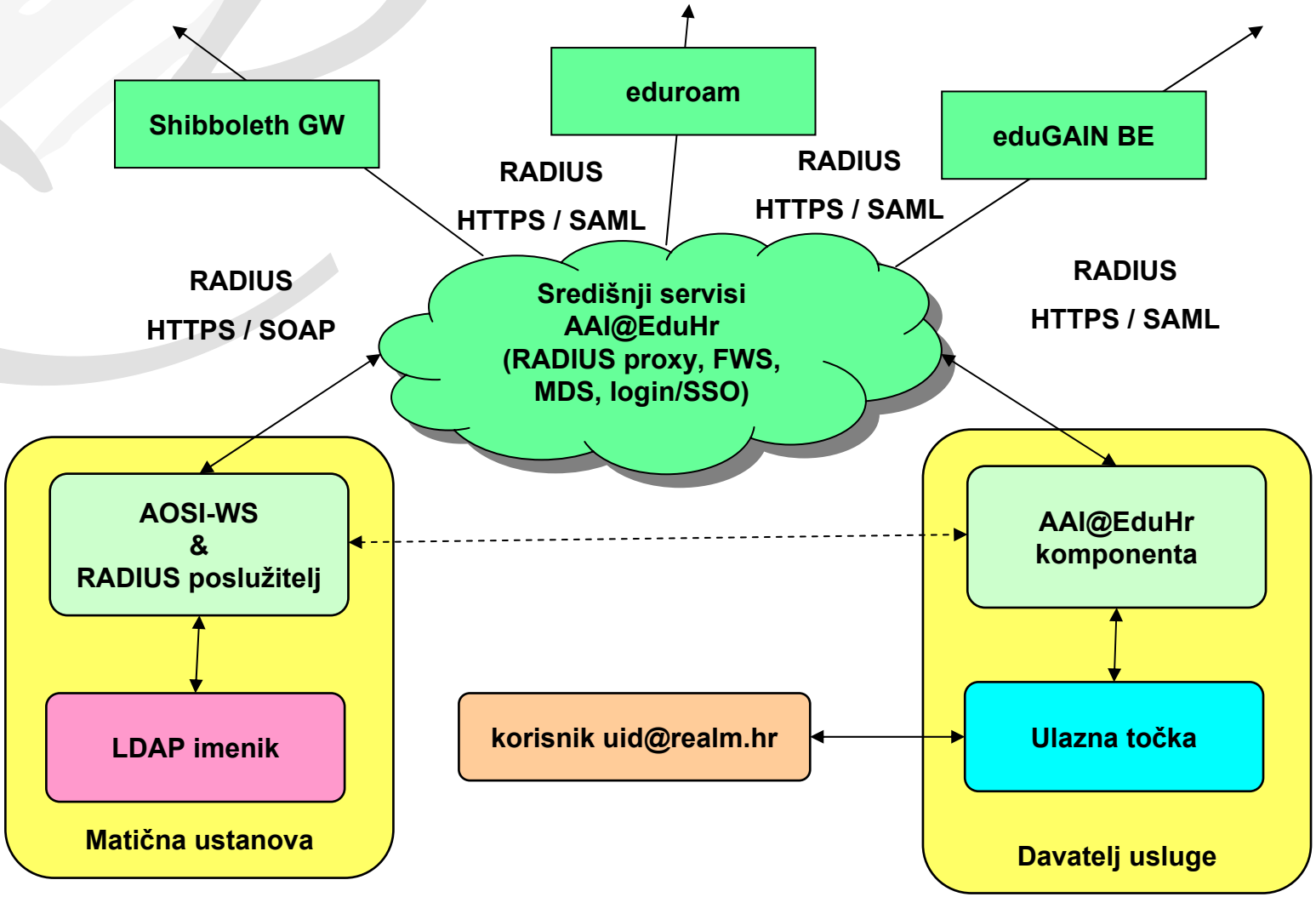
Miroslav Milinović, Mijo Đerek, Dubravko Penezić,
Denis Stančer, Dario Šafar, Dubravko Vončina
<team@aaiedu.hr>
Sveučilište u Zagrebu, Sveučilišni računski centar

Sadržaj

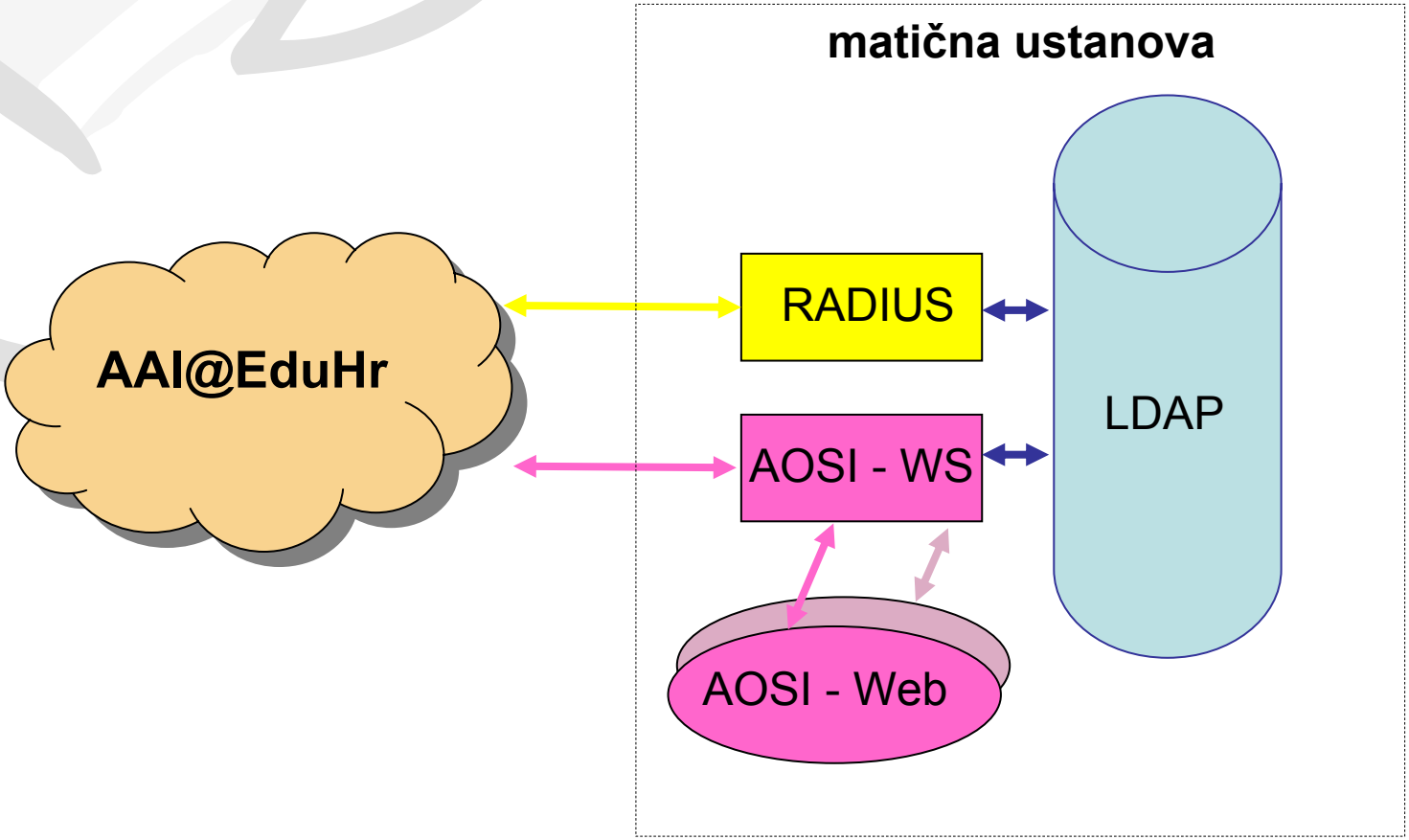
- **pravila rada i godišnje certificiranje matičnih ustanova**
- **povezivanje sustava AAI@EduHr sa sustavom NIAS (e-Građani)**
- **uključivanje usluga iz AAI@EduHr u eduGAIN**
- **"enabling users" - suradnja zajednice na razvoju sustava AAI@EduHr**
- **diskusija (teme iz prakse ...)**

Pravila rada i godišnje certificiranje matičnih ustanova

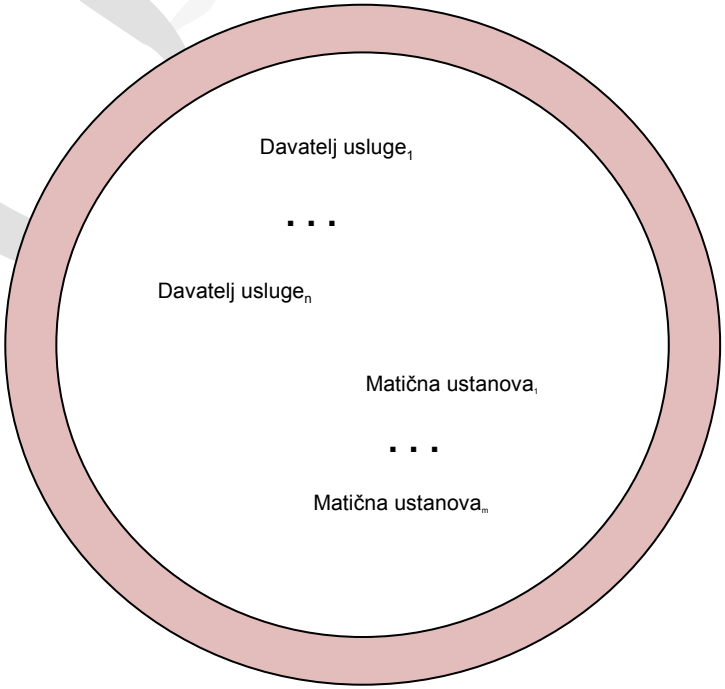
AAI@EduHr

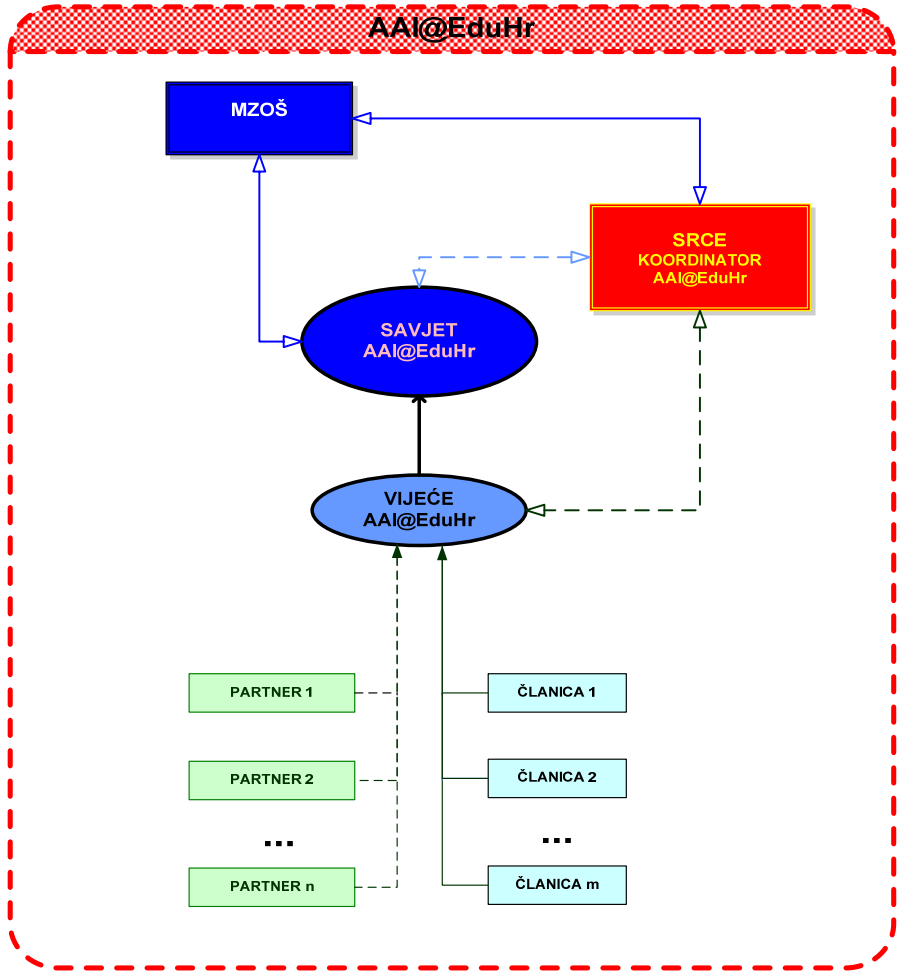

Shibboleth GW
eduroam
eduGAIN BE
RADIUS
HTTPS / SAML
RADIUS
HTTPS / SAML
RADIUS
HTTPS / SOAP
RADIUS
HTTPS / SAML
Središnji servisi
AAI@EduHr
(RADIUS proxy, FWS,
MDS, login/SSO)
AOSI-WS
&
RADIUS poslužitelj
LDAP imenik
Matična ustanova
korisnik uid@realm.hr
AAI@EduHr
komponenta
Ulazna točka
Davatelj usluge

AAI@EduHr: IdM



Organizacija AAI@EduHr

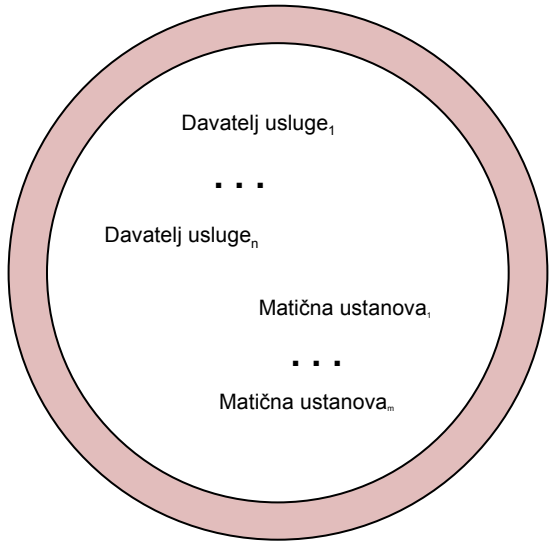




Pravilnik o ustroju, ver.1.3.1. (http://www.aaiedu.hr/docs/AAI@EduHr-pravilnik-ver1.3.1.pdf)

Registri sustava AAI@EduHr

- registar matičnih ustanova
  - http://www.aaiedu.hr/aai_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/



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)
- certificiranje provodi:
  - subjekt (samoprovjerom)
  - Srce - Koordinator AAI@EduHr (neposrednim uvidom ili korištenjem nadzornih/testnih programa/uređaja)

Certificiranje matičnih ustanova

- redovito provodimo jednom godišnje (od 2011.)

- certificiranje za 2014. godinu
  - **bez izmjena u načinu provedbe**
    (potreban je ispravno instaliran ***AOSI plugin libcertify-aosi-aai***)
  - **osnovni rok: 19.05. – 13.07.**
  - (dopunski rok: 01.09. – 30.09.)

- http://www.aaiedu.hr/certificiranje/

Norme za matične ustanove – 2014. (1)

Norma	Opis uvjeta koji se provjerava	Status	Provjerava
1. Formalno članstvo	Je li potpisan, ovjeren i odobren odgovarajući zahtjev za članstvo u AAI@EduHr sustavu?	obavezno	Koordinator
2. Imenovani predstavnici	Jesu li imenovane ovlaštene osobe i predstavnik u Vijeću AAI@EduHr te jesu li Koordinatoru dostavljeni ispravni kontakt podaci tih osoba?	obavezno	Koordinator
3. Prijava AZOP-u	Je li LDAP imenik prijavljen Agenciji za zaštitu osobnih podataka kao zbirka podataka?	preporučeno	Matična ustanova (samoprovjerom)
4. Procedura za informacijsko održavanje imenika utvrđena	Je li utvrđena procedura za informacijsko održavanje imenika?	obavezno	Matična ustanova (samoprovjerom)
4. Procedura za informacijsko održavanje imenika javno dostupna	Je li procedura za informacijsko održavanje imenika javno dostupna?	preporučeno	Matična ustanova (samoprovjerom)
5. Informiranje korisnika	Jesu li korisnici informirani o svojim pravima i obavezama prilikom preuzimanja e-identiteta?	obavezno	Matična ustanova (samoprovjerom)

Norme za matične ustanove – 2014. (2)

Norma	Opis uvjeta koji se provjerava	Status	Provjerava
6. Postojanje evidencije	Vodi li matična ustanova evidenciju o dodijeljenim e-identitetima?	obavezno	Matična stanova (samoprovjerom)
7. Kontakt podaci za korisnike	Jesu li kontakt podaci za korisnike objavljeni na adresi http://www.aaiedu.hr/aai_status.php točni?	obavezno	Matična ustanova (samoprovjerom)
8. Obuhvaćenost e-identitetima	**Posjeduju li svi zaposlenici (uključeni u nastavni ili znanstvenoistraživački proces) i studenti e-identitete?**	preporučeno	Matična ustanova (samoprovjerom)
9. Provjera identiteta osobe pri dodjeli e-identiteta	**Obavlja li se dodjela e-identiteta se na temelju dokumenta sa slikom ili kroz proces zapošljavanja/upisa?**	**obavezno**	**Matična ustanova (samoprovjerom)**
10. Postupak uručenja e-identiteta	**Uručuju li se podaci o e-identitetu osobno ili pisanim putem (ne telefonom ili e-mailom)? Odnosi se i na promjenu lozinke.**	**obavezno**	**Matična ustanova (samoprovjerom)**
11. Brisanje e-identiteta	E-identiteti osoba koje su prestale biti povezane s ustanovom se pravodobno i redovito se brišu (sukladno utvrđenoj proceduri).	obavezno	Matična ustanova (samoprovjerom)

Norme za matične ustanove – 2014. (3)

Norma	Opis uvjeta koji se provjerava	Status	Provjerava
12. Informacijska kvaliteta imenika - istekli e-identiteti (obavezno)	Je li broj e-identiteta koji su označeni kao istekli prije više od 3 mjeseca (u to se broje i studentski e-identiteti bez podatka o isteku) manji od 1% ukupnog broja korisnika u LDAP imeniku?	obavezno	Koordinator (putem programa za analizu sadržaja imenika)
12. Informacijska kvaliteta imenika - istekli e-identiteti (preporučeno)	U LDAP imeniku nema nijedan e-identitet označen kao istekao prije više od 3 mjeseca (u to se broje i studentski e-identiteti bez podatka o isteku).	preporučeno	Koordinator (putem programa za analizu sadržaja imenika)
13. Informacijska kvaliteta imenika - elektroničke adrese (obavezno)	U LDAP imeniku nema nijedan e-identitet koji nema ispravan podatak o e-mail adresi.	obavezno	Koordinator (putem programa za analizu sadržaja imenika)
14. Informacijska kvaliteta imenika - OIB	Uz svaki je e-identitet zabilježen odgovarajući OIB. Iznimka mogu biti samo korisnici kojima je vrijednost atributa hrEduPersonPrimaryAffiliation „gost“	obavezno	Koordinator (putem programa za analizu sadržaja imenika)
15. Informacijska kvaliteta imenika - brojčani identifikator	Vrijednost atributa brojčani identifikator osobe je jedinstvena na nivou ustanove.	obavezno	Koordinator (putem programa za analizu sadržaja imenika)
16. Informacijska kvaliteta imenika - podaci o ustanovi (hrOrg atributi)	Jesu li podaci o ustanovi zapisani u org zapisu LDAP imenika potpuni i ispravni?	obavezno	Koordinator (putem programa za analizu sadržaja imenika)

Norme za matične ustanove – 2014. (4)

Norma	Opis uvjeta koji se provjerava	Status	Provjerava
17. Nadzor AAI@EduHr komponente	Koordinatoru je omogućen nadzor rada LDAP, RADIUS i AOSI-WS poslužitelja.	obavezno	Koordinator
18. Programska podrška - LDAP (obavezno)	**Je li instalirana i ispravno konfigurirana inačica novija ili jednaka 2.4.31 (AAI@EduHr LDAP paket 2.4.31~srce0)?**	obavezno	Koordinator
18. Programska podrška - LDAP (preporučeno)	**Je li instalirana i ispravno konfigurirana inačica novija ili jednaka 2.4.31 (AAI@EduHr LDAP paket 2.4.31~srce1)?**	preporučeno	Koordinator
19. Programska podrška - RADIUS (obavezno)	**Je li instalirana i ispravno konfigurirana inačica novija ili jednaka 2.1.12 (AAI@EduHr RADIUS paket 2.1.12~srce6)?**	obavezno	Koordinator
19. Programska podrška - RADIUS (preporučeno)	**Je li instalirana i ispravno konfigurirana inačica novija ili jednaka 2.1.12 (AAI@EduHr RADIUS paket 2.1.12~srce6)?**	preporučeno	Koordinator
20. Programska podrška – AOSI - WS (obavezno)	**Je li instalirana i ispravno konfigurirana inačica novija ili jednaka 3.2.3 (AAI@EduHr AOSI WS paket 3.2.3)?**	obavezno	Koordinator
20. Programska podrška – AOSI - WS (preporučeno)	**Je li instalirana i ispravno konfigurirana inačica novija ili 3.2.4 (AAI@EduHr AOSI WS paket 3.2.4)?**	preporučeno	Koordinator

Norme za matične ustanove – 2014. (5)

Norma	Opis uvjeta koji se provjerava	Status	Provjerava
21. Sekundarni servisi	U produkciji su sekundarni LDAP, RADIUS i AOSI-WS.	preporučeno	Koordinator
22. Postojanje uputa i web sučelja za vlasnike e-identiteta	Postoji li web sučelje za vlasnike e-identiteta putem kojeg oni mogu promijeniti zaporku i ostale podatke koje im je dozvoljeno mijenjati (AOSI-web sučelje, ISVU web sučelje ili vlastito rješenje)?	obavezno	Koordinator
23. Certifikat RADIUS poslužitelja – ispravan i dostupan korisnicima	Certifikat RADIUS poslužitelja ustanove je ispravan i dostupan korisnicima kroz uporabu eduroam installera (installer.eduroam.hr)	obavezno	Koordinator
24. Elektronički identiteti izdaju se isključivo fizičkim osobama	Elektronički identitet u sustavu AAI@EduHr odnosno slog u imeniku s identifikatorom (DN-om) oblika uid=oznaka, dc=domena, dc=hr izdaje se isključivo fizičkim osobama	obavezno	Matična ustanova (samoprovjerom)
25. AOSI-WS ima ispravan certifikat	AOSI WS koristi poslužiteljski certifikat dobiven putem CARNetove usluge TCS (ili drugi certifikat kojeg web-preglednici automatski prepoznaju)	preporučeno	Koordinator
26. RADIUS poslužitelj ispravno isporučuje atribut CUI	RADIUS poslužitelj ustanove ispravno isporučuje RADIUS atribut CUI (*Chargeable-User-Identity*)	preporučeno	Koordinator

Što je CUI i čemu služi?

- CUI je:
  - RADIUS atribut: *Chargeable-User-Identity*
  - RFC4372
  - jedinstvena oznaka korisnika na nivou pojedinog davatelja usluge
  - ne sadrži osobne podatke (depersonaliziran)
- svrha:
  - rješava „problem” s vanjskom korisničkom oznakom
  - omogućuje jednostavno i pouzdano uskraćivanje usluge pojedinom korisniku (*blacklisting*)
  - dodatne mogućnosti analize korištenja usluge bez ugrožavanja privatnosti
- kako omogućiti CUI (na strani matične ustanove):
  - dovoljno je instalirati najnoviju inačicu *freeradius-aai* paketa

Kako sve to radi?

- RADIUS poslužitelj davatelja usluge generira zahtjev za autentikacijom pri čemu taj zahtjev sadrži RADIUS atribute:
  - Operator-Name
    - jedinstveni identifikator davatelja usluge (vrijednost dodjeljuje Srce)
  - Chargeable-User-Identity s vrijednošću NULL
- RADIUS poslužitelj matične ustanove na autentikacijski zahtjev odgovara:
  - Autentikacija je neuspješna – standardni REJECT
  - Autentikacija je uspješna – standardni ACCEPT dodajući CUI koji se generira kao MD5 hash vrijednosti RADIUS atributa Operator-Name i korisničke oznake
- RADIUS poslužitelj davatelja usluge dohvaća vrijednost CUI atributa i po potrebi obavlja autorizaciju (npr. onemogućuje pristup nepoželjnim korisnicima).

Povezivanje sustava AAI@EduHr sa sustavom NIAS (e-Građani)

AAI@EduHr u NIAS-u

- Nacionalni identifikacijski i autenti(fi)kacijski sustav (NIAS)
  - jedna od tri glavne sastavnice infrastrukture projekta e-Građani Vlade RH
  - NIAS-om upravlja Ministarstvo Uprave RH, a operativno ga izvodi FINA
  - prihvaća vjerodajnice (e-identitete) koje zadovolje norme NIAS-a
  - (http://www.aaiedu.hr/docs/DanAAI@EduHr-2013-bozic.pdf)

- sustav AAI@EduHr uspješno je prošao je proces provjere
  - ocjenjivanje je temeljeno na sustavu certificiranja subjekata u sustavu AAI@EduHr
  - posebno su važne obvezne norme 9. i 10. za matične ustanove (postupak upravljanja e-identitetima) te briga o kvaliteti lozinke
  - potrebnu razinu sigurnosti autentikacijskog mehanizma garantira korištenje HTTPS/SOAP/SAML protokola

AAI@EduHr u NIAS-u

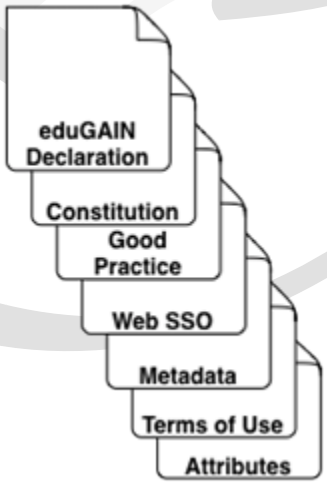
- vjerodajnice izdane u sustavu AAI@EduHr prihvaćene su u NIAS s **razinom 2** sigurnosti vjerodajnice (skala od 1-4)

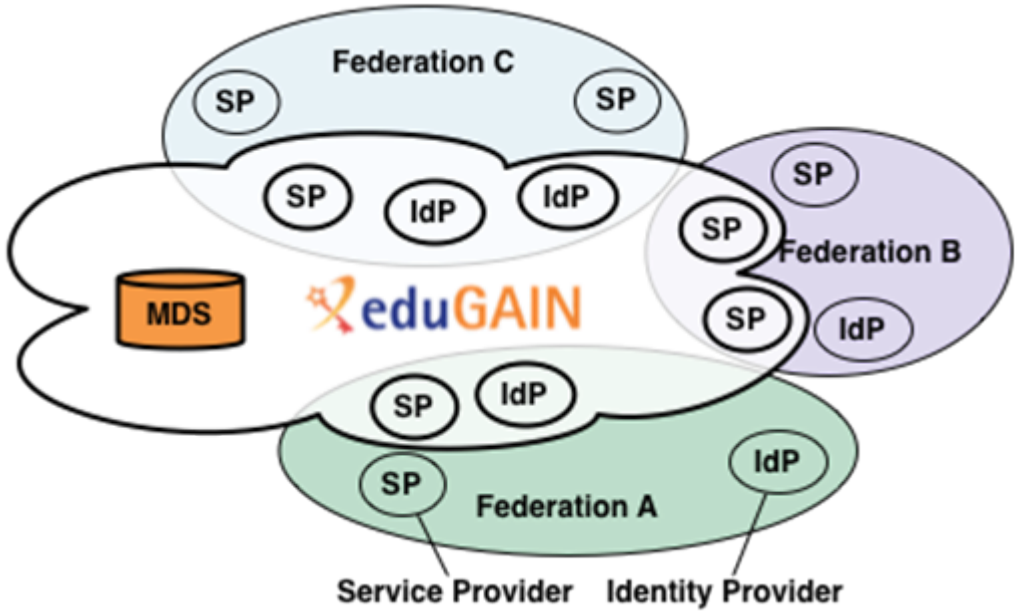
- **u NIAS će biti uključene samo AAI@EduHr vjerodajnice koje izdaju ustanove članice sustava AAI@EduHr, za koje je Srce u postupku godišnje provjere utvrdilo da ispunjavaju dovoljnu razinu usklađenosti s normama sustava AAI@EduHr**

- **Srce će izvijestiti matične ustanove o početku produkcijskog rada sustava NIAS i mogućnosti korištenja AAI@EduHr (vjerodajnica) identiteta za pristup uslugama u okviru projekta e-Građani**

eduGAIN – kako internacionalizirati uslugu usklađenu s AAI@EduHr?

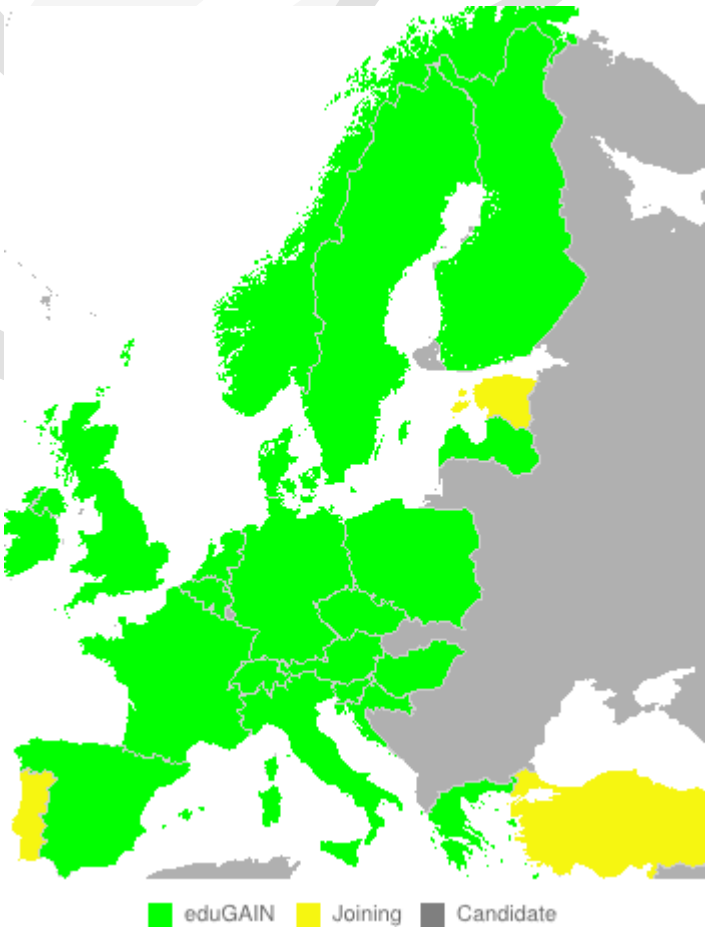
Što je eduGAIN?

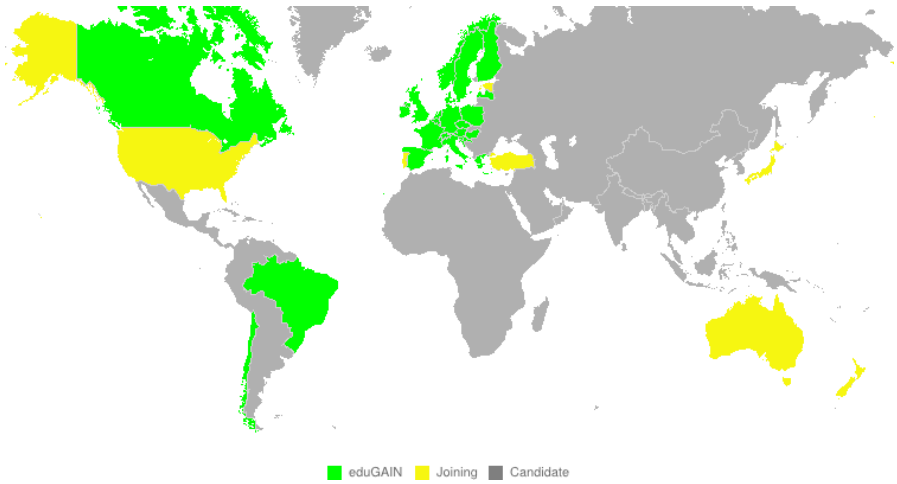




- **edu**cational **G**lobal **A**uthentication **In**frastructure
- dvije temeljne komponente:
  - pravila i norme: eduGAIN Policy Framework
  - tehnički sustav: MDS (Metadata Distribution Service)

Koliko je eduGAIN raširen?





- u produkciji od 2011. godine
- 24 federacije članice
- 7 federacija u postupku pristupanja
- www.edugain.org

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

Koliko je povjerenje važno?

- SP vjeruje IdP-u
  - **LoA:** IdP garantira dogovorenu kvalitetu identiteta i procesa autentikacije
  - **Schema:** dogovorena je semantika i sintaksa atributa
- IdP vjeruje SP-u
  - **Privacy**: SP se obvezuje čuvati privatnost korisnika
- Svi čimbenici imaju povjerenje u koordinatora federacije
  - **Federation Policy**: pravilima ustroja federacije reguliraju se prava i obveze svih čimbenika
- Osobni podaci i zaštita privatnosti poseban su izazov u interfederacijskom modelu

eduGAIN Policy Framework

- organizacijski okvir
- definira ustroj sustava eduGAIN
- obuhvaća temeljna pravila, tehničke norme i preporuke

- Code of Conduct (CoC) – pravila postupanja
  - cilj je osigurati povjerenje IdP-a u SP-ove

- dokumenti su javno dostupni na adresi:
  - http://www.geant.net/service/eduGAIN/resources/Pages/home.aspx

eduGAIN MDS

- Metapodatkovni servis (http://mds.edugain.org)
  - sadrži metapodatke o svim IdP-ovima i SP-ovima koji su putem svojih federacija uvršteni u eduGAIN
  - federacije osiguravaju ažurnost metapodataka iz svoje nadležnosti

- Uobičajen je *opt-in* model:
  - federacija publicira metapodatke o odabranim IdP-ovima i SP-ovima temeljem svojih pravila/njihove odluke

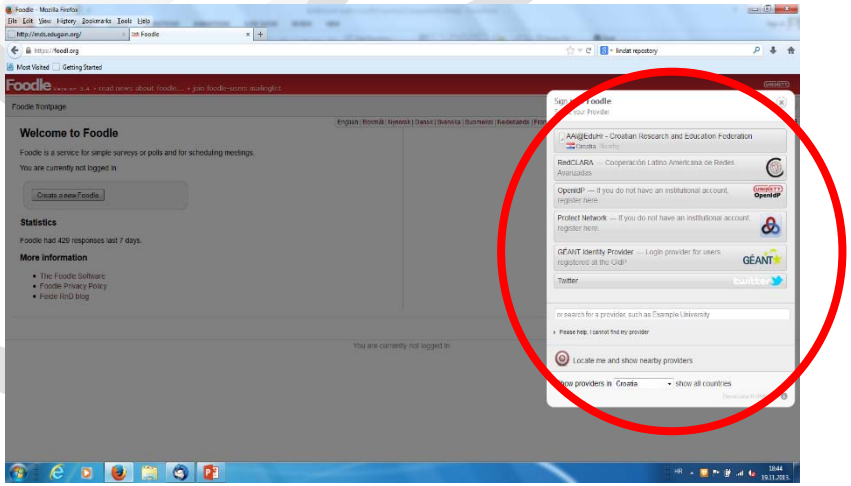
AAI@EduHr u eduGAIN-u

- 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

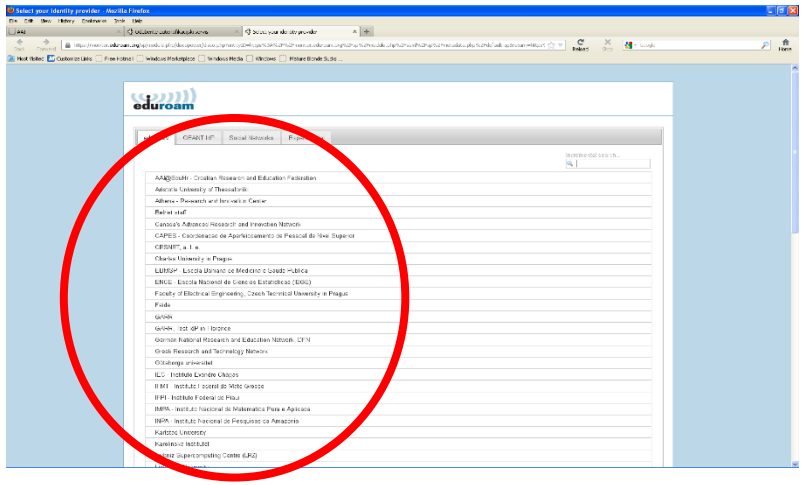
Osnovni koraci za usluge

- 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

Primjeri prilagodbe login sučelja



https://foodl.org/



http://monitor.eduroam.org/db_web

Enabling users

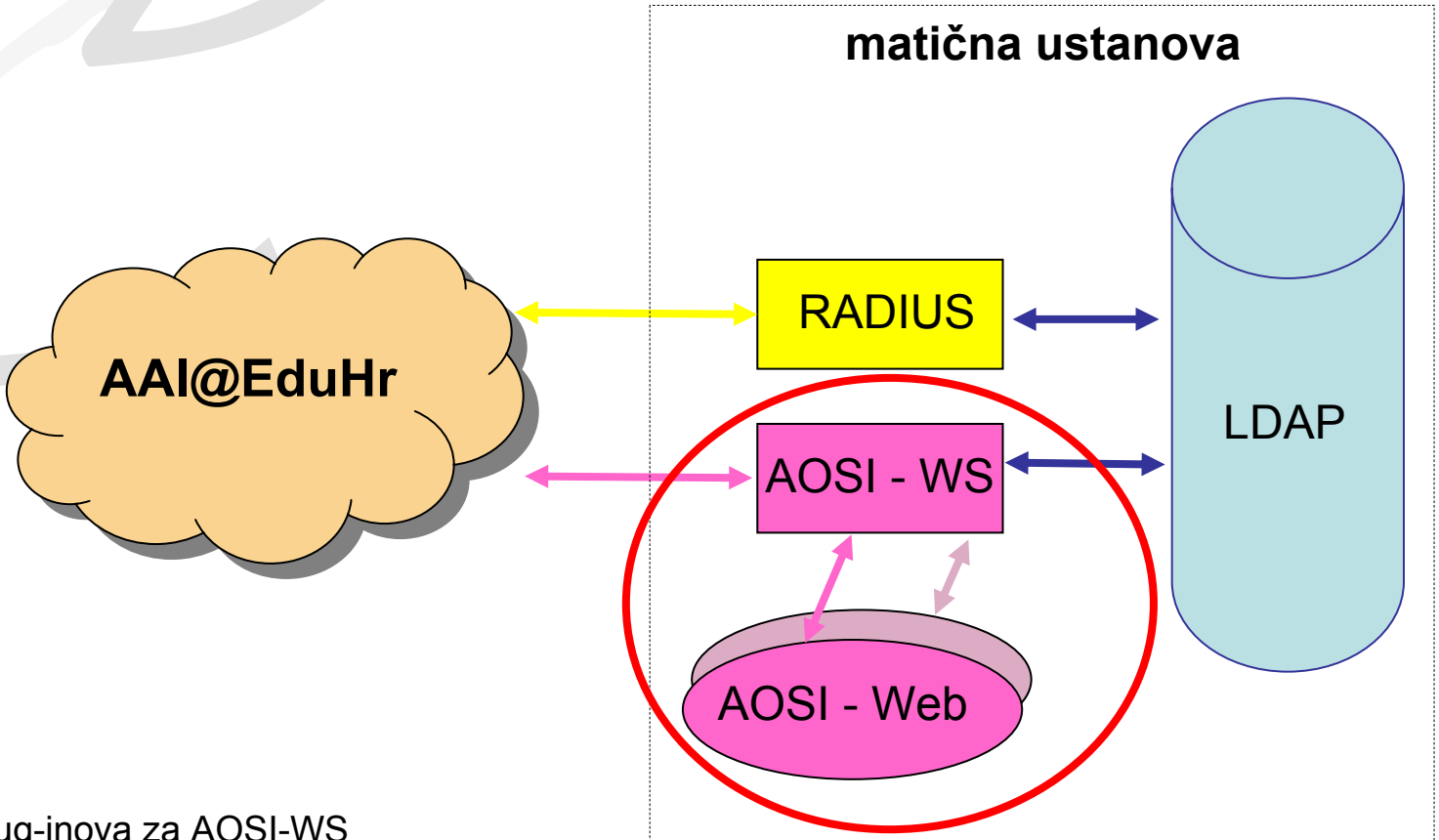
Enabling AAI@EduHr users

- **Pozivamo na suradnju!**
- Javite nam se sa svojim konkretnim prijedlogom za suradnju ili problemom koji ne znate riješiti
- 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
  - …

Izazovi

- 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
- …

AAI@EduHr: IdM



- sustav plug-inova za AOSI-WS
  - http://developer.aaiedu.hr/faq.html
  - http://developer.aaiedu.hr/faq/AOSI-2-Plugins-List.html

Domestifikacija aplikacije

- *domestifikacija* = prilagodba aplikacije korištenju elektroničkog identiteta
  - ovisi o okolini u kojoj se aplikacija razvija i koristi
  - ovisi o internoj arhitekturi aplikacije
  - ovisi o sustavu e-identiteta koji se koristi
  - moguće kombiniranje uporabe različitih sustava e-identiteta
- standardni protokol u AAI@EduHr je SAML ver. 2.0
  - Shibboleth ≈ SAML (treba paziti na verzije)
- dokumentacija i upute
  - http://developer.aaiedu.hr/

Podržane platforme

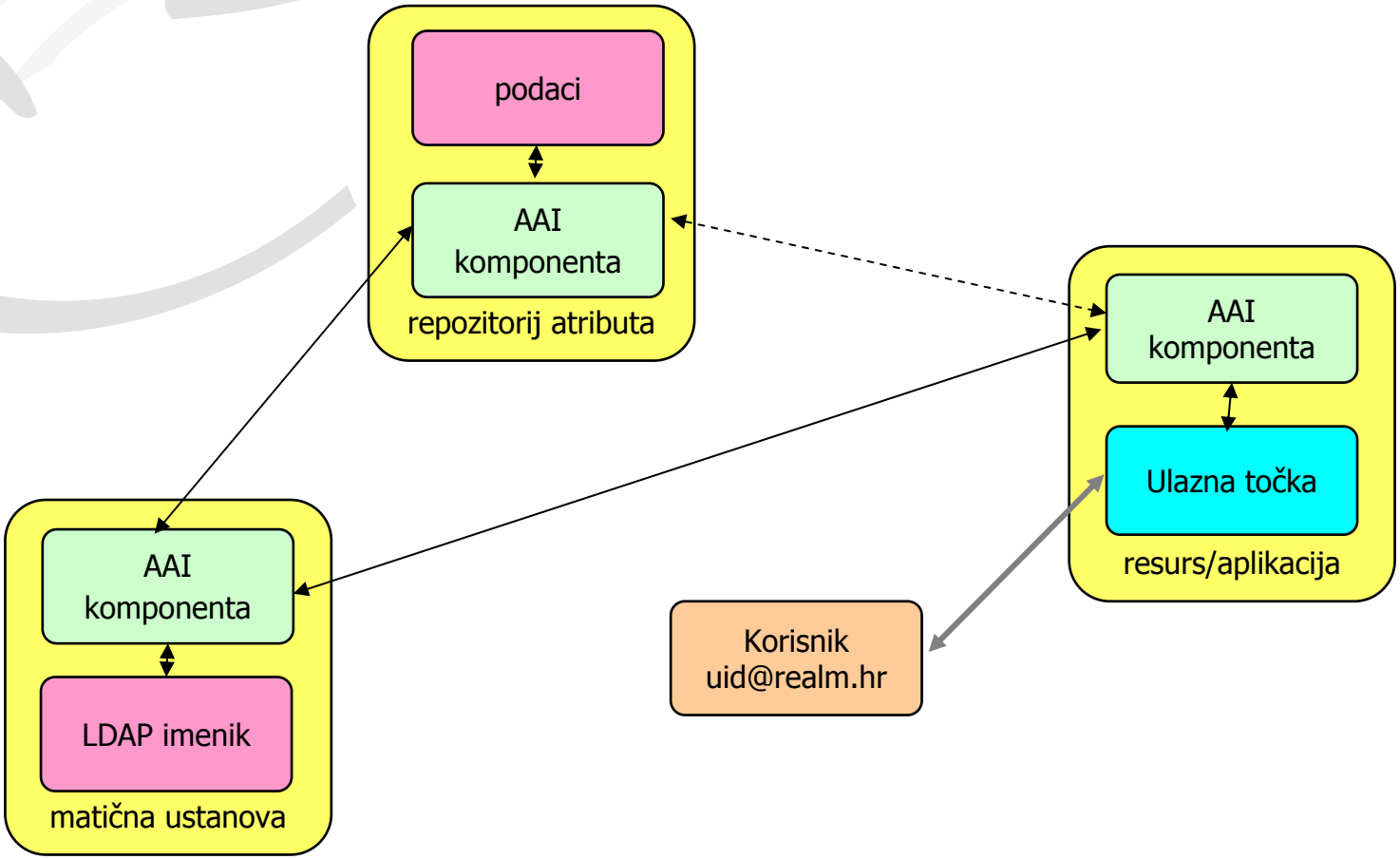
- sve platforme koje imaju podršku za SAML 2.0
- izdvajamo:
  - PHP
    - preporučamo uporabu alata simpleSAMLphp (SSP) (http://developer.aaiedu.hr/faq/8.html)
    - za SSP dostupan je i odgovarajući Debian paket (http://www.aaiedu.hr/faq_paketi_verzije.html)
  - MS .NET
    - preporučamo uporabu OIOSAML modula (http://developer.aaiedu.hr/faq/OIOSAML.html)
    - mogućnost korištenja ADFS-a (2.0 ?)
    - valja znati: Shibboleth 2.0 = SAML 2.0

Aplikacije koje ne koriste Web

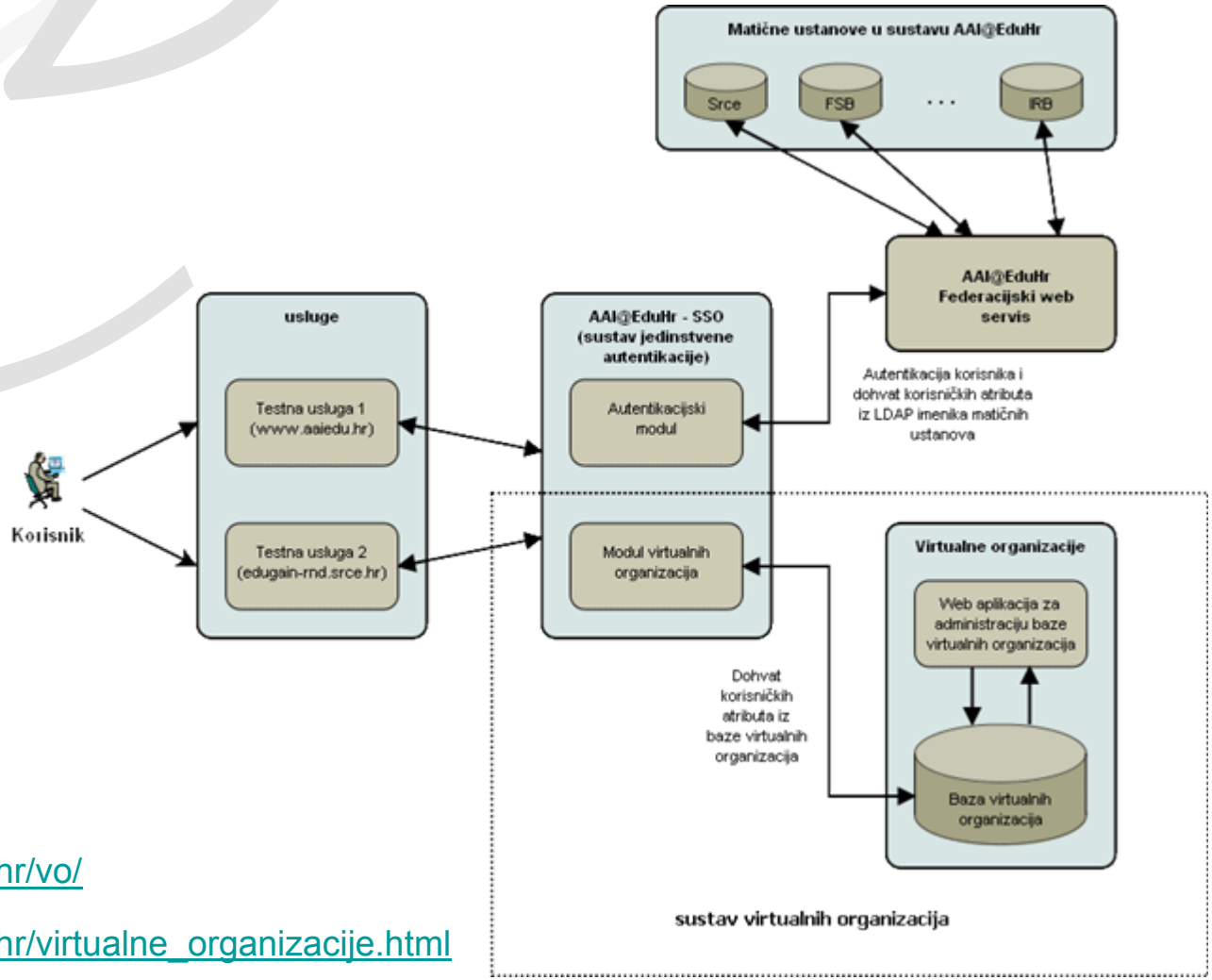
- nove tehnologije, stalne izmjene/nadogradnje
- OpenID Connect 1.0 / OAuth 2.0
- Shibboleth ECP (Enhanced Client or Proxy)
  - koristi SOAP
  - za aplikacije koje ne koriste Web preglednike
- Moonshot (https://community.ja.net/groups/moonshot)

Virtualne organizacije (VO)

Koncept dodatnih repozitorija atributa



VO u sustavu AAI@EduHr



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

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

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

- kontakt: team@aaiedu.hr

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

team@aaiedu.hr

Dodatni slajdovi - Rijeka

Ujedinjenje više imenika u jedan

- što transparentnije i jednostavnije za krajnje korisnike, uz što manje promjena
  - uid ostaje isti,
  - zaporka ostaje nepromijenjena,
  - mijenja se samo domena.
- organizacijom imenika na organizacijske jedinice (ou) omogućiti administraciju imenika po odjelima / fakultetima / studijima.
- Jedan imenik zahtjeva manje računalnih resursa, manje ljudskih resursa, jednostavnije održavanje programske podrške

Dosadašnja iskustva

- Sveučilište u Osijeku
- Sveučilište u Zadru
- Prirodoslovno matematički fakultet u Zagrebu
  - Bez problema za korisnike,
  - Jednostavnije za sistemce,
  - Ovisno o organizaciji, administratorima jednako ili manje posla.
- AAI@EduHr team nudi pomoć (savjetodavnu, tehničku, …)

Postupak

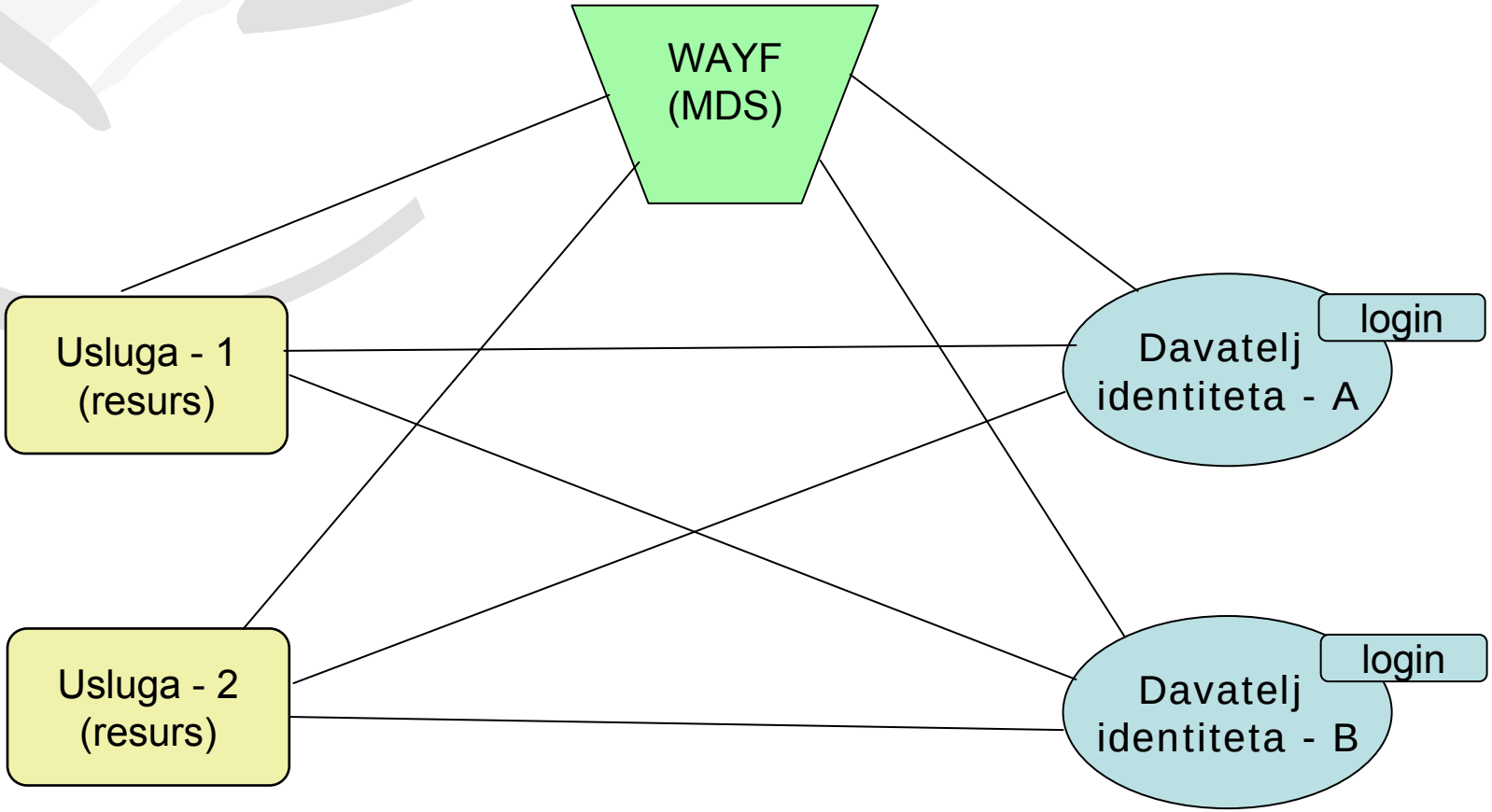
- Usporediti sadržaj imenika
  - Pronaći uid-ove koji su jednaki – takvim korisnicima morat će se promijeniti uid.
  - Potražiti postoje li osobe sa više elektroničkih identiteta (po OIB-u) – takvim korisnicima ostaje jedan elektronički identitet
- Odrediti datum ujedinjenja
- Obavijestiti korisnike
  - Što se točno mijenja i kakve posljedice promjene imaju za njih
  - Posebno obavijestiti korisnike kojima se mijenja i uid

Postupak

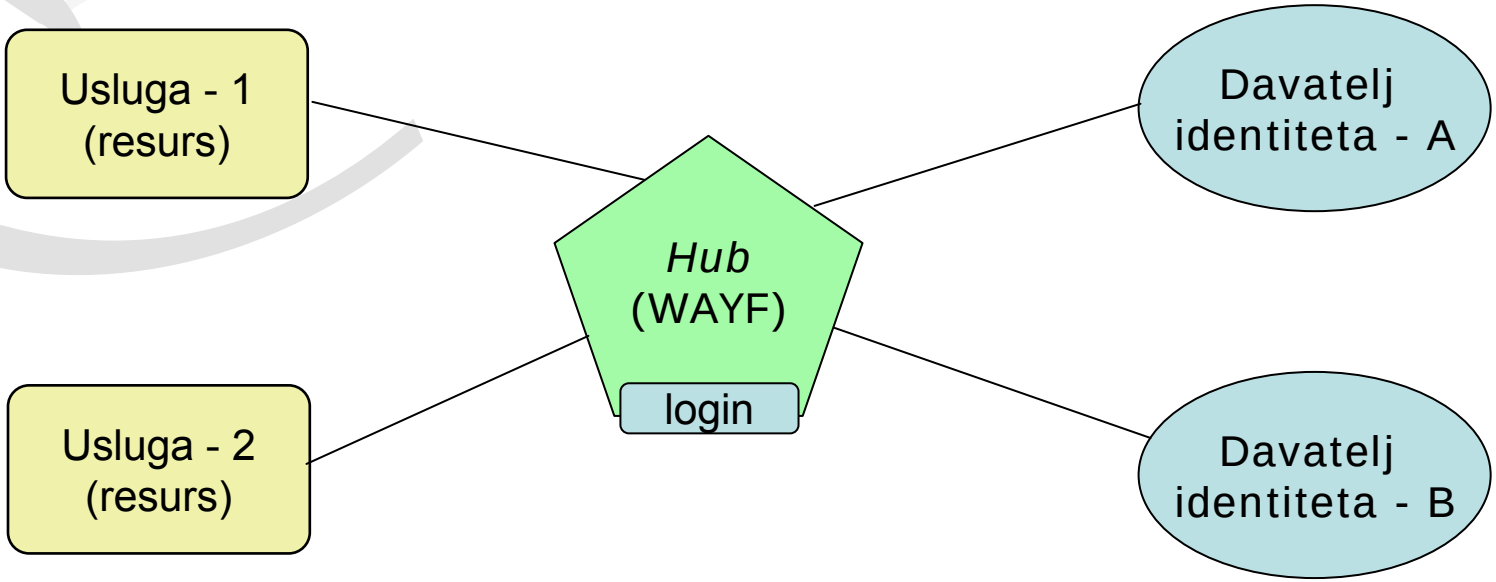
- Na dan ujedinjenja:
  1. Onemogućiti pisanje u imenike
  2. Eksportirati sadržaj svih imenika u ldif
  3. Promijeniti podatke
     - Iz ldif-a izbaciti org zapis i cn=hreduadmin zapis
     - Mijenjaju li se e-mail adrese?
     - Organizirati imenik po organizacijskim jedinicama (ou)
  4. Instalirati i podesiti zajednički imenik
  5. Uvesti podatke u zajednički imenik
  6. Ovlastiti administratore imenika
  7. AAI@EduHr team isključuje stare imenike. Ostaje samo novi.

Rezervni slajdovi

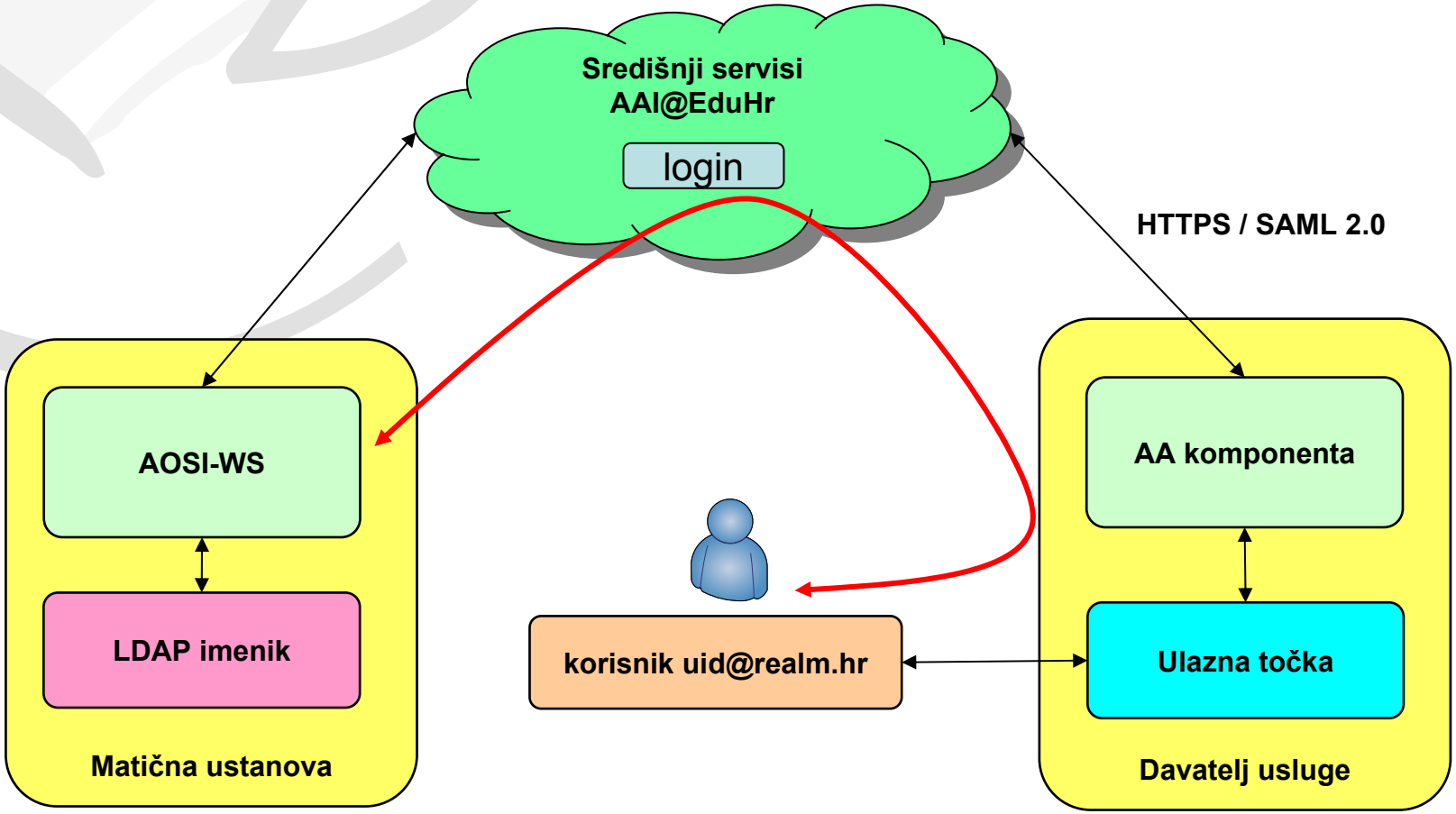
Mash federacija



Hub-and-spoke federacija



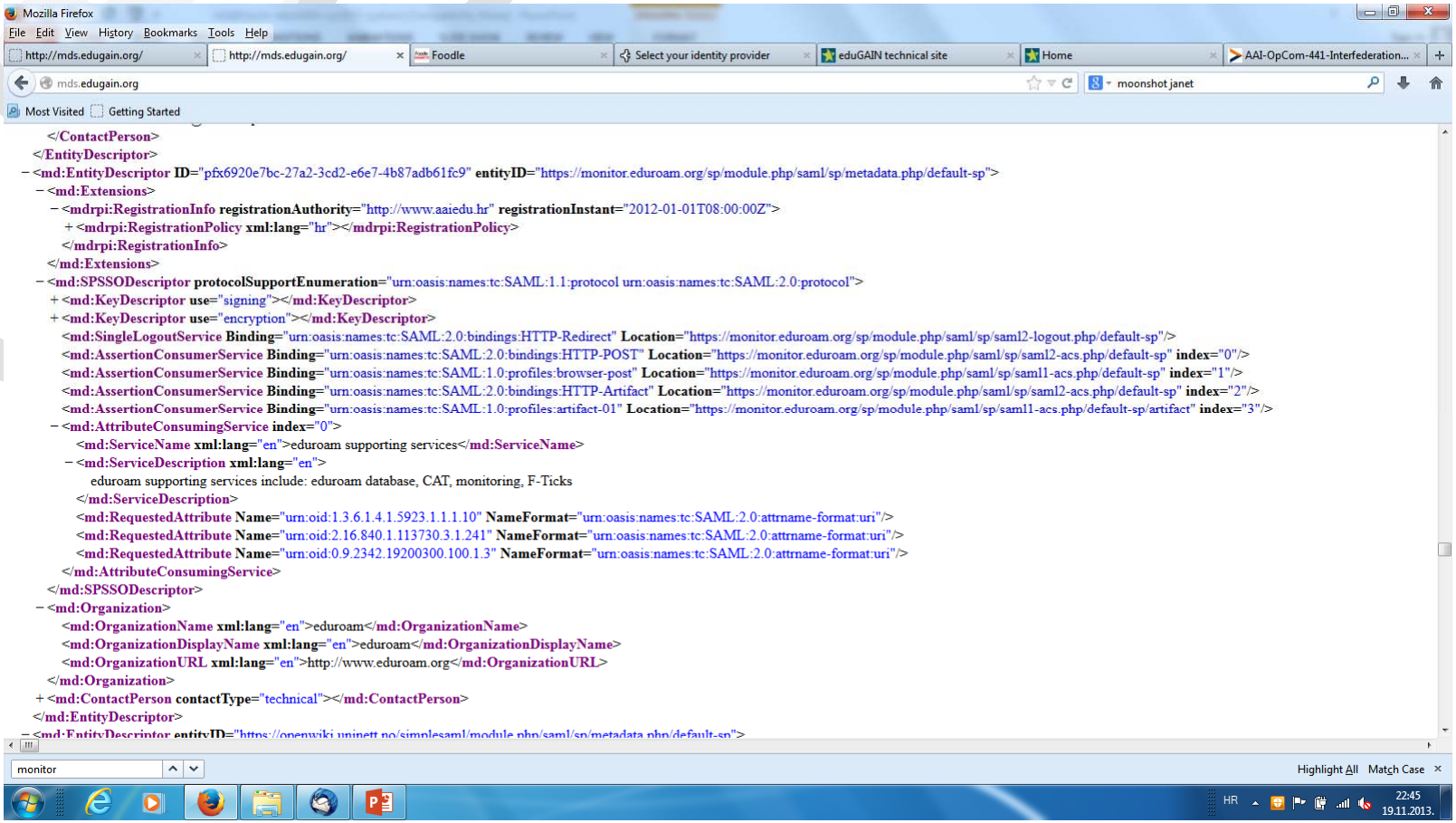
AAI@EduHr


Središnji servisi
AAI@EduHr
login
HTTPS / SAML 2.0
AOSI-WS
LDAP imenik
Matična ustanova
korisnik uid@realm.hr
AA komponenta
Ulazna točka
Davatelj usluge

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/

Primjer metapodatkovnog zapisa usluge

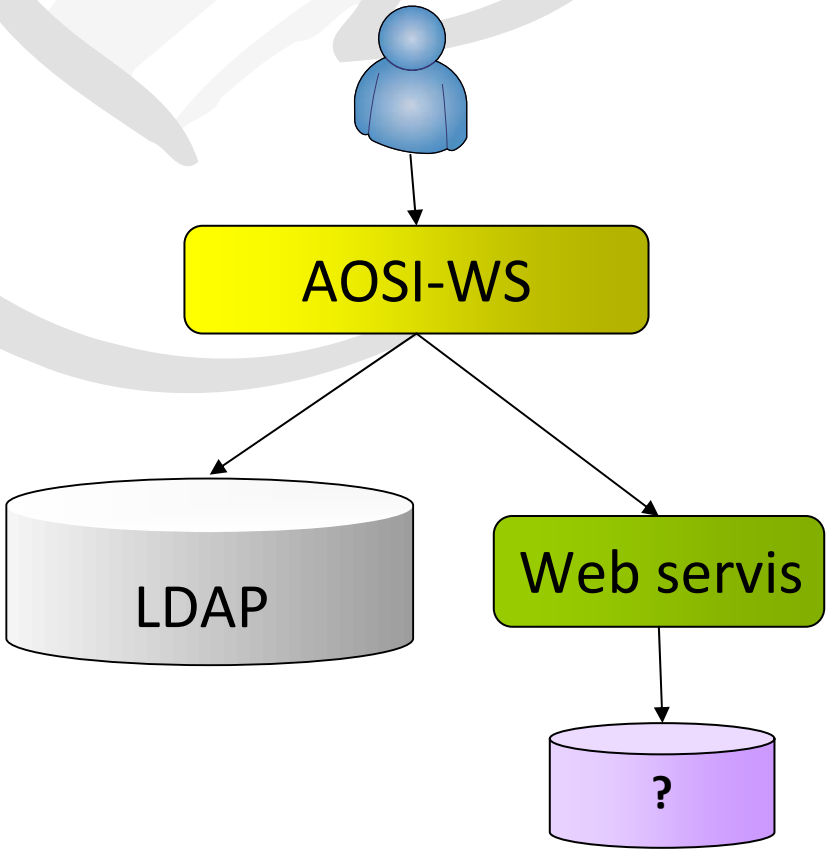


Usluga je SP proxy za skup aplikacija za potporu eduroam operatera (http://monitor.eduroam.org/db_web)

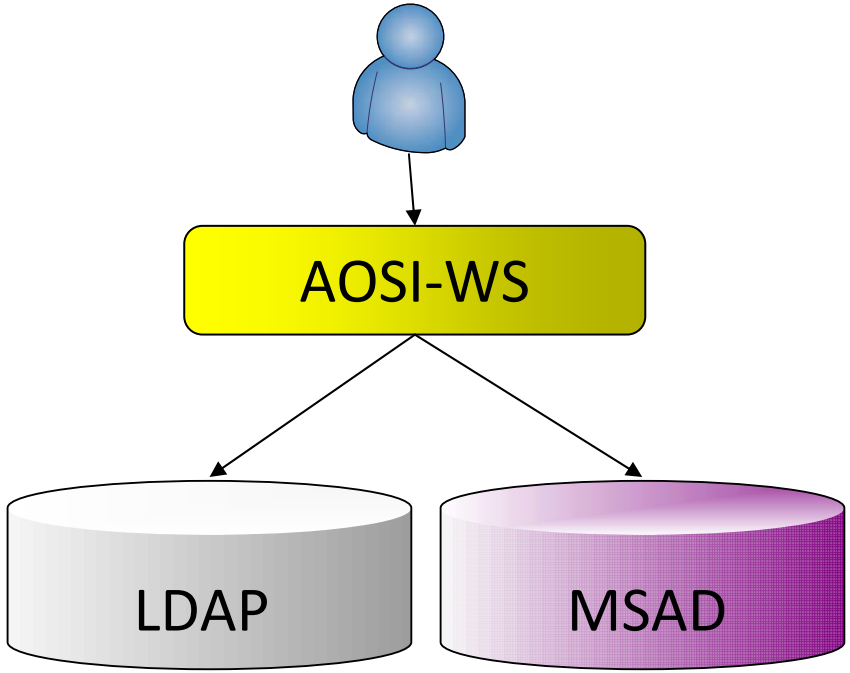
AOSI sustav plug-inova

- 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:
  - http://developer.aaiedu.hr/faq.html
  - http://developer.aaiedu.hr/faq/AOSI-2-Plugins-List.html

AOSI plug-inovi: primjeri

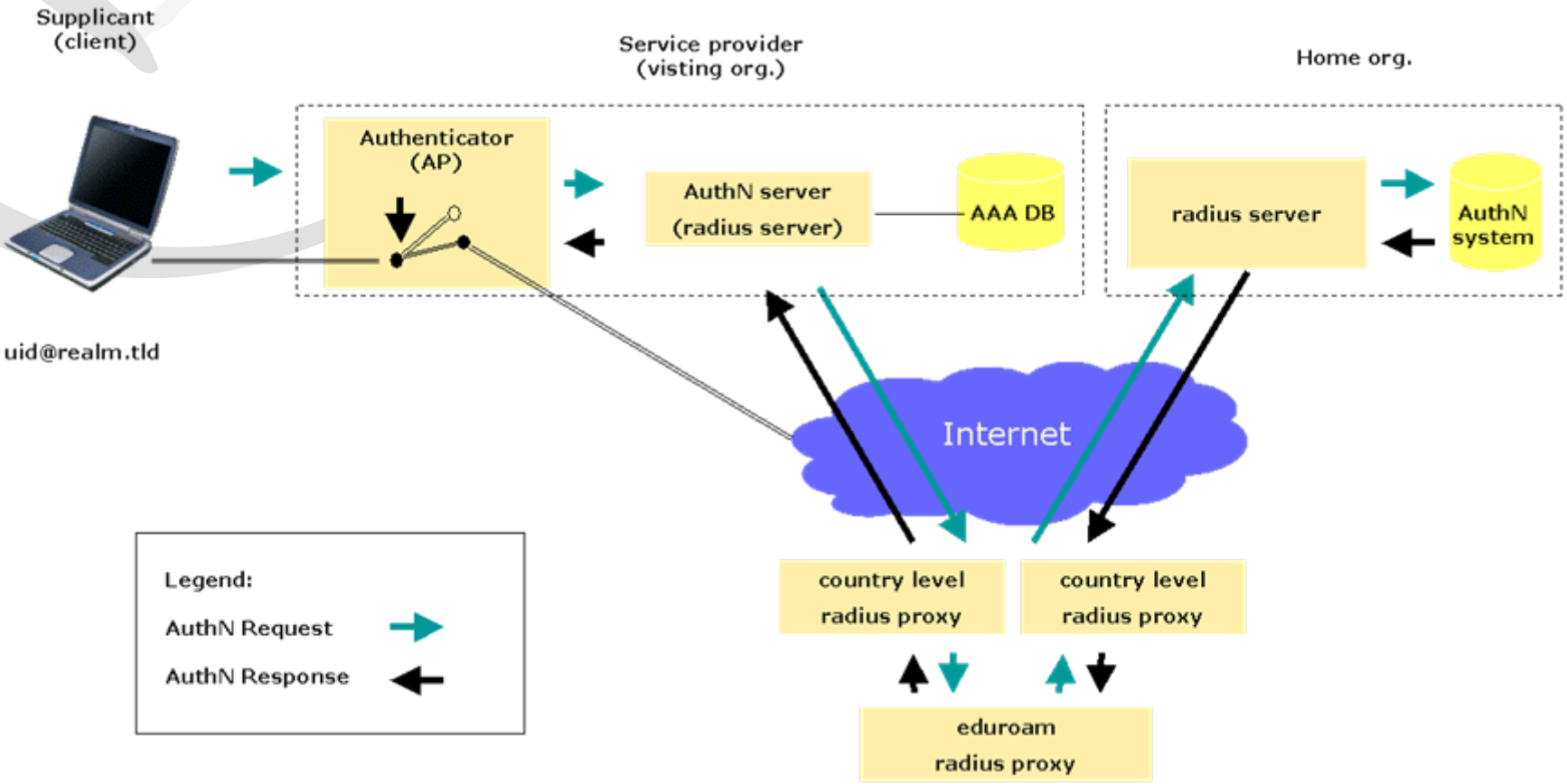


Web service plug-in

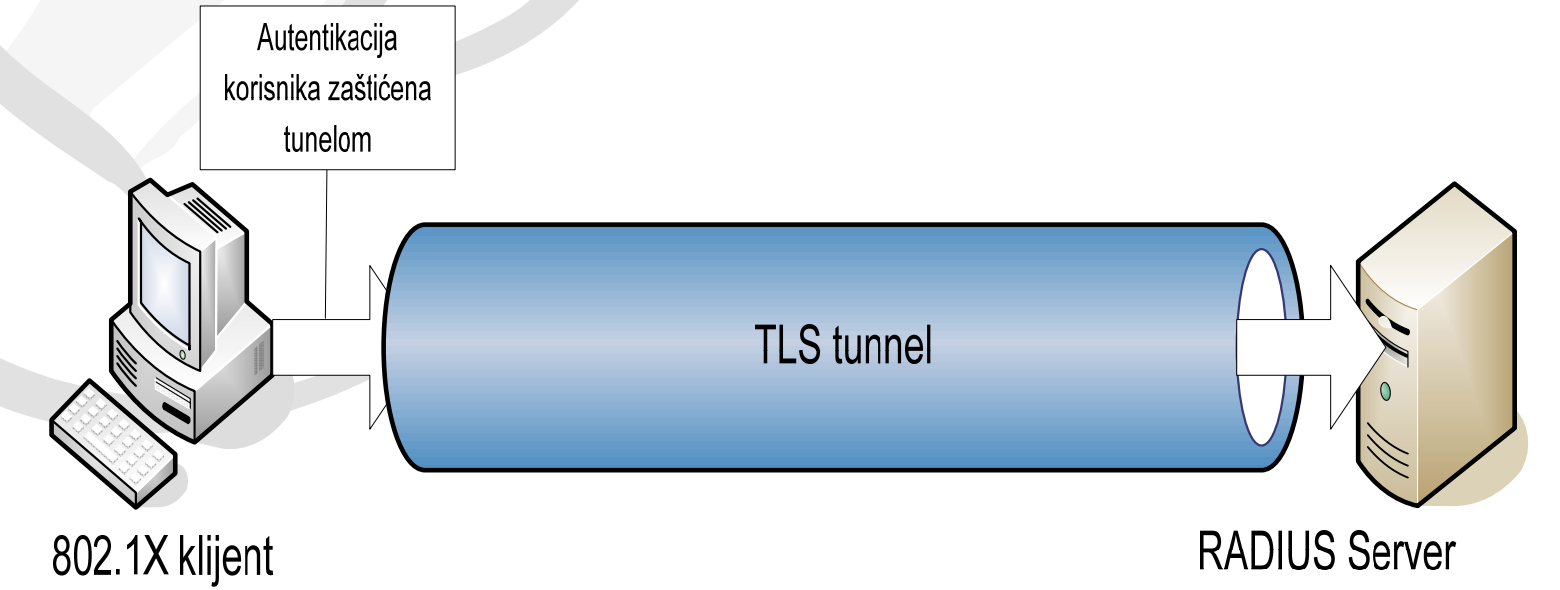


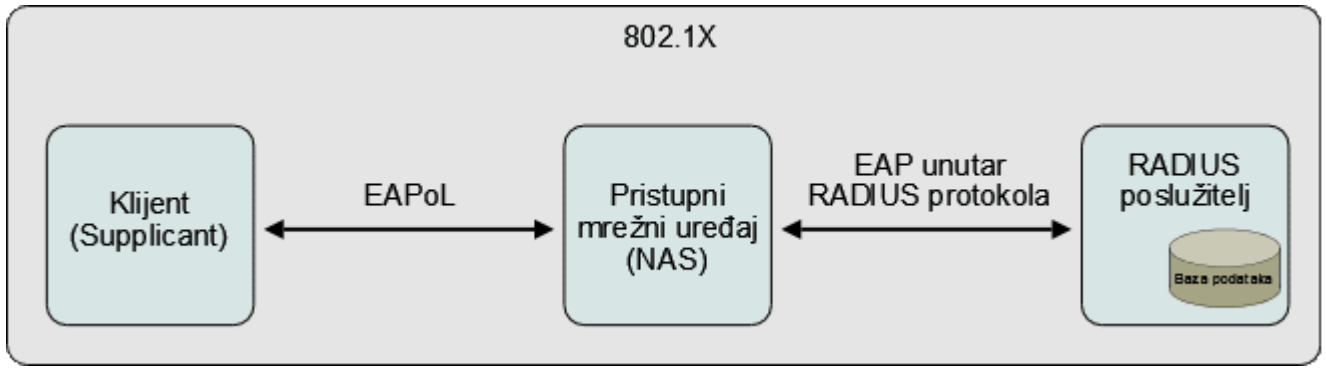
MS Active Directory plug-in

Primjer: eduroam™



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