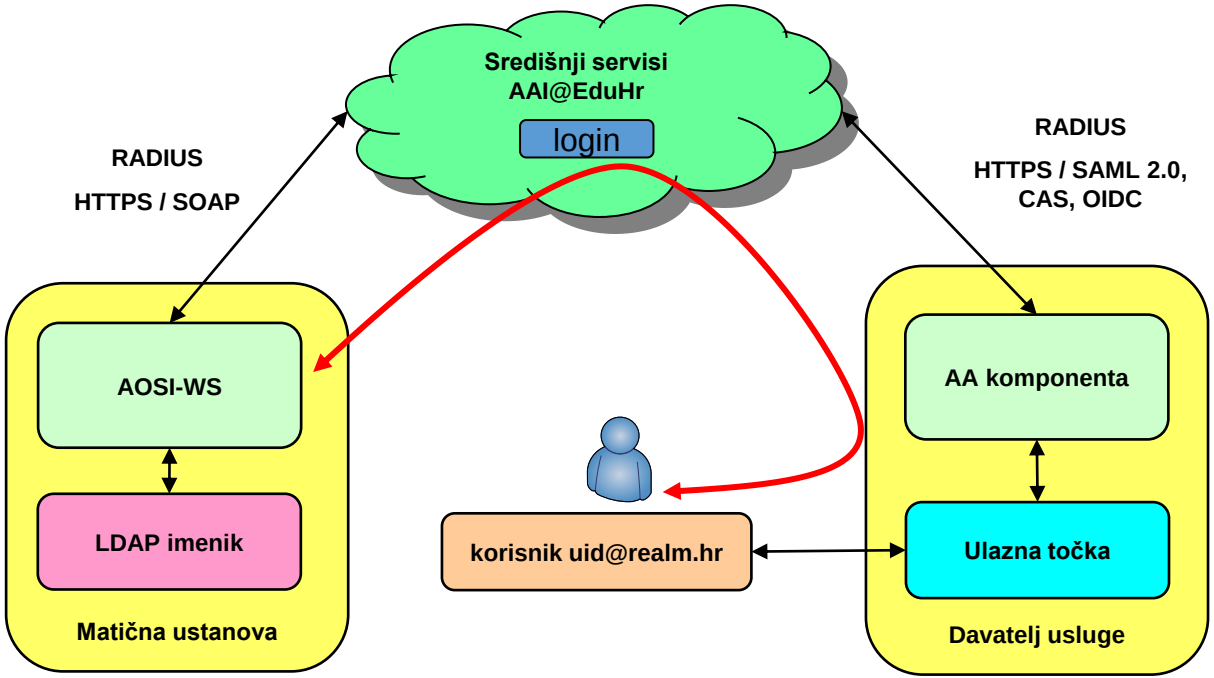
AAI@EduHr u međunarodnom okruženju

Miroslav Milinović,
Sveučilište u Zagrebu, Sveučilišni računski centar (Srce)

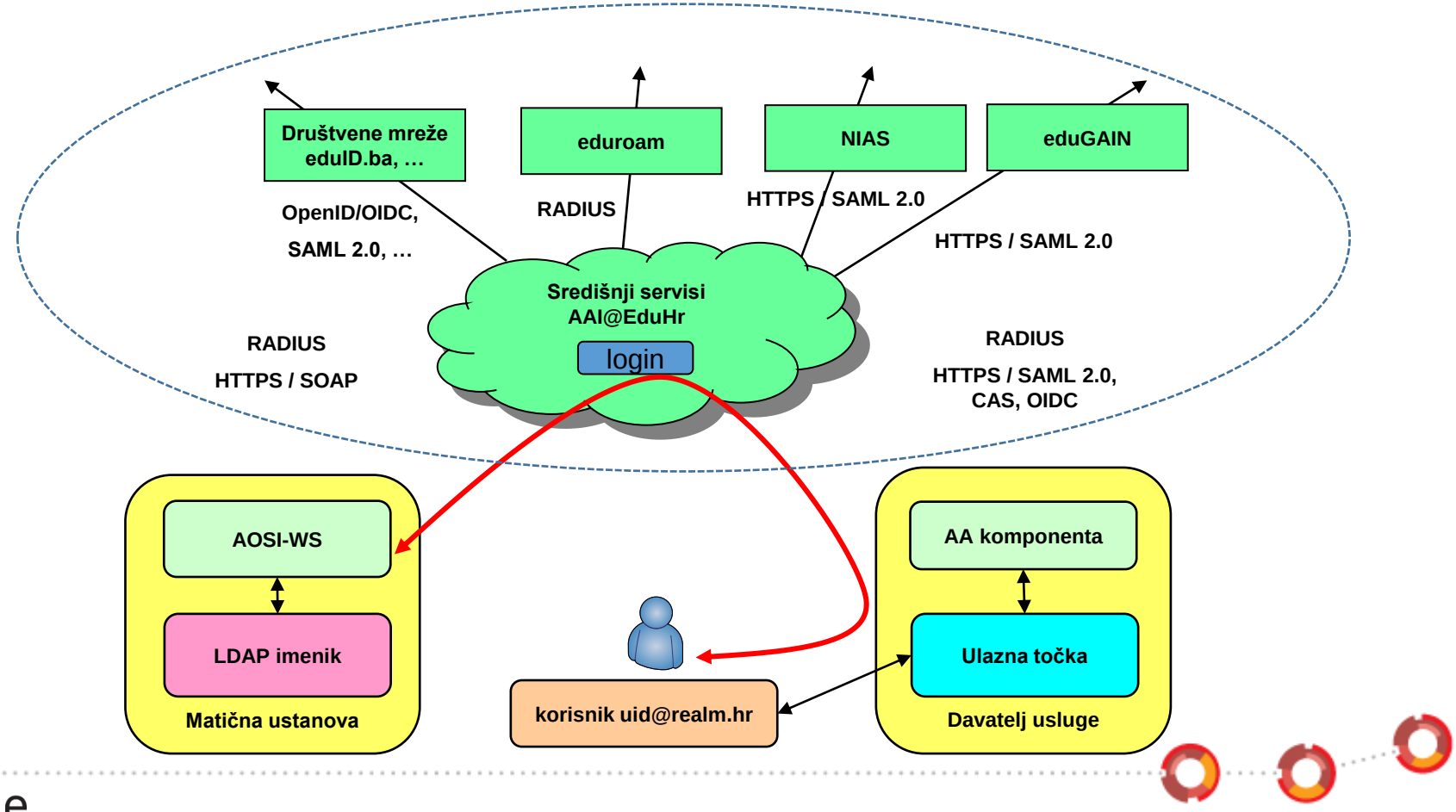
Dani e-infrastrukture – Srce DEI 2021
Konferencija projekta HR-ZOO

28. i 29. travnja 2021.

AAI@EduHr

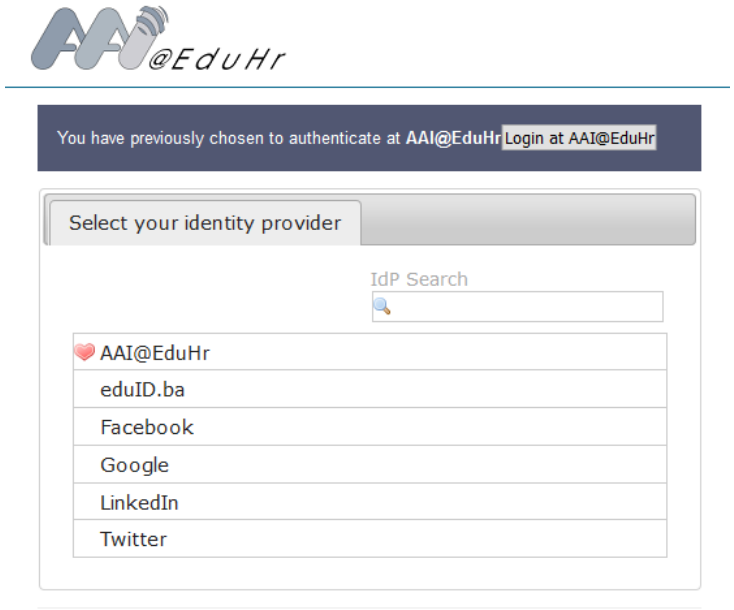

Središnji servisi
AAI@EduHr
login
RADIUS
HTTPS / SOAP
RADIUS
HTTPS / SAML 2.0,
CAS, OIDC
AOSI-WS
LDAP imenik
Matična ustanova
korisnik uid@realm.hr
AA komponenta
Ulazna točka
Davatelj usluge

Povezanost AAI@EduHr s okolinom



Vanjski izvori autentikacije

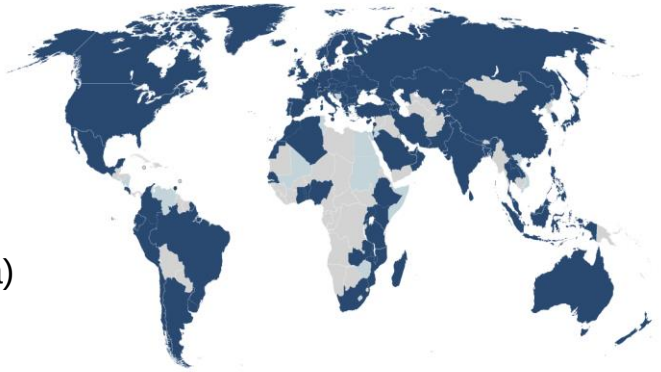
- davatelj usluge
  - prilikom registracije
  - odabire iz ponude izvora autentikacije (autentikacijskih servisa)
- na raspolaganju su:
  - Facebook
  - Google
  - LinkedIn
  - Twitter
  - eduID.ba (AAI obrazovnih institucija u BiH koje izvode nastavu na hrvatskom jeziku)
  - NIAS (u planu)



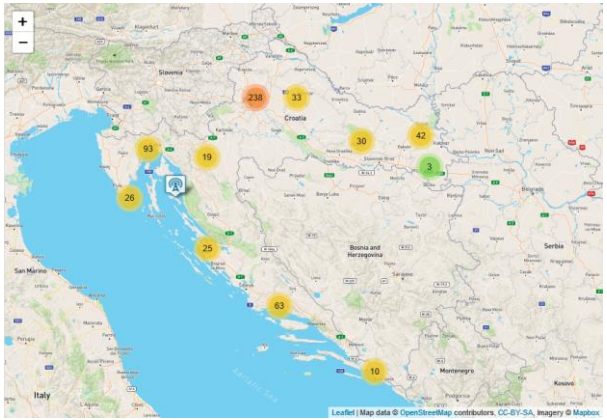
Povezivanje s drugim sustavima

- NIAS (eIDAS)
- eduroam
- eduGAIN

eduroam™



- e**duroam**™: skraćenica od **EDU**cation **ROAM**ing
- moto: “Open your laptop and be online”
- globalna roaming usluga (za korisnike iz sustava znanosti i obrazovanja)
  - siguran i jednostavan (bežični) pristup mreži za krajnje korisnike
  - neovisan o mjestu i vremenu pristupa
  - konzistentan i uniforman
  - čuva privatnost
  - besplatan za kranjeg korisnika
- globalno dostupan
  - u 106 zemalja na preko 29000 lokacija
  - više informacija www.eduroam.org
- informacije o eduroamu u RH
  - za autentikaciju se koristi AAI@EduHr identitet
  - Srce je nacionalni koordinator i operater
  - www.eduroam.hr



srce

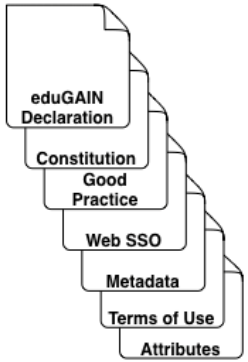
NIAS (eIDAS)

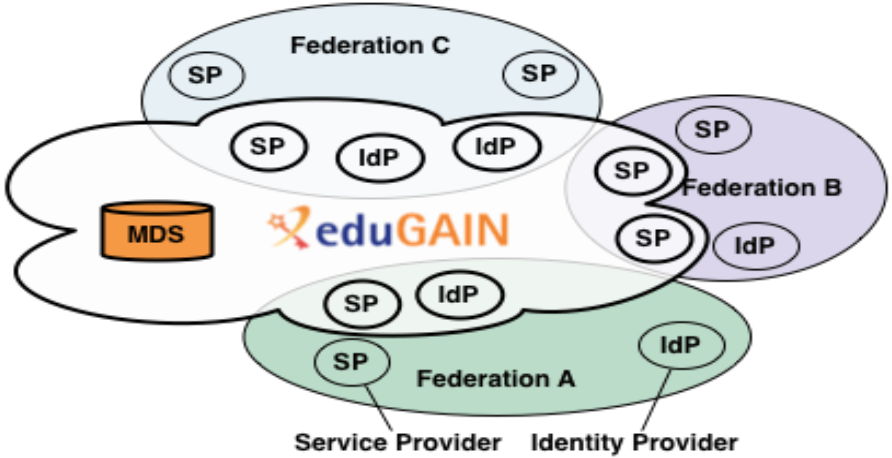
- **Nacionalni Identifikacijski i Autentifikacijski Sustav (NIAS)**
- omogućuje krajnjim korisnicima pristup uslugama u sustavu e-Građani korištenjem prihvaćenih vjerodajnica
- https://gov.hr/
- veza AAI@EduHr s NIAS-om:
  - AAI@EduHr elektronički identitet je prihvaćena vjerodajnica s niskom razinom sigurnosti
  - planiramo:
    - AAI@EduHr 2FA prihvaćena vjerodajnica sa značajnom razinom sigurnosti
    - NIAS kao vanjski izvor autentikacije
- putem NIAS-a moguće je povezivanje s eIDAS-om
  - **e**lectronic **ID**entification, **A**uthentication and trust **S**ervices
  - sustav i EU regulativa vezana uz sigurno (prekogranično) korištenje elektroničkih identiteta
  - primjer: AAI@EduHr HfH servis

eduGAIN

- inter-federacijska usluga razvijena u okviru serije projekta GÉANT
- www.edugain.org
- povezuje federacije e-identiteta (AAI infrastrukture)
  - primarno nacionalne znanstvene i obrazovne AAI
- temeljni cilj: olakšati međunarodnu suradnju i razmjenu informacija kroz povezivanje (nacionalnih) AAI
- izazovi u inter-federacijskom modelu:
  - zaštita privatnosti
  - isporuka atributa (podataka o osobi) između matične ustanove (IdP) i davatelja usluge (SP)
- ključno je osigurati povjerenje među svim čimbenicima (federacije, IdP-ovi, SP-ovi)
  - jasno definirana pravila i norme (*Policy Framework*)
  - sigurna i pouzdana tehnička rješenja

eduGAIN





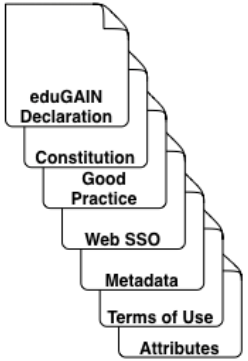
- **edu**cational **G**lobal **A**uthentication **In**frastructure
- dvije temeljne komponente:
  - pravila i norme: eduGAIN Policy Framework
  - tehnički sustav: MDS (Metadata Distribution Service)

eduGAIN Policy Framework

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

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

- dokumenti su javno dostupni na adresi:
  - https://technical.edugain.org/documents



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 MDS

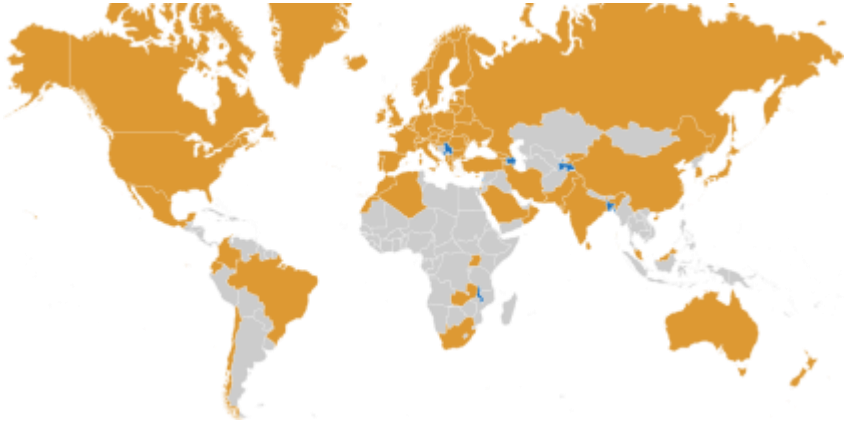
- metapodatkovni servis (https://mds.edugain.org)
  - sadrži metapodatke o svim IdP-ovima i SP-ovima koji su putem svojih federacija uvršteni u eduGAIN
  - federacije osiguravaju ažurnost metapodataka iz svoje nadležnosti

- mogući modeli sudjelovanja su *opt-in* i *opt-out*:
  - federacija publicira metapodatke o odabranim IdP-ovima i SP-ovima temeljem svojih pravila/njihove odluke
  - uobičajeni model:
    - *opt-out* za IdP-ove
    - *opt-in* za SP-ove

- više informacija: https://technical.edugain.org/

Koliko je eduGAIN raširen?

- u produkciji od 2011. godine
- više od 70 članica, više od 3000 usluga
- više informacija: www.edugain.org



Federations in eduGAIN	
Participants	72
Voting-only Members	1
Candidates	7
Entities in eduGAIN	
All entities	7472
IdPs	4253
SPs	3225
Standalone AAs	3

REFEDS

- **R**esearch and **E**ducation **FED**eration**s** group (https://refeds.org)
- forum koji okuplja federacije e-identiteta iz znanstvene i obrazovne zajednice
- zastupa interese svojih članova, otvoren svima zainteresiranim
- aktivnosti obuhvaćaju i definiranje standarda i preporuka:
  - imeničke sheme
    - eduPerson, SCHAC, …
  - SAML entitetne kategorije i atributi
    - R&S – Research & Scholarship (https://refeds.org/research-and-scholarship)
    - SIRTFI - Security Incident Response Trust Framework for Federated Identity (https://refeds.org/sirtfi)
    - …
  - SAML profili
  - …
  - https://refeds.org/specifications

AAI@EduHr u eduGAIN-u

- AAI@EduHr je punopravna članica eduGAIN-a (od lipnja 2011.)
- Srce kao koordinator/operator zastupa AAI@EduHr u tijelima eduGAIN-a
- model koji primjenjujemo:
  - **opt-out za matične ustanove**
    - uključene su samim pristupanjem u AAI@EduHr
    - isporuka atributa prema važećim preporukama i definiciji entitetne kategorije R&S
    - moguće je zatražiti isključivanje (opt-out)
  - **opt-in za usluge**
    - ulaze isključivo na vlastiti zahtjev
    - moraju ispuniti potrebne tehničke i organizacijske uvjete
- AAI@EduHr je usklađena s REFEDS SAML entitetnim kategorijama
  - R&S, SIRTFI
  - daje podršku svojim uslugama koje žele deklarirati usklađenost s normom CoCo

Isporuka atributa uslugama u eduGAIN-u

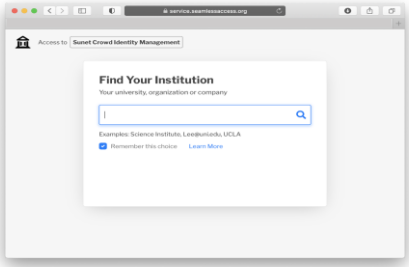
Isporučeni atribut	Izvorni atribut (hrEduPerson shema)	Transformacija
displayName	displayName	
cn	cn	
sn	sn	
givenName	givenName	
mail	mail	
eduPersonAffiliation	hrEduPersonAfiliation	djelatnik → employee, member student → student, member vanjski suradnik → affiliate, member
eduPersonScopedAffiliation		eduPersonAffiliation@schacHomeOrganization
eduPersonPrincipalName	hrEduPersonUniqueID	
eduPersonTargetedID	hrEduPersonPersistentID	
schacHomeOrganization	hrEduPersonHomeOrg	

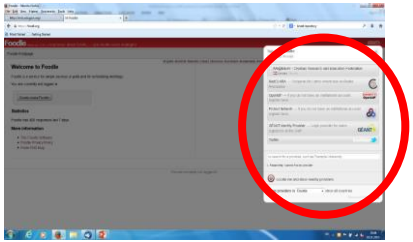
schacPersonalUniqueCode - samo na eksplicitni zahtjev

- vrijednost se izvodi prema pravilima za *European Student Identifier* iz vrijednosti atributa *hrEduPersonUniqueNumber*, ako ona sadrži JMBAG

Kako uslugu povezati u eduGAIN?

- obavijestiti Srce (koordinatora federacije) o namjeri
  - Srce pruža tehničku i organizacijsku potporu
- prilagoditi pravila usluge
  - Privacy policy / CoCo, R&S, ...
- 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 u eduGAIN i publiciranje odgovarajućih metapodataka





srce

Hvala!

aai@srce.hr

srce
Sveučilište u Zagrebu
Sveučilišni računski centar

www.srce.unizg.hr

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/otvoreni-pristup

srce otvoreni pristup