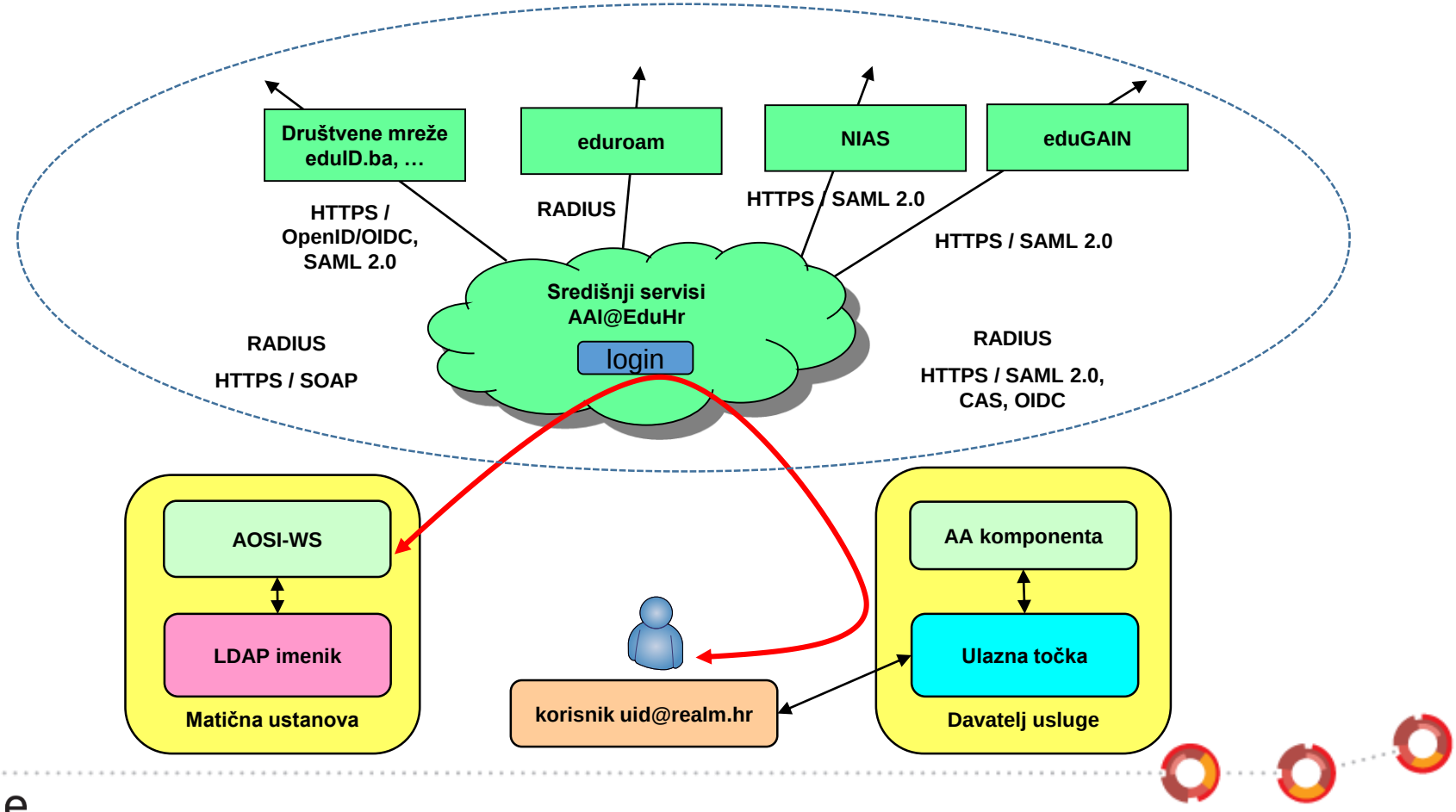
AAI@EduHr u sustavu eduGAIN

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

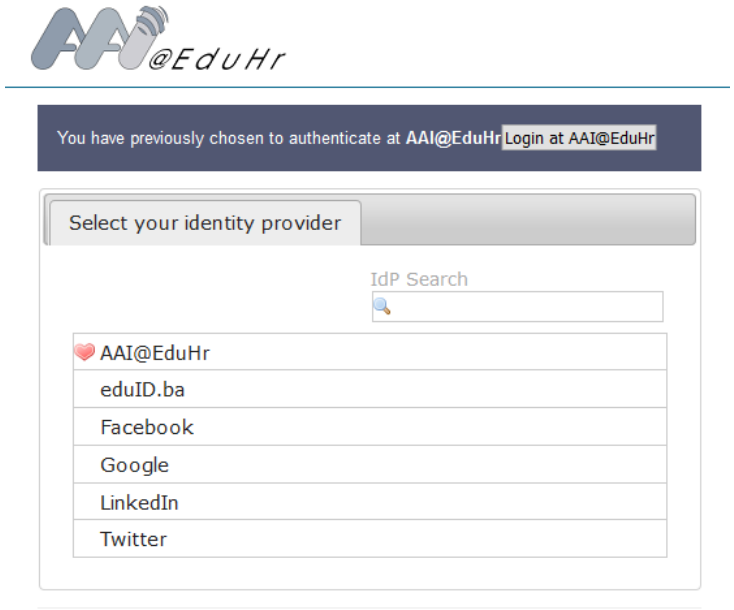
27. svibnja 2021.

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)



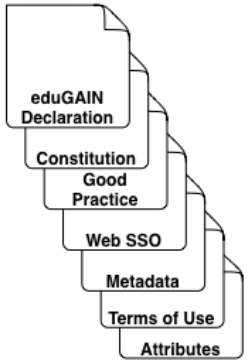
Povezivanje s drugim sustavima

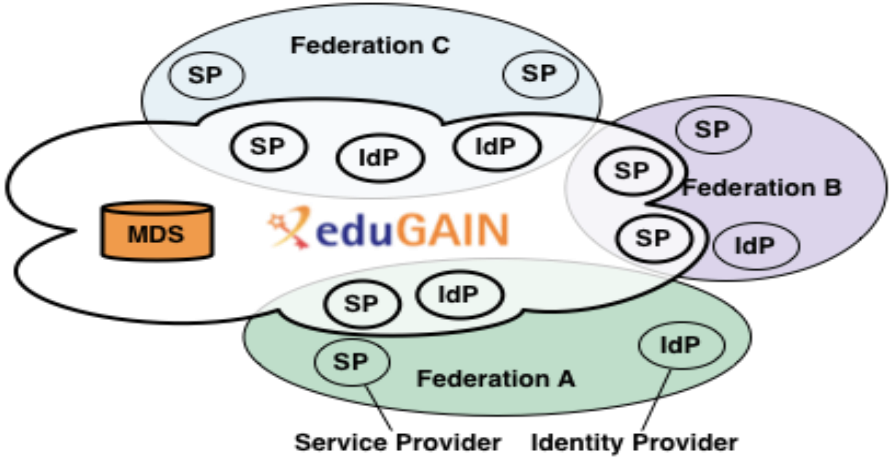
- NIAS (eIDAS)
- eduroam
- eduGAIN

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





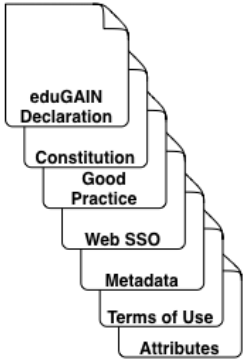
- **edu**cational **G**lobal **A**uthentication **In**frastructure
- dvije temeljne komponente:
  - pravila i norme: eduGAIN Policy Framework
  - tehnički sustav: MDS (Metadata Distribution Service)

eduGAIN Policy Framework

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

- Code of Conduct (CoCo) – 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

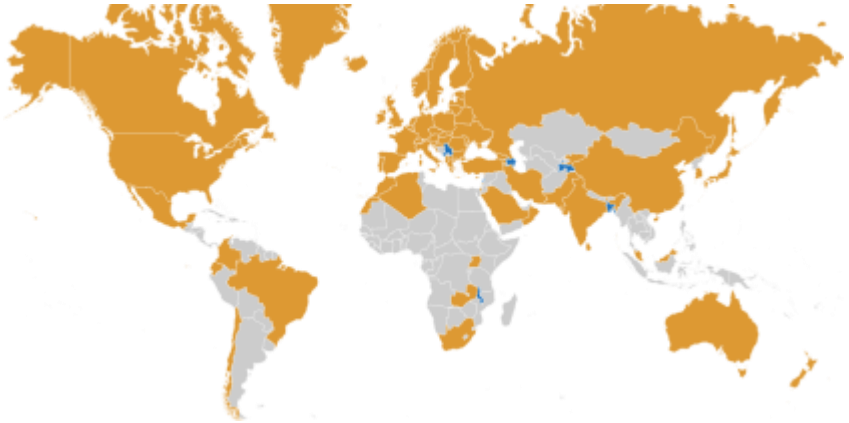
- metapodatkovni servis (https://mds.edugain.org)
  - sadrži metapodatke o svim IdP-ovima i SP-ovima koji su putem svojih federacija uvršteni u eduGAIN
  - federacije osiguravaju ažurnost metapodataka iz svoje nadležnosti

- 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, technical.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 (https://wiki.refeds.org/display/STAN/Schemas)
    - eduPerson, SCHAC, …
  - SAML entitetne kategorije i atributi
    - R&S – Research & Scholarship
    - SIRTFI - Security Incident Response Trust Framework for Federated Identity …
  - SAML profili
  - …
  - https://refeds.org/specifications

CoCo – (Data Protection) Code of Conduct

- pravila ponašanja za subjekte u federacijskom (AAI) okruženju
  - zaštita privatnosti (GDPR)
  - uspostava povjerenja između IdP-a i SP-a
  - norme za SP-ove:
    - načela obrade (osobnih) podataka
    - objaviti politiku privatnosti (*privacy statement/policy*)
    - https://wiki.refeds.org/display/CODE/Code+of+Conduct+for+Service+Providers?preview=/1606087/7864339/GEANT_DP_CoCo_ver1.0.pdf

- CoCo Entity Category
  - tehnička pravila – način deklariranja sukladnosti s normom CoCo
  - aktivni nadzor / moguća provjera: https://monitor.edugain.org/coco
  - https://wiki.refeds.org/display/CODE/Entity+Category+Definition%3A+Data+protection+Code+of+Conduct?preview=/1606124/6553601/GEANT_DP_CoCo_Entity_Category_ver1.2.pdf

- cjelovita dokumentacija: https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home

R&S EC - Research & Scholarship Entity Category

- entitetna kategorija kojom se definira skup atributa za usluge (SP-ove) u ZiVO
  - minimalni skup atributa za potrebe SP-a u okruženju ZiVO
  - oslanja se na eduPerson i SCHAC sheme
  - sukladnost deklariraju i IdP i SP u svojim metapodacima
  - definirani skup atributa:
    - *shared user identifier* (eduPersonPrincipalName, eduPersonTargetedID)
    - *person name* (displayName, givenName + sn)
    - *email address* (mail)
    - (opcionalno) *affiliation* (eduPersonScopedAffiliation)
  - dokumentacija: https://refeds.org/research-and-scholarship
  - u tijeku aktivnosti na EC R&S v. 2.0 (https://wiki.refeds.org)

SIRTFI - Security Incident Response Trust Framework for Federated Identity

- usklađivanje aktivnosti vezanih uz sigurnosne incidente u federacijama e-identiteta
- pravila i preporuke za federacije, ali i IdP-ove i SP-ove
- prvi korak: pouzdani kontakti u slučaju incidenta (deklarirani u metapodacima)
- dokumentacija: https://refeds.org/sirtfi

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 (iz AAI@EduHr) uslugama u eduGAIN-u

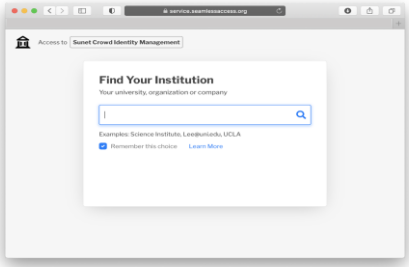
Isporučeni atribut	Izvorni atribut (hrEduPerson shema)	Transformacija
displayName	displayName	
cn	cn	
sn	sn	
givenName	givenName	
mail	mail	
eduPersonAffiliation	hrEduPersonAfiliation	djelatnik → employee, member student → student, member vanjski suradnik → affiliate, member
eduPersonScopedAffiliation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

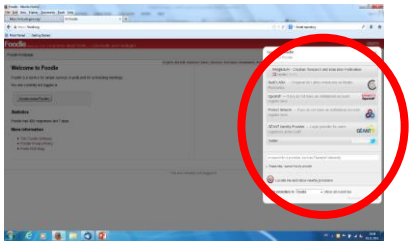
schacPersonalUniqueCode - samo na eksplicitni zahtjev

- 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**, kreiranje i publiciranje odgovarajućih metapodataka**





eduGAIN i atributi

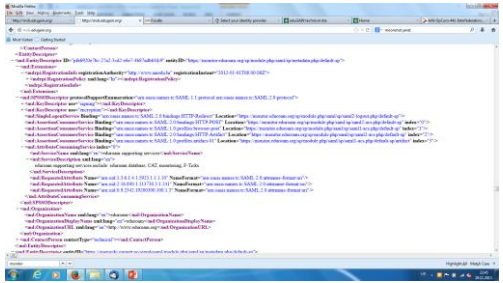
- osnovne scheme su eduPerson i SCHAC (https://wiki.refeds.org/display/STAN/Schemas)
- minimizirati broj atributa
- očekuje se da usluga deklarira koje atribute traži putem svojih metapodataka (**required attributes**)
- Preporuka za usluge:
  - deklarirati CoCo
  - koristiti samo nužne atribute
  - birati iz skupa atributa definiranih R&S entitetnom kategorijom i globalno prepoznatim potrebama (ESI za mobilnost)
    - *displayName*
    - *cn*
    - *sn*
    - *givenName*
    - *mail*
    - *eduPersonAffiliation*
    - *eduPersonScopedAffiliation*
    - *eduPersonPrincipalName*
    - *eduPersonTargetedID*
    - *schacHomeOrganization*
    - *schacPersonalUniqueCode*

WhereAreYouFrom (WAYF) sučelje

- discovery service
  - korisnik odabire odakle dolazi (svoj IdP/federaciju/login servis)
- različita rješenja (sva temelje na metapodacima)
- izazovi
  - arhitekture federacija
  - nazivi IdP-ova
  - prezentacija podataka korisniku (dostupnih putem MDS-a)
    - sučelja su različita: dizajnom i tehnologijom
    - HTML geolocation – rješenje nije savršeno
- rješenja:
  - DiscoJuice (uz SimpleSamlPhp)
  - SeamlessAccess (https://seamlessaccess.org/)
  - vlastito rješenje
- primjeri:
  - https://monitor.eduroam.org, https://events.geant.org, https://spaces.at.internet2.edu/, https://wiki.sunet.se/, https://edusign.sunet.se/, https://learning-agreement.eu/

Upravljanje (SAML) metapodacima usluge (SP-a)

- metapodaci se publiciraju u suradnji sa Srcem



- SP, uz ostalo, kroz metapodatke deklarira:
  - atribute koje traži/očekuje od IdP-a
  - entitetne kategorije i norme kojih se pridržava (CoCo, R&S, …)

- Srce
  - publicira podatke SP-a u eduGAIN MDS
  - osigurava adresu s koje SP osvježava metapodatke o subjektima u eduGAIN-u
    - osvježavanje metapodataka treba automatizirati (min. jednom dnevno?)
    - sadrže popis IdP-ova

Metapodaci AAI@EduHr:
https://login.aaiedu.hr/edugain/aaieduhr_edugain.xml

Pitanja?

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