AAI@EduHr radionica

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

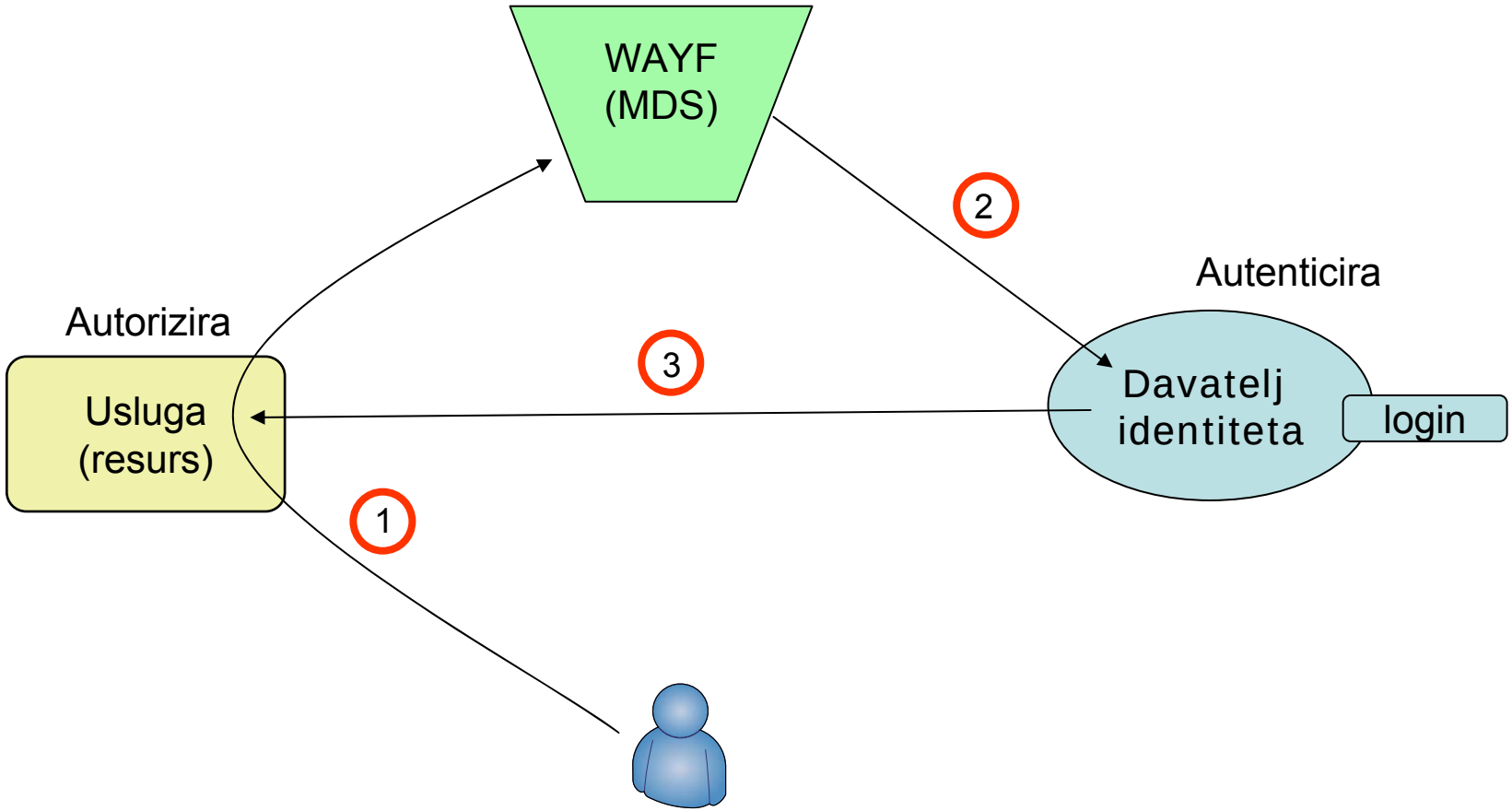
studeni 2012.

Sadržaj

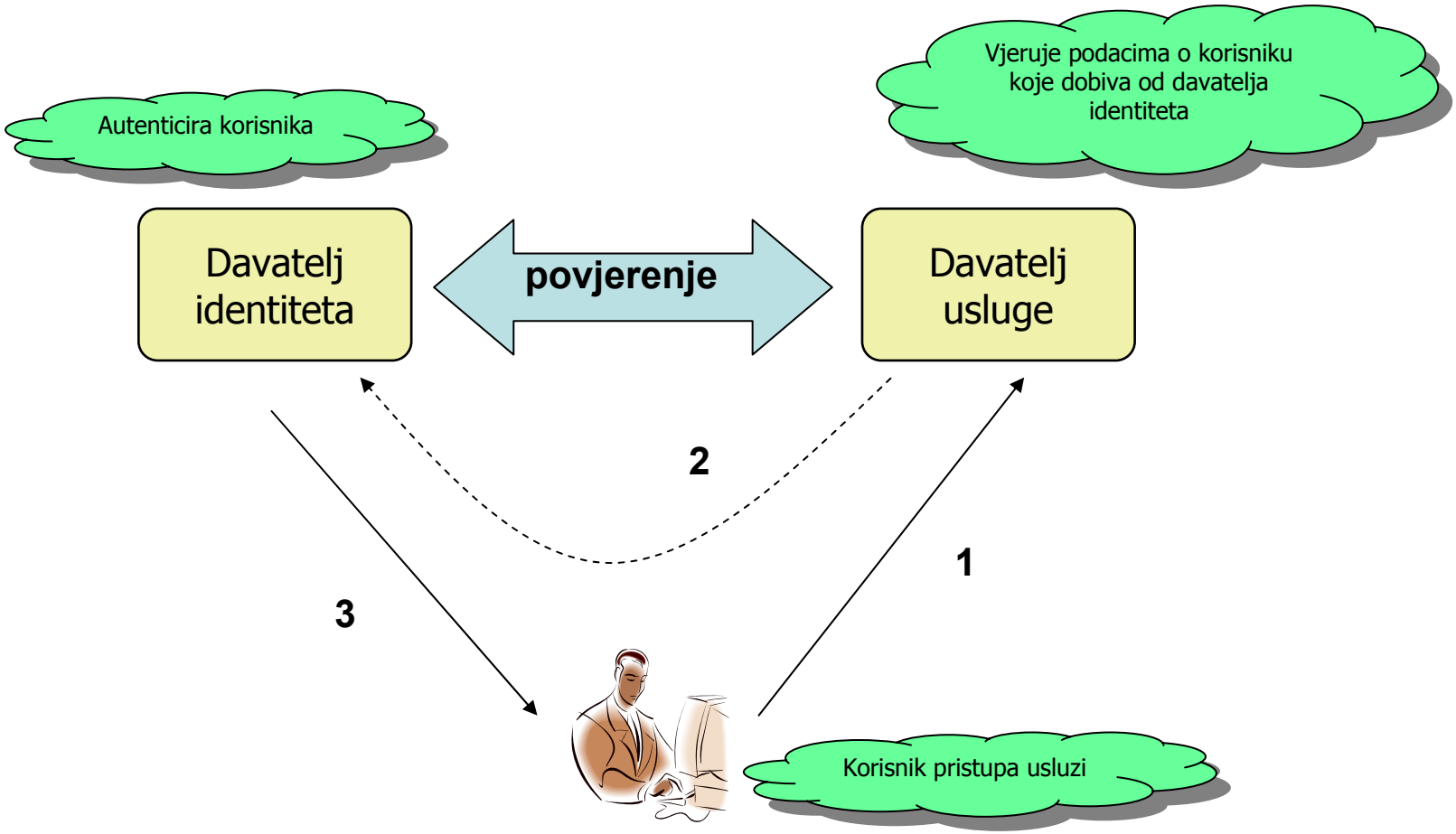
- 11:00 – 12:30: **organizacijski i informacijski aspekti**
  - ustroj AAI@EduHr, registri subjekata
  - certificiranje matičnih ustanova
  - certificiranje usluga
  - AAI@EduHr Lab
- 12:30 – 12:45: pauza
- 12:45 – 14.15: **tehnički aspekti**
  - kako uslugu uskladiti s AAI@EduHr?
  - alternativni načini autentikacije (društvene mreže/OpenID, eduGAIN)
  - virtualne organizacije
- 14:15 – 14:30: pauza
- 14:30 – 15:00: **korisnici pitaju (otvorena rasprava)**

Organizacijski i informacijski aspekti

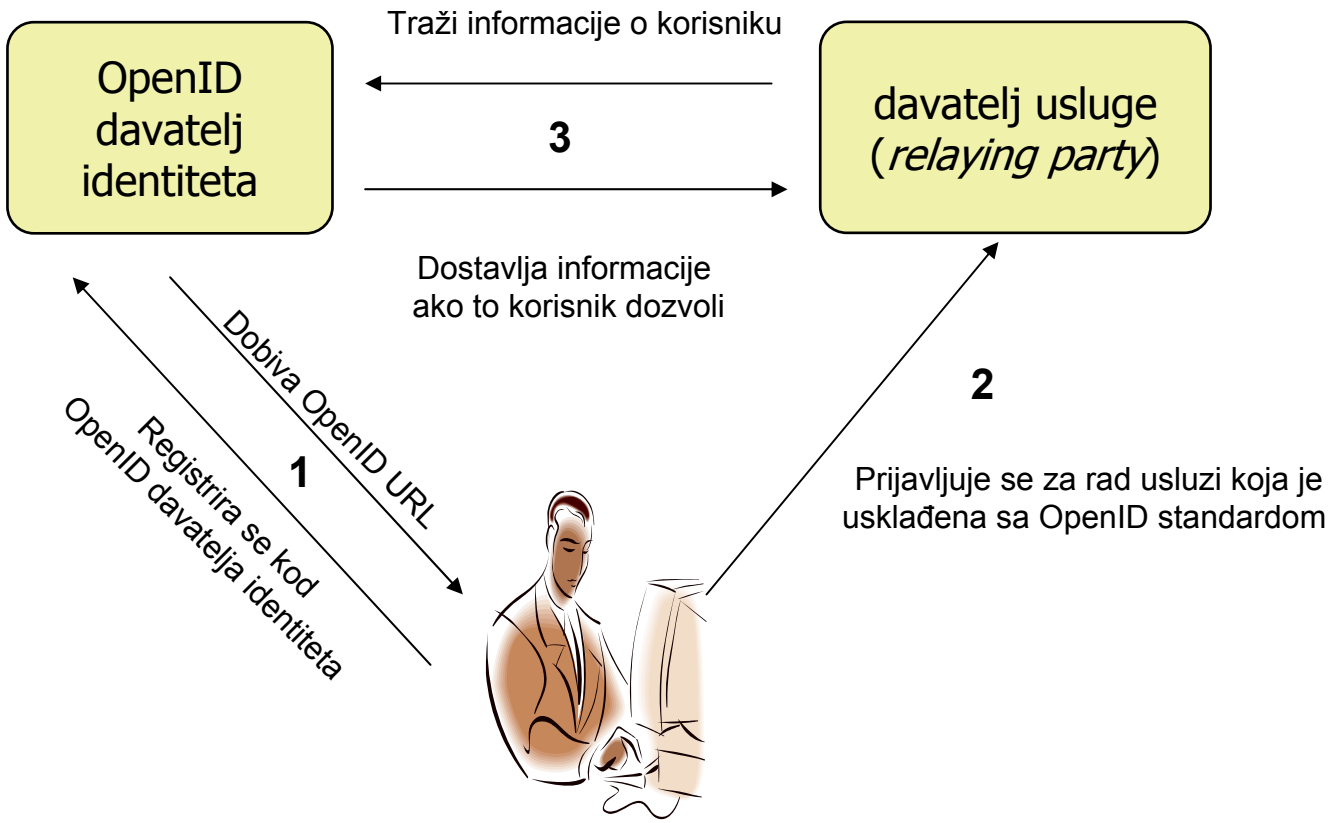
AAI: osnovni model



Federacijski model



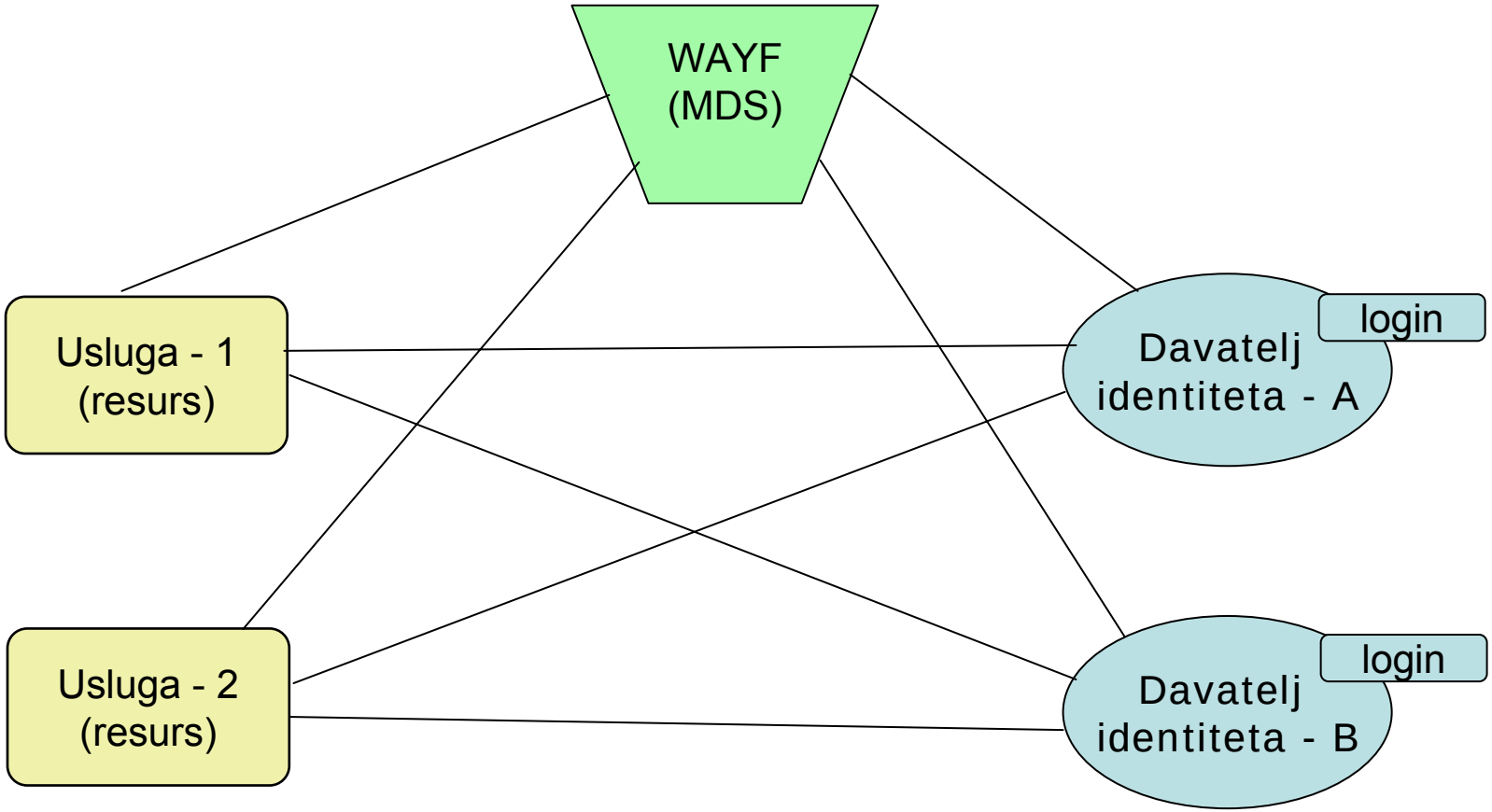
Model utemeljen na korisniku (primjer: OpenID)



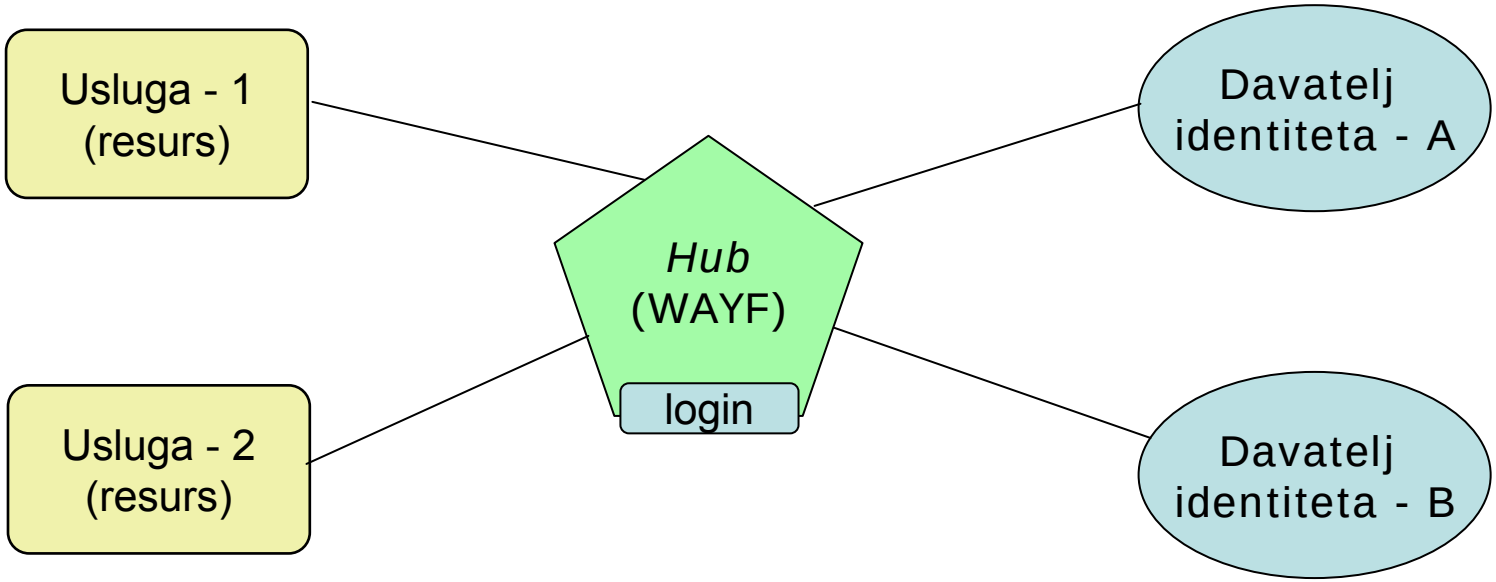
Federacije

- distribuirano rješenje (*mash*)
  - distribuirane točke autentikacije (login)
  - WAYF
- centralizirano rješenje (*hub-and-spoke*)
  - centralna točka – hub (login)
- hibridna rješenja

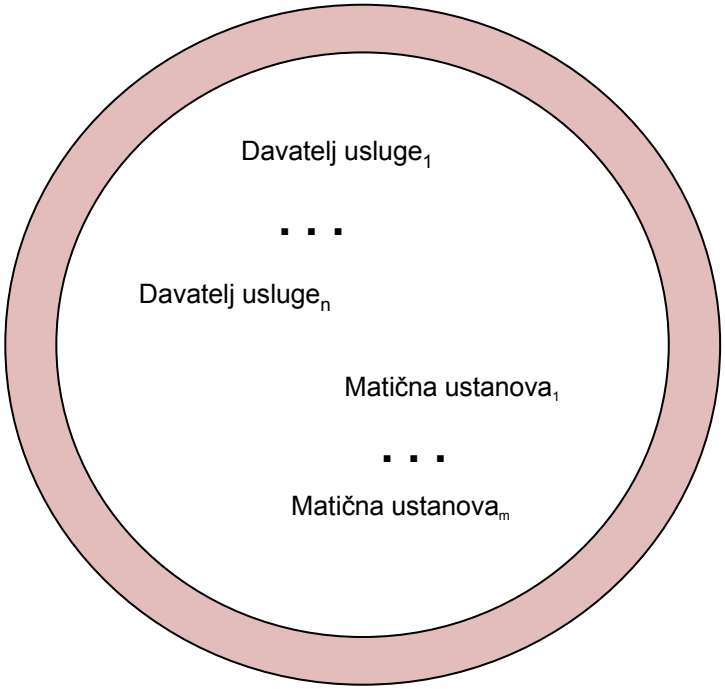
Mash federacija

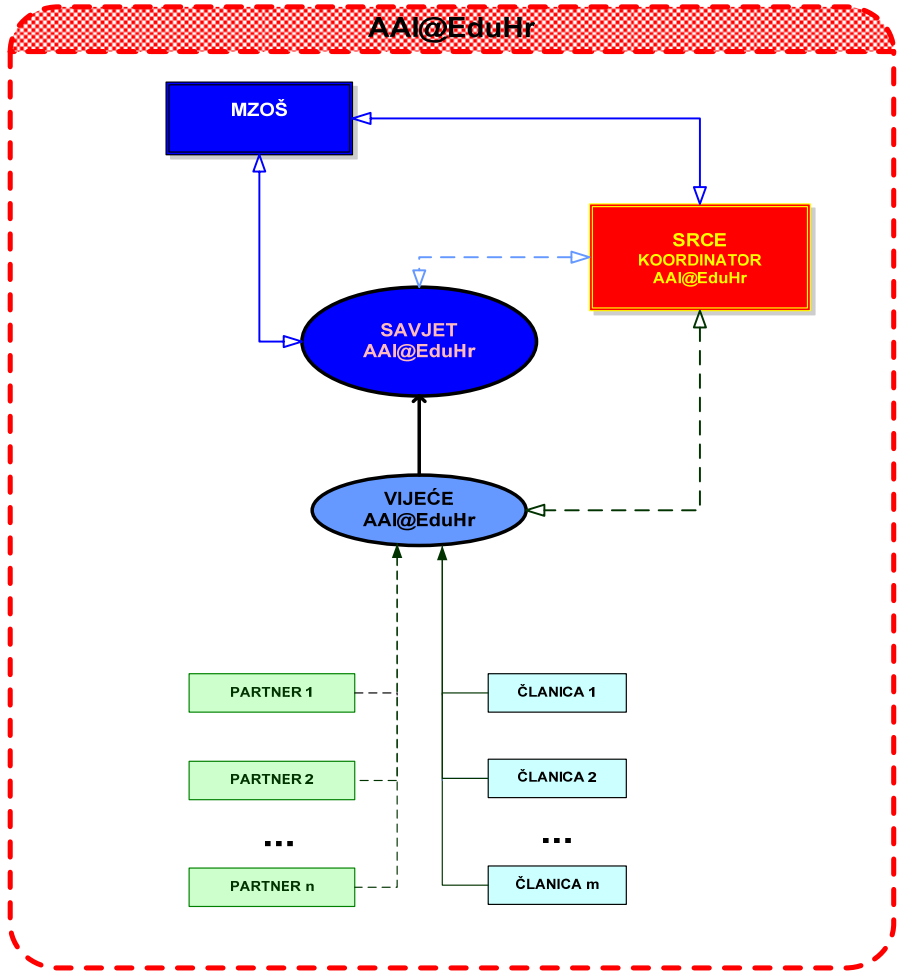


Hub-and-spoke federacija



Organizacija AAI@EduHr





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 sustav AAI@EduHr

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/

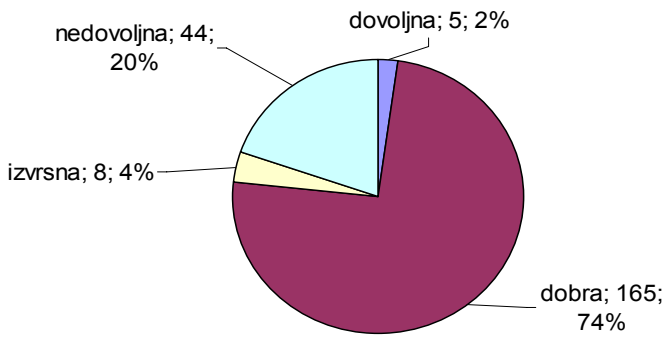
Sustav certificiranja

- 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/

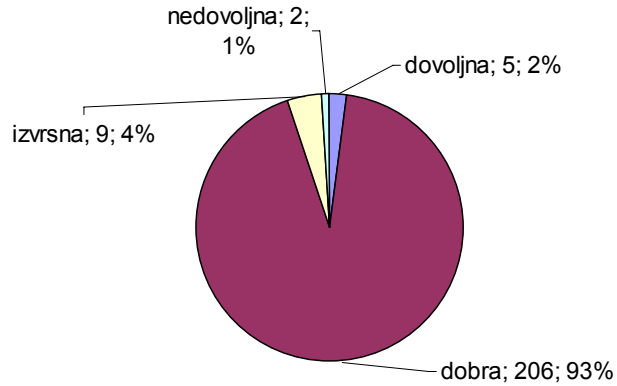
Certificiranje matičnih ustanova

- provodi se redovito, jednom godišnje
- certificiranje 2011.
  - 30 uvjeta (18 obaveznih + 12 preporučenih)
  - 222 subjekta
  - osnovni rok: 01.03. – 18.04.
  - dopunski rok: 02.05. – 08.07.
- certificiranje 2012.
  - 29 uvjeta (19 obaveznih +10 preporučenih)
  - 220 subjekata
  - osnovni rok: 15.05. - 09.07.
  - dopunski rok: 01.09. – 30.09.

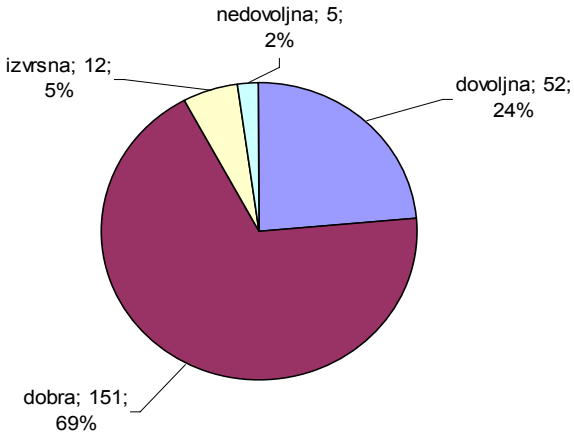
Rezultati certificiranja matičnih ustanova



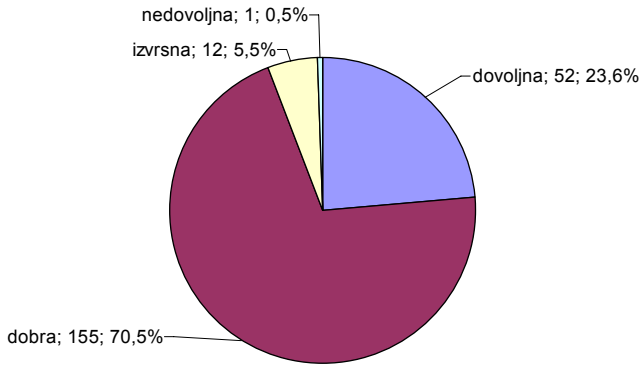
osnovni rok 2011.



dopunski rok 2011.



osnovni rok 2012.



dopunski rok 2012.

Norme za matične ustanove: obavezno u 2012. (1)

- Je li potpisan, ovjeren i odobren odgovarajući zahtjev za članstvo u AAI@EduHr sustavu?
- Jesu li imenovane kontakt osobe i predstavnik u Vijeću AAI@EduHr?
- Je li utvrđena procedura za informacijsko održavanje imenika?
- Jesu li korisnici informirani o svojim pravima i obavezama prilikom preuzimanja e-identiteta?
- Vodi li matična ustanova evidenciju o dodijeljenim e-identitetima?
- Jesu li podaci o ovlaštenim osobama te kontakt podaci za korisnike objavljeni na adresi http://www.aaiedu.hr/aai_status.php točni?
- Obavlja li se dodjela e-identiteta na temelju dokumenta sa slikom ili kroz proces zapošljavanja/upisa?
- Uručuju li se podaci o e-identitetu osobno ili pisanim putem (ne telefonom ili e-mailom)? (Odnosi se i na promjenu lozinke.)

Norme za matične ustanove: obavezno u 2012. (2)

- E-identiteti osoba koje su prestale biti povezane s ustanovom se pravodobno i redovito se brišu (sukladno utvrđenoj proceduri)!
- 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 imeniku?
- U LDAP imeniku nema nijedan e-identitet s neispravnim podatkom o e-mail adresi!
- Vrijednost atributa brojčani identifikator osobe je jedinstvena na nivou ustanove!
- Jesu li podaci o ustanovi zapisani u org zapisu LDAP imenika potpuni i ispravni!
- Koordinatoru je omogućen nadzor rada LDAP, RADIUS i AOSI-WS poslužitelja!

Norme za matične ustanove: obavezno u 2012. (3)

- Je li inačica LDAP programskog paketa iz distribucije AAI@EduHr ili drugog odgovarajućeg programa instalirana i ispravno konfigurirana na poslužitelju ustanove novija ili jednaka inačici 2.4.11 (AAI@EduHr LDAP paket 2.4.11-4)?
- Je li inačica RADIUS programskog paketa iz distribucije AAI@EduHr ili drugog odgovarajućeg programa instalirana i ispravno konfigurirana na poslužitelju ustanove novija ili jednaka inačici 2.1.3 (AAI@EduHr RADIUS paket 2.1.3-4)?
- Je li inačica AOSI web servisa iz distribucije AAI@EduHr instalirana i ispravno konfigurirana na poslužitelju ustanove novija ili jednaka inačici 3.0.7 (AAI@EduHr AOSI WS paket 3.0.7)?
- 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)?
- Izdaje li se elektronički identitet u sustavu AAI@EduHr odnosno slog u imeniku s identifikatorom (DN-om) oblika uid=oznaka, dc=domena, dc=hr isključivo fizičkim osobama?

Norme za matične ustanove: preporučeno u 2012. (1)

- Je li LDAP imenik prijavljen Agenciji za zaštitu osobnih podataka kao zbirka podataka?
- Je li procedura za informacijsko održavanje imenika javno dostupna?
- Posjeduju li svi zaposlenici i studenti e-identitete?
- 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)?
- Uz svaki je e-identitet zabilježen odgovarajući OIB. Iznimka mogu biti samo korisnici kojima je vrijednost atributa hrEduPersonAffiliation 'gost'!
- Je li na poslužitelju ustanove instalirana i ispravno konfigurirana najnovija inačica LDAP programskog paketa iz distribucije AAI@EduHr (2.4.23-1) ili drugog odgovarajućeg programa?

Norme za matične ustanove: preporučeno u 2012. (2)

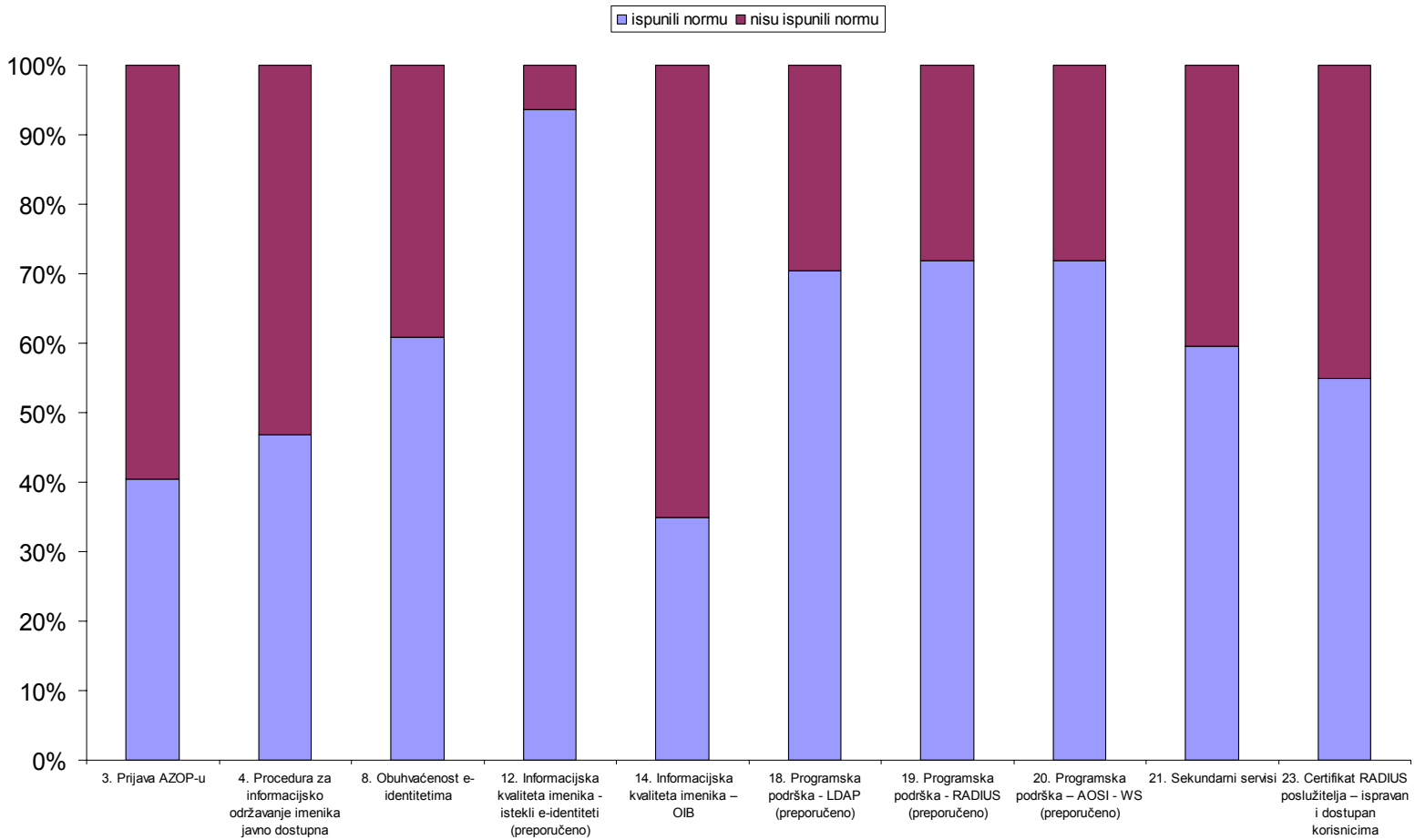
- Je li na poslužitelju ustanove instalirana i ispravno konfigurirana posljednja inačica RADIUS programskog paketa iz distribucije AAI@EduHr (2.1.10-1) ili drugog odgovarajućeg programa?

- Je li na poslužitelju ustanove instalirana i ispravno konfigurirana posljednja inačica AOSI web servisa (programski paket iz distribucije AAI@EduHr verzije 3.1.4)?

- U produkciji su sekundarni LDAP, RADIUS i AOSI-WS!

- Je li certifikat RADIUS poslužitelja ustanove ispravan i dostupan korisnicima kroz uporabu eduroam installera (installer.eduroam.hr)?

Rezultati certificiranja matičnih ustanova



nakon osnovnog rok 2012. – preporučeni uvjeti

Certificiranje usluga

- provodit će se redovito, jednom godišnje
- prvo certificiranje
  - od 15.11. do 31.12. 2012.
  - pravila i popis normi javno su dostupni http://www.aaiedu.hr/certificiranje/AAIEduHr-SP-certificiranje2012-v1.1.pdf
  - provjerava se usklađenost usluga koje su registrirane kao produkcijske
- usluge koje su registrirane kao testne (razvojne) bit će premještene u testnu inačicu sustava (AAI@EduHr Lab)
- rezultati su dostupni na: http://www.aaiedu.hr/certificiranje/SP2012/

Certificiranje usluga: obavezno u 2012.

- Je li potpisan, ovjeren i odobren odgovarajući zahtjev za članstvo ili status partnera u sustavu AAI@EduHr?
- Odgovorna osoba davatelja usluge je prilikom registracije usluge potvrdila kako će usluga biti pružana sukladno odredbama Pravilnika o ustroju AAI@EduHr (točka 3.7.)!
- U registar resursa upisan je naziv usluge!
- U registar resursa upisana je točna URL adresa:
  - usluge (ako se radi o usluzi dostupnoj HTTP(S) protokolom)
  - web stranice s informacijama o usluzi (ako se radi o usluzi koja nije dostupna HTTP(S) protokolom)!
- U registar resursa upisan je jasan i točan opis usluge!
- U registar resursa upisani su točni podaci o administratoru (odgovornoj osobi) usluge!
- Za pristup središnjim servisima usluga koristi protokol:
  - SAML 2.0 (ako se radi o usluzi dostupnoj HTTP(S) protokolom)
  - RADIUS (ako se radi o usluzi koja nije dostupna HTTP(S) protokolom)!

Certificiranje usluga: norme za web-usluge u 2012.

- **(P)** - Usluga koristi isključivo HTTPS protokol!
- **(P)** - Usluga ima implementiranu središnju odjavu korisnika single log-out (SLO)!
- **(P)** - Usluga koristi certifikat izdan putem CARNetove TCS usluge ili izravno od izdavača evidentiranog u početnim postavkama popularanih web-preglednika!

Certificiranje usluga: norme za RADIUS-usluge u 2012.

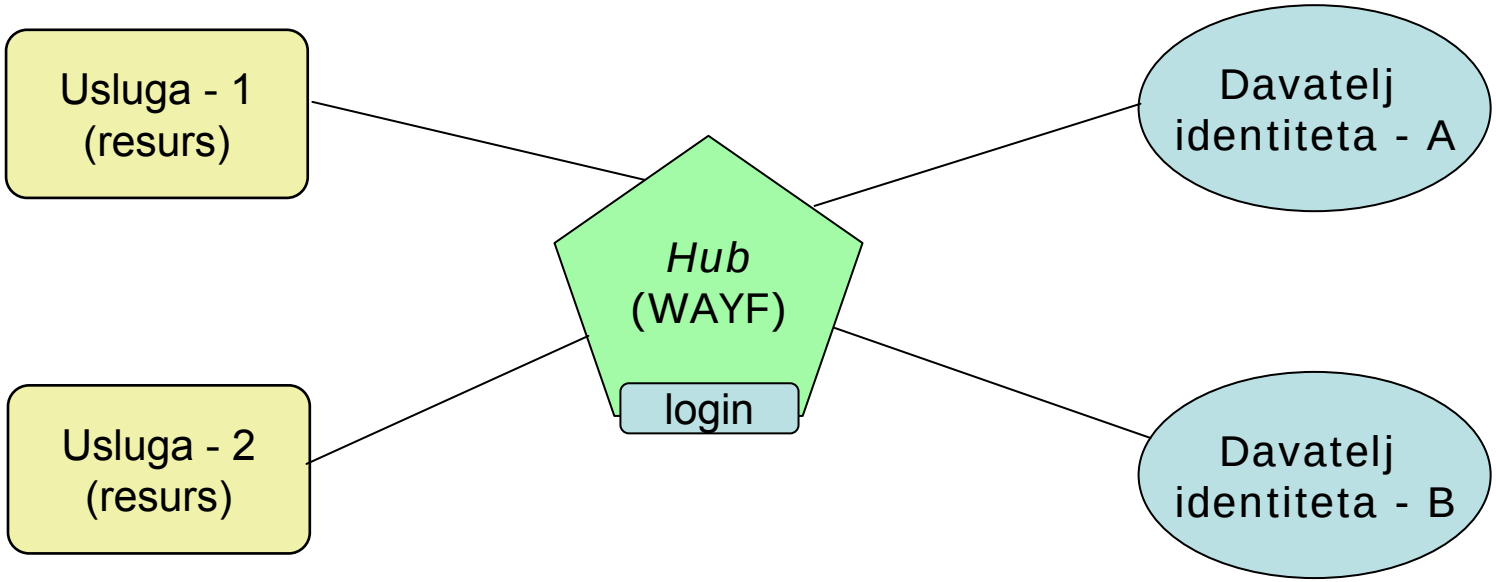
- **(O)** - RADIUS poslužitelj usluge ispravno prosljeđuje upite središnjim poslužiteljima, koristeći EAP protokol!
- **(O)** - RADIUS poslužitelj usluge ne modificira atribute koje prosljeđuje središnjim poslužiteljima!
- **(P)** - RADIUS poslužitelj usluge ispravno isporučuje RADIUS atribut ON (OperatorName)!

AAI@EduHr Lab

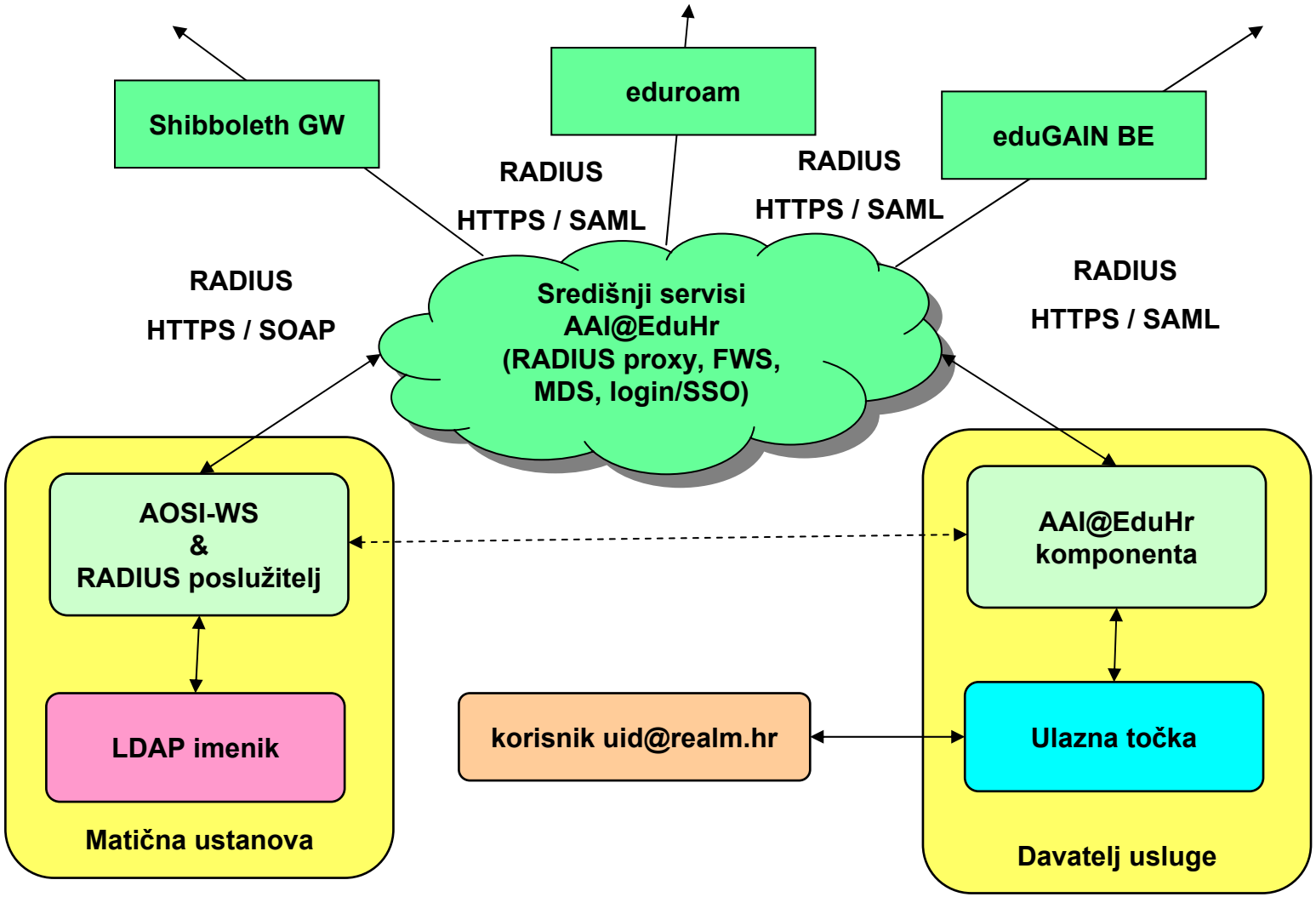
- okruženje za testiranje i razvoj novih aplikacija
- tehnološki identično produkcijskom sustavu, ali bez mogućnosti korištenja produkcijskih središnjih servisa i podataka (tj. e-identiteta)
- na raspolaganju svim davateljima usluga
- obavezno za usluge označene u registru kao testne / razvojne (nakon 31.12.2012.)

Tehnički aspekti

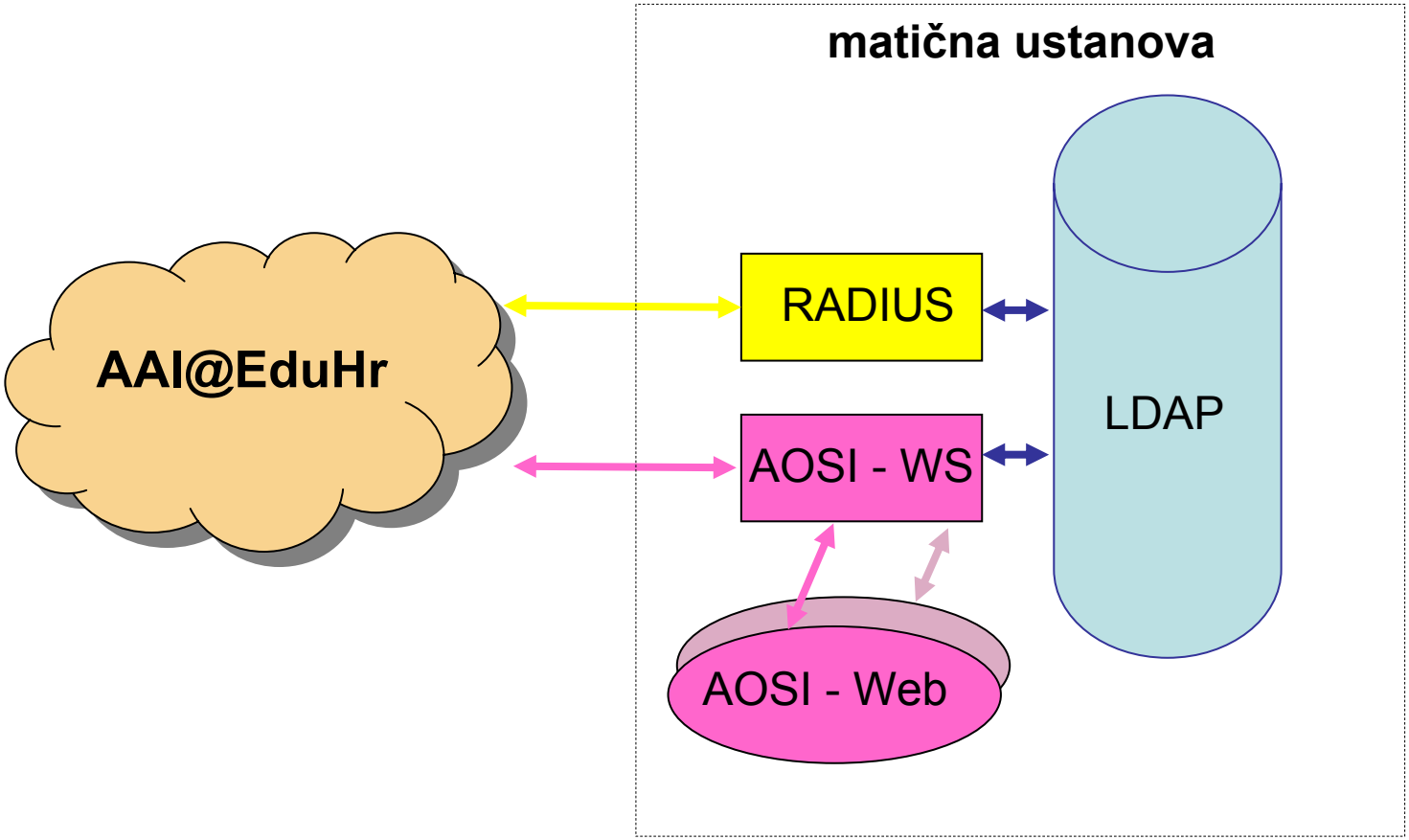
Hub-and-spoke federacija



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

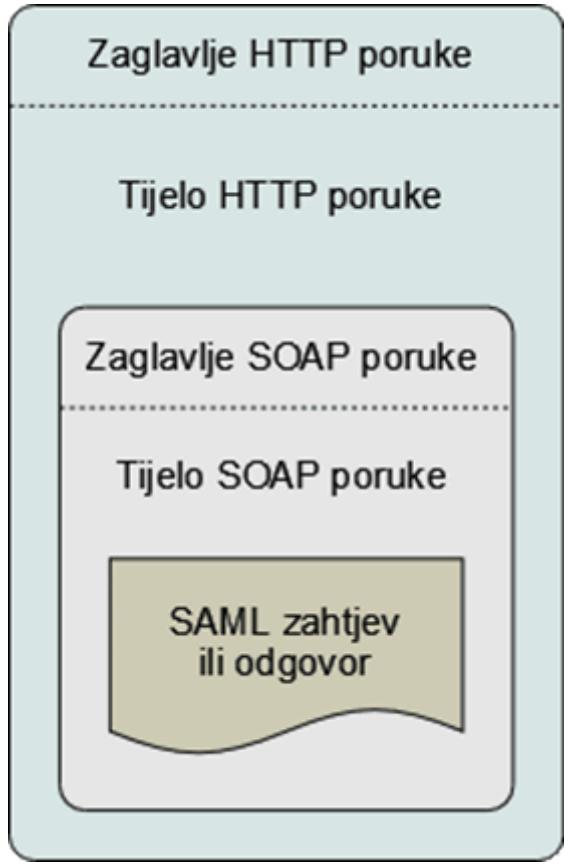


RADIUS

- **R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice
- protokol koji omogućuje upravljanje AAA procesom
  - klijent – poslužitelj model
  - definiran na aplikacijskom sloju
  - koristi UDP
  - RADIUS over TCP je trenutno u procesu standardizacije pri IETF-u
- široko korišten pri AA(A) za usluge pristupa mreži:
  - dial-up, wired, wireless, cable, (A)DSL, VPN, ...
- puno implementacija
  - serveri: FreeRADIUS, RADIATOR, Cisco, MS IAS, ...
- koristi se (kao transportni protokol) uz 802.1x i EAP

SAML

- ***S**ecurity **A**ssertion **M**arkup **L**anguage*
- kreiran od strane organizacije OASIS (*Organization for the Advancement of Structured Information Standards)*
- aktualna inačica SAML 2.0 (ranije 1.0, 1.1)
- cjeloviti okvir za razmjenu povjerljivih informacija
- temelji na potvrdama *(SAML assertions)*
- oslanja na XML, SOAP i HTTP(S)
- **SOAP** *(Simple Object Access Protocol)* je protokol za razmijenu strukturiranih informacija u *Web services* arhitekturi



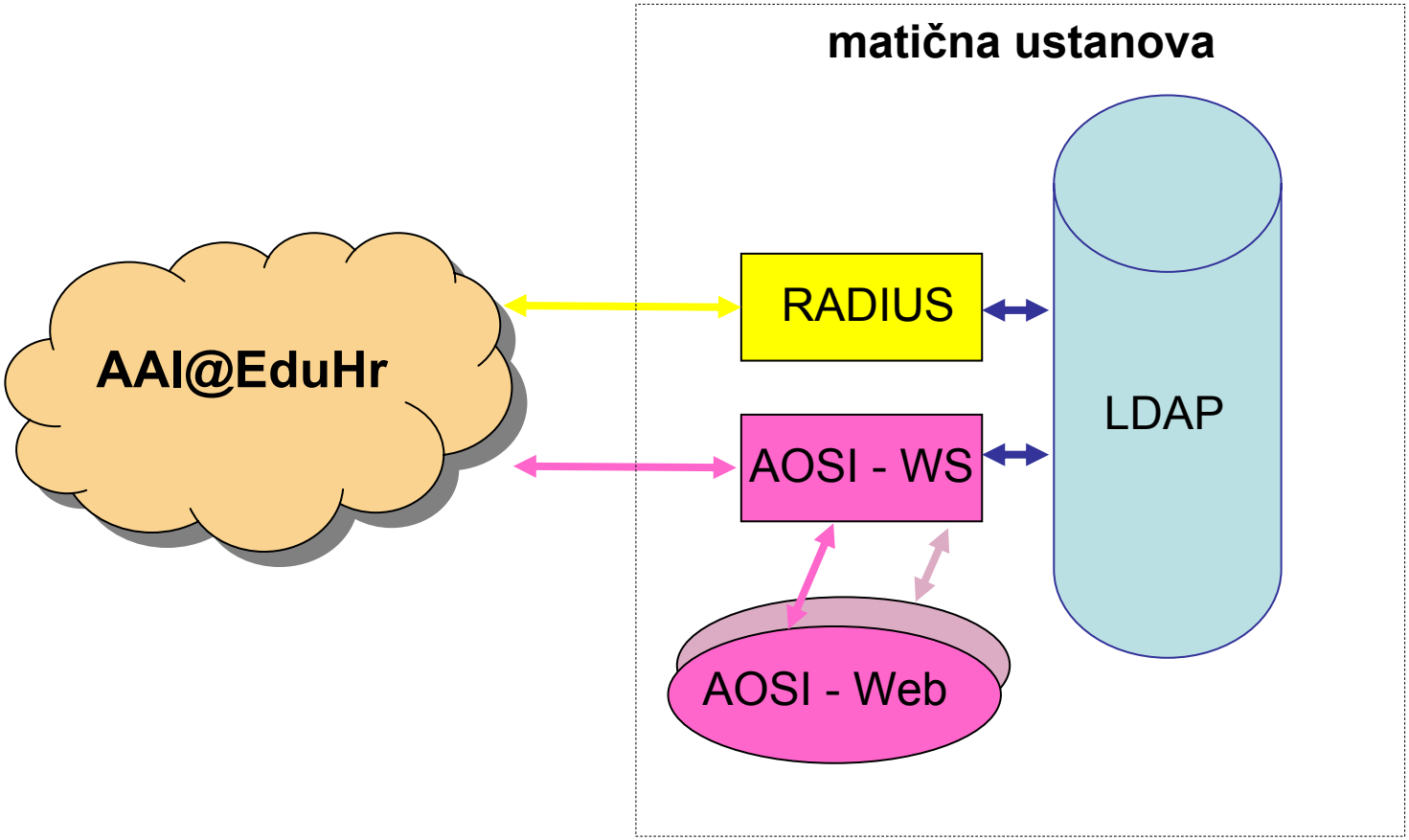
Povezivanje usluga s AAI@EduHr

Kako početi?

- odredite kakvu uslugu nudite/gradite:
  - internu (samo za svoju ustanovu)
  - interinstitucionalnu (za RH ili šire?)
- na raspolaganju su 2 protokola:
  - SAML (v.2.0) za usluge koje rabe HTTP(S)
  - RADIUS za ostale usluge

Modifikacije IdM sustava za interne potrebe

AAI@EduHr: IdM

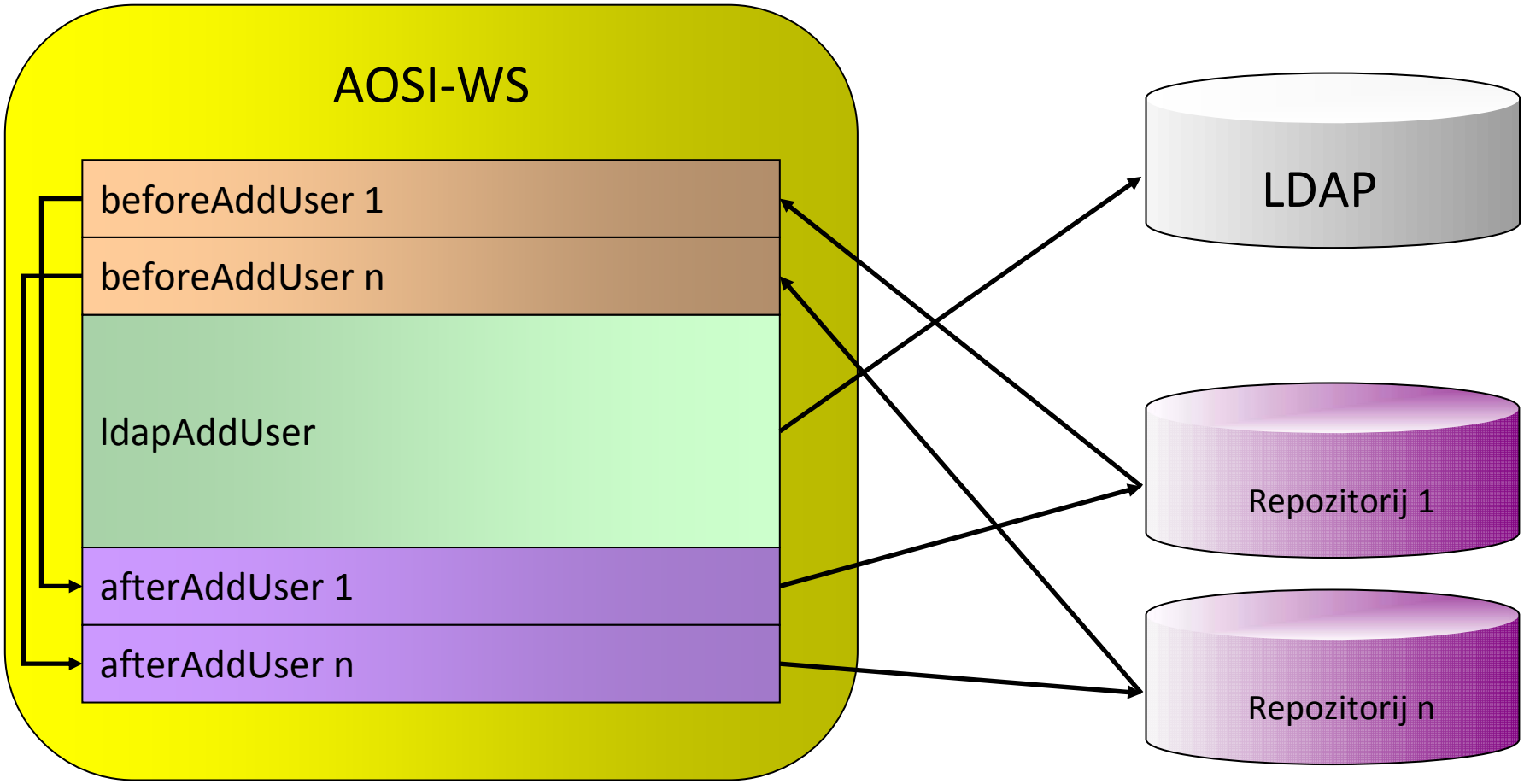


Dokumentacija: http://developer.aaiedu.hr/
AOSI - dokumentacija: http://developer.aaiedu.hr/aosi/index.html

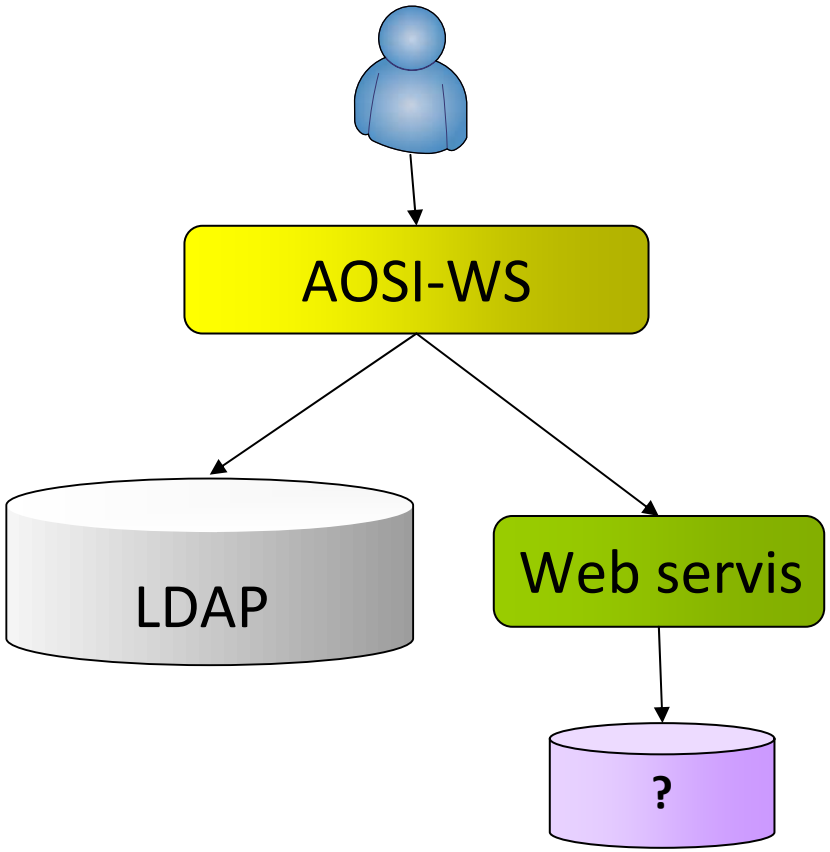
AOSI sustav plug-inova

- 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

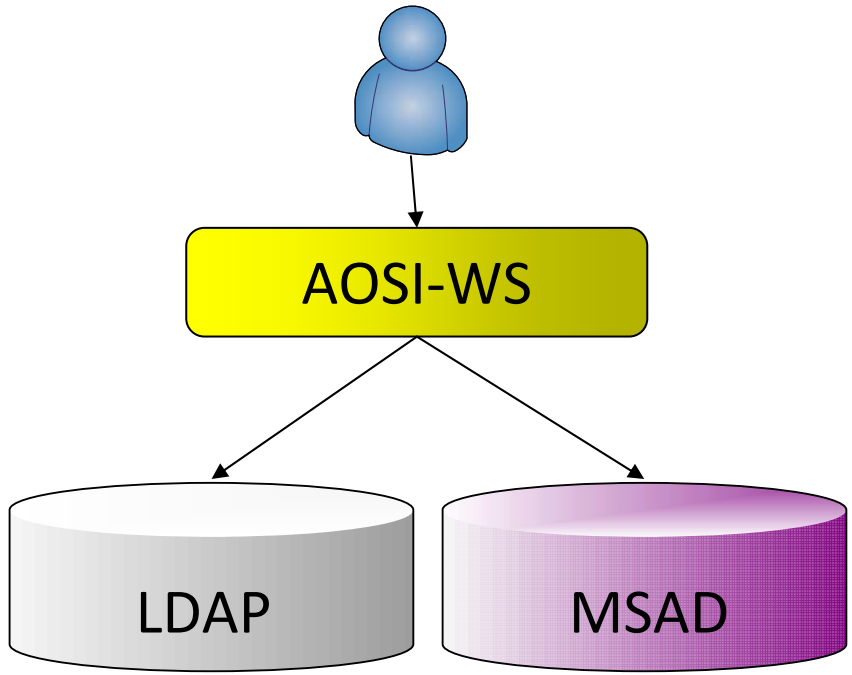
Primjer – dodavanje korisnika



AOSI plug-inovi: primjeri



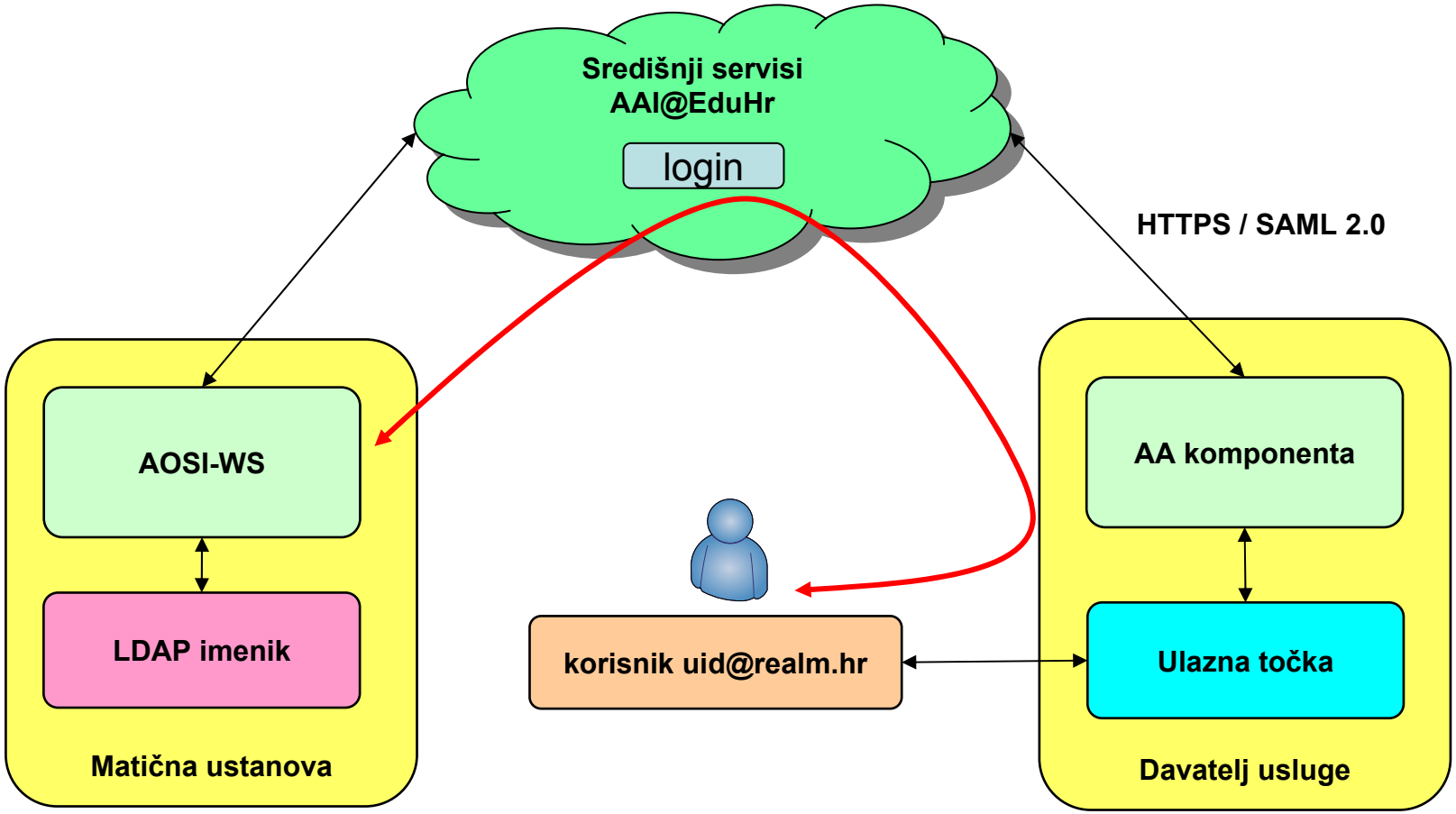
Web service plug-in



MS Active Directory plug-in

Povezivanje aplikacija s AAI@EduHr

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

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

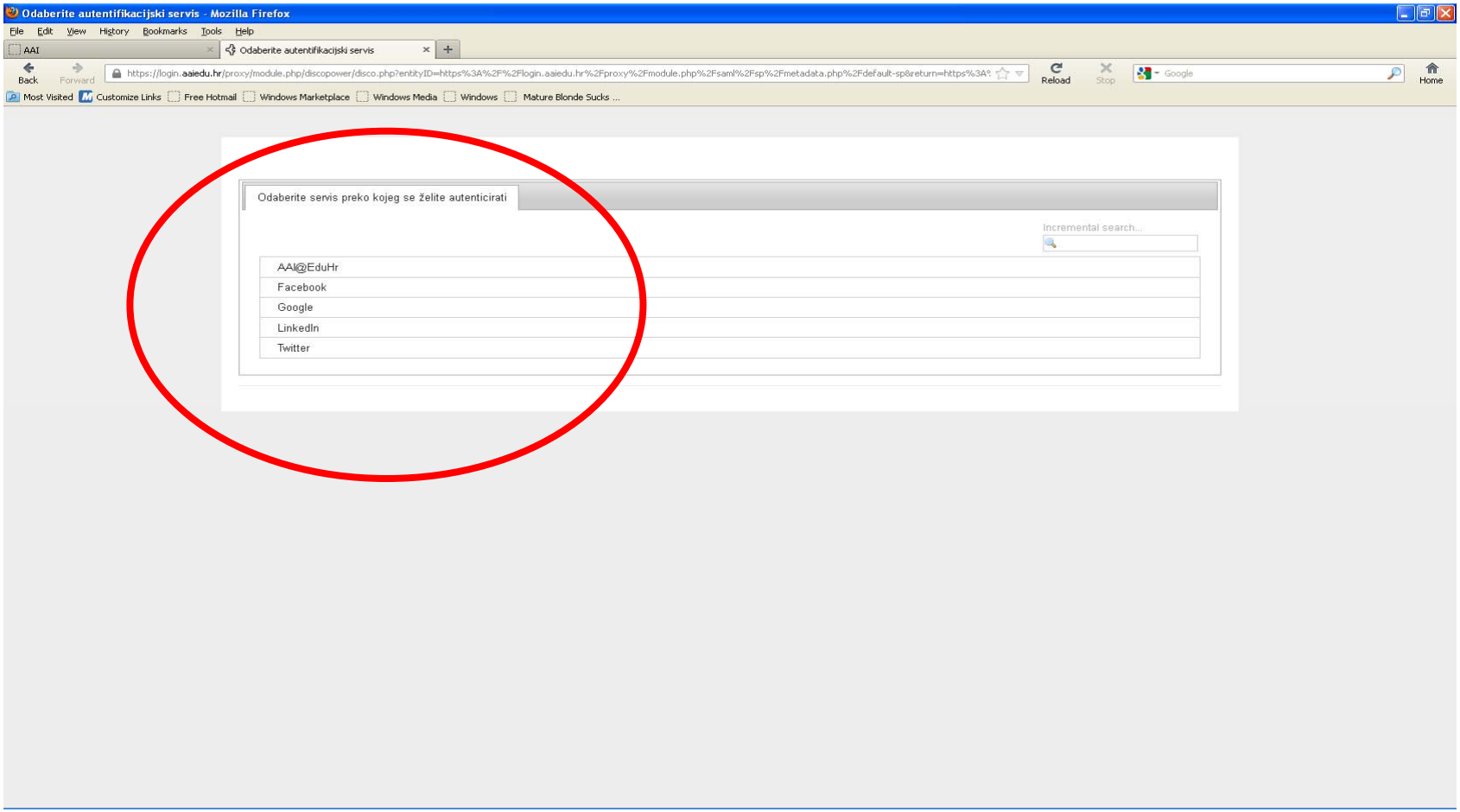
- sve platforme koje imaju podršku za SAML 2.0
- izdvajamo:
  - PHP
    - preporučamo uporabu alata simpleSAMLphp (SSP) (http://developer.aaiedu.hr/faq/8.html)
    - za SSP dostupan je i odgovarajući Debian paket (http://www.aaiedu.hr/faq_paketi_verzije.html)
  - MS .NET
    - preporučamo uporabu OIOSAML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

Alternativni načini autentikacije

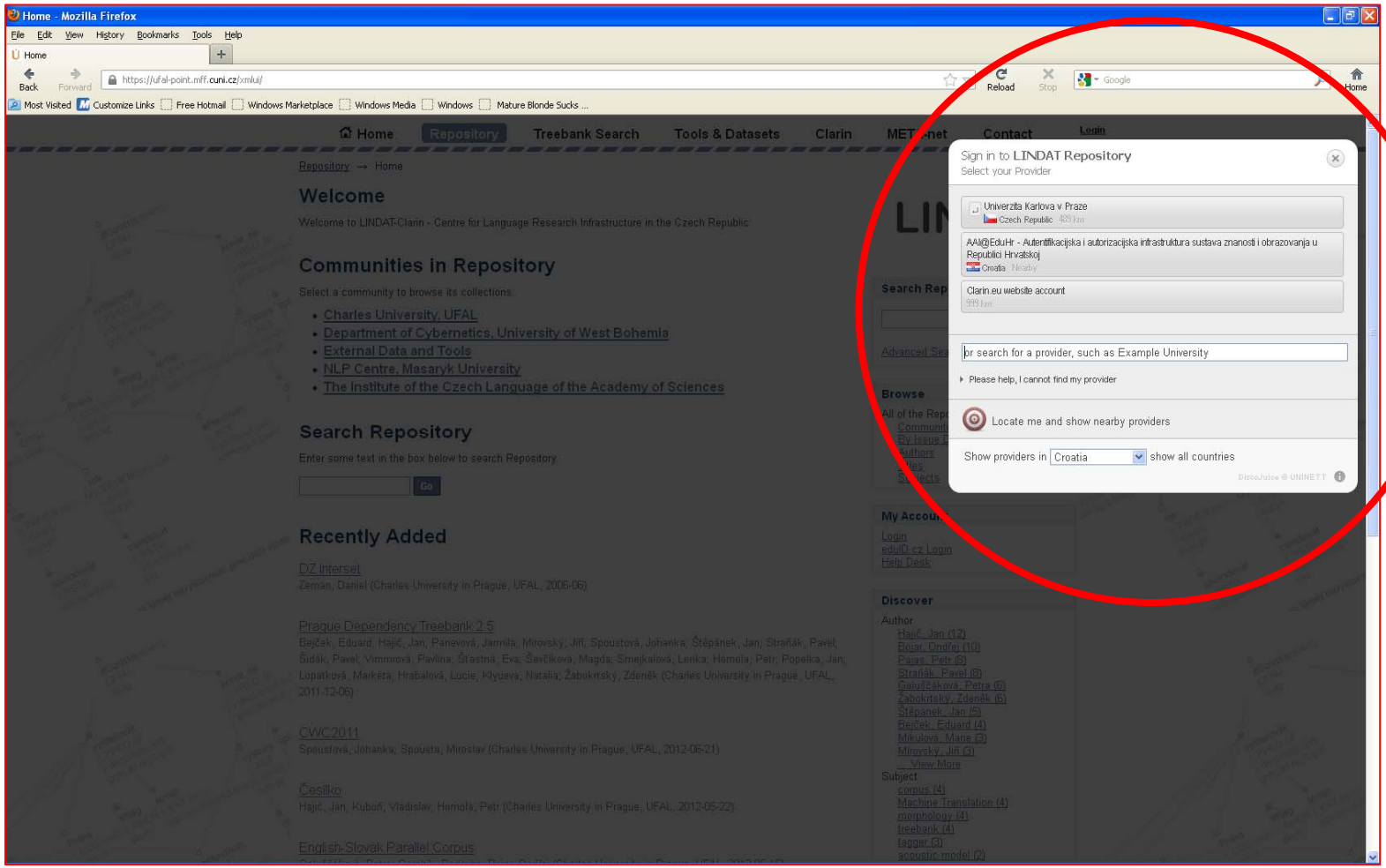
- društvene mreže / OpenID
  - Facebook, Google, Twitter, LinkedIn, ...

- eduGAIN – globalna mreža akademskih AAI sustava (nacionalnih federacija e-identiteta)
  - www.edugain.org
  - opt-in koncept:
    - usluge ulaze po vlastitoj želji
    - matične ustanove su uključene samim povezivanjem AAI@EduHr u eduGAIN

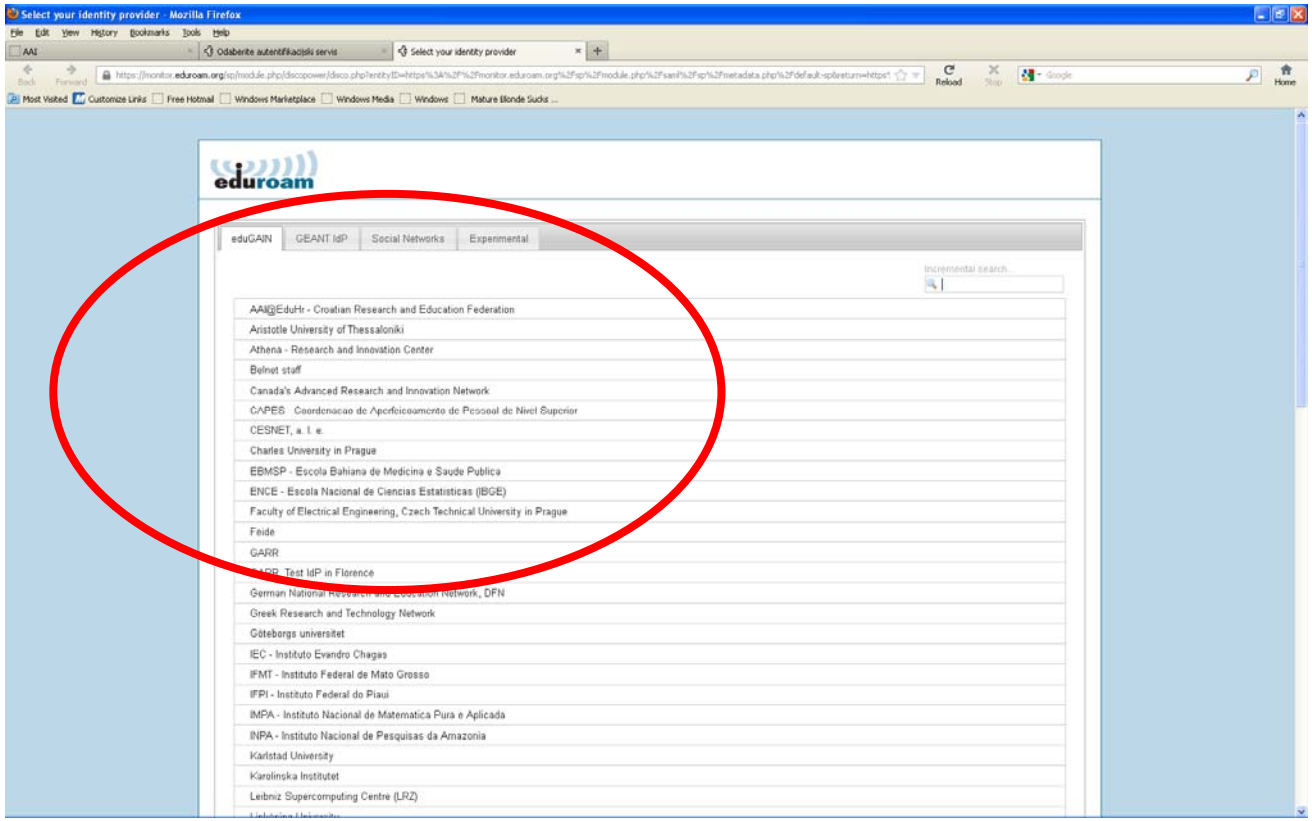
AAI@EduHr i društvene mreže



AAI@EduHr i eduGAIN (1)

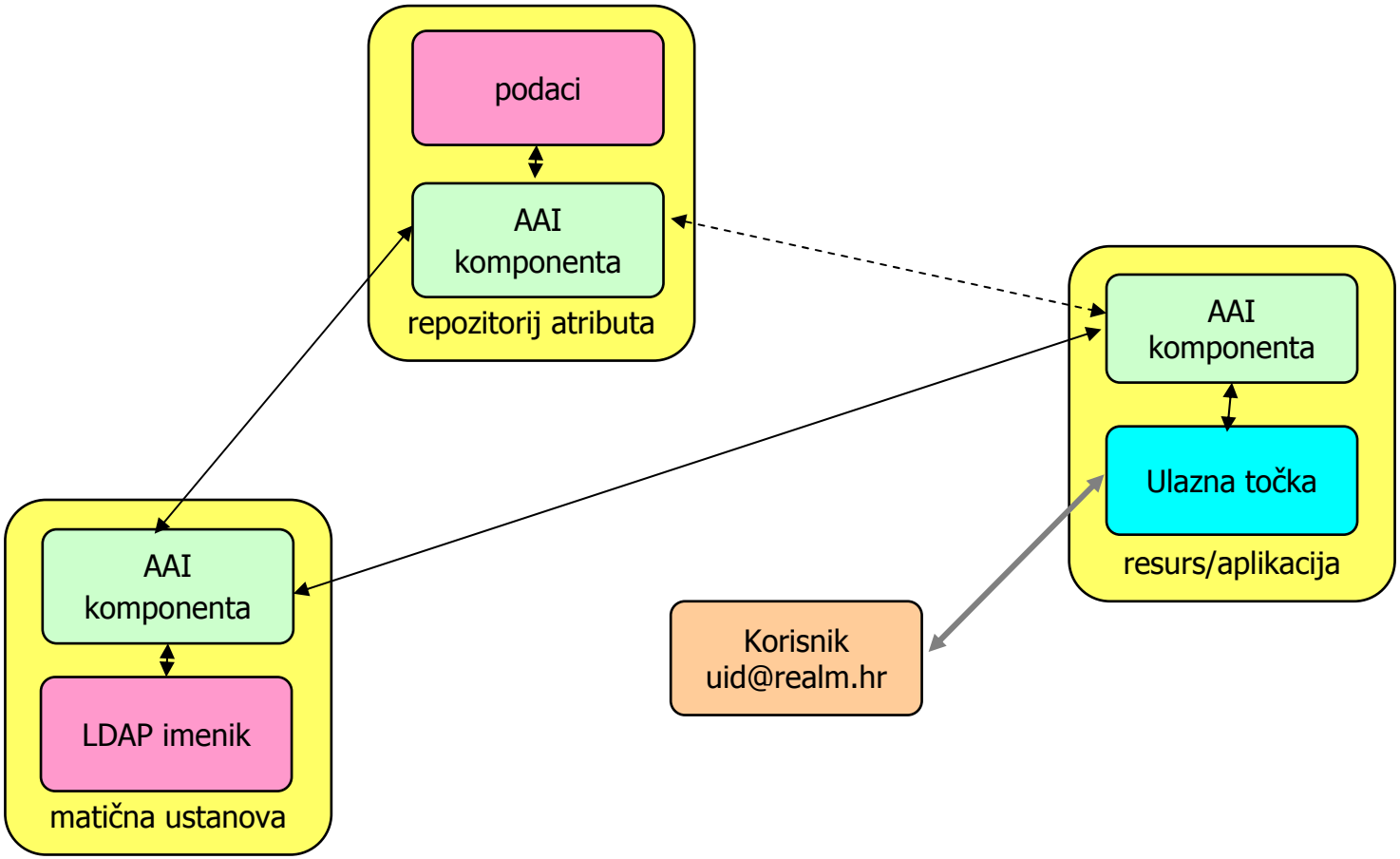


AAI@EduHr i eduGAIN (2)

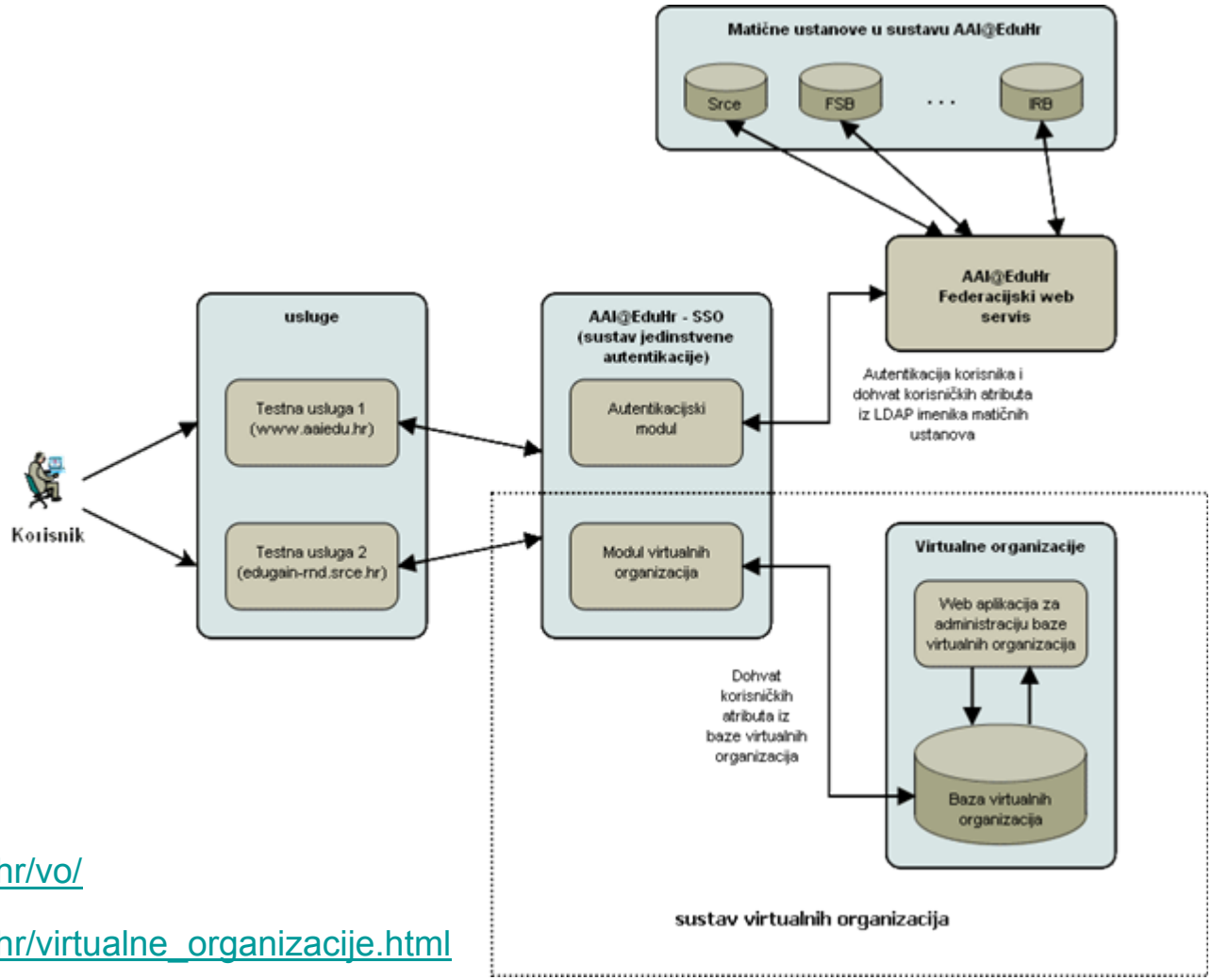


Virtualne organizacije (VO)

Koncept dodatnih repozitorija atributa



VO u sustavu AAI@EduHr



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

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

Kako početi?

- prijavite svoju aplikaciju u registar resursa (usluga) http://www.aaiedu.hr/aairr/
- javite nam ukoliko želite svoju aplikaciju učiniti dostupnom putem eduGAIN-a (www.edugain.org)
- javite nam ukoliko želite koristiti:
  - VO u sustavu AAI@EduHr
  - alternativne načine autentikacije (npr. društvene mreže)
- kontakt: team@aaiedu.hr

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

team@aaiedu.hr

Vaši prijedlozi i pitanja

- Što bi trebalo napraviti u 2013. godini (koje poslove/razvojne iskorake)?
- Koje elemente (točke u sustavu) treba unaprijediti u 2013. godini?
- O kojim temama biste željeli čuti više na slijedećoj radionici?

team@aaiedu.hr

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

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

team@aaiedu.hr

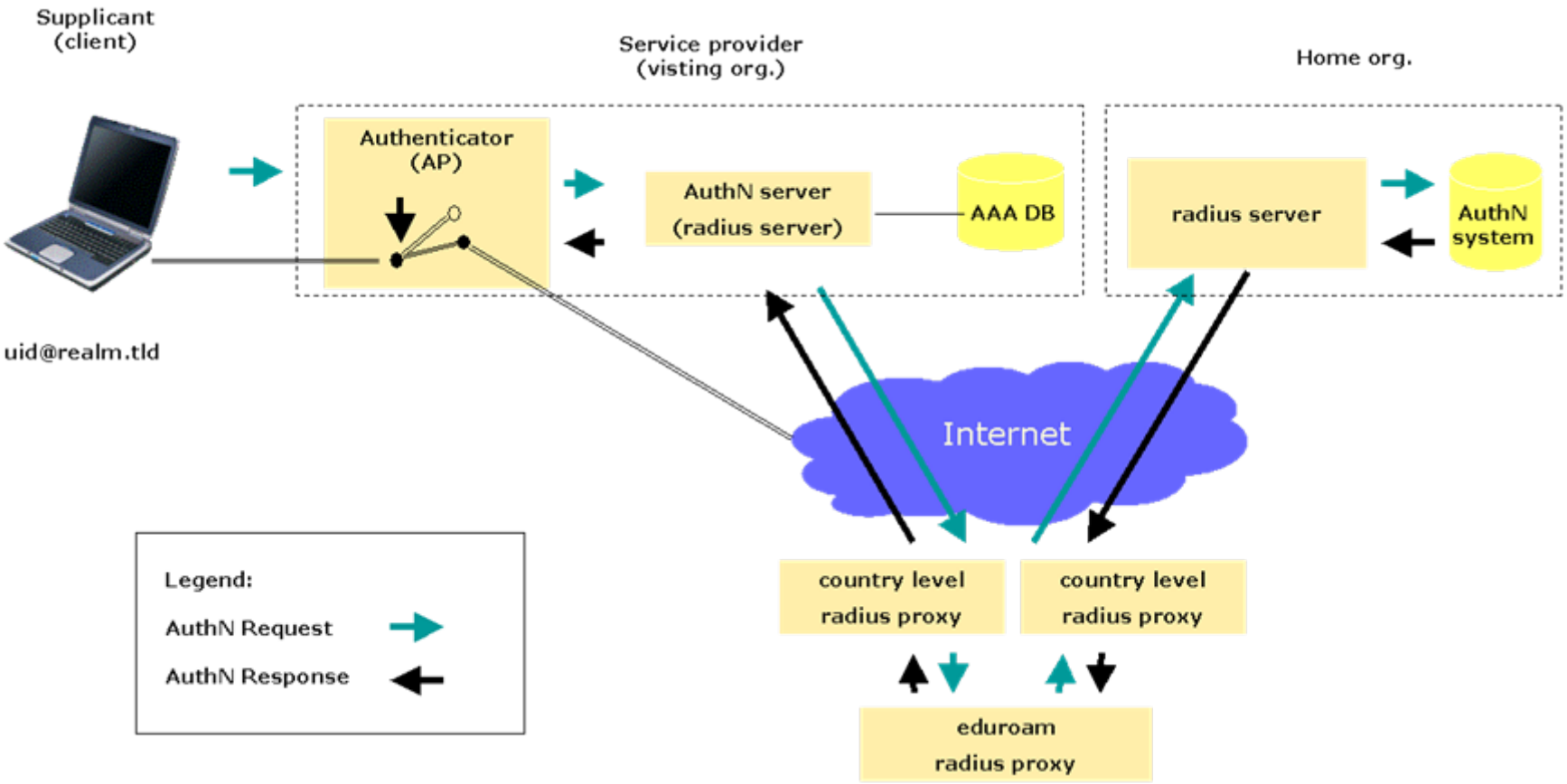
Rezervni slajdovi

Pristup mreži uz uporabu AAI@EduHr

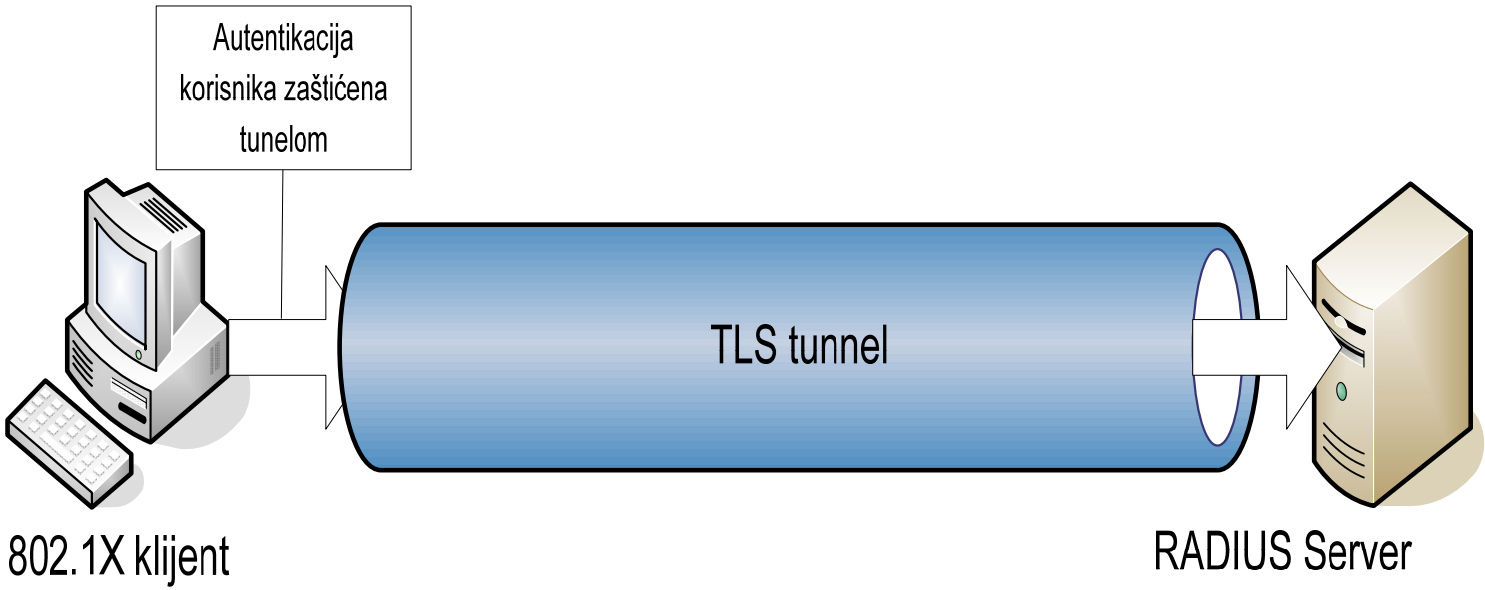
srce

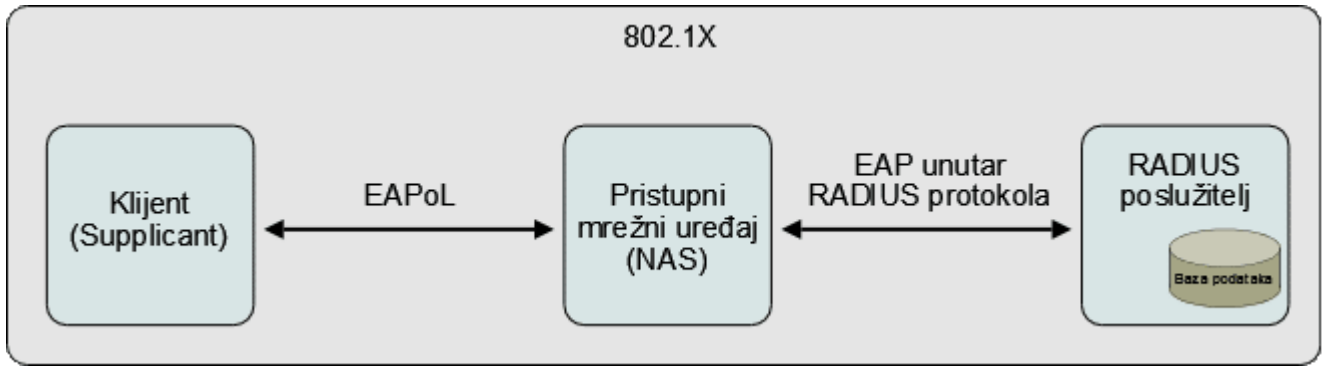
@EduHr

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