Autentikacijska i autorizacijska infrastruktura (AAI) akademske zajednice

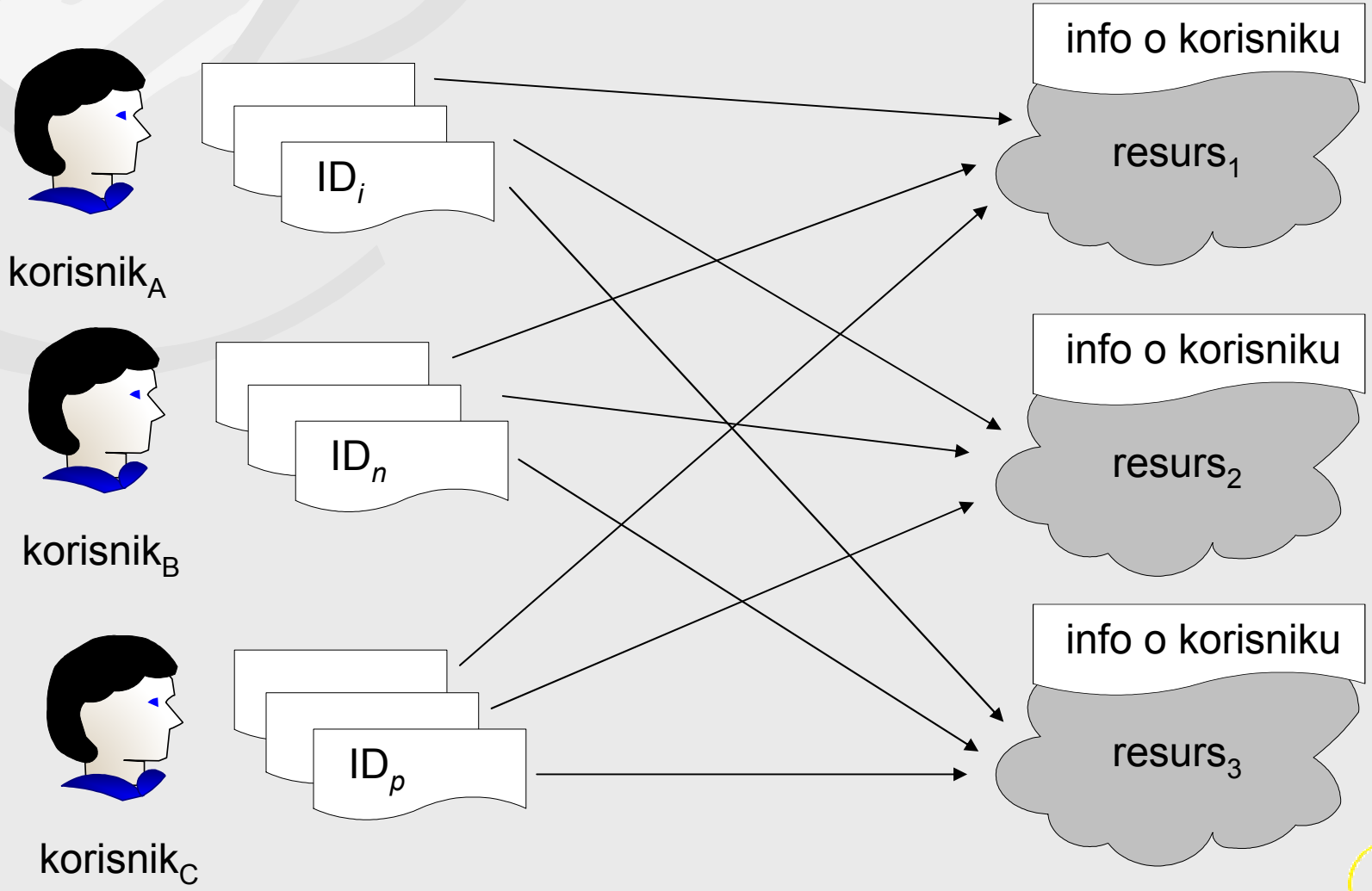
Miroslav Milinović
Sveučilište u Zagrebu
Sveučilišni računski centar - Srce
Miroslav.Milinovic@srce.hr

Dan Srca, 04.05.2005.

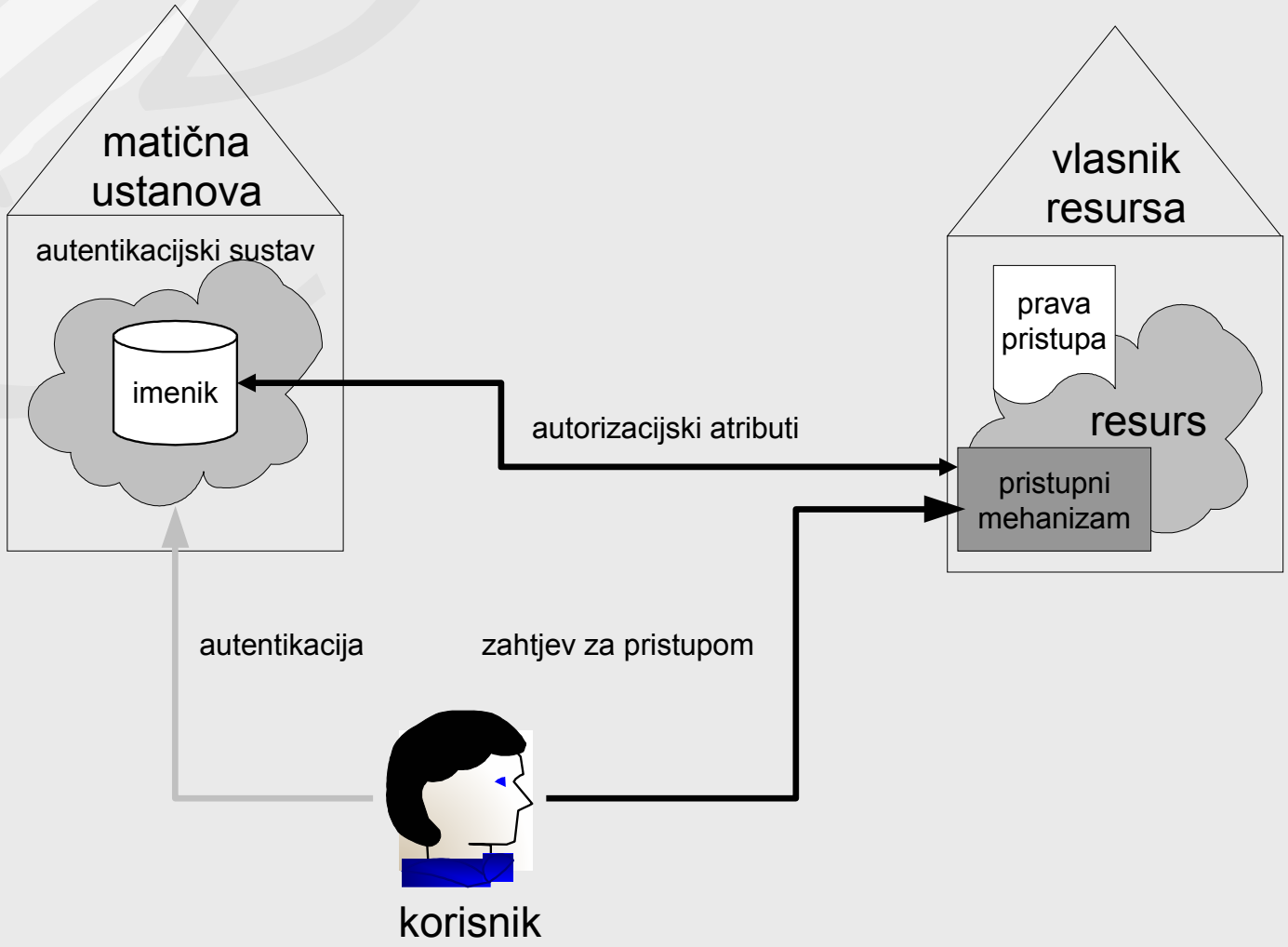
Sadržaj

- AAI: motivi & koncepti
- projekt AAI@EDU.HR
- upravljanje elektroničkim identitetima
  - hrEdu imeničke sheme
  - sustav AOSI
- AAI@EduHr u uporabi
- razvoj, planovi

AA problem


info o korisniku
resurs1
info o korisniku
resurs2
info o korisniku
resurs3
IDi
IDn
IDp
korisnikA
korisnikB
korisnikC

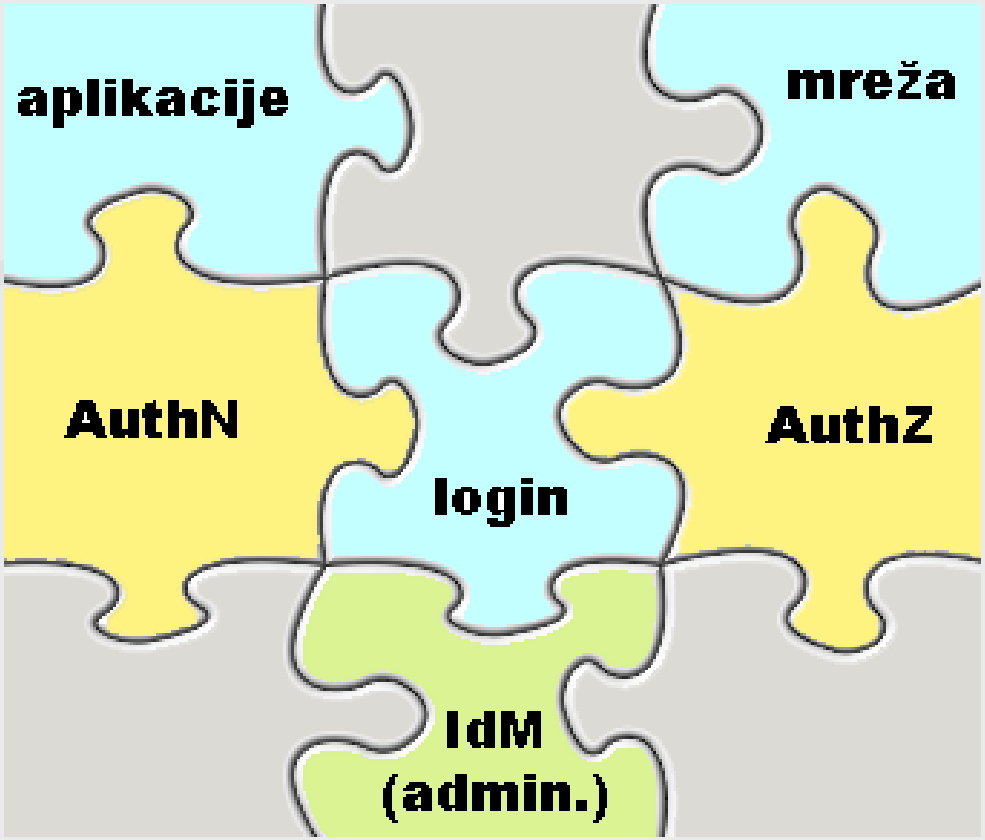
Model AAI


matična ustanova
autentikacijski sustav
imenik
vlasnik resursa
prava pristupa
resurs
pristupni mehanizam
autorizacijski atributi
autentikacija
zahtjev za pristupom
korisnik

Zašto AAI?

- mobilnost korisnika
  - u obrazovanju (Bolonjska deklaracija)
  - ...
- pristup mreži
  - neovisno o lokaciji, načinu/tehnologiji pristupa ...
- personalizacija usluga
- minimiziran broj elektroničkih identiteta po korisniku

Od čega se sastoji AAI?



Autentikacija (AuthN)

- proces kojim se provjerava elektronički identitet korisnika
- metoda autentikacije se temelji na:
  - onom što korisnik zna
    - korisnička oznaka/zaporka, ...
  - onom što korisnik ima
    - certifikat, ...
  - onom što korisnik jest
    - biometrija (npr. otisak prsta)
- metodu biramo prema (sigurnosnim) potrebama resursa

Autorizacija (AuthZ)

- proces kojim se korisniku dodjeljuje odnosno oduzima pravo pristupa resursu
- 3 temeljna scenarija:
  - AuthZ = AuthN
  - AuthZ = AuthN + dodatni atributi (iz imenika)
    - *strong privacy*: “pregovaranje” o atributima koji se razmjenjuju
  - AuthZ = AuthN + dodatni atributi (iz imenika) + informacije koje pamti resurs lokalno
    - *quota*, *black list*, ...

Projekt AAI@EDU.HR

- Projekt uspostave autentikacijske i autorizacijske infrastrukture (AAI) u sustavu znanosti i visokog obrazovanja
- zajednički projekt Srca i CARNeta koji financira MZOŠ
- trajanje – 2 godine:
  - FAZA I (svibanj 2004. – svibanj 2005.): definiranje i uspostava temeljne AAI
  - FAZA II (2. godina projekta): sveobuhvatna primjena AAI uz stvaranje preduvjeta za uvođenje certifikata (PKI)

http://www.aaiedu.hr/

Očekivani rezultati (obje faze)

- **AAI.1**: uspostavljeno Vijeće korisnika AAI;
- **AAI.2**: snimka stanja aktivnosti u području AA u RH;
- **AAI.3**: tehnički i organizacijski standardi AAI sustava znanosti i visokog obrazovanja;
- **AAI.4**: pravila i procedure informacijskog i tehničkog održavanja AAI;
- **AAI.5**: nadogradiva hrEduPerson imenička shema i postupci za održavanje;
- **AAI.6**: pravila i procedure informacijskog i tehničkog održavanja LDAP imenika;
- **AAI.7**: nadogradiva i funkcionalna AAI utemeljena na sustavu LDAP imenika;
- **AAI.8**: ostvarena uporaba AAI za pristup resursima;
- **AAI.9**: centar obuke i potpore za korisnike AAI;
- AAI.10: realizirana primjena certifikata / PKI;
- AAI.11: provedeno ispitivanje i implementacija SSO usluge;
- **AAI.12**: ostvarena aktivna veza (usklađenost) s ostalim AAI sustavima

Upravljanje e-identitetima (IdM)

- kako upravljati podacima o osobama (korisnicima) u sustavu AAI@EduHr?
- (LDAP) imenik i imenička shema
  - **hrEduPerson**
  - **hrEduOrg**
  - **Registar shema: http://schema.aaiedu.hr/**
- upravljanje sadržajem imenika
  - **aplikacija za održavanje sadržaja imenika (AOSI)**
    - poslužiteljska komponenta
    - klijentska komponenta
- pravila, upute i tehnička dokumentacija
- pomoć u implementaciji i primjeni (team@aaiedu.hr)

hrEduPerson (ver.1.1.)

naziv atributa	LDAP naziv	Status atributa		frekvencija
		obvezan	opcionalan	
korisnička oznaka	hrEduPersonUniqueID	x		1
brojčani identifikator osobe	hrEduPersonUniqueNumber	x		n
identifikator korisnika u ustanovi	uid	x		1
zaporka	userPassword	x		1
ime i prezime	cn	x		n
prezime	sn	x		n
ime	givenName	x		n
naziv matične ustanove	o	x		n
oznaka matične ustanove	hrEduPersonHomeOrg	x		1
poštanska adresa	postalAddress	x		1
mjesto	l	x		1
elektronička adresa	mail	x		n
povezanost s ustanovom	hrEduPersonAffiliation	x		n
temeljna povezanost s ustanovom	hrEduPersonPrimaryAffiliation	x		1
datum isteka temeljne povezanosti	hrEduPersonExpireDate	x		1

hrEduPerson (ver.1.1.)

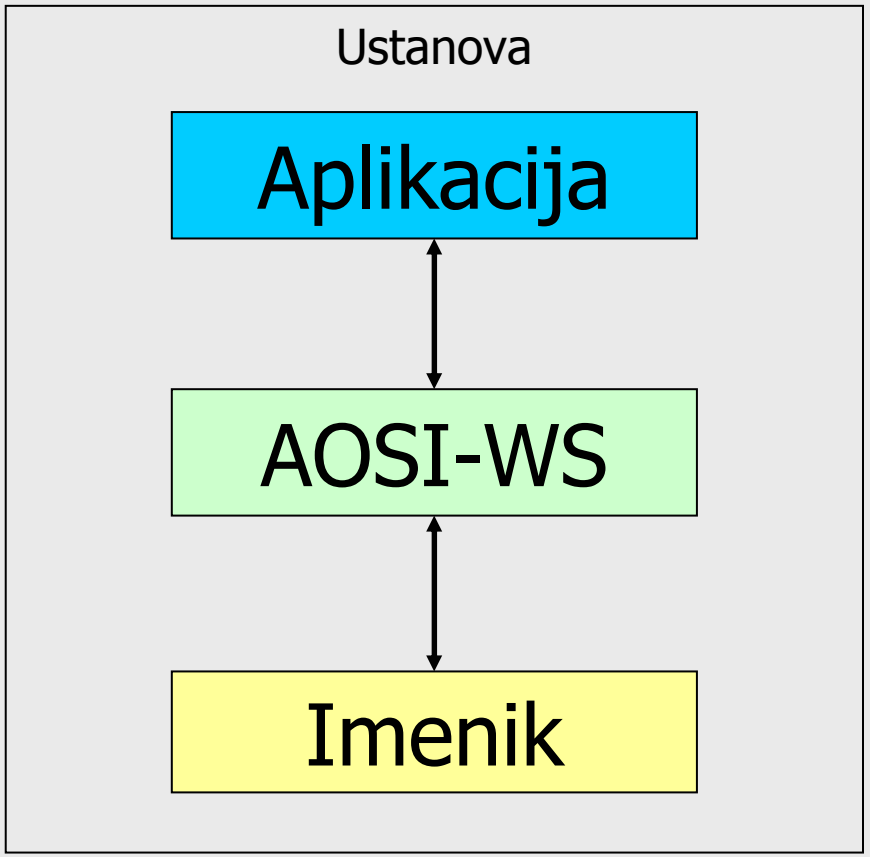
naziv atributa	LDAP naziv	Status atributa		frekvencija
		obvezan	opcionalan	
organizacijska jedinica	ou		x	n
poštanski broj	postalCode		x	1
ulica i kućni broj	street		x	1
broj sobe	roomNumber		x	n
telefonski broj	telephoneNumber		x	n
lokalni telefonski broj	hrEduPersonExtensionNumber		x	n
fax broj	facsimileTelephoneNumber		x	n
broj mobilnog telefona	mobile		x	n
kućna poštanska adresa	homePostalAddress		x	n
kućni telefonski broj	homeTelephoneNumber		x	n
URI adresa	labeled URI		x	n
slika	jpegPhoto		x	n
spol	hrEduPersonGender		x	1
datum rođenja	hrEduPersonDateOfBirth		x	1
stručni status	hrEduPersonProfessionalStatus		x	1
zvanje	hrEduPersonAcademicStatus		x	1
područje znanosti	hrEduPersonScienceArea		x	1
položaj u ustanovi	hrEduPersonTitle		x	1
vrsta posla u ustanovi	hrEduPersonStaffCategory		x	n
uloga u ustanovi	hrEduPersonRole		x	n
pripadnost grupi	hrEduPersonGroupMember		x	n
certifikat	userCertificate		x	n
desktop uređaj	hrEduPersonCommURI		x	n
oznaka privatnosti	hrEduPersonPrivacy		x	n

hrEduOrg (ver.1.1.)

Naziv atributa	LDAP naziv	Status atributa		frekvencija
		obvezan	opcionalan	
naziv ustanove	o	x		n
identifikator ustanove	dc	x		n
brojčani identifikator ustanove	hrEduOrgUniqueNumber	x		n
poštanska adresa	postalAddress	x		n
mjesto	l	x		n
poštanski broj	postalCode		x	n
ulica i kućni broj	street		x	n
telefonski broj	telephoneNumber		x	n
fax broj	facsimileTelephoneNumber		x	n
broj mobilnog telefona	hrEduOrgMobile		x	n
elektronička adresa	hrEduOrgMail	x		n
tip ustanove	hrEduOrgType	x		1
pripadnost ustanovi	hrEduOrgMember		x	n
URL adresa ustanove	hrEduOrgURL	x		n
URI adresa politike	hrEduOrgURI		x	n

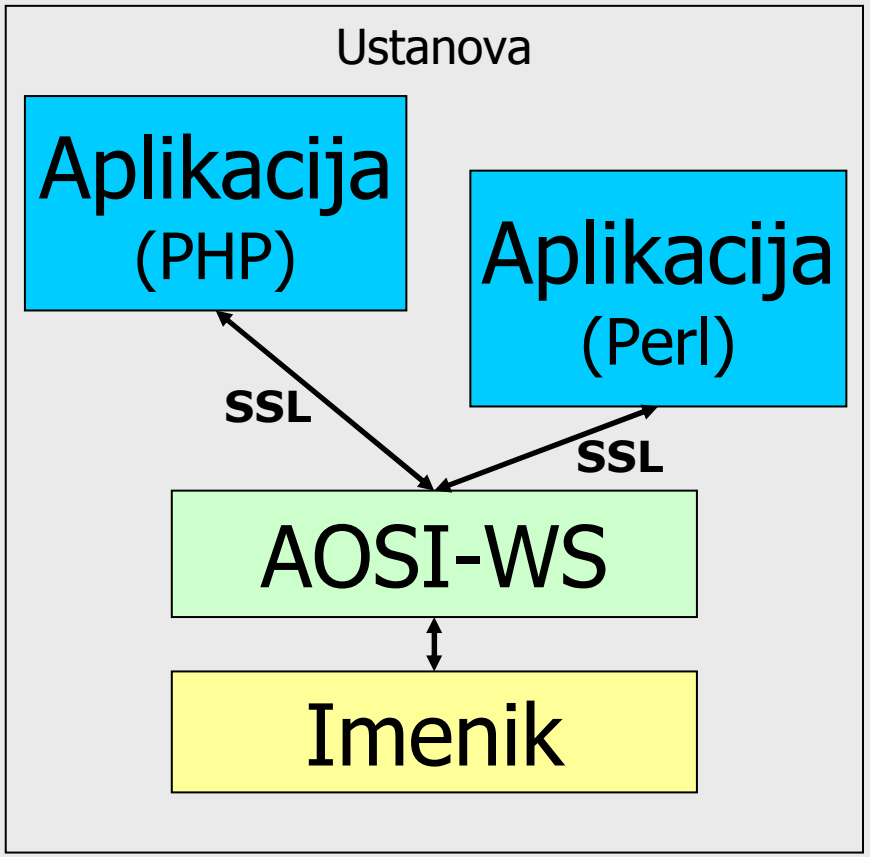
AOSI: novi način uporabe imenika

- Imeniku se pristupa posredno preko web servisa (SOAP)
- Svako povezivanje je autenticirano (tj. potrebni su korisnička oznaka i zaporka)
- Administratori imenika se autenticiraju svojim korisničkim oznakama i zaporkama (tj. ne "dijeli se" administratorska zaporka)

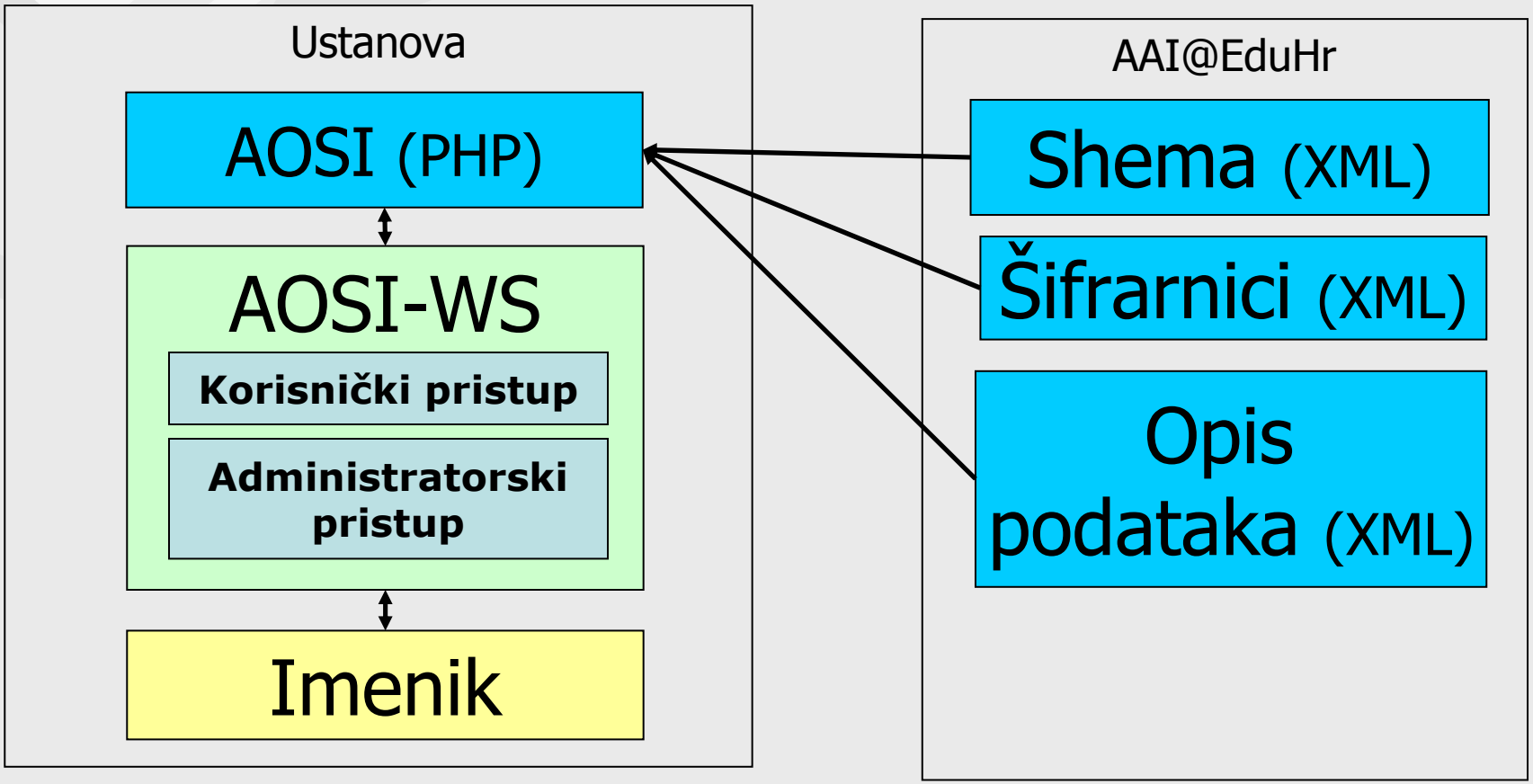


AOSI: novi način uporabe imenika

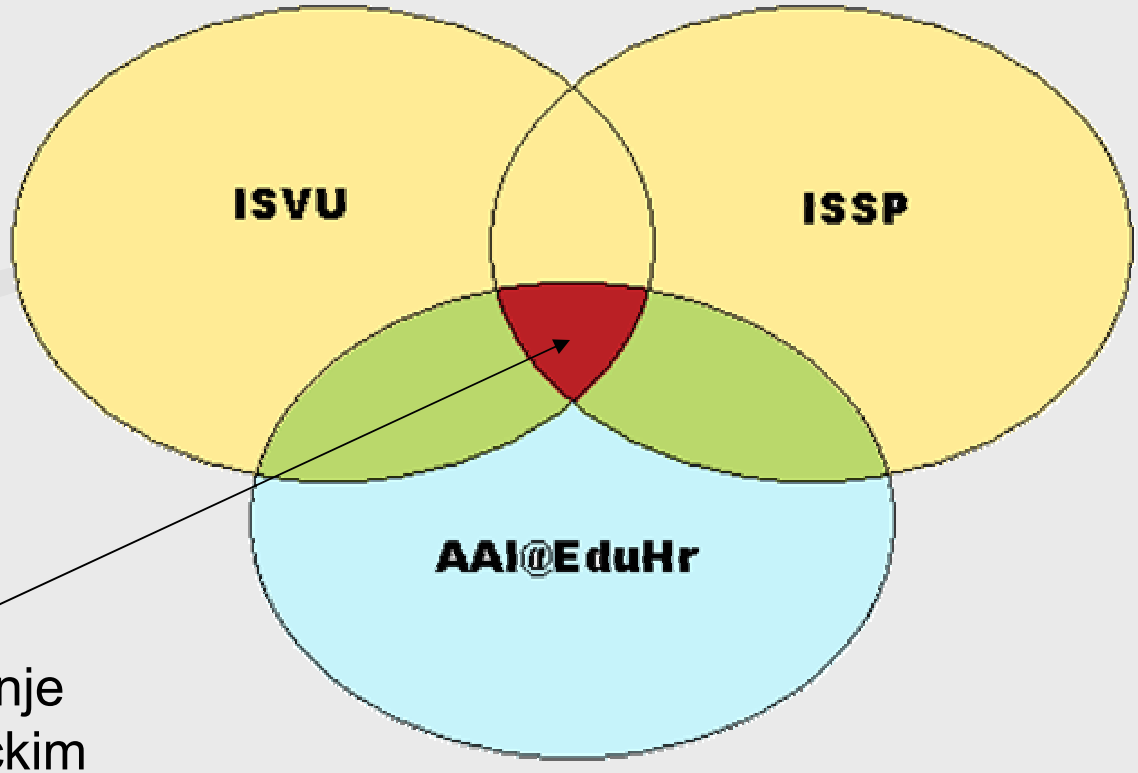
- Administrator imenika više ne mora biti administrator LDAP servisa
- Komunikacija od aplikacije do web servisa je zaštićena (SSL)



AOSI sustav

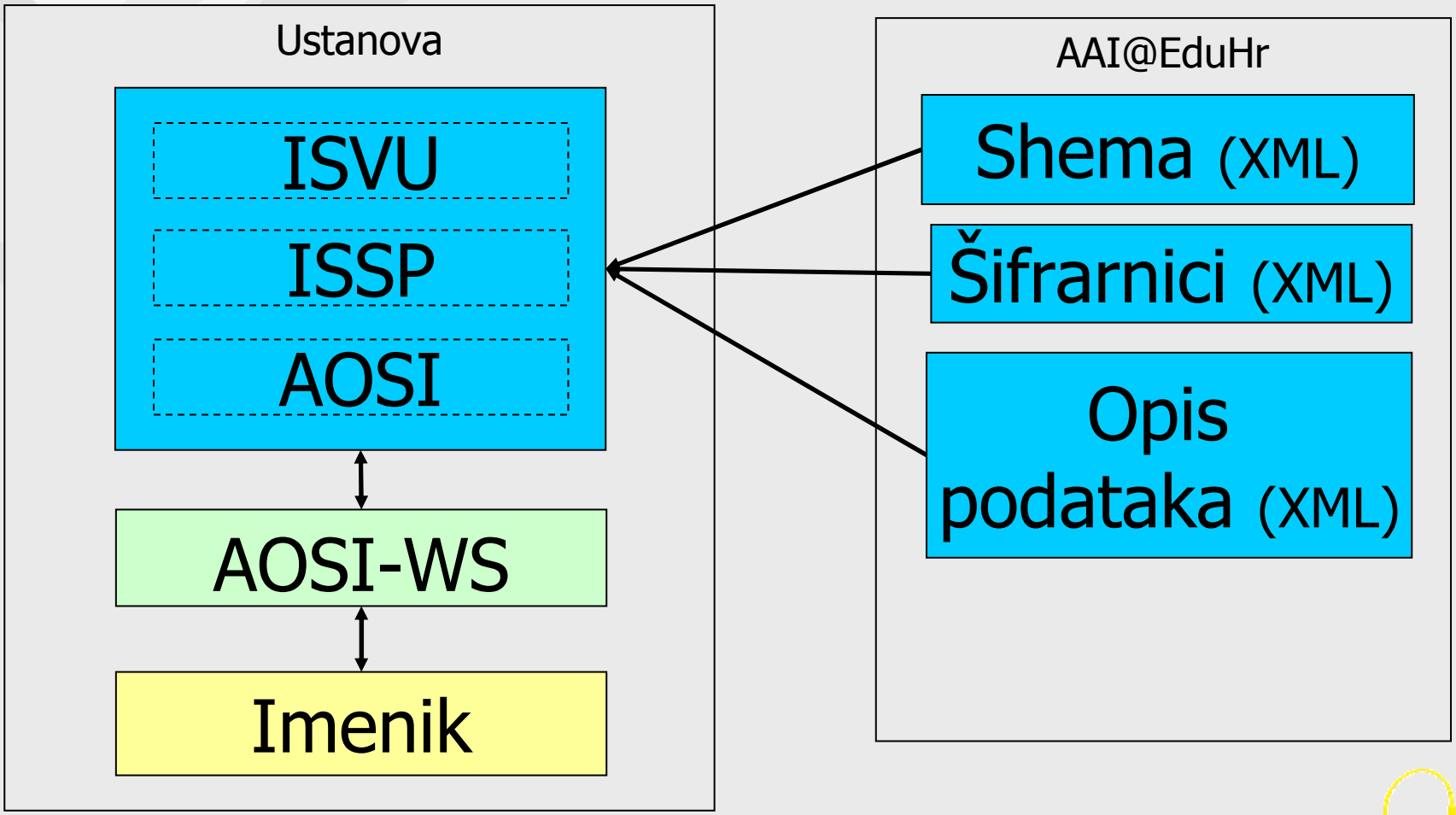

Ustanova
AOSI (PHP)
AOSI-WS
Korisnički pristup
Administratorski pristup
Imenik
AAI@EduHr
Shema (XML)
Šifrarnici (XML)
Opis podataka (XML)

AAI@EduHr vs. ISSP vs. ISVU

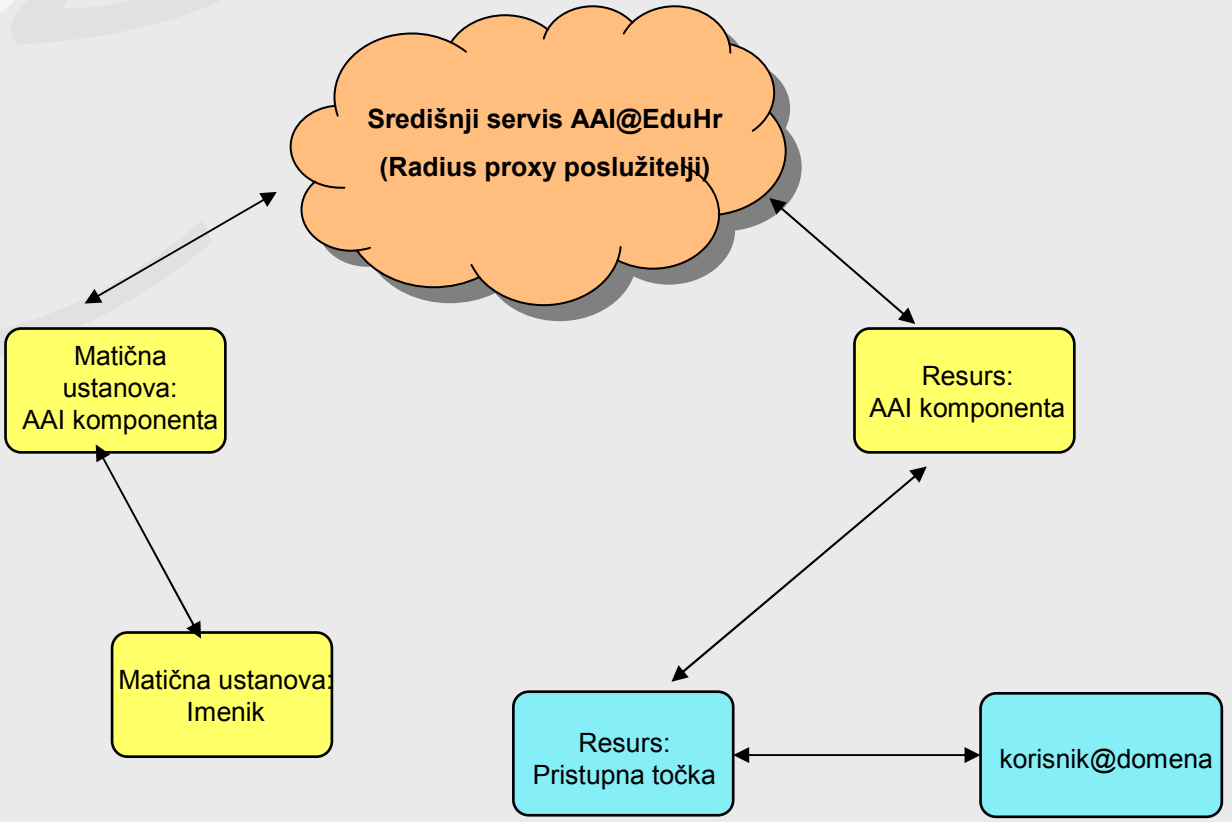


Upravljanje elektroničkim identitetima

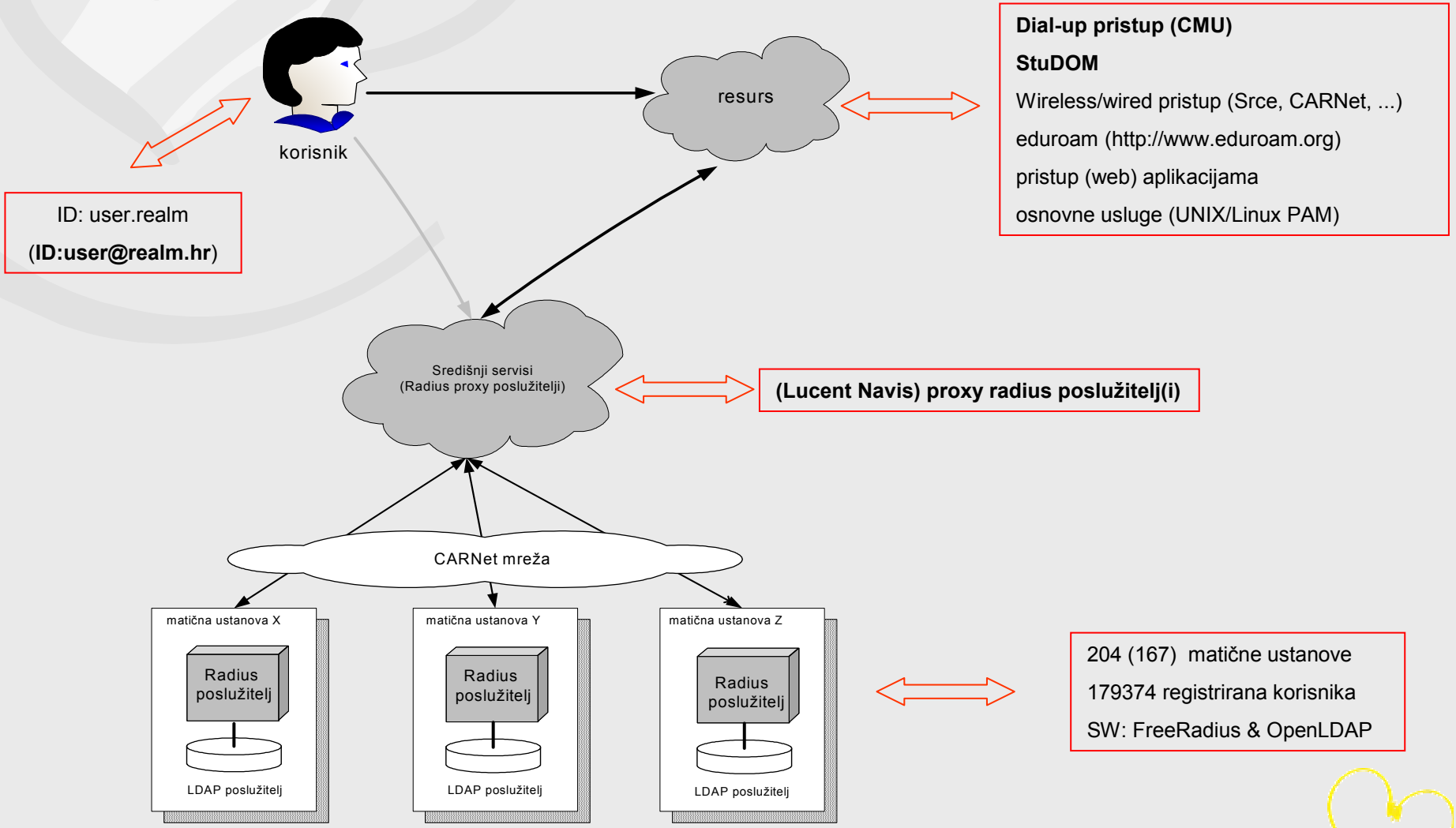
AOSI vs. ISSP vs. ISVU



AAI@EduHr danas



Aktualno stanje



Tko i kako već rabi AAI@EduHr?

- pristup mreži:
  - CMU, StuDOM
  - wireless & wired pristup mreži za potrebe ustanova:
    - pristup za djelatnike, goste; javni pristup; učionice; konferencije
    - Srce, CARNet, ETF Osijek, FESB Split, ...
- pristup aplikacijama:
  - pristup Web stranicama (web usluge Srca i CARNeta, ...)
  - aplikacije za udaljeno učenje: Moodle (FF Zagreb), Web CT (CARNet)
  - uPortal (Srce), ...
- pristup osnovnim servisima (login)
  - javni poslužitelj CARNeta u Srcu
  - SAS (Srce), ...
- povezivanje s međunarodnim projektima/infrastrukturama
  - eduroam (http://www.eduroam.org)
  - sučelje za Shibboleth (Internet2)
  - učešće u Geant 2 (JRA5) projektu

Razvoj, planovi ...

- implementacija hrEdu shema i sustava AOSI na svim ustanovama u sustavu (najkasnije do 1.10.2005.)
- pružanje potpore ustanovama, vlasnicima resursa i korisnicima u sustavu AAI@EduHr
- sveobuhvatna primjena AAI@EduHr (posebno u sustavima ISSP, ISVU, CRO-GRID)
- nove pilot primjene, generička rješenja za primjenu AAI@EduHr
- nastavak razvoja AAI@EduHr
- uvođenje certifikata za servise (do kraja 2005.)
- ispitivanje mogućnosti i uspostava SSO usluge u sustavu
- PKI: ispitivanje mogućnosti/opravdanosti uvođenja i planiranje implemenatacije
- suradnja s međunarodnom zajednicom (GEANT2/JRA5)
- pripremiti AAI@EduHr za rad nakon završetka projekta

AAI@EduHr
http://www.aaiedu.hr/

Miroslav Milinović
Sveučilište u Zagrebu
Sveučilišni računski centar - Srce
Miroslav.Milinovic@srce.hr

Dan Srca, 04.05.2005.