AAI@EduHr

Miroslav Milinović, Dubravko Penezić, Denis Stančer
Mijo Đerek, Dubravko Vončina
Srce

2. AAI@EduHr seminar

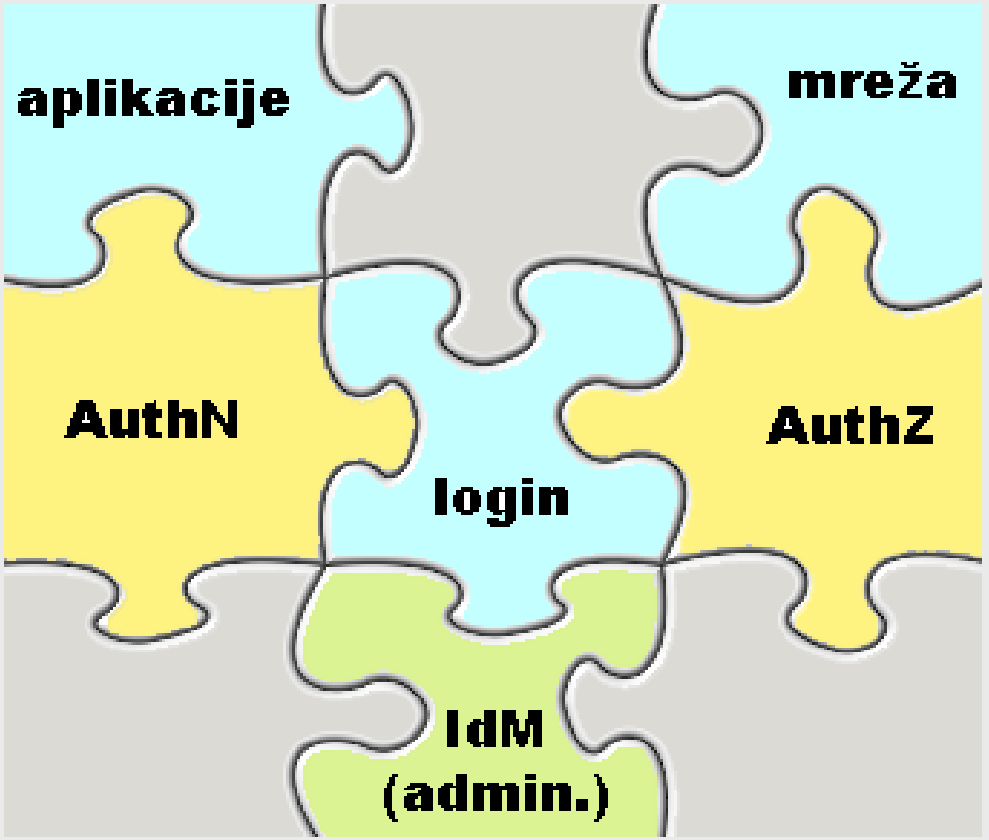
listopad 2005.

Rijeka, Osijek, Zagreb, Split

Sadržaj

- Pregled aktivnosti (IdM & uspostava AAI@EduHr)
- Aplikacija za održavanje sadržaja imenika (AOSI)
- AAI@EduHr: pristup mreži i računalnim resursima

Od čega se sastoji AAI?



Upravljanje e-identitetima (IdM)

- kako upravljati podacima o osobama (korisnicima) u sustavu AAI@EduHr?
- (LDAP) imenik i imenička shema
  - **hrEduPerson (ver.1.2)**
  - **hrEduOrg (ver.1.2)**
  - **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

hrEduPerson (ver.1.2.)

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.1.2.)

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 studenta	**hrEduPersonStudentCategory**		**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.1.2.)

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		1
URI adresa politike	hrEduOrgPolicyURI		x	n

Dokumentacija uz hrEdu sheme

- Dostupna na adresi:
  http://www.aaiedu.hr/dokumenti.html

- Pravila informacijskog održavanja imenika u sustavu AAI@EduHr
  - jasnija prava i obveze ustanova i korisnika
  - odvajanje brige o informacijskoj ispravnosti od brige o tehničkoj ispravnosti
  - ustanova preuzima odgovornost za točnost podataka

- Upute za migraciju LDAP imenika ustanova na hrEdu imeničku shemu

Što treba napraviti do 1. 12. 2005. ?

- Instalirati odgovarajuću programsku podršku:
  - OpenLDAP + FreeRadius + AOSI (poslužitelj + klijent)
  - koristi se postojeći koncept programskih paketa u CARNetu (podržana platforma je Debian Linux v.3.1 (Sarge))
  - novi paketi: **aai-preinstall**, **openldap-aai**
  - dokumentacija: http://www.aaiedu.hr/dokumenti.html
- Obaviti migraciju podataka:
  - instalacijom paketa aai-preinstall započinje proces (aktualni imenik je prebačen u read-only mode)
  - potrebno je kreirati novu ldif datoteku pa tek onda instalirati openldap-aai
  - ne zaboravite instalirati AOSI pakete i najnoviju verziju Radiusa!

Pripremite podatke

- Pribavite sve potrebne podatke o ustanovi
  - brojčani identifikator ustanove (hrEduOrgUniqueNumber)
  - ostali obvezni atributi definirani hrEduOrg shemom
- Ažurirajte postojeće podatke (LDAP imenik)
  - obrišite sve korisnike koji više ne trebaju biti u LDAP imeniku
  - provjerite imaju li (svi) korisnici u vašem LDAP imeniku unesenu e-mail adresu
- Za svakog korisnika pribavite sve potrebne podatke
  - brojčani identifikator osobe (hrEduPersonUniqueNumber)
  - e-mail adresa (ako već nije unesena u LDAP imeniku)
  - datum isteka temeljne povezanosti (hrEduPersonExpireDate)
- Napravite sigurnosnu kopiju vašeg LDAP imenika
  - eksportirajte podatke iz LDAP imenika u org.ldif datoteku (upute na adresi http://cmung.cmu.carnet.hr/backup.html)

Uz migraciju podataka

- LDIF datoteka s podacima iz postojećeg imenika automatski se dostavlja AAI@EduHr timu prilikom instalacije aai-preinstall paketa
- odmah nakon instalacije aai-preinstall paketa osoba koja vrši instalaciju obavezno se treba javiti mailom na adresu ldif@aaiedu.hr (kako bismo znali kome trebamo poslati prepravljenu LDIF datoteku)
- ustanova treba donijeti odluku o popunjavanju nužnim podacima i obaviti potrebno ažuriranje podataka
- korisnici ISVU sustava mogu se koristiti podacima iz sustava ISVU (nužno je da ustanova te podatke zatraži od ISVU tima)
- korisnici ISSP sustava mogu se koristiti podacima iz sustav ISSP (nužno je da to ustanova zatraži od AAI@EduHr tima)
- AAI@EduHr tim daje (samo) tehničku pomoć

Konverzija podataka ...

hrEduPerson shema	CMU shema	Napomena
HrEduPersonUniqueID	CARNetuniqueName	.srce -> @srce.hr
HrEduPersonUniqueNumber	-	ustanova mora osigurati
uid	uid	-
userPassword	userPassword	-
givenName	-	razlika atributa *cn* i *sn*
mail	mail	ustanova mora osigurati
hrEduPersonPrimaryAffiliation	CMUstatID	automatski prekodirano
hrEduPersonAffiliation	CMUstatID	automatski prekodirano
hrEduPersonExpireDate	-	ustanova mora osigurati

Što to znači za korisnike?

- Promijenit će se korisnička oznaka iz oblika

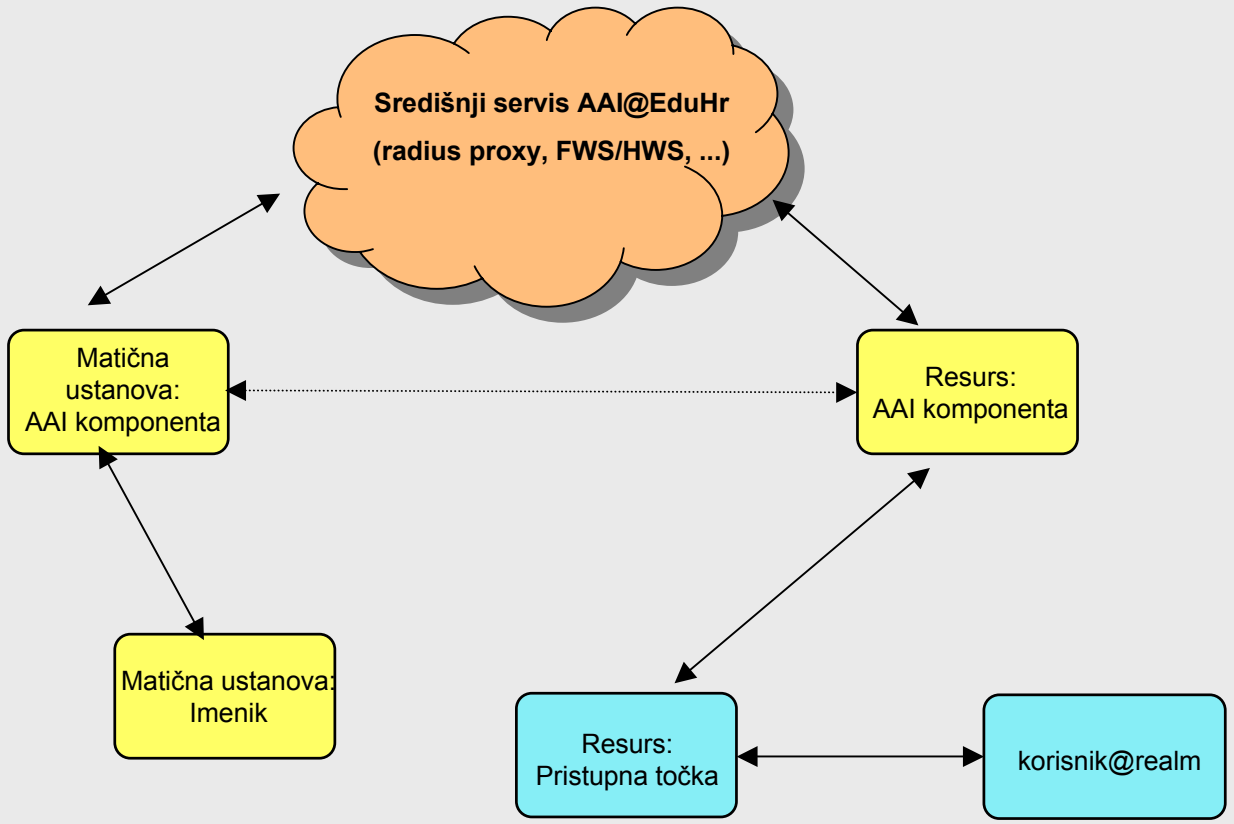
  id_korisnika.domena

  u novi oblik

  id_korisnika@oznaka_ustanove

- Primjer: *pero.fesb postaje pero@fesb.hr*
- Središnji servisi (CMU, StuDOM) podržavat će oba oblika još neko vrijeme (do 1.2.2006.)
- Mijenja se adresa i izgled sučelja za pristup i ažuriranje podataka u imeniku (AOSI/ISVU/ISSP/...)

AAI@EduHr danas



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)
  - MZOŠ Web (u izradi) ...
- pristup osnovnim servisima (login)
  - javni poslužitelj CARNeta u Srcu
  - SAS (Srce), ...
- povezivanje s međunarodnim projektima/infrastrukturama
  - eduroam (http://www.eduroam.org)
  - učešće u Geant 2 (JRA5) projektu

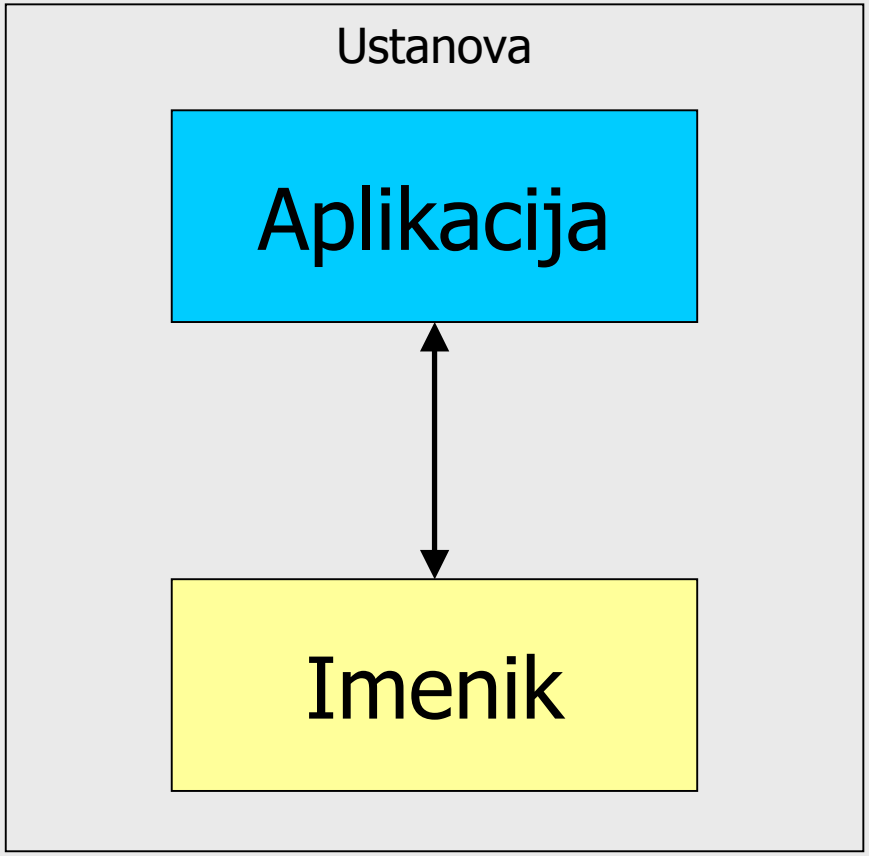
Aplikacija za održavanje sadržaja imenika (AOSI)

Sadržaj

- Uporaba imenika
- Novi način uporabe imenika
- AOSI sustav
- Pristup sustavu
- Funkcije i format podataka
- AOSI u funkciji AAI@EduHr
- Tehnički podaci o sustavu
- Interoperabilnost

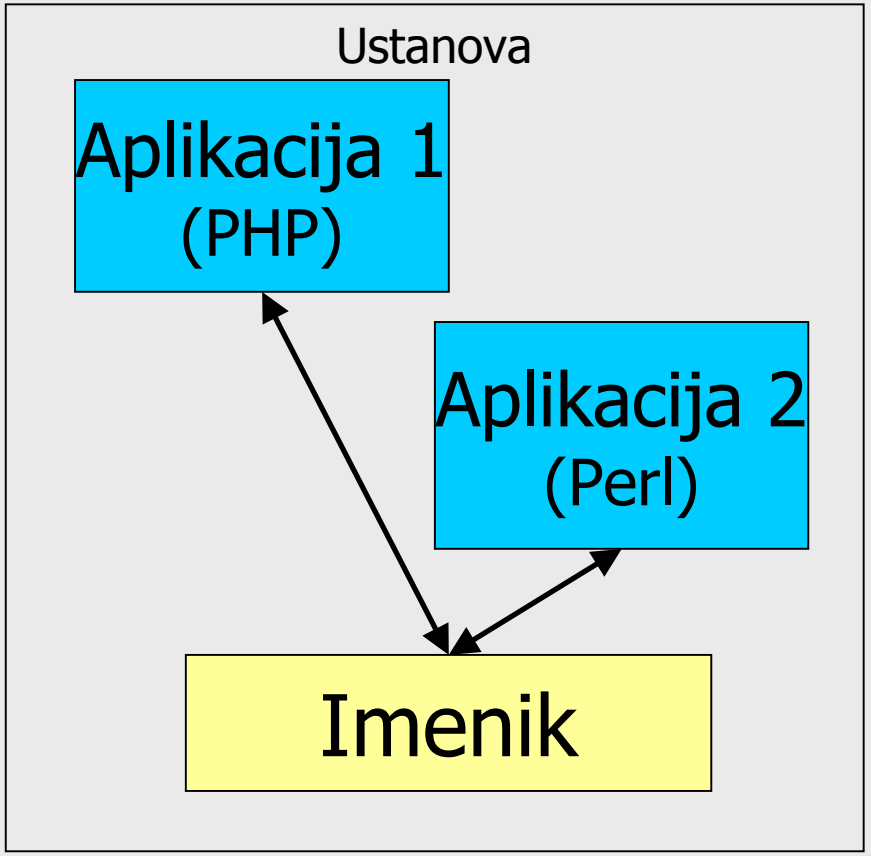
Uporaba imenika

- Imeniku se pristupa neposredno LDAP protokolom
- Samo administrator LDAP servisa (najčešće sistemac) može mijenjati atribute DRUGIM korisnicima



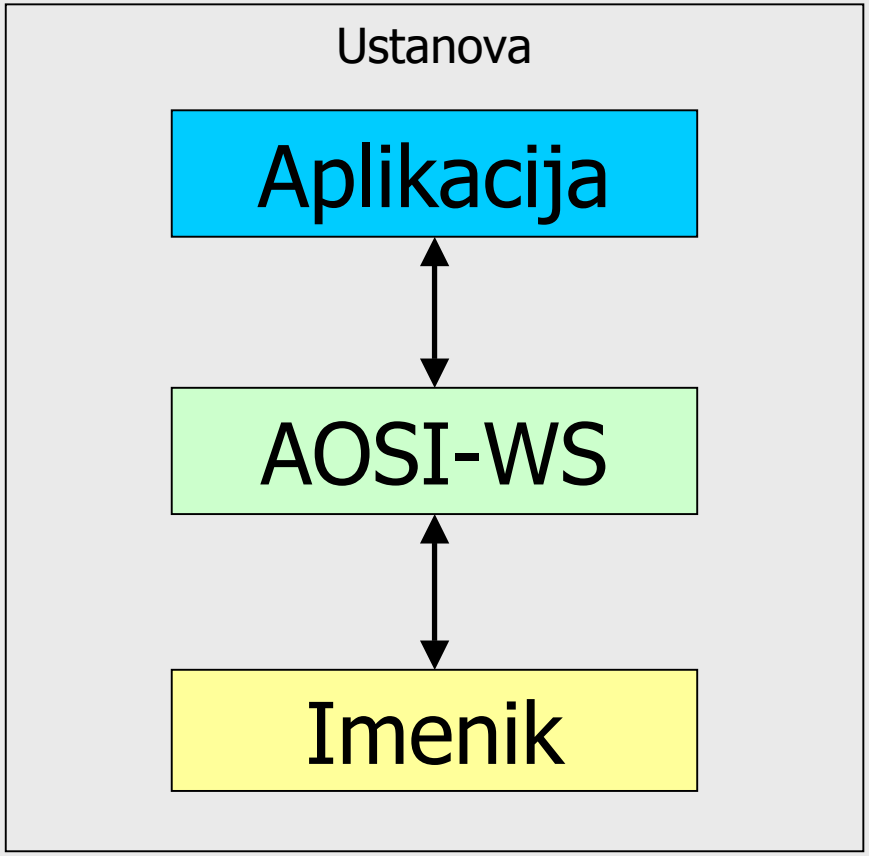
Uporaba imenika (2)

- Za promjenu atributa drugim korisnicima svaka aplikacija treba administratorsku zaporku
- Nesigurno!!!
- Komunikacija od aplikacije do imenika nije zaštićena
- Nesigurno!!!!!!



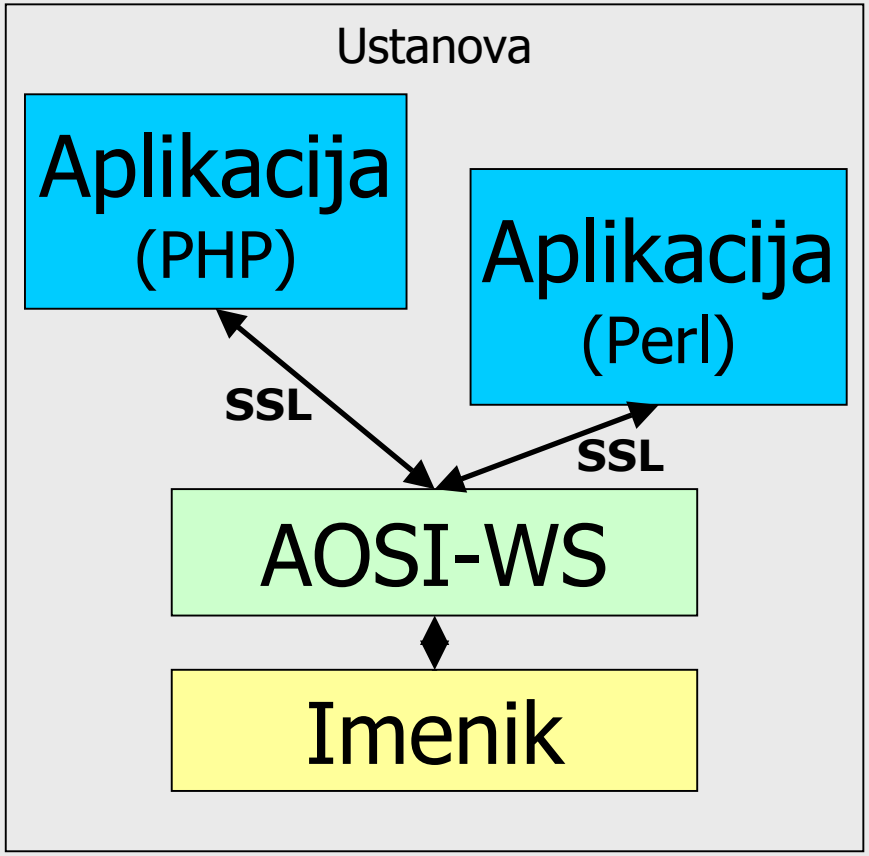
Novi način uporabe imenika

- Imeniku se pristupa posredno preko AOSI web servisa
- 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)

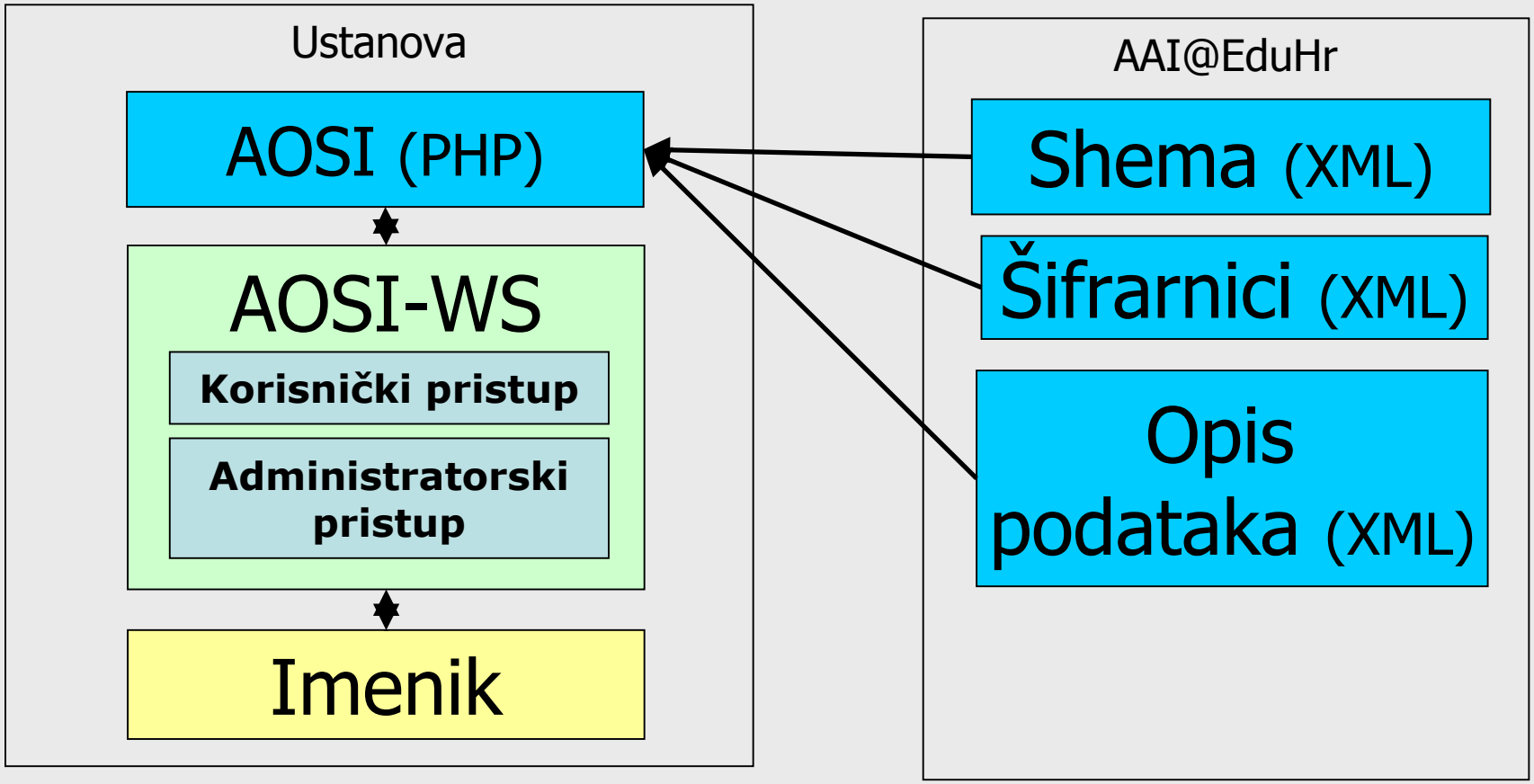


Novi način uporabe imenika (2)

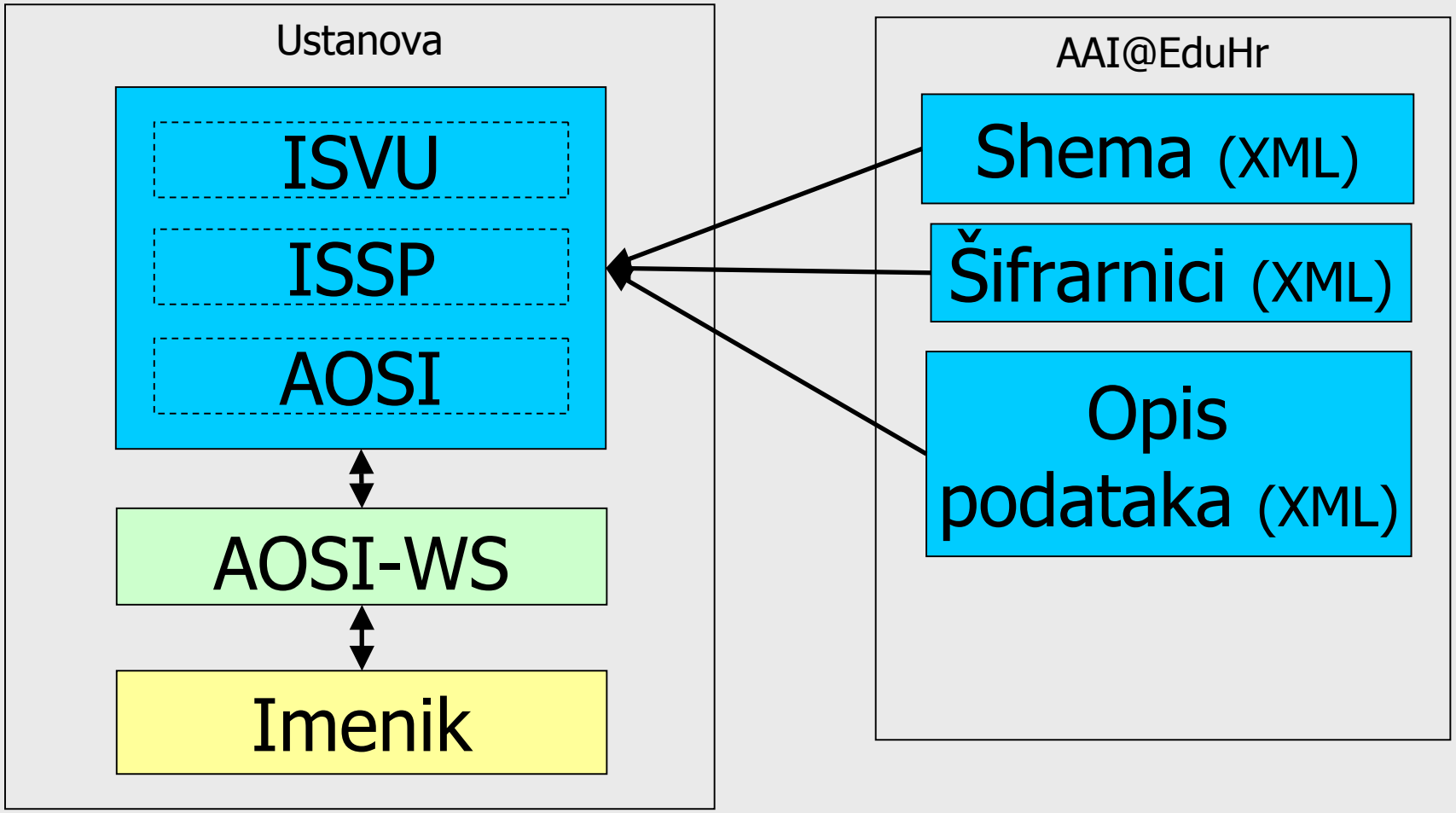
- Administrator imenika više ne mora biti administrator LDAP servisa
- Komunikacija od aplikacije do web servisa je zaštićena (SSL)



AOSI sustav


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

AOSI sustav (2)



Administratorski pristup

- Svaka ustanova mora imenovati barem jednu osobu za održavanje sadržaja imenika
- Te osobe imaju administratorski pristup LDAP imeniku ustanove što znači da mogu:
  - dobiti popis svih korisnika u LDAP imeniku
  - dobiti sve podatke o pojedinom korisniku
  - dodati novog korisnika u LDAP imenik
  - obrisati korisnika iz LDAP imenika
  - mijenjati podatke o pojedinom korisniku u LDAP imeniku

Korisnički pristup

- Korisnici mogu:
  - dobiti sve podatke u LDAP imeniku o sebi
  - dobiti samo javne podatke iz LDAP imenika o pojedinom korisniku
  - mijenjati (određene) podatke o sebi u LDAP imeniku

Administratorske funkcije

- ldapSearch(user, password, base, filter, attribute)
- ldapList(user, password, base, filter, attribute, from, size)
- ldapBinSearch(user, password, base, filter, attribute, md5)
- ldapBind(user, password, base)
- ldapUserExists(user, password, base, uid)
- ldapAddUser(user, password, base, xml)
- ldapAddUserLE(user, password, base, xml)
- ldapDeleteUser(user, password, base, dn)
- ldapAddAttribute(user, password, base, xml)
- ldapDeleteAttribute(user, password, base, xml)
- ldapModifyAttribute(user, password, base, xml)

Korisničke funkcije

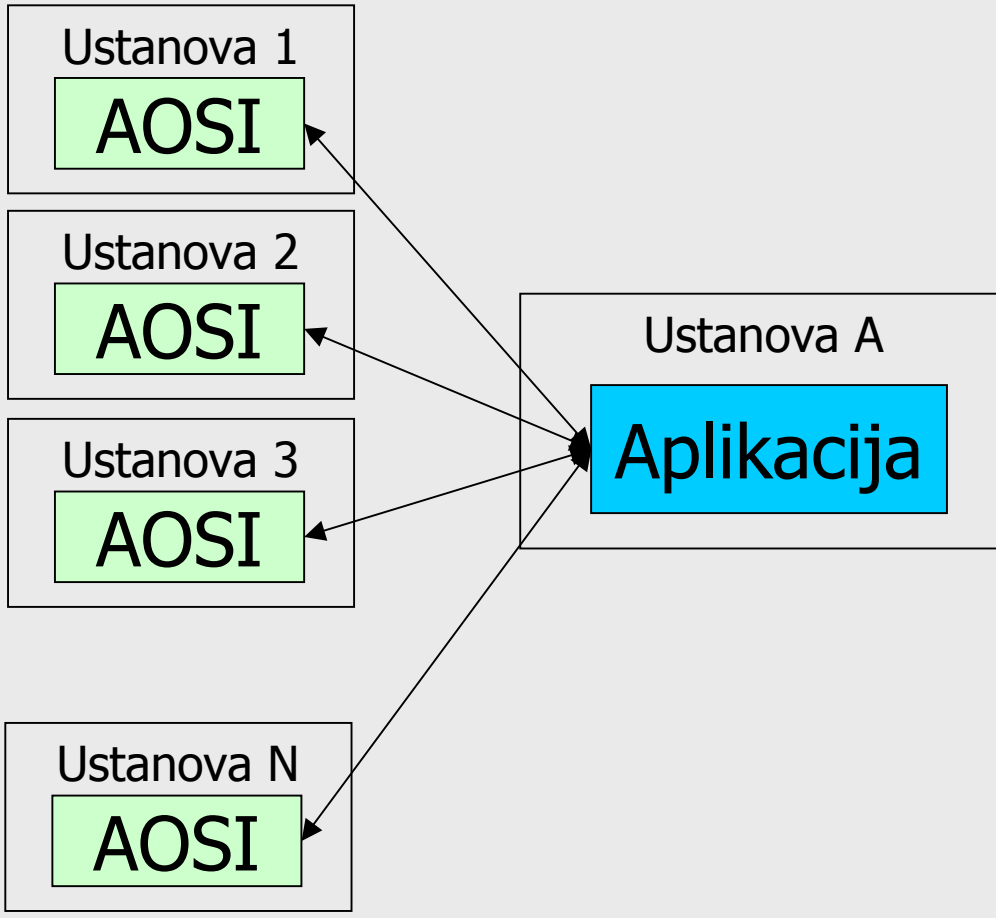
- userSearch(user, password, base, filter, attribute)
- userBinSearch(user, password, base, filter, attribute, md5)
- userAddAttribute(user, password, base, xml)
- userDeleteAttribute(user, password, base, xml)
- userModifyAttribute(user, password, base, xml)

Format podataka

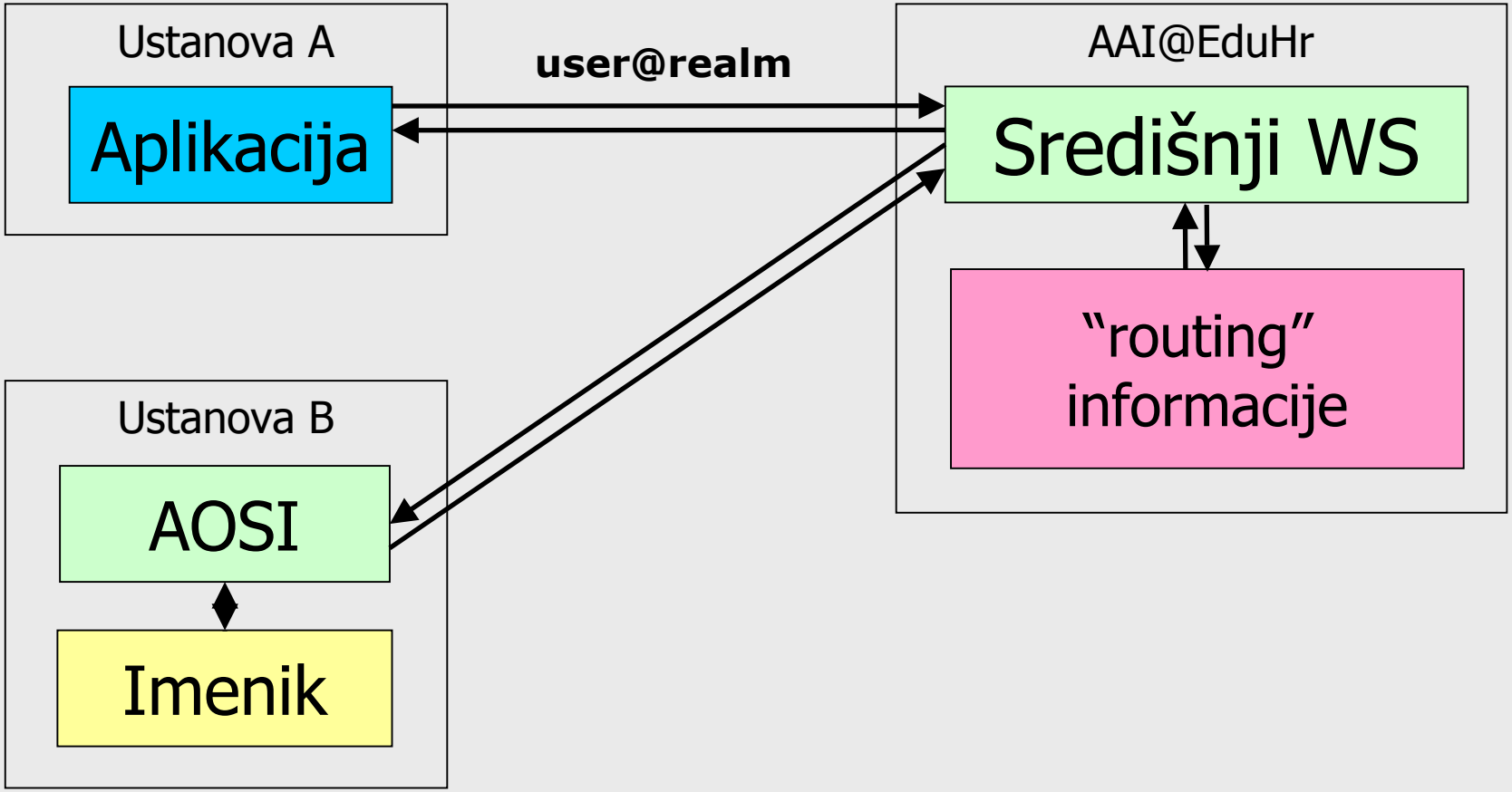
```
<ldap>
    <entry dn="uid=utest,dc=srce,dc=hr">
     <attribute ldapname="sn">
          <value>UTest</value>
          <value>UTest 2</value>
     </attribute>
     <attribute ldapname="uid">
          <value>utest</value>
     </attribute>
</ldap>
```

AOSI u funkciji AAI@EduHr

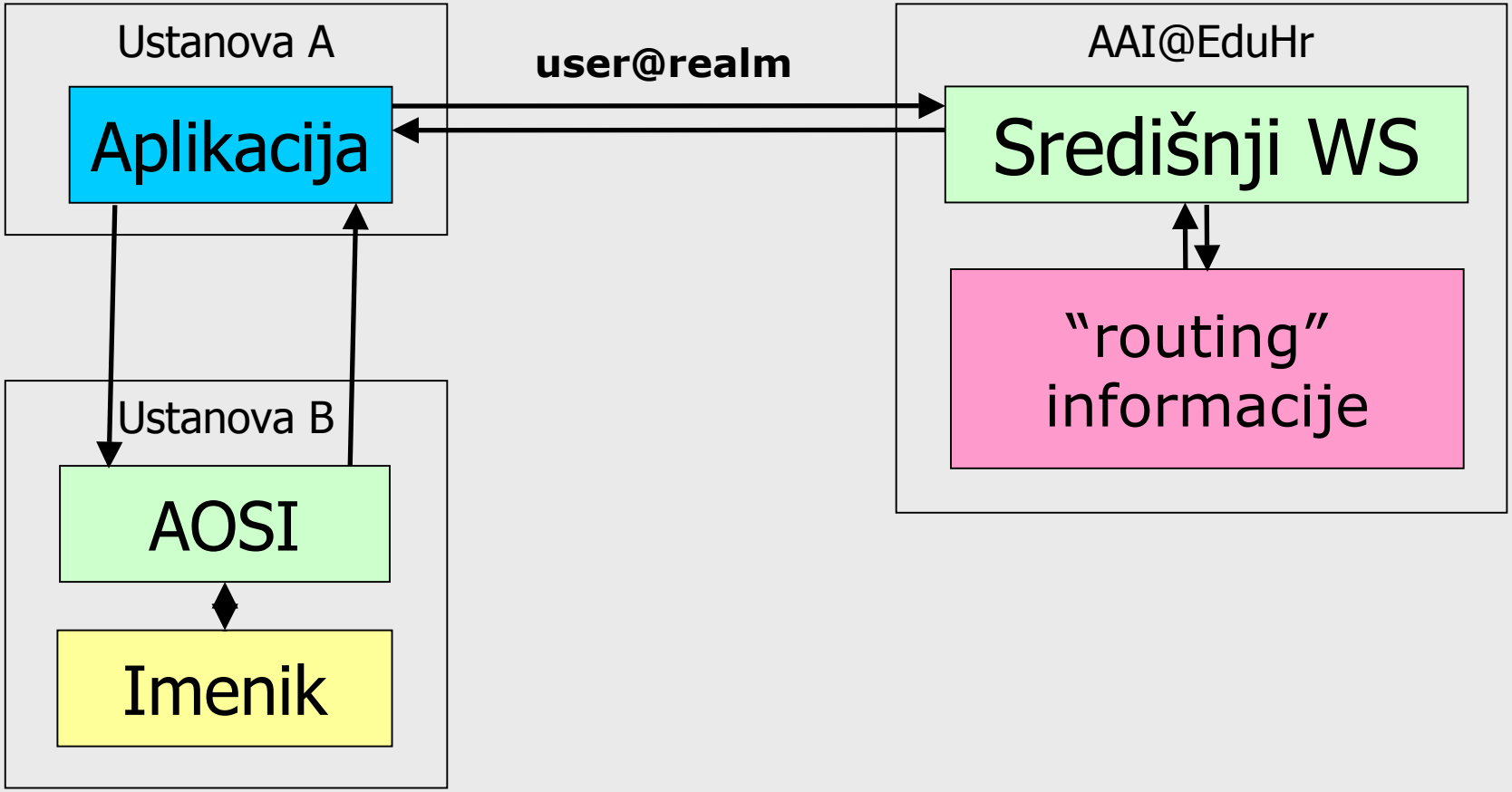
- Aplikacija mora “poznavati” infrastrukturu
- Aplikacija mora “znati” gdje se nalazi pojedini imenik



AOSI u funkciji AAI@EduHr (2)

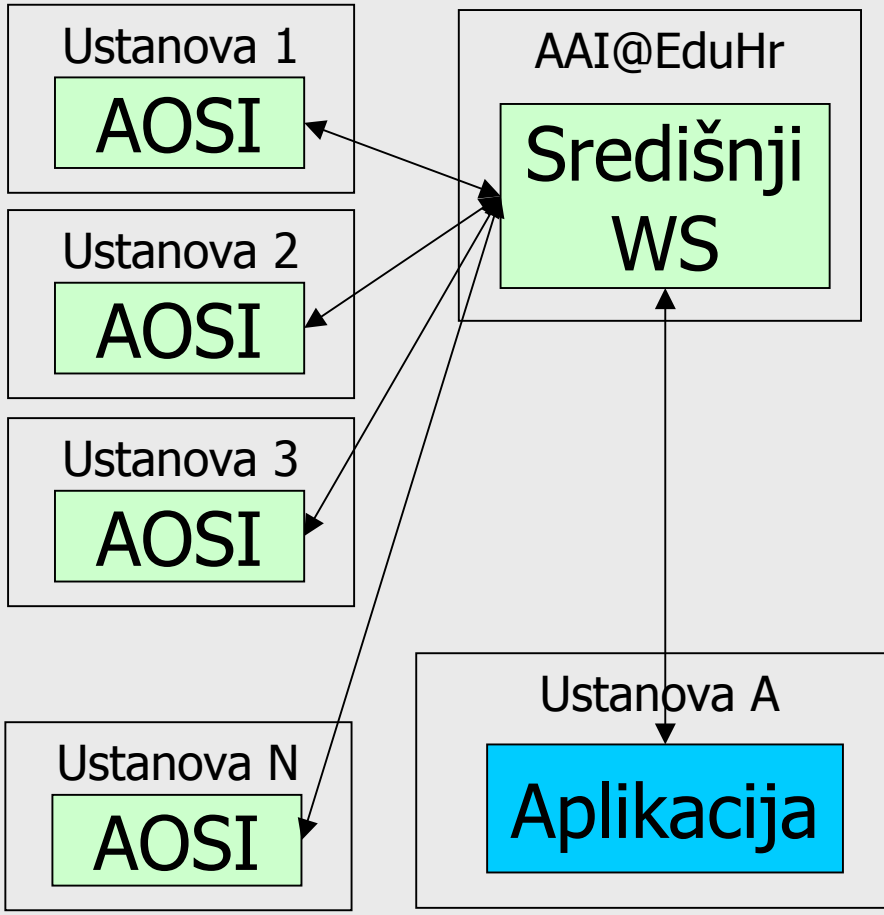


AOSI u funkciji AAI@EduHr (3)



AOSI u funkciji AAI@EduHr (4)

- Aplikacija mora “znati” samo adresu središnjeg servisa
- Središnji servis “zna” gdje se nalazi odgovarajući imenik
- Središnji servis ima politiku prosljeđivanja atributa (tko traži, od koga traži, što traži)
- Read only pristup podacima



Prednosti za autore aplikacija

- Aplikacije imaju središnje mjesto na kojem:
  - autenticiraju korisnike
  - dohvaćaju atribute potrebne za autorizaciju
- Autori aplikacija ne trebaju poznavati infrastrukturu (tj. gdje se nalazi imenik za određenu osobu), već samo adresu WSDL datoteke (http://www.aaiedu.hr/aosi/fws.wsdl)
- Pristup aplikacijama za sve osobe koje su u AAI sustavu (a dozvoljavaju čitanje potrebnih atributa!)

Prednosti za ustanove

- Pristup imeniku je dozvoljen samo s određenih mjesta:
  - iz unutarnje mreže ustanove
  - iz određene točke u AAI@EduHr sustava (središnji WS)
- Ustanova vjeruje samo određenim točkama – veća sigurnost
- Korisnici u ustanovi mogu (potencijalno) koristiti sve aplikacije koje su u sustavu

Web servis

- Napisan u Perl-u
- Opisan u http://ldaphost.ustanova.hr/ldap/aosi.wsdl
- Najčešće https://ldaphost.ustanova.hr:1443/AOSI
- Klijenti koji potvrđeno rade:
  - Perl
  - PHP
  - .Net
  - Java

AOSI klijent

- Napisan u PHP-u
- Dva sučelja
  - Korisničko
  - Administratorsko
- Korisničko sučelje:
  - Dodavanje, promjena i brisanje vlastitih (neobaveznih) atributa
  - Promjena lozinke

AOSI klijent (2)

- Administratorsko sučelje:
  - Popis korisnika
  - Pretraživanje po oznaci, imenu, prezimenu, AAA, BBB uz podršku za univerzalni kvalifikator (*)
  - Dodavanje, promjena i brisanje gotovo svih atributa
  - Masovno dodavanje korisnika iz CSV i XML datoteka
  - Masovno brisanje korisnika, uz prethodno filtriranje

Interoperabilnost

Aplikacija za održavanje imenika	Studenti	Nastavno osoblje	Ostali zaposlenici
AAI	☑	☑	☑
ISVU	☑	☑	☑
ISSP	☑	☒	☒

Interoperabilnost (2)

Sustav	Studenti	Nastavno osoblje	Ostali zaposlenici
AAI	AAI	AAI	AAI
ISVU	ISVU	ISVU	ISVU
ISSP	ISSP	AAI	AAI

Scenarij A

- Ustanova je u ISVU sustavu i želi kroz taj sustav održavati elektroničke identitete
  - Šalje zamolbu ISVU timu da se izvade podaci o njihovoj ustanovi
  - ISVU tim šalje podatke ustanovi
  - Ustanova šalje podatke AAI timu
  - AAI tim uparuje podatke s već postojećima iz LDAP imenika
- Elektronički identiteti se održavaju **isključivo** kroz ISVU sustav

Scenarij B

- Ustanova je u ISSP sustavu i želi kroz taj sustav održavati elektroničke identitete studenata
  - Šalje obavijest AAI timu što želi
  - ISSP tim šalje podatke AAI timu
  - AAI tim uparuje podatke s već postojećima iz LDAP imenika
- Elektronički identiteti studenata se održavaju kroz ISSP sustav
- Elektronički identiteti nastavnog osoblja i ostalih zaposlenika se održavaju kroz AAI sustav

Scenarij C

- Ustanova nije niti u ISVU niti u ISSP sustavu ili ne želi kroz niti jedan od tih sustava održavati elektroničke identitete
  - Ustanova šalje potrebne podatke AAI timu
  - AAI tim dopunjuje već postojeće podatke iz LDAP imenika
- Elektronički identiteti se održavaju **isključivo** kroz AAI sustav

AAI@EduHr: pristup mreži i računalnim resursima

Sadržaj

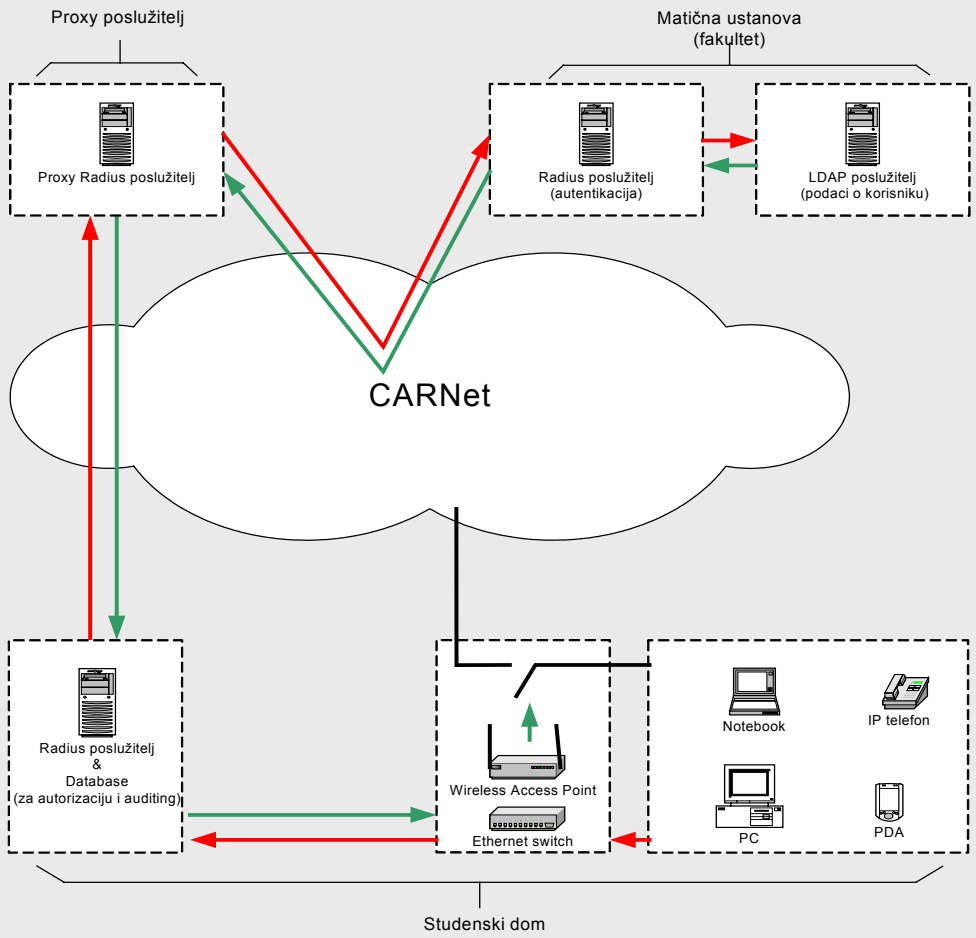
- Wireless/Wired AA
- pGina
- Unix/Linux PAM

Wireless/Wired AA

Wireless/Wired AA

- Postupak AA
- Standardi i implementacija
- Mrežni uređaji
  - Wireless
  - Wired
- Autentikacijski klijenti

Postupak AA


Proxy poslužitelj
Matična ustanova
(fakultet)
Proxy Radius poslužitelj
Radius poslužitelj
(autentikacija)
LDAP poslužitelj
(podaci o korisniku)
CARNet
Radius poslužitelj
&
Database
(za autorizaciju i auditing)
Wireless Access Point
Ethernet switch
Notebook
IP telefon
PC
PDA
Studenski dom

Standardi i implementacija

- 802.1x standard za komunikaciju pristupnog uređaja i pristupnog klijenta
- Podaci se prenose putem EAP-a
- Preporuka je korištenje EAP-TTLS-a
  - Jednostavnost primjene
  - Lagano održavanje
  - Dovoljna zaštita

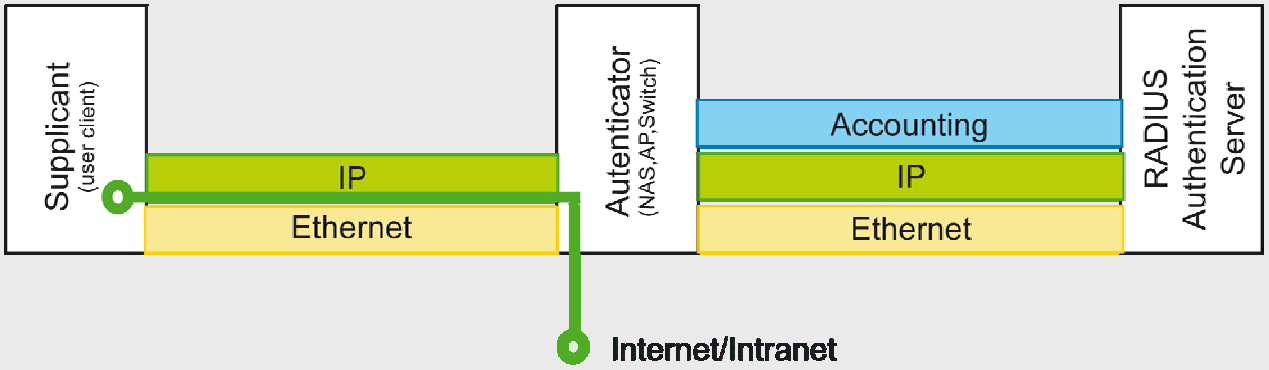
Neautencirani klijent

- Klijent nema IP Layer
- Klijent osluškuje EAPOL broadcast

Postupak AA

- Korisnički podaci se prenose EAPOL-om
- Pristupni uređaj prebacuje EAPOL u EAP pakete i šalje ih RADIUS protokolom do RADIUS servera

Autenticiran pristup



- Ako je AA uspjela pristupni uređaj uspostavlja IP Layer s klijentom
- Klijent putem pristupnog uređaja prolazi na Internet/Intranet

Mrežni uređaji - Wireless

- Pristupni AP mora podržavati native 802.1x/EAP
  (ne samo neke nego sve EAP protokole)
- Accounting je poželjan
- Preporuka WPA/TKIP pristupni kripto protokol
- Eduroam http://www.eduroam.org/
  (više od običnog wireless pristupa)
- Linksys/OpenWrt
  http://www.linksys.com/
  http://www.openwrt.org/

Mrežni uređaji - Wired

- Pristupni uređaj mora podržavati native 802.1x/EAP
  (ne samo neke nego sve EAP protokole)
- Accounting je potreban
- Cisco i HP switchevi
- StuDOM http://www.srce.hr/StuDOM
- Autentikacijski izazov za korisnike

Autentikacijski klijenti

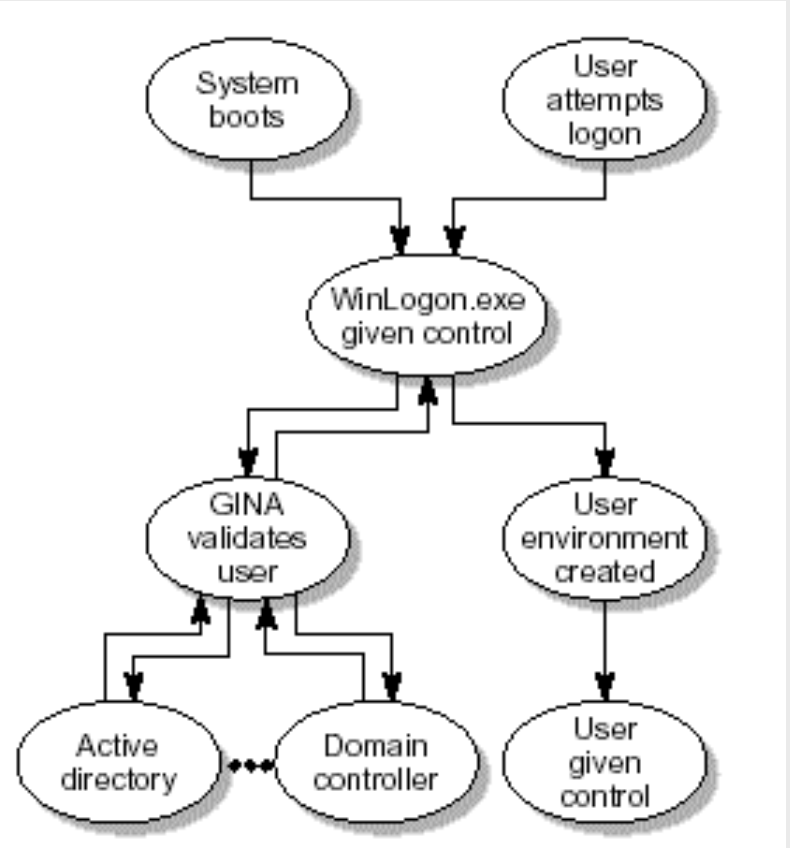
- SecureW2 – GNU
  Microsoft Windows 2000, XP, 2003
- Xsupplicant, wpa_suplicant - GNU
  Linux/UNIX/MS Windows
- Native podrška u MAC OS 10.3+
- Veći broj komercijalnih supplicant riješenja

pGina

pGina

- GINA engine unutar MS Windows OS-a
- pGina – *Making the big boys play nice*
- Autentikacija pojedinačnih računala
- Autentikacija računala u Microsoft domeni

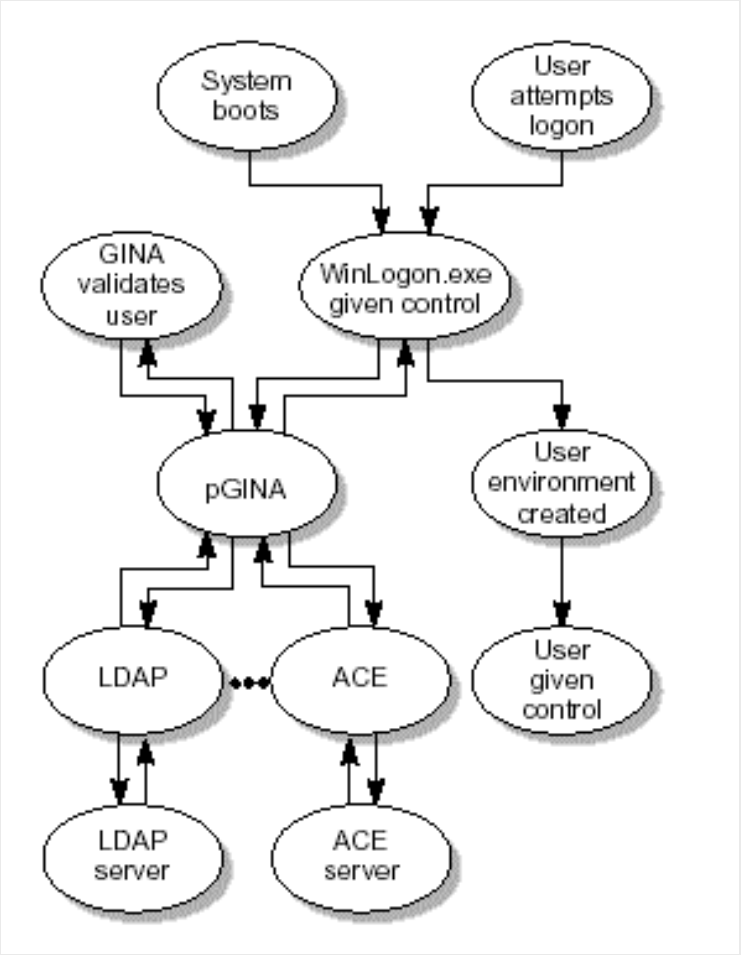
GINA engine unutar MS Windows OS-a



pGina
Making the big boys play nice

- Zamjena za Microsoft GINA sustav
- Modularna – više različitih načina autentikacije
- Preporuka korištenje RADIUS plugina
- GNU licenca
- Nije savršena
- http://pgina.xpasystems.com/

pGina


System boots
User attempts logon
GINA validates user
WinLogon.exe given control
pGINA
User environment created
LDAP
ACE
User given control
LDAP server
ACE server

Autentikacija pojedinačnih računala

- Računalo se može nalaziti u Workgroupi
- Na računalu se mogu koristiti svi oblici grupiranja korisnika po Microsoft pravilima
- Korisnički profili se ne zadržavaju na računalu nakon završetka rada pojedinog korisnika
- Javni terminali, laboratoriji i slično
- Primjer javni terminali u zgradi Srca

Autentikacija računala u Microsoft domeni

- Računala se nalaze u domeni ili Forest-u
- Na računalu se mogu koristiti svi oblici grupiranja korisnika po Microsoft pravilima
- Korisnički profili se nalaze na Active Directoryu uz korištenje svih mogućnosti
- Privatne lokalne mreže

Unix/Linux PAM

Unix/Linux PAM

- PAM (pam_auth_radius) - autentikacija
- Svi aplikavni servis na samom sustavu
- Moguća dodatna autorizacija
- Administratori imaju redudantni pristup sustavu
- Primjeri :
  - Javno računalo CARNeta
  - Srce centralni serveri
  - SAS server

AAI@EduHr kontakti

http://www.aaiedu.hr/

team@aaiedu.hr

aosi@aaiedu.hr

ldif@aaiedu.hr