Kako svoju Web aplikaciju uskladiti sa SSO sustavom?

Alen Vodopijevec,
Institut Ruđer Bošković, Zagreb

alen@irb.hr

LDAP

- Lightweight directory access protocol
- LDAP imenik
  - baza podataka u kojoj su pohranjeni elektronički identiteti
  - eduHr imeničke sheme
    - hrEduPerson
    - hrEduOrg

```
dn: uid=fsmith, ou=employees, dc=foobar, dc=com
  objectclass: person
  objectclass: organizationalPerson
  objectclass: inetOrgPerson
  objectclass: foobarPerson
  uid: fsmith
  givenname: Fran
  sn: Smith
  cn: Fran Smith
  cn: Frances Smith
  telephonenumber: 510-555-1234
  roomnumber: 122G
  o: Foobar, Inc.
  mailRoutingAddress: fsmith@foobar.com
  mailhost: mail.foobar.com
  userpassword: {crypt}3x1231v76T89N
  uidnumber: 1234
  gidnumber: 1200
  homedirectory: /home/fsmith
  loginshell: /usr/local/bin/bash
```

LDAP i web aplikacije

- php-ldap
- Net::LDAP
- mod_auth_ldap

testic@realm.hr

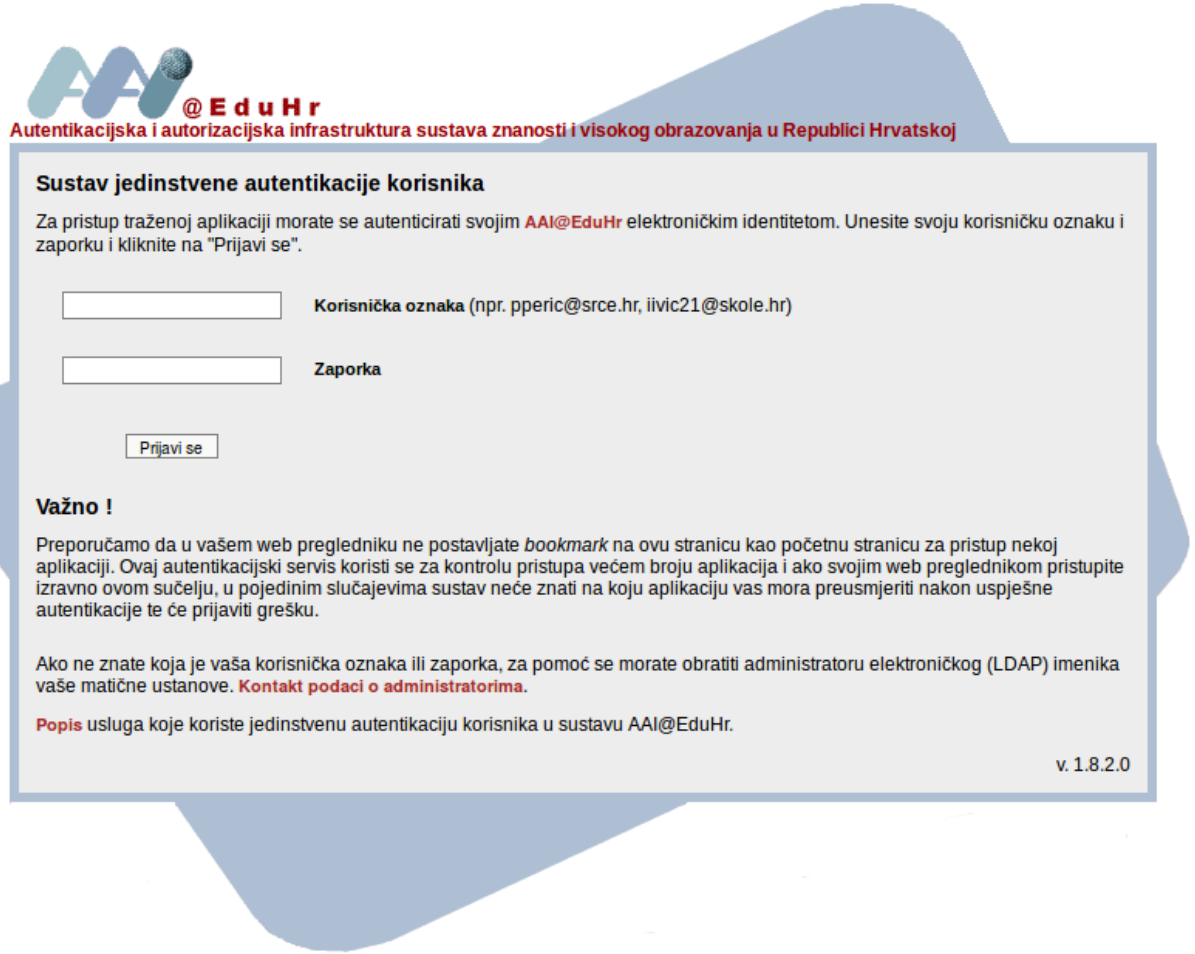
```
<Location /livada>
        AuthType Basic
        AuthName "Library // LDAP login"
        AuthBasicProvider ldap
        AuthzLDAPAuthoritative off
        AuthLDAPUrl ldap://ldap.irb.hr/dc=irb,dc=hr???objectClass=person
        Require user alen bojan
 </Location>
```

FWS

Federacijski Web Servis

- Proxy
  - prosljeđuje upit aplikacije na određeni LDAP server
- Home Locator Service
  - vraća informaciju o lokaciji LDAP servisa ustanove
- bib.irb.hr (perl), proxy.znanstvenici.hr (authmem_cookie), sestar.irb.hr (PHP prebačen na SSO)

SSO

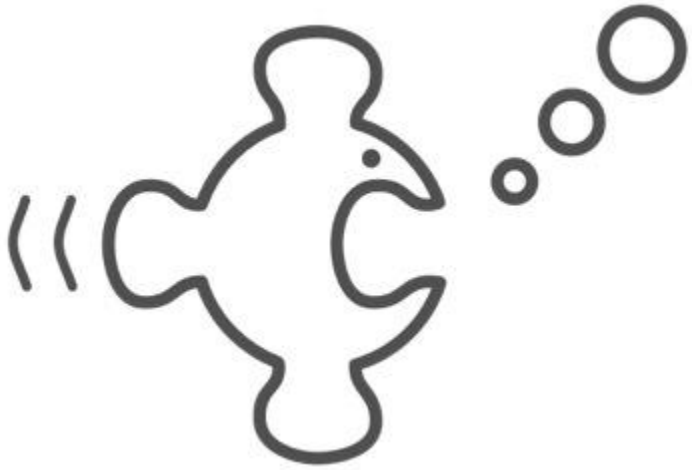

@EduHr
Autentikacijska i autorizacijska infrastruktura sustava znanosti i visokog obrazovanja u Republici Hrvatskoj
Sustav jedinstvene autentikacije korisnika
Za pristup traženoj aplikaciji morate se autenticirati svojim AAI@EduHr elektroničkim identitetom. Unesite svoju korisničku oznaku i zaporku i kliknite na "Prijavi se".
Korisnička oznaka (npr. pperic@srce.hr, iivic21@skole.hr)
Zaporka
Prijavi se
Važno !
Preporučamo da u vašem web pregledniku ne postavljate bookmark na ovu stranicu kao početnu stranicu za pristup nekoj aplikaciji. Ovaj autentikacijski servis koristi se za kontrolu pristupa većem broju aplikacija i ako svojim web preglednikom pristupite izravno ovom sučelju, u pojedinim slučajevima sustav neće znati na koju aplikaciju vas mora preusmjeriti nakon uspješne autentikacije te će prijaviti grešku.
Ako ne znate koja je vaša korisnička oznaka ili zaporka, za pomoć se morate obratiti administratoru elektroničkog (LDAP) imenika vaše matične ustanove. Kontakt podaci o administratorima.
Popis usluga koje koriste jedinstvenu autentikaciju korisnika u sustavu AAI@EduHr.
v. 1.8.2.0

SSO - Prednosti

- jedinstveno sučelje za prijavu
  - vizualno
  - sigurnost
  - nebitno koristi li web aplikacija SSL

- jednom prijavljen, uvijek prijavljen :)
  - u početku je nedostajala SLO funkcionalnost

SSO - implementacija

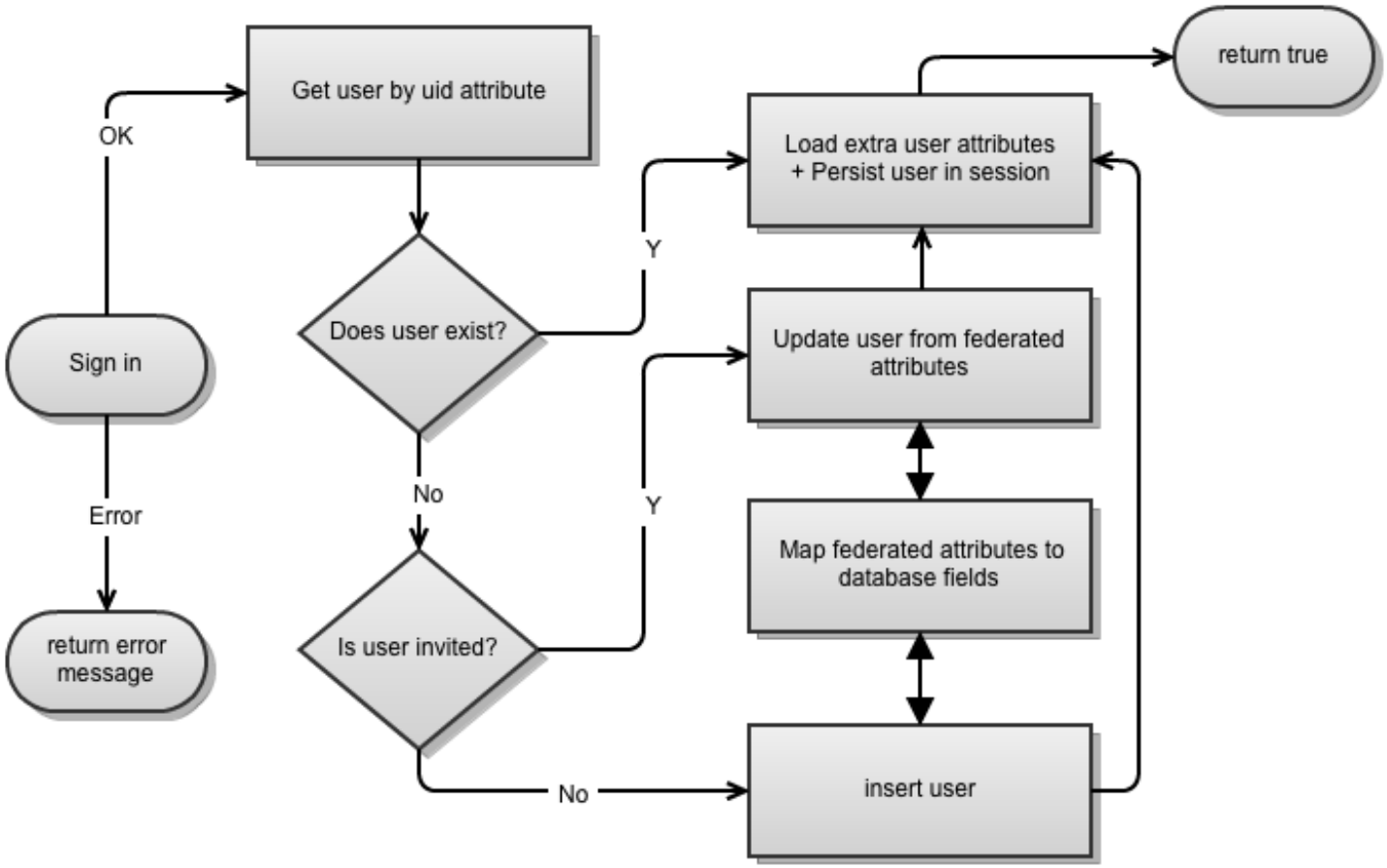


- SimpleSAMLphp
  - PHP aplikacija
  - IdP
  - SP
  - podržava i Shibboleth 1.3, A-Select, CAS, OpenID, WS-Federation and OAuth
    - npr. pristup Elsevier bazama podataka http://www.webofknowledge.com/?locale=en_US

SSO - koraci

1. instalacija simpleSAMLphp
   a. http://developer.aaiedu.hr/faq/8.html
2. prijava servisa u registar resursa
   a. http://www.aaiedu.hr/aairr/
3. prilagodba aplikacije
   a. PHP standardno
   b. auth_memcookie
   c. korištenje PHP session-a
4. testiranje
5. produkcija :)

SSO - proces autentikacije



Izvor: https://confluence.terena.org/display/core/Users

SSO - PHP implementacija

- web aplikacija u PHP-u
- korištenje postojećeg primjera Srca
  - http://developer.aaiedu.hr/faq.html
- za postojeće aplikacije otvorenog koda provjeriti da li postoji neka SAML implementacija (npr. Owncloud, Joomla)

SSO - ostali skriptni jezici

- npr. auth_memcookie
- redirekcija na štićenu lokaciju
- preuzimanje podataka
  - cookie
  - SERVER varijable
- logout preko SLO URL-a

https://cloud.irb.hr/simplesaml/module.php/core/as_logout.php?AuthId=default-sp&ReturnTo=http://www.srce.hr

SSO - auth_memcookie (1)

- Preduvjeti (osim simpleSAMLphp)

```
# apt-get install memcached

# apt-get install apache2-dev
# apt-get install build-essential
# apt-get install libmemcache-dev
# (wget authmemcookie)
http://authmemcookie.sourceforge.net/

# cat Makefile
MY_APXS=/usr/bin/apxs2
MY_LDFLAGS=-lmemcache -L/usr/lib
MY_CFLAGS=-I/usr/include
```

SSO - auth_memcookie (2)

- build Apache modula

```
# cat Makefile
MY_APXS=/usr/bin/apxs2
MY_LDFLAGS=-lmemcache -L/usr/lib
MY_CFLAGS=-I/usr/include

# make && make install
```

SSO - auth_memcookie (3)

- omogućiti modul

cat /etc/apache2/mods-available/auth_memcookie.load

LoadModule mod_auth_memcookie_module /usr/lib/apache2/modules/mod_auth_memcookie.so

cd /etc/apache2/mods-enabled && ln -s ../mods-available/auth_memcookie.load

SSO - auth_memcookie (4)

- konfiguriranje štićene lokacije (Apache)

```
<LocationMatch /(aai-test/authmemcookie|impressionist)>

        Auth_memCookie_Memcached_AddrPort "127.0.0.1:11211"

        Auth_memCookie_Authoritative on

        Auth_memCookie_SessionTableSize "40"

        AuthType Cookie
        AuthName "My Login"

        ErrorDocument 401 "/simplesaml/authmemcookie.php"

        Require valid-user

</LocationMatch>
```

SSO - auth_memcookie (5)

- konfiguracija authmemcookie modula u simpleSAMLphp

```
# cp /usr/share/doc/simplesamlphp/examples/config-templates/authmemcookie.
php /etc/simplesamlphp

# grep 'hrEdu' /etc/simplesamlphp/authmemcookie.php
    'username' => 'hrEduPersonUniqueID',
```

SSO - auth_memcookie (6)

- restart web servera

- Primjeri:
  - https://cloud.irb.hr/aai-test/authmemcookie/
  - https://cloud.irb.hr/impressionist/ (Chrome)

Postojeće implementacije

- SSO
  - http://www.irb.hr
  - http://sestar.irb.hr
  - http://cloud.irb.hr
  - http://rezervacije.irb.hr (Otvoreni dani IRB-a)
- FWS - planirana migracija na SSO
  - http://bib.irb.hr
  - http://proxy.znanstvenici.hr
  - http://tkojetko.irb.hr
- Popis svih registriranih servisa:
  - http://www.aaiedu.hr/faq_sso_aplikacije.html

Hvala!

alen@irb.hr