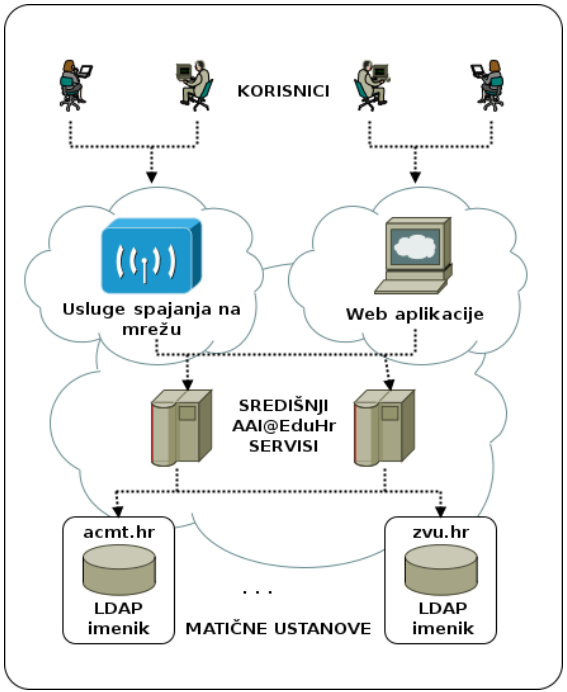
Nova verzija AOSI web sučelja i servisa

Zagreb, 18. veljače 2021., Srce, AAI@EduHr tim
Mijo Đerek, Marko Ivančić, Matija Lovrić, Miro Mačinković, Miroslav Milinović

Sadržaj

- Uvod:
  - Općenito o sustavu AAI@EduHr
  - uloga AOSI web servisa i web sučelja u sustavu AAI@EduHr
- “Stari” AOSI
- Novi AOSI
- SOAP sučelje
- Web sučelje

Što je AAI@EduHr



- Autentikacijska i autorizacijska infrastruktura sustava znanosti i (visokog) obrazovanja u Republici Hrvatskoj;
- u produkciji od 1. ožujka 2006.
- hub-and-spoke arhitektura
- povezana u globalne sustave eduroam i eduGAIN
- web: http://www.aaiedu.hr
- e-mail: aai@srce.hr

Sustav AAI@EduHr kroz brojeve

- 241 matična ustanova, više od 900.000 elektroničkih identiteta

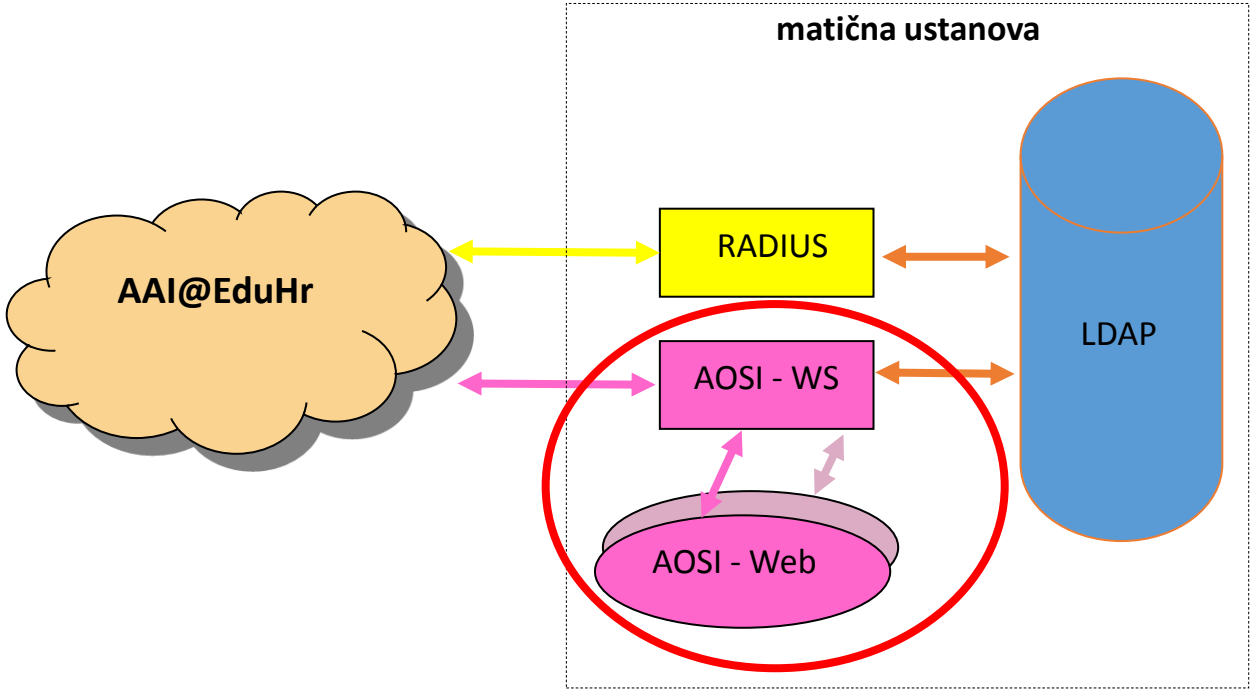
  https://www.aaiedu.hr/statistika-i-stanje-sustava/maticne-ustanove/statusi-servisa
- 102 usluge pristupa mreži

  https://www.aaiedu.hr/statistika-i-stanje-sustava/usluge-pristupa-mrezi
- 763 web aplikacije koje koriste AAI@EduHr SSO servis za autentikaciju korisnika (bez eduGAIN-a)

  https://www.aaiedu.hr/statistika-i-stanje-sustava/web-aplikacije
- U zadnjih 30 dana:
  - 26.153.526 uspješnih RADIUS autentikacija
  - 14.718.574 uspješnih SSO autentikacija
  - 479.639 uspješnih FWS autentikacija

  https://www.aaiedu.hr/statistika-i-stanje-sustava

Matična ustanova u sustavu AAI@EduHr



AOSI web servis

- Pisan u perlu
- SOAP over HTTPS
- Implementira neka pravila koja OpenLDAP ne nudi sam po sebi, a nama su bila potrebna.
  - Delegacija prava pristupa imeniku
  - Semantika i sintaksa pojedinih atributa u imeniku
  - Šifrarnici
  - Dodatna validacija kod pisanja u imenik
- Omogućuje administraciju imenika u skladu s pravilima i shemama
- Odgovara na autentikacijske zahtjeve središnjih servisa sustava AAI@EduHr
- Po uspješnoj autentikaciji vraća korisničke atribute iz LDAP imenika
- Proširiv dodatcima – pluginovima
- Omogućuje povezivanje / sinkronizaciju imenika s drugim informacijskim sustavima
- http://www.aaiedu.hr/za-maticne-ustanove/programska-podrska/aplikacija-za-odrzavanje-sadrzaja-imenika-aosi

AOSI web sučelje

- Web sučelje za informacijsko održavanje imenika
- Ustanove ga po želji mogu zamijeniti svojim alatom
- Pisano u php-u

Stara inačica AOSI-a

- Dvije aplikacije:
  - AOSI (SOAP) web servis (perl)
  - AOSI web sučelje (php)
- Kompleksno održavanje
- Zastarjele verzije knjižnica – potencijalni sigurnosni problemi
- Dodatci (plugin-ovi) se pišu u perl-u
- U najčešćem scenariju korištenja (web sučelje – web servis) puno nepotrebnog procesiranja
- Rješenje: izrada nove inačice

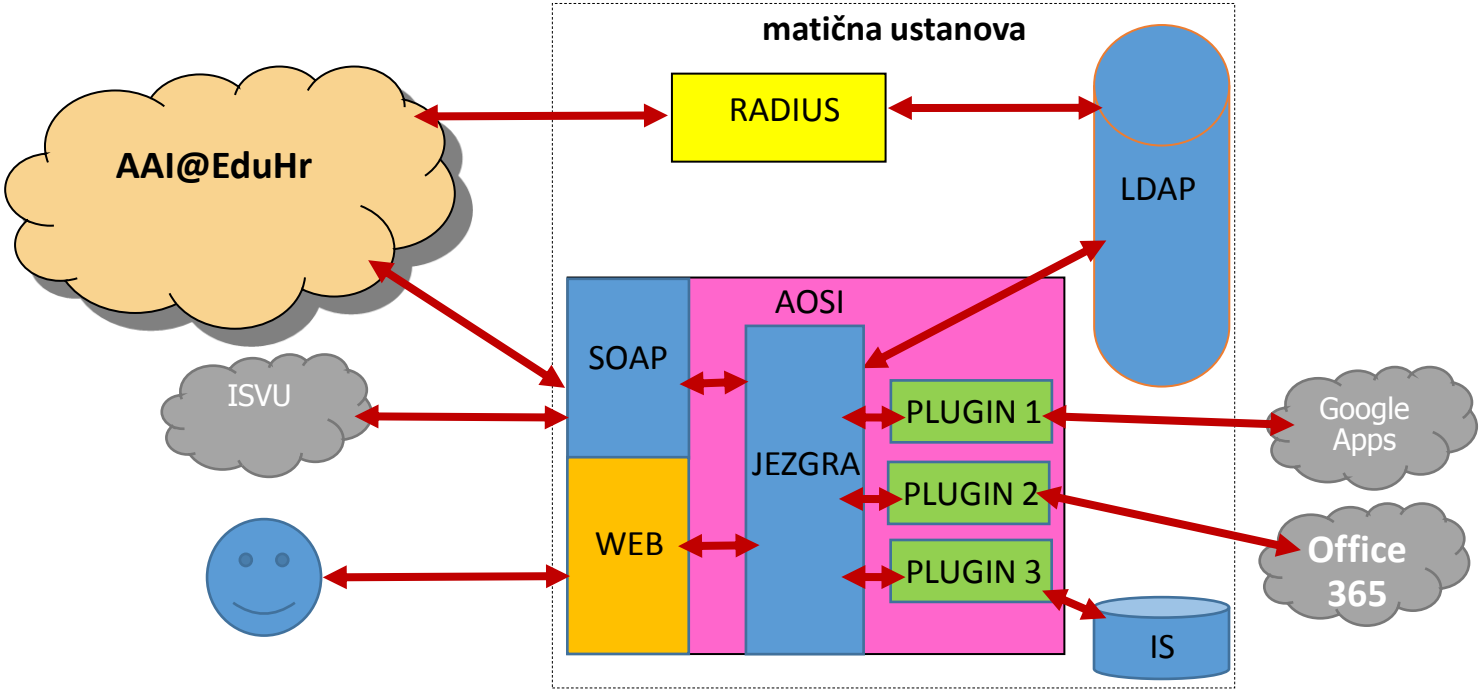
Nova inačica AOSI 4.0

- Pisana u php-u (Laravel framework)
- Zadržava sve postojeće funkcionalnosti
- Jedna aplikacija s više sučelja i jezgrom
- SOAP sučelje uz zadržavanje kompatibilnosti s AOSI web servisom
- HTML sučelje – redizajnirano, osvježeno, responzivno
  - Za administratore: administracija LDAP imenika, dodavanje, brisanje korisnika, ažuriranje podataka
  - Za korisnike: promjena svojih podataka, promjena zaporke
  - Adresar
- XYZ sučelje

Nova inačica AOSI 4.0

- Sva sučelja koriste jezgru aplikacije koja implementira
  - validaciju i oblikovanje podataka,
    - AAI@EduHr sheme, šifrarnici
  - delegaciju prava,
  - čitanje i pisanje u imenik,
  - pisanje dnevničkih zapisa
  - sustav dodataka (plugin-ova)
- Izvedena je u obliku php klase koja nudi metode za upravljanje podacima u imeniku
- Moguće je dodati sučelje po želji

Nova inačica AOSI 4.0



Nova inačica AOSI 4.0

- Izrada svih podržanih dodataka
  - neki dodaci su integrirani: dodatak za certificiranje i dodatak koji omogućuje provjeru jedinstvenosti vrijednosti atributa

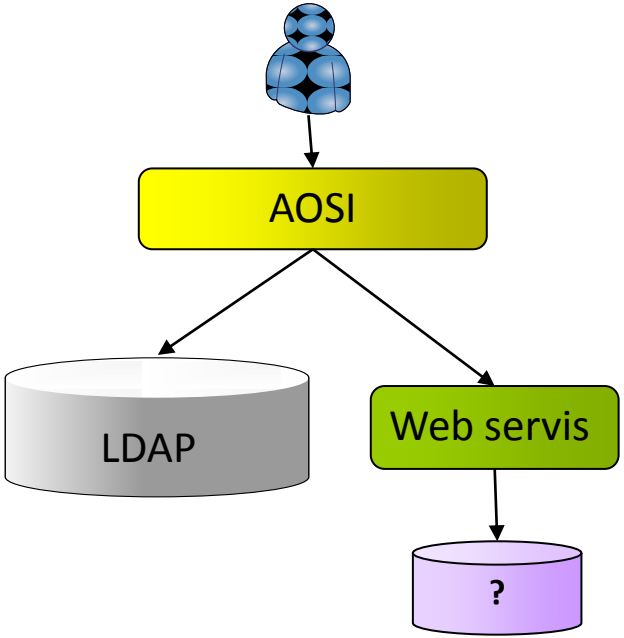
https://www.aaiedu.hr/koji-postojeci-moduli-su-dostupni-za-aosi

- Distribucija putem instalacijskih paketa za Linux Debian (od inačice 10)
- Dostupna u AAI@EduHr Lab-u

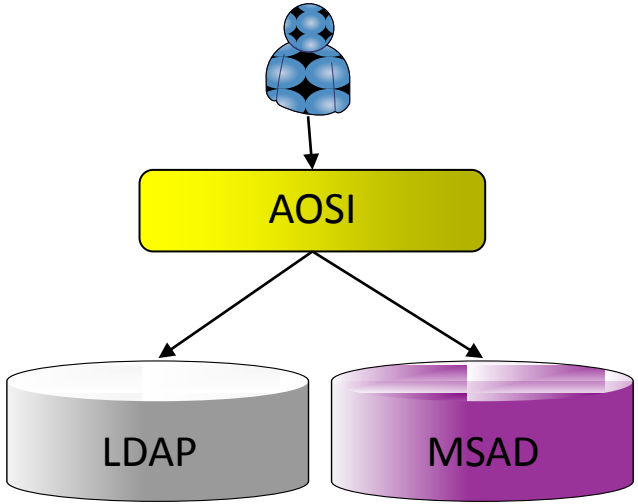
https://fed-lab-imenik.aaiedu.hr/v4/

- Prelazak na novu inačicu
  - paziti na korištene dodatke
  - dodaci koji nisu među podržanima će morati biti reimplementirani u php-u
  - podržani dodaci dolaze u obliku paketa

AOSI sustav plug-inova



Web service plug-in



MS Active Directory plug-in

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

AOSI SOAP

- Za dohvat i razmjenu podataka koristi se Simple Object Access Protocol (SOAP)
- Za opis podataka koristi se Extended Markup Language (XML)
- Funkcije AOSI web servisa maskiraju posebnosti i nepravilnosti koje se skrivaju u neposrednom pristupu LDAP imeniku, čime je olakšano pisanje klijentskih aplikacija koje dohvaćaju podatke iz LDAP imenika;
- Komunikacija između SOAP klijenta i SOAP web servisa je zaštićena (HTTPS)

SOAP

- RPC/encoded.
- RPC/literal.
- Document/encoded (not used in practice).
- Document/literal.

AOSI SOAP

- RPC/encoded.
- RPC/literal. 
- Document/encoded (not used in practice).
- Document/literal.

AOSI SOAP

anonBinSearch
anonSearch
ldapAddAttribute
ldapAddUser
ldapAddUserLE
ldapAdminInfo
ldapBind
ldapBinSearch
ldapDeleteAttribute
ldapDeleteUser
ldapList
ldapModifyAttribute
ldapOrgInfo
ldapSearch
ldapUserExists
userAddAttribute
userBind
userBinSearch
userDeleteAttribute
userModifyAttribute
userOrgInfo
userSearch
userValidateXML

AOSI SOAP

- https://www.aaiedu.hr/za-maticne-ustanove/programska-podrska/aplikacija-za-odrzavanje-sadrzaja-imenika-aosi
- https://www.aaiedu.hr/sites/default/files/content_files/docs/aosi_wsdl.html

https://vasa-domena.hr/AOSI
https://vasa-domena.hr/AOSI?wsdl

AOSI SOAP

ldapAddUserLE:

Zahtjev: (tns:ldapAddUserRequest)

user	xsd:string	UID korisnika u imeniku (npr. 'testa').
password	xsd:string	Lozinka korisnika u imeniku (Base 64 enkodirano).
base	xsd:string	Base DN imenika (npr. 'dc=srce,dc=hr').
xml	xsd:string	Podaci u XML obliku (XML Schema Definition: http://www.aaiedu.hr/aosi/ldap.xsd).

Odgovor: (tns:ldapModifyResponse)

code	xsd:int	Kod rezultata. Nula (0) označava uspješnu operaciju, pozitivne vrijednosti su greške iz imenika, negativne vrijednosti su greške u web servisu.
error	SOAP-ENC:base64	Opis greške ako kod rezultata nije nula.
result	SOAP-ENC:base64	Obavijest o uspješnosti akcije u XML obliku (XML Schema Definition: http://www.aaiedu.hr/aosi/ldap.xsd).

AOSI SOAP

```
$user=‘horvat';
$pwd=‘xX3F7Nn0';
$password=base64_encode($pwd);
$base='dc=srce,dc=hr';
$filter='(uid=pero)';
$attributes = array('uid','mail','givenname','cn');
$attribute = implode(',', $attributes);
```

AOSI SOAP

```
$opts = array(
        'location' => 'https://domena.hr/AOSI',
            'uri' => 'urn:AOSI'
    );

$client = new SOAPClient(null, $opts);
$result = $client->__soapCall("userSearch", array($user,$password, $base, $filter, $attribute) );

print_r($result);
```

AOSI SOAP

```
Array
(
    [code] => 49
    [error] => Invalid credentials
    [result] => <?xml version="1.0"?><ldap></ldap>
)
```

AOSI SOAP

Array

(

[code] => 0

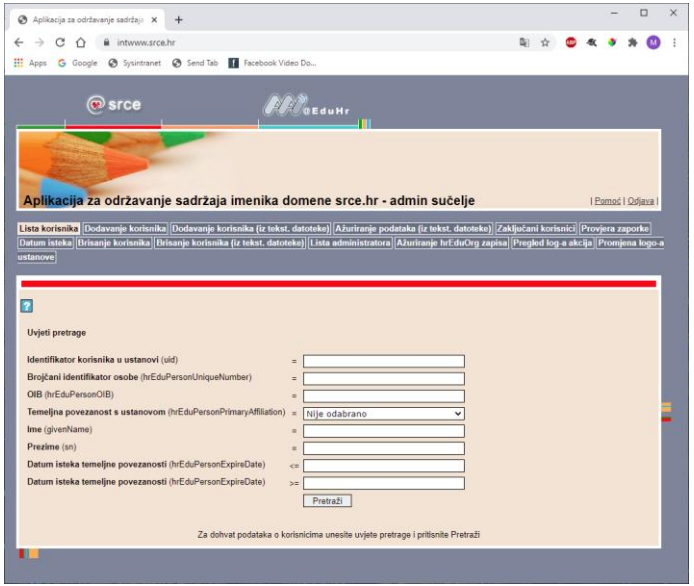
[error] =>

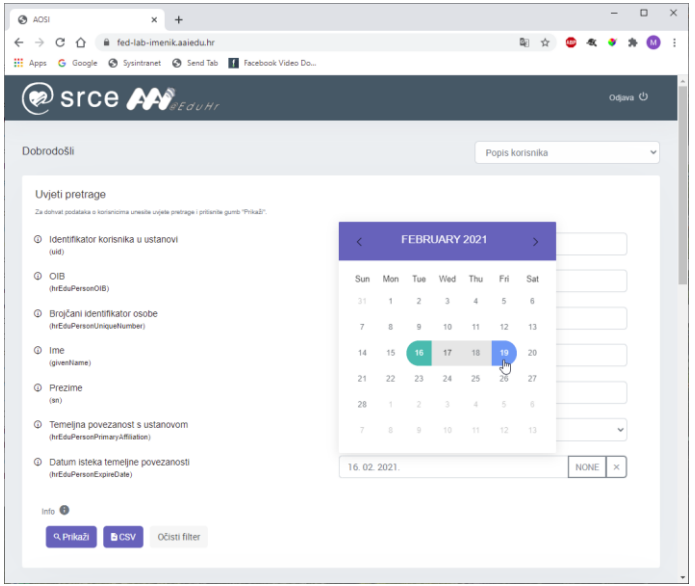
[result] => <?xml version="1.0"?><ldap><entry dn="uid=pero,dc=srce,dc=hr"><attribute ldapname="uid"><value>pero</value></attribute><attribute ldapname="givenName"><value>Pero</value></attribute><attribute ldapname="mail"><value>pero@srce.hr</value></attribute><attribute ldapname="cn"><value>Pero Perić</value></attribute></entry></ldap>

)

Modernije sučelje bazirano na okosnici Twitter Bootstrap

- Jednostavnost, prepoznatljivost, konzistentnost



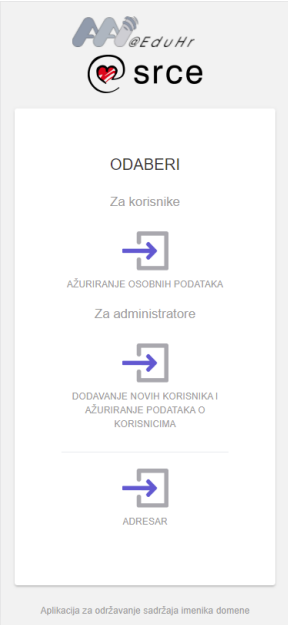


Modernije sučelje bazirano na okosnici Twitter Bootstrap

- Responzivnost

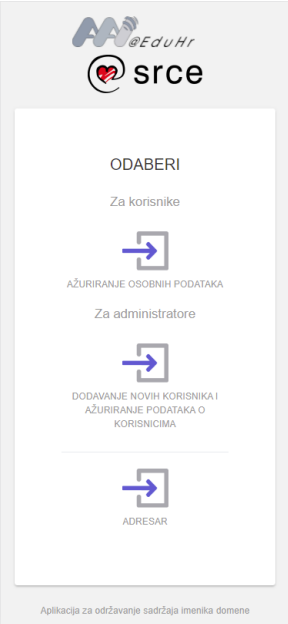
Modernije sučelje bazirano na okosnici Twitter Bootstrap

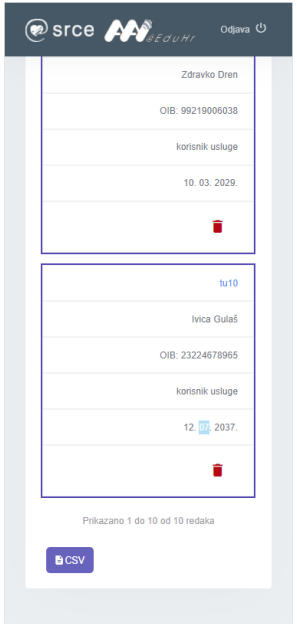
- Responzivnost



Modernije sučelje bazirano na okosnici Twitter Bootstrap

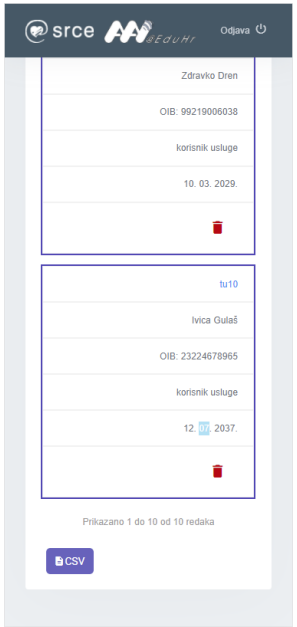
- Responzivnost

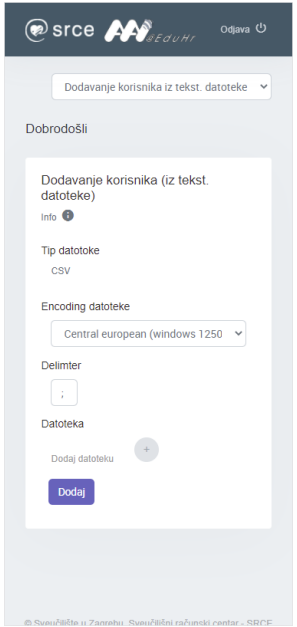




Modernije sučelje bazirano na okosnici Twitter Bootstrap

- Responzivnost





Za kraj

- Pitanja?
- OpenID Connect (OIDC) - novi protokol za autentikaciju korisnika
- Teme za sljedeće webinare?

Hvala na pažnji

Srce, AAI@EduHr tim, 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