Demistificirani AAI@EduHr za developere

Dubravko Vončina

Dani e-infrastrukture, travanj 2017.

srce
Sveučilište u Zagrebu
Sveučilišni računski centar

Predstavljanje

Predavač:

- Dubravko Vončina
- Srce, Sektor za posredničke sustave i podatkovne usluge
- Zaposlen u Srcu od 2003. godine, u početku na razvoju internih informacijskih servisa te razvoju i održavanju programske podrške za potrebe sustava CARNetovih modemskih ulaza, od 2006. godine član AAI@EduHr razvojnog tima;

Predstavljanje polaznika:

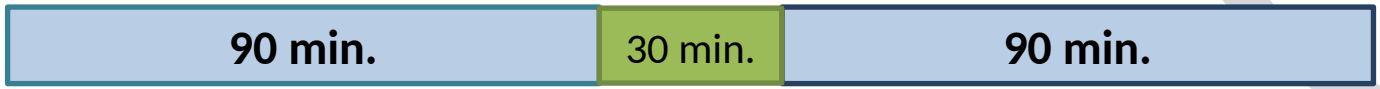
- Ime i prezime, ustanova
- Očekivanja od radionice
- Dosadašnje iskustvo

Sadržaj radionice

- Općenito o sustavu AAI@EduHr;
- AAI@EduHr (SAML) SSO autentikacija na različitim platformama;
- Alati i servisi za developere;
- Za one kojima sustav AAI@EduHr nije dovoljan;
- Novosti u 2017. godini;
- Pitanja, prijedlozi, komentari...

Plan rada

- Trajanje: do 4 šk. sata;
- Pregled satnice (pauze, završetak):

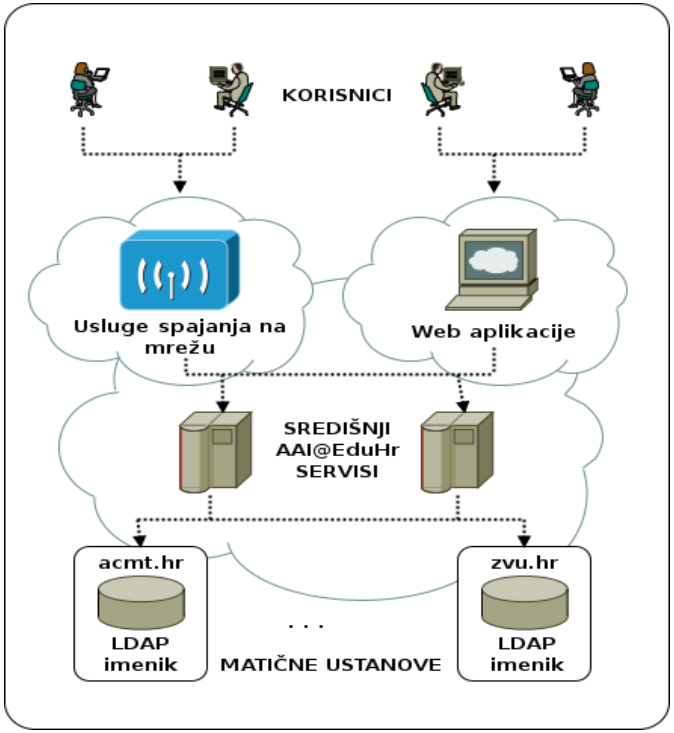


- Način izvedbe: PowerPoint prezentacija s praktičnim primjerima i odgovorima na pitanja polaznika;

Prije nego što počnemo...

- U slučaju telefonskog poziva ili neke druge neplanirane situacije slobodno možete napustiti učionicu u bilo kojem trenutku (WC se nalazi niz stepenice lijevo, pored Srce Helpdeska);
- Radionica je zamišljena kao PowerPoint prezentacija kombinirana s primjerima implementacije novih i napredni(ji)h funkcionalnosti središnjeg autenikacijskog servisa, te odgovorima na pitanja koja polaznici postavljaju tijekom radionice;
- Radionica je namijenjena i polaznicima koji se prvi put susreću sa sustavom AAI@EduHr, kao i već iskusnijim korisnicima sustava. Trajanje radionice ovisit će i o količini pitanja. Budete li imali bilo kakvih pitanja ili primjedbi, slobodno me prekinite u bilo kojem trenutku;

AAI@EduHr za početnike



- Autentikacijska i autorizacijska infrastruktura sustava znanosti i (visokog) obrazovanja u Republici Hrvatskoj;
- U produkciji od 1. ožujka 2006. godine;
- Hub-and-spoke arhitektura;
- Povezana s globalnim i nacionalnim autentikacijsko-autorizacijskim sustavima: eduroam, eduGAIN i NIAS (e-Građani)
- Web: http://www.aaiedu.hr
- E-mail: aai@srce.hr

Sustav AAI@EduHr kroz brojeve

- **231 matična ustanova, više od 877.000 elektroničkih identiteta:**

  http://www.aaiedu.hr/statistika-i-stanje-sustava/maticne-ustanove/statusi-servisa

- **88 davatelja usluga pristupa mreži:**

  http://www.aaiedu.hr/statistika-i-stanje-sustava/usluge-pristupa-mrezi

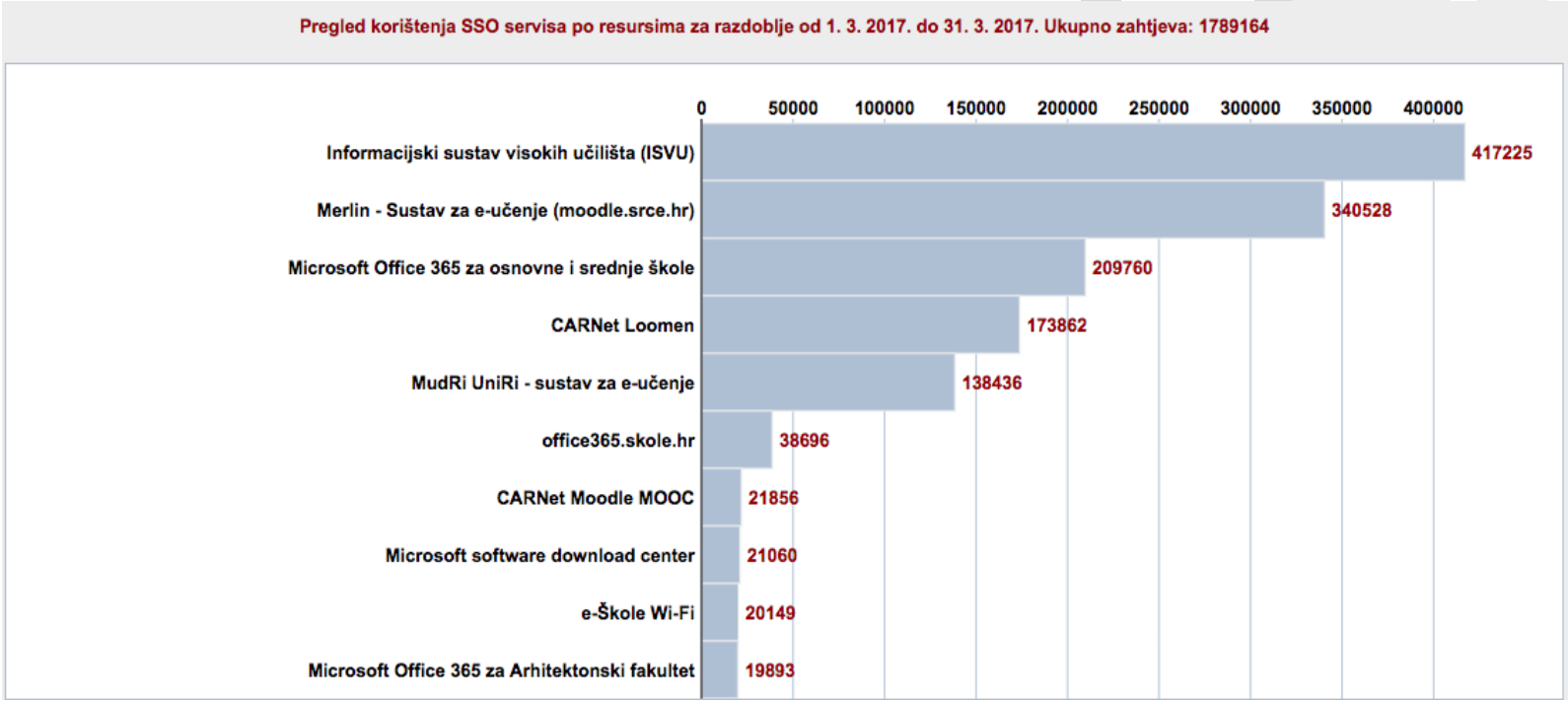
- **Više od 500 web aplikacija koje koriste AAI@EduHr SSO servis za autentikaciju korisnika:**

  http://www.aaiedu.hr/statistika-i-stanje-sustava/web-aplikacije

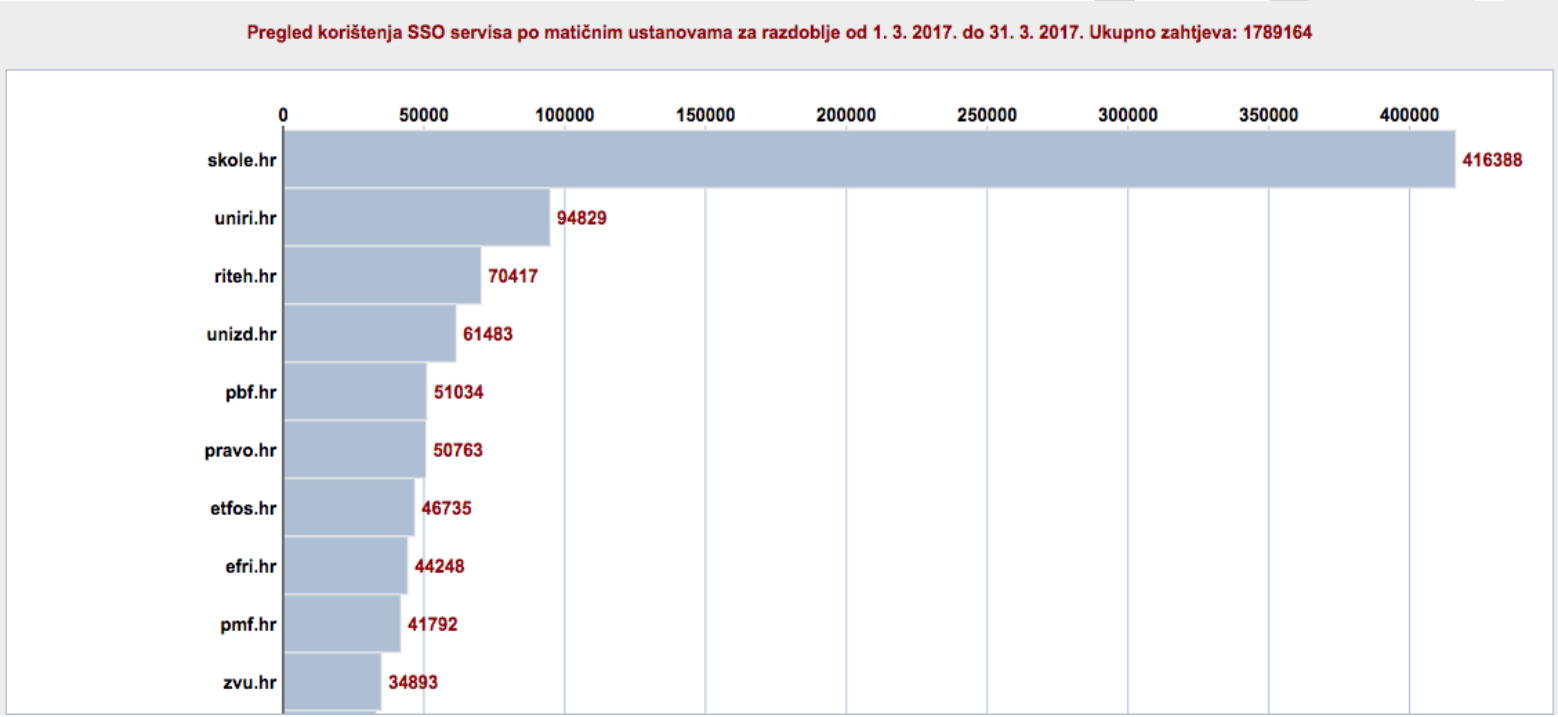
- **Tijekom zadnjih 30 dana:**
  - 17.602.200 uspješnih RADIUS autentikacija
  - 4.339.900 uspješnih FWS autentikacija
  - 1.590.330 uspješnih SSO autentikacija

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

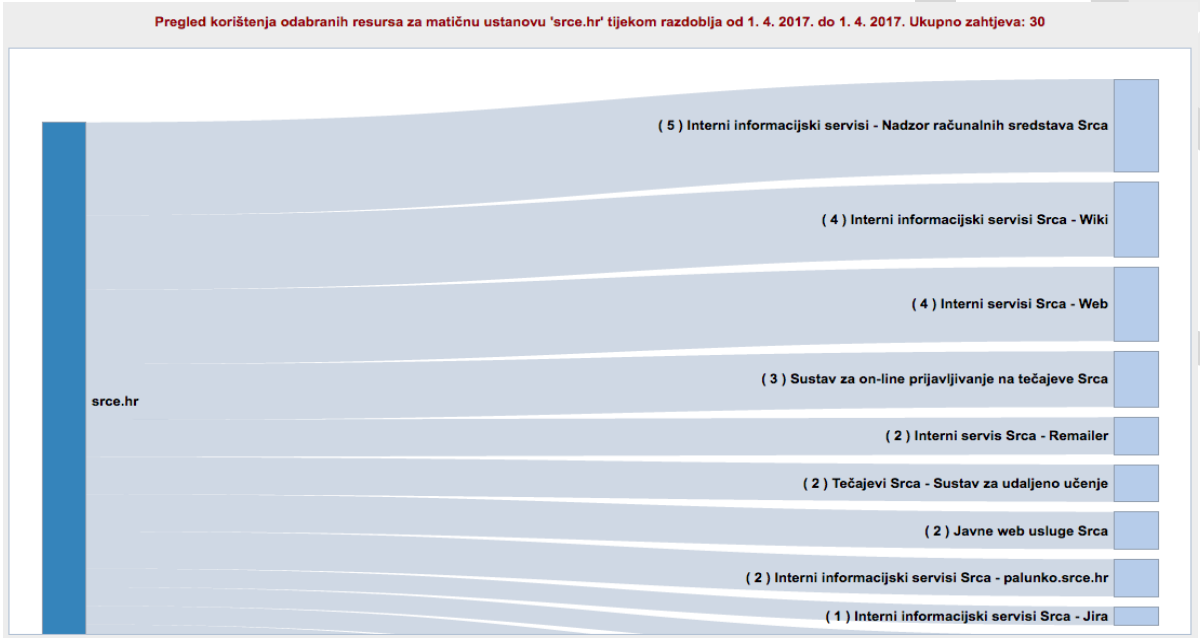
Najveći korisnici SSO servisa (aplikacije)



Najveći korisnici SSO servisa (mat. ustanove)



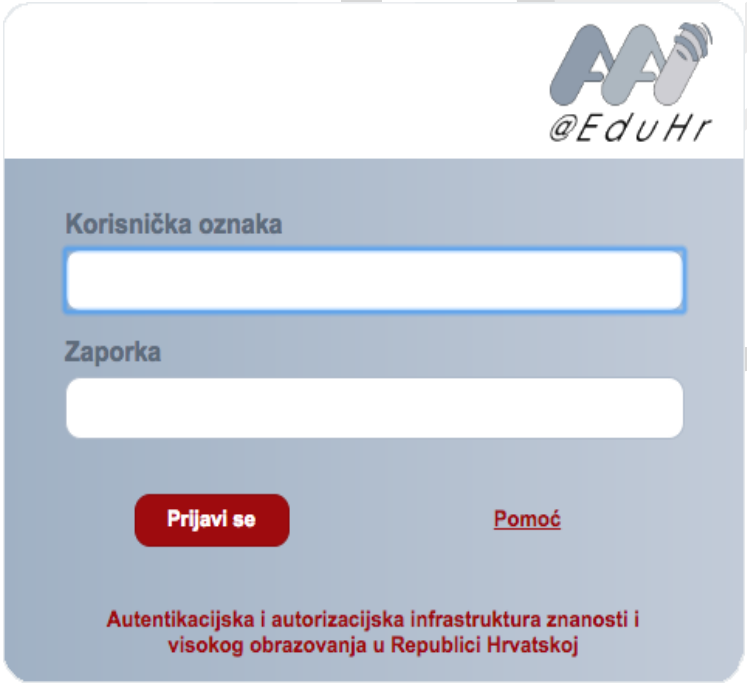
Pregled statistika u realnom vremenu



http://f-ticks.aaiedu.hr/statistike/admin/

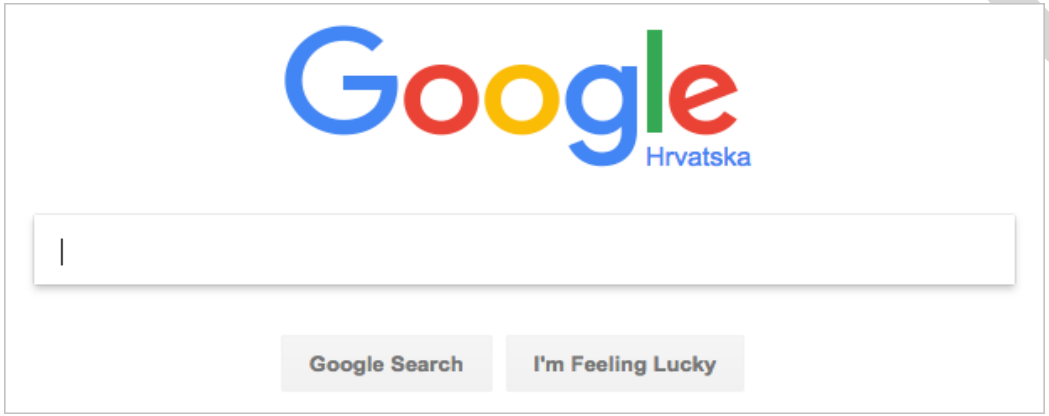
Središnji autentikacijski servisi

Što je tu komplicirano, pa to su samo dva polja?

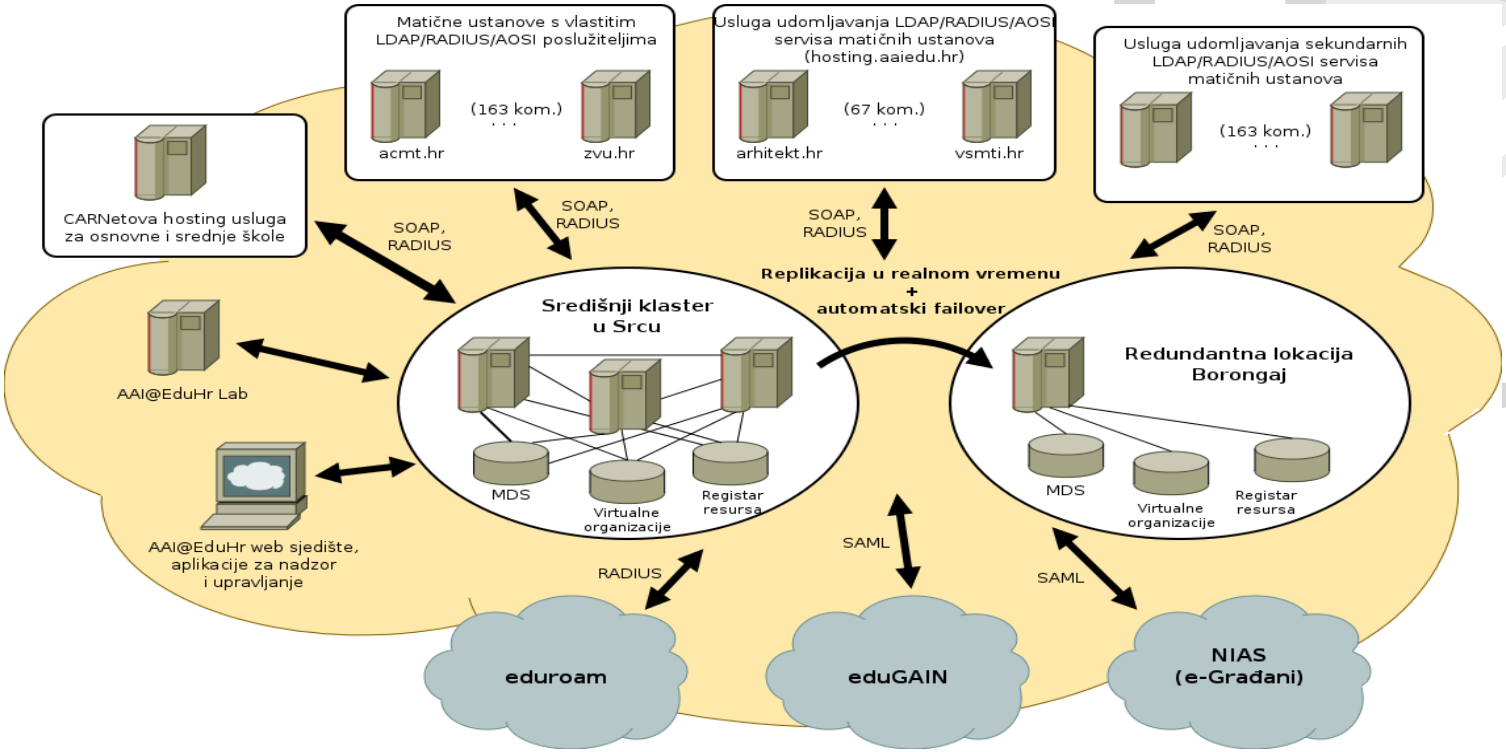


Središnji autenikacijski servisi

Ovi su još gori, imaju samo jedno polje...



Arhitektura sustava AAI@EduHr



Središnji poslužitelji sustava AAI@EduHr

- **Tri poslužitelja u klasteru u Srcu + jedan na izdvojenoj lokaciji (Borongaj);**
- **Servisi:**
  - **Središnji (posrednički) RADIUS poslužitelji:**
    - Prosljeđuju autentikacijske zahtjeve dobivene od RADIUS poslužitelja usluge odgovarajućem RADIUS poslužitelju matične ustanove te dobiveni odgovor vraćaju natrag RADIUS poslužitelju ustanove;
    - Pronalaze odgovarajući RADIUS poslužitelj matične ustanove na osnovu domene u korisničkoj oznaci te podataka pohranjenih u MDS bazi;
    - U slučaju nedostupnosti primarnog RADIUS poslužitelja matične ustanove, autentikacijski zahtjev prosljeđuju sekundarnom poslužitelju;
    - NavisRADIUS;
  - **Federacijski Web Servis (FWS):**
    - SOAP over HTTPS;
    - Slično kao i središnji RADIUS poslužitelji, na osnovu korisničke oznake i podataka u MDS bazi autentikacijske zahtjeve prosljeđuje odgovarajućem AOSI web servisu matične ustanove te u slučaju uspješne autentikacije vraća korisničke atribute;
    - Razvijen u Srcu, nije izravno dostupan davateljima usluga;

Središnji poslužitelji sustava AAI@EduHr (2)

- **Servisi (nastavak):**
  - **Središnja baza metapodataka (MDS):**
    - Baza podataka o matičnim ustanovama - davateljima elektroničkih identiteta u sustavu AAI@EduHr;
    - Podaci o RADIUS, LDAP, AOSI komponentama davatelja elektroničkih identiteta;
    - Ključan servis sustava;
    - MySQL;
  - **Sustav jedinstvene autentikacije korisnika (SSO):**
    - SAML 2.0, SimpleSAMLphp, Shibboleth;
    - Zahtjeve za autentikacijom prosljeđuje Federacijskom web servisu, u slučaju uspješne autentikacije korisnika aplikaciji vraća korisničke atribute;
    - Filtrira atribute ovisno o podacime evidentiranim u Registru resursa;
    - Visok stupanj zaštite povjerljivih korisničkih podataka (korisnička zaporka nikada se ne isporučuje davatelju usluge);
    - Omogućuje povezivanje s vanjskim nacionalnim i međunarodnim autentikacijsko-autorizacijskim infrastrukturama (NIAS, eduGAIN);

Što ako dođe do ispada središnjih servisa?

- **Središnji servisi sustava AAI@EduHr:**
  - Realizirani kao klaster od tri poslužitelja (čvora) smještena u Srcu;
  - U slučaju ispada bilo kojeg čvora preostali čvorovi preuzimaju njegovu funkciju;
  - U slučaju ispada cijelog klastera sve funkcije preuzima poslužitelj na izdvojenoj lokaciji - novi podatkovni centar Srca na Borongaju;
- **Izdvojena lokacija na Borongaju:**
  - U produkciji od rujna 2015 godine;
  - Svi podaci ključni za funkcioniranje središnjih AAI@EduHr servisa repliciraju se u realnom vremenu;
  - Seljenje je potpuno automatsko i neprimjetno za korisnike (u nekoliko navrata provjereno u praksi);
- **Nadzor:**
  - Dostupnost SSO servisa nadziru tri međusobno neovisna poslužitelja - jedan iz mreže Srca, jedan iz CARNetove mreže i jedan izvan CARNetove mreže;
  - Redundantni servisi na Borongaju aktiviraju se u slučaju da barem dva od tri nadzorna servisa zaključe da SSO servis nije dostupan;

Imeničke sheme i šifrarnici

- U sustavu AAI@EduHr definirane su dvije LDAP imeničke sheme: hrEduPerson i HrEduOrg;
- Imeničke sheme definirane su na temelju međunarodnih iskustava i lokalnih potreba;
- Aktualni popis svih atributa dostupan je na adresi:
  - http://www.aaiedu.hr/o-sustavu/imenicke-sheme/shema
- Aktualni šifrarnici dostupni su na adresi:
  - http://www.aaiedu.hr/o-sustavu/imenicke-sheme/sifrarnici
- Razmjerno mali (ograničen) skup korisničkih podataka da bi se osigurao brzi rad autentikacijskih servisa i urednost podataka u LDAP imenicima matičnih ustanova;

Imeničke sheme i šifrarnici (2)

- Sustav AAI@EduHr aplikaciji za svakog autenticiranog korisnika uvijek može isporučiti sljedeće atribute:
  - **hrEduPersonUniqueID** - korisnička oznaka;
  - **uid** - lokalni identifikator korisnika u ustanovi;
  - **cn** - ime i prezime;
  - **givenName** - ime;
  - **sn** - prezime;
  - **mail** - elektronička adresa;
  - **hrEduPersonUniqueNumber** - jedinstveni brojčani identifikator korisnika;
  - **hrEduPersonOIB** - osobni identifikacijski broj (OIB);
  - **hrEduPersonAffiliation** - povezanost s ustanovom;
  - **hrEduPersonPrimaryAffiliation** - temeljna povezanost s ustanovom;
  - **hrEduPersonExpireDate** - datum isteka temeljne povezanosti;
  - **hrEduPersonPersistentID** - trajna nepromjenljiva korisnička oznaka;

Imeničke sheme i šifrarnici (3)

- Sustav AAI@EduHr aplikaciji za svakog autenticiranog korisnika uvijek može isporučiti sljedeće atribute (nastavak):
  - **o** - puni službeni naziv matične ustanove;
  - **hrEduPersonHomeOrg** - oznaka (LDAP domena) matične ustanove;
  - **postalAddress** - službena poštanska adresa matične ustanove;
  - **l** - mjesto (lokalitet);
- Poželjno je aplikacije ograničiti na prethodno naveden skup korisničkih atributa;
- Ostale, opcionalne podatke definirane hrEdu imeničkim shemama sustav može isporučiti ovisno o tome jesu li uneseni u LDAP imenik i jesu li u konfiguraciji LDAP imenika matične ustanove postavljene odgovarajuće dozvole;

Certificiranje matičnih ustanova i resursa

Zašto iz godine u godinu administratore LDAP imenika i davatelje usluga gnjavimo certifiranjem matičnih usluga i resursa u sustavu AAI@EduHr?

Certificiranje matičnih ustanova i resursa (2)

Zato što možemo!!!

Certificiranje matičnih ustanova i resursa (3)

I zato što moramo...

Certificiranje matičnih ustanova i resursa (4)

- Redovna godišnja certificiranja Srce provodi s ciljem osiguravanja točnih i pouzdanih podataka u LDAP imenicima matičnih ustanova te u Registru resursa u sustavu AAI@EduHr. Certificiranjem se, između ostaloga, nastoji:
  - osigurati siguran i pouzdan rad osnovnih AAI@EduHr servisa (LDAP, RADIUS, AOSI) matičnih ustanova u sustavu AAI@EduHr;
  - osigurati da su u LDAP imenicima matičnih ustanova pohranjeni isključivo elektronički identiteti korisnika koji imaju pravo na elektronički identitet u sustavu AAI@EduHr;
  - za krajnje korisnike osigurati što kvalitetnije informacije o mrežnim resursima i aplikacijama koje za autentikaciju i autorizaciju korisnika koriste AAI@EduHr infrastrukturu;
- Uključivanjem u nacionalne (NIAS) i međunarodne (eduroam, eduGAIN) autentikacijsko-autorizacijske sustave Srce se kao koordinator sustava AAI@EduHr obvezalo osigurati provedbu sigurnosnih normi koje nameću ti sustavi;
- Srce u Ministarstvo znanosti i obrazovanja redovno šalje godišnje izveštaje o stanju AAI@EduHr infrastrukture. Za slučaj da te izvještaje u Ministarstvu (ipak) netko čita, poželjno je da informacije u izvještajima budu točne i pouzdane, a jedan od načina za osiguravanje točnosti podataka su i aktivnosti koje se provode tijekom redovnih godišnjih certificiranja;

Alati i servisi za developere

- Lokalna autentikacija putem AOSI web servisa matične ustanove;
- Security Assertion Markup Language (SAML) i sustav jedinstvene autentikacije korisnika;
- Programska podrška za autentikaciju putem sustava AAI@EduHr;
- Registar resursa;
- Vanjski repozitoriji atributa - Virtualne organizacije;
- Okruženje za razvoj i testiranje - AAI@EduHr Lab;

Što ako će se aplikacija koristiti samo na jednoj ustanovi?

- **Za autentikaciju se može koristiti i lokalna Aplikacija za održavanje imenika (AOSI) matične ustanove;**
- **Klasični SOAP over HTTPS web servis, napisan u Perl-u;**
- **Za razliku od SSO servisa, omogućuje dvosmjernu komunikaciju s LDAP imenikom:**
  - autentikacija korisnika i dohvat korisničkih podataka;
  - ažuriranje podataka u LDAP imeniku;
- http://www.aaiedu.hr/za-maticne-ustanove/programska-podrska/aplikacija-za-odrzavanje-sadrzaja-imenika-aosi
- http://www.aaiedu.hr/sites/default/files/content_files/docs/aosi_wsdl.html
- **Proširiv programskim dodacima (modulima, odnosno plugin-ovima), mogućnost okidanja akcija:**
  - beforeAddUser
  - afterAddUser
  - beforeDeleteUser
  - afterDeleteUser
  - beforeChangeAttribute
  - afterChangeAttribute
- http://www.aaiedu.hr/za-maticne-ustanove/programska-podrska/kako-pisati-module-za-aosi

Sustav jedinstvene autentikacije korisnika (Single Sign-On)

- Autentikacijski mehanizam koji omogućuje da se korisnik u sustav prijavi samo jednom i nakon toga pristupa svim aplikacijama koje koriste SSO servis bez potrebe za ponovnim unosom korisničke oznake i zaporke;
- Znatno poboljšava doživljaj korisnika prilikom prijavljivanja u veći broj aplikacija, za prijavu u sve aplikacije korisnik rabi isti elektronički identitet;
- Za implementaciju Single Sign-On funkcionalnosti u sustavu AAI@EduHr koristi se Security Assertion Markup Language (SAML 2.0) - tehnologija temeljena na XML standardu koja definira standardni okvir za formatiranje i razmjenu poruka korištenih za autentikaciju i autorizaciju korisnika te prijenos korisničkih podataka;
- Jedini podržani način autentikacije za web aplikacije koje žele koristiti sustav AAI@EduHr za autentikaciju korisnika;
- Uporaba SAML 2.0 standarda omogućuje povezivanje sustava AAI@EduHr s nacionalnim (NIAS) i međunarodnim (eduGAIN) autentikacijsko-autorizacijskim infrastrukturama;

Koliko je siguran AAI@EduHr SSO servis?

- SAML tehnologija omogućuje da se povjerljivi korisnički podaci (zaporka) nikada ne prosljeđuju davateljima usluga;
- Jednom godišnje provodi se redovito certificiranje matičnih ustanova čime se osigurava visoka razina kvalitete korisničkih podataka u imenicima, provjerava razina sigurnosti instalirane programske podrške te procedura vezanih uz otvaranje elektroničkih identiteta;
- AAI@EduHr infrastruktura je prošla certificiranje FINA-e i zadovoljila sve kriterije za uključivanje u sustav e-Građani;
- I velike međunarodne tvrtke (Microsoft, Google, online baze podataka) omogućavaju prijavu korisnika putem AAI@EduHr SSO servisa za pristup svojim uslugama;
- Od 2017. godine implementirana politika obavezne promjene zaporke - mehanizam koji korisnicima nameće obavezu promjene zaporke odmah po otvaranju elektroničkog identiteta te nakon što im administrator promjeni zaporku;

Koliko je pouzdan AAI@EduHr SSO servis?

- Koristi ga sustav ISVU za prijavu na studomat i ostale aplikacije;
- Koristi ga nekoliko velikih sustava za e-učenje (Merlin, Loomen, MudRi) kod kojih su zbog online polaganja ispita pouzdanost i raspoloživost središnjeg autentikacijskog servisa iznimno važne;
- Sam sustav jedinstvene autentikacije realiziran je kao klaster poslužitelja s implementiranom “failover” funkcionalnošću;
- Implementiran je kontinuirani nadzor središnjih autentkacijskih servisa i lokalnih imeničkih servisa na matičnim ustanovama;
- Većina matičnih ustanova ima i sekundarni LDAP imenik, cilj je s vremenom postići da sve matične ustanove u sustavu AAI@EduHr imaju uspostavljen i sekundarni imenik;
- Osigurana je potpuna redundancija SSO servisa na poslužitelju na izdvojenoj lokaciji podatkovnog centra Srca na kampusu Borongaj;

Što je sve potrebno napraviti da bi aplikacija mogla koristiti AAI@EduHr SSO?

- Prijaviti (registrirati) aplikaciju u sustavu AAI@EduHr putem online registra resursa:

  http://www.aaiedu.hr/node/80#p1

- Davatelji usluga (vlasnici aplikacija) koji nisu u sustavu znanosti i visokog obrazovanja moraju se registrirati kao partneri AAI@EduHr federacije:

  http://www.aaiedu.hr/za-davatelje-usluga/cesto-postavljana-pitanja/kako-postati-partner-aaieduhr-federacije

- Proučiti dokumentaciju i implementirati odgovarajuću programsku podršku, odnosno autentikacijski modul za autentikaciju putem AAI@EduHr SSO servisa:

  http://www.aaiedu.hr/za-davatelje-usluga/za-web-aplikacije

Koliko je komplicirano implementirati SSO autentikaciju u aplikacijama?

```
<?php

    require_once('/usr/share/simplesamlphp/lib/_autoload.php');

    $as = new SimpleSAML_Auth_Simple('default-sp');

    $as->requireAuth();

    $attributes = $as->getAttributes();

?>
```

Koje sve platforme i programski jezici su podržani?

- PHP (SimpleSAMLphp):

  http://www.aaiedu.hr/za-davatelje-usluga/za-web-aplikacije/kako-implementirati-autentikaciju-putem-sustava-aaieduhr-u-php

- Java (Spring Security SAML):

  http://www.aaiedu.hr/o-sustavu/web-aplikacije/kako-implementirati- autentikaciju-putem-sustava-aaieduhr-u-java/

- .NET (OIOSAML.NET):

  http://www.aaiedu.hr/za-davatelje-usluga/za-web-aplikacije/implementacija-autentikacije-putem-sustava-aaieduhr-u-net-web

- Aplikacije koje koriste Shibboleth kao autentikacijski modul za implementaciju SSO autentikacije uporabom SAML 2.0 protokola;

Zašto nije podržan šiti spektar platformi i programskih jezika?

- Ograničeni ljudski resursi - najbolje su podržani programski jezici koje i sami koristimo u Srcu;
- Razvoj programskih jezika i tehnologija je toliko dinamičan da realno ne stignemo pratiti veći broj platformi i programskih jezika;

Međutim...

Korisnik 1:

Na AAI@EduHr stranicama vidim da postoji plugin za autentikaciju za Joomla 2.5. Znate li možda ima li takav plugin za Joomla verziju 3.x?

AAI@EduHr tim:

U Srcu već godinama ne koristimo CMS sustav Joomla i u tom smislu nemamo nikakvih iskustava s AAI-zacijom Joomla verzije 3.x. Međutim, kad je u pitanju odabir SAML autentikacijskog modula, u nekim drugim aplikacijama imamo dobrih iskustava s autentikacijskim modulima tvrtke 'miniorange' koja je prema svemu sudeći razvila i SAML autentikacijski modul za Joomla CMS. Osnovna verzija navedenog autentikacijskog modula je besplatna pa ako Vam je funkcionalnost te besplatne verzije dovoljna, vjerojatno Vam možemo pomoći iskonfigurirati autentikacijski modul za autentikaciju putem sustava AAI@EduHr...

Korisnik 1:

Nakon još malo dodatnih modifikacija sada nam sve radi, imamo AAI@EduHr autentikaciju na Joomli 3.6. Hvala Vam puno na pomoći.

...

Korisnik 2:

So I am trying to implement SAML support using Passport (a Node library for authentication) and passport-saml (a Passport plugin implementing SAML) in Xen Orchestra and I have some issues configuring it... Dubravko V. can you help us with this?

AAI@EduHr tim:

I've never worked with Passport or Passport-SAML framework(s), but if it doesn't support loading IdP metadata from XML file, you can try using values the other Dubravko suggested:

entryPoint: 'https://fed-lab.aaiedu.hr/ms/saml2/idp/SSOService.php'

issuer: 'xen-orc-dev'

Korisnik 2:

Evo ovo sad radi: http://xen-orc-dev.srce.hr/

Idem sad pokusati taj modul gurnut u aplikaciju.

... uglavnom:

- Gdje ima volje, ima i načina;
- To što na AAI@EduHr webu ne postoje upute za neki programski jezik ili aplikaciju ne znači da nije moguće implementirati autentikaciju putem sustava AAI@EduHr na toj platformi;
- Sada već postoji veliki broj aplikacija i programskih jezika koje podržavaju autentikaciju uporabom SAML / Shibboleth tehnologija, samo je potrebno znati na koji način iskonfigurirati SAML API;
- Potražite dostupnu dokumentaciju za SAML autentikaciju na platformi na kojoj razvijate vašu aplikaciju ili uslugu. Mi ćemo nastojati u najkraćem mogućem roku proučiti dokumentaciju i ako je ikako moguće pomoći vam implementirati autentikaciju putem sustava AAI@EduHr u vašoj aplikaciji;

Napredni alati za developere

- SAML tracer - modul za web preglednike Firefox i Chrome;
- SAML Developer Tools:

  https://www.samltool.com

Primjer:

Demonstracija kako koristiti SAML tracer.

Registar resursa u sustavu AAI@EduHr

- Web aplikacija koja služi za registraciju novih resursa, ažuriranje podataka o postojećim resursima i brisanje resursa u sustavu AAI@EduHr;
- Da bi resurs mogao koristiti sustav jedinstvene autentikacije korisnika, mora biti registriran putem Registra resursa;
- Registru mogu pristupiti samo korisnici koji u svom zapisu u LDAP imeniku imaju kao vrijednost atributa **hrEduPersonRole** postavljeno **administrator imenika** ili **CARNet sistem inženjer**, te korisnici koji su već evidentirani kao administratori podataka o nekom resursu;
- Resursi koji su registrirani kao testni za autentikaciju korisnika mogu koristiti isključivo AAI@EduHr Lab okruženje;
- http://www.aaiedu.hr/registar-resursa
- http://www.aaiedu.hr/aairr/

Najvažniji parametri prilikom registracije SSO resursa

- Ključni SAML metapodaci:
  - **entityID** - jedinstveni identifikator resursa u sustavu AAI@EduHr;
  - **AssertionConsumerService URL** - adresa na kojoj autentikacijski modul očekuje SAML autentikacijski odgovor od SSO autentikacijskog servisa;
  - **SingleLogoutService URL** - adresa na kojoj autentikacijski modul očekuje SAML Single-Logout odgovor od SSO autentikacijskog servisa (potvrdu o poništenju SSO sjednice);
- Ako se kao autentikacijski modul koristi programski alat **SimpleSAMLphp**, navedeni metapodaci obično se mogu pronaći na adresi:

  http://dns.adresa.posluzitelja/simplesaml/module.php/saml/sp/metadata.php/default-sp
- Ako se kao autentikacijski modul koristi **Shibboleth** Service Provider, metapodaci bi se trebali nalaziti na adresi:

  http://dns.adresa.posluzitelja/Shibboleth.sso/Metadata
- Ako se kao autentikacijski modul koristi **OIOSAML.NET**, metapodaci bi trebali biti na adresi:

  http://dns.adresa.posluzitelja/metadata.ashx

Kako (ne) registrirati SSO resurs

Ovakav zahtjev najvjerojatnije neće biti odobren:

Opće informacije

Naziv resursa:	Zakon!
Opis resursa:	Najbolja aplikacija na svijetu
Vrsta resursa:	produkcija

SAML metapodaci

Jedinstveni identifikator resursa (entityID):	http://www.zakon.hr
AssertionConsumerService URL:	http://www.zakon.hr
SingleLogoutService URL:	http://www.zakon.hr

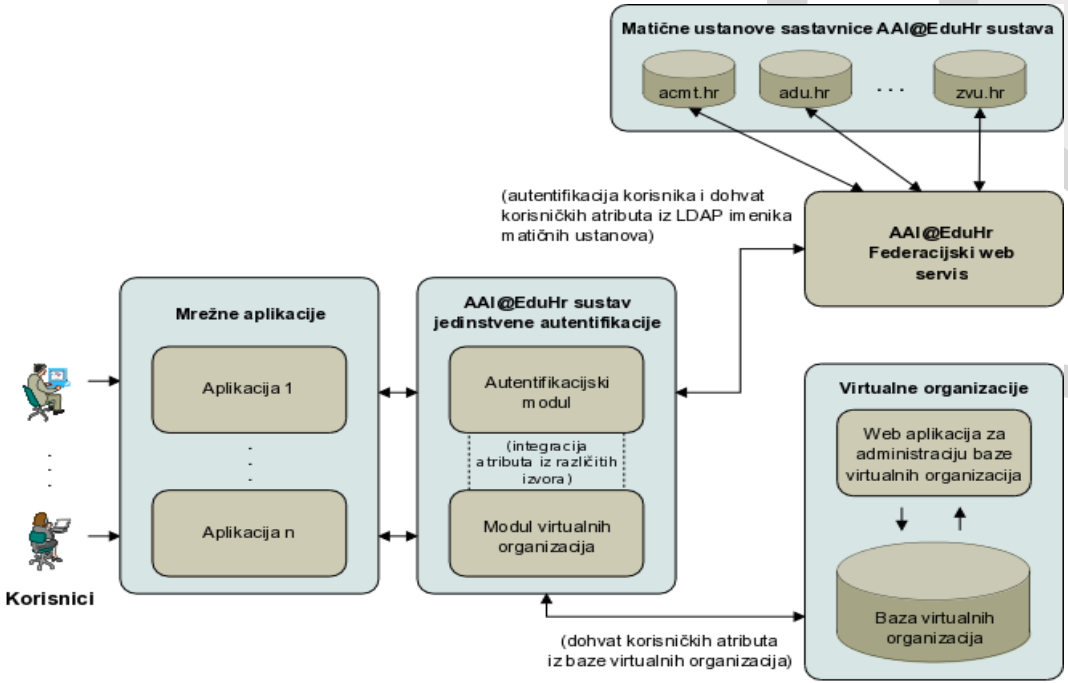
Kontakt osobe i službe

	Ime osobe ili naziv službe	Elektronička adresa	Broj telefona	Uloga
☐	Pero	pero@inet.hr		voditelj proizvoda
☐	Žiža	dugave_do_karlovca@gmail.com		tehnička podrška
☐	Beli	kajtebriga@gmail.com		podrška korisnicima

Vanjski repozitoriji atributa u sustavu AAI@EduHr

- Klasični model autentikacijsko-autorizacijske infrastrukture u kojem postoje davatelj elektroničkih identiteta i davatelj usluge ne može uvijek odgovoriti na sve potrebe davatelja usluga vezane uz podatke koji se koriste u procesu autorizacije;
- Model je potrebno proširiti dodatnim izvorima informacija - vanjskim repozitorijima atributa;
- Koncept virtualnih organizacija zamišljen je i realiziran kao vanjski repozitorij atributa koji služe kao nadopuna podacima pohranjenim u LDAP imenicima matičnih ustanova;
- Atributi pohranjeni unutar virtualne organizacije primarno se koriste za autorizaciju (kontrolu pristupa), npr. nekom zajedničkom repozitoriju dokumenata;
- Za razliku od matičnih ustanova, kod virtualnih organizacija davatelj usluge ima kontrolu nad autorizacijskim atributima;
- Implementacija u obliku dodatnog modula unutar sustava jedinstvene autentikacije korisnika - atributi iz vanjskog repozitorija stužu u SAML odgovoru nakon autentikacije korisnika;

Implementacija vanjskih repozitorija atributa



- http://www.aaiedu.hr/vo/
- http://www.aaiedu.hr/za-davatelje-usluga/virtualne-organizacije

Kako koristiti vanjski repozitorij atributa?

- **Registrirati virtualnu organizaciju;**
- **Prema potrebi definirati atribute unutar kreirane virtualne organizacije - inicijalno postoji samo atribut voMember;**
- **Odabrati usluge (aplikacije) kojima će se isporučivati atributi pohranjeni u repozitoriju virtualne organizacije;**
- **Unijeti članove virtualne organizacije:**
  - Unosom korisničke oznake kroz web sučelje;
  - Slanjem pozivnica koje sadrže pozivnicu za samoregistraciju korisnika;
  - Pozivnice mogu sadržavati jednokratnu poveznicu različitu za svakog korisnika ili jedinstvenu poveznicu koja se može koristiti više puta za učlanjivanje više članova u virtualnu organizaciju;
- **Za svakog člana virtualne organizacije moguće je postaviti više proizvoljnih atributa s proizvoljnim vrijednostima;**

AAI@EduHr Lab

- Da bi se izbjegla mogućnost eventualnog negativnog utjecaja nedovršenih aplikacija na produkcijski SSO servis (npr. nehotično izazivanje DoS napada), za aplikacije koje se nalaze u fazi razvoja na raspolaganju je AAI@EduHr Lab okruženje s testnim SSO servisom;
- Tehnološki identično produkcijskom sustavu, ali bez mogućnosti korištenja produkcijskih središnjih servisa i elektroničkih identiteta;
- Korisnički podaci se dohvaćaju iz testnih imenika u kojima elektroničke identitete mogu imati i osobe koje nemaju pravo na AAI@EduHr elektronički identitet (partneri AAI@EduHr federacije);
- Jedna osoba može zatražiti više testnih elektroničkih identiteta što u produkcijskom okruženju nije moguće:

  https://fed-lab.aaiedu.hr/zahtjev.php?show=zahtjev_identitet

AAI@EduHr Lab (2)

- Prema potrebi moguće je zatražiti i kreiranje cijelog testnog LDAP imenika nad kojim će razvijatelji aplikacije imati administratorske ovlasti:

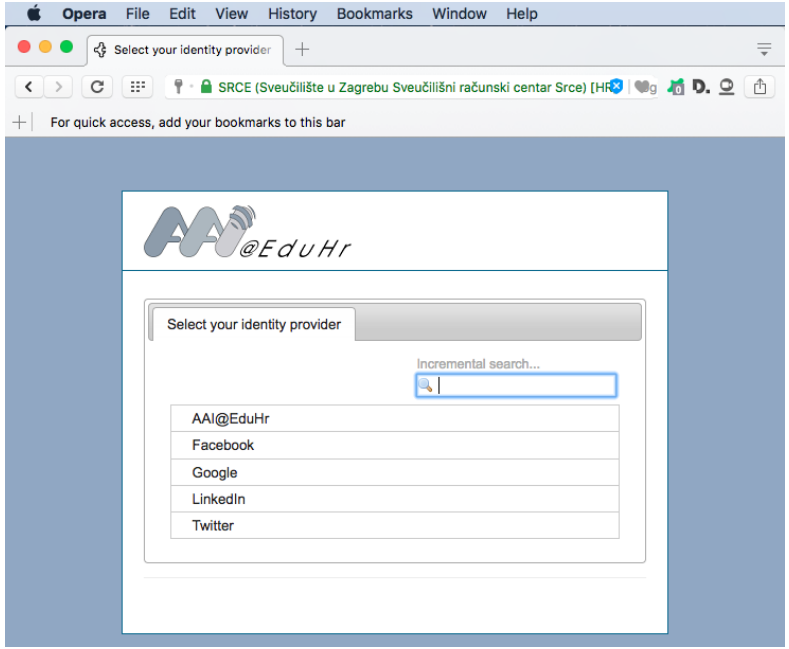
  https://fed-lab.aaiedu.hr/zahtjev.php?show=zahtjev_imenik

- Usluge koje su u Registru resursa označene kao testne mogu rabiti samo AAI@EduHr Lab okruženje;

Što je s autentikacijom za desktop i mobilne aplikacije?

- Za sada još nemamo ništa ‘opipljivo’;
- Najveći problem predstavlja činjenica da SAML protokol zahtijeva da se aplikacija nalazi na fiksnoj DNS / IP adresi;
- Usavršava se nova generacija protokola (OAuth, OpenID Connect) koji bi se najvjerojatnije mogli iskoristiti i za autentikaciju u desktop i mobilnim aplikacijama;
- Autentikacija funkcionira na način da se korisnik autenticira uporabom web preglednika, a njegov uređaj ili desktop aplikacija uporabom tokena;

Za aplikacije kojima autentikacija putem sustava AAI@EduHr nije dovoljna



- Mogućnost korištenja vanjskih autentikacijskih servisa (društvene mreže):
  - trenutno su podržani Facebook, Google, LinkedIn i Twitter;
  - prilikom dizajniranja aplikacije treba uzeti u obzir da svaki od navedenih autentikacijskih servisa ima vlastite nazive i formate atributa te da isporučuju znatno manji skup korisničkih podataka od sustava AAI@EduHr;
  - kod autentikacije uporabom društvenih mreža nema Single-Logout funkcionalnosti;
  - http://www.unizg.hr/authdemo/

Primjer:

Autentikacija putem društvenih mreža:

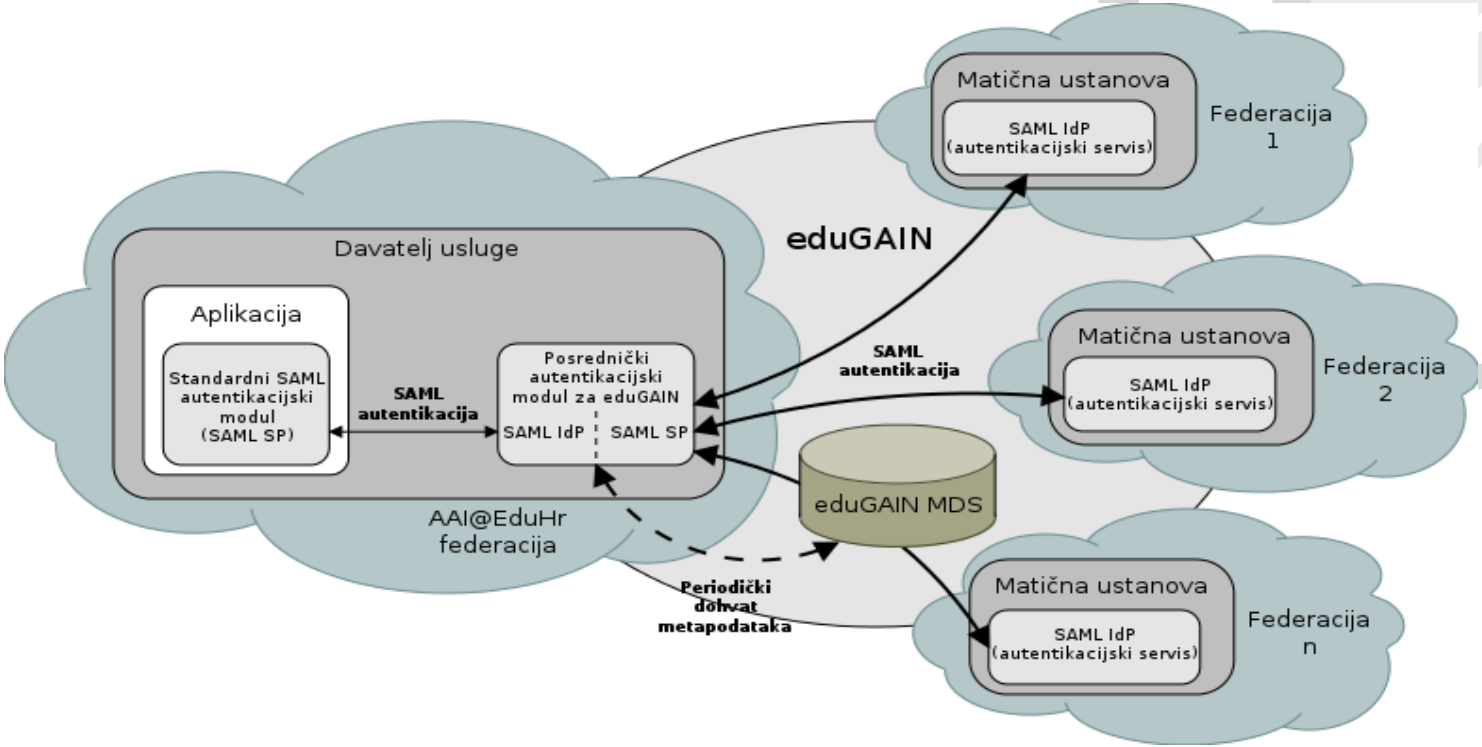
https://monitor.eduroam.org/sp/

https://monitor.eduroam.org/snbridge/

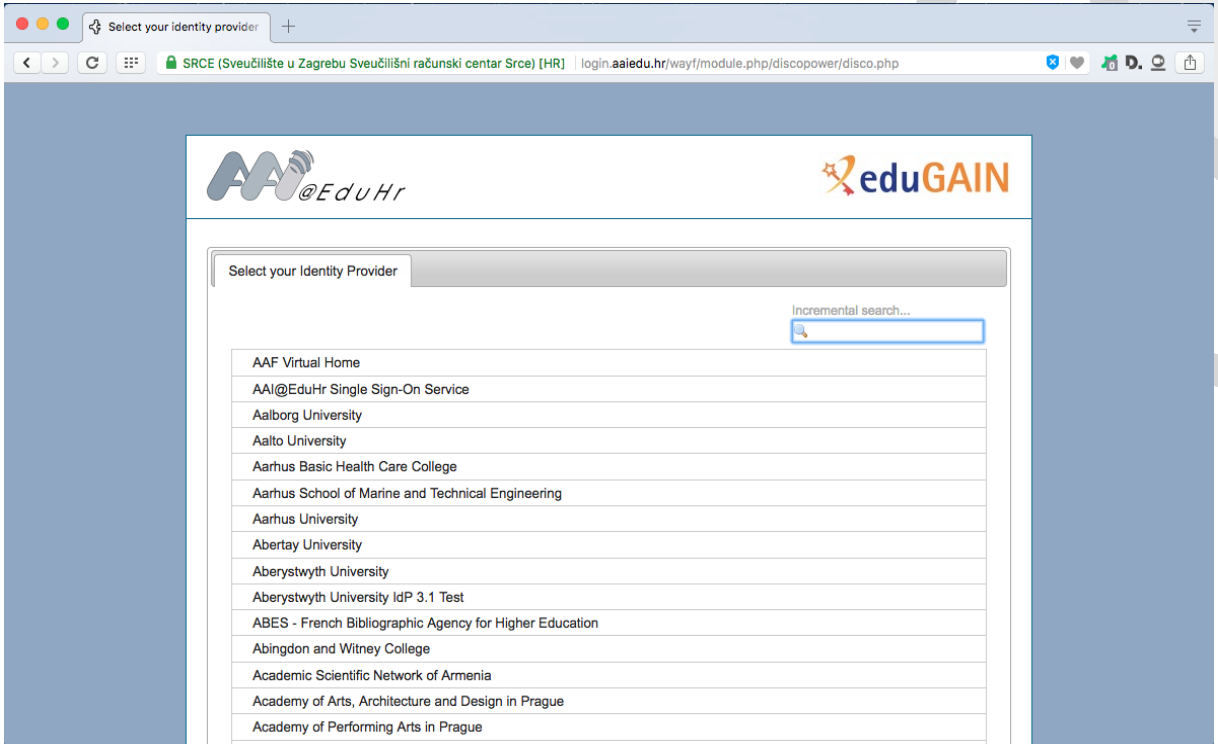
Posrednički autentikacijski modul za eduGAIN infrastrukturu

- Davatelji usluga koji žele proširiti skup korisnika izvan okvira sustava AAI@EduHr, osim društvenih mreža za autentikaciju korisnika mogu koristiti eduGAIN infrastrukturu;
- eduGAIN - interfederacijski servis koji na međunarodnoj razini povezuje davatelje usluga s davateljima elektroničkih identiteta iz akademske i istraživačke zajednice;
- https://www.geant.org/Services/Trust_identity_and_security/eduGAIN
- posrednički autentikacijski modul za eduGAIN infrastrukturu realiziran je kao modificirana verzija programskog alata SimpleSAMLphp (poželjno ga je instalirati u LAMP okruženju) jer je to u ovom trenutku jedini način da se u potpunosti zadovolje svi tehnički i informacijski preduvjeti koje sustav eduGAIN nameće;

Posrednički autentikacijski modul za eduGAIN infrastrukturu (2)



Posrednički autentikacijski modul za eduGAIN infrastrukturu (3)



Posrednički autentikacijski modul za eduGAIN infrastrukturu (4)

- **Korisnički atributi koje isporučuju davatelji elektroničkih identiteta u sustavu eduGAIN, uključujući i AAI@EduHr SSO servis:**
  - urn:oid:2.16.840.1.113730.3.1.241 (displayName)
  - urn:oid:2.5.4.3 (common name, cn)
  - urn:oid:0.9.2342.19200300.100.1.3 (mail)
  - urn:oid:1.3.6.1.4.1.5923.1.1.1.1 (eduPersonAffiliation)
  - urn:oid:1.3.6.1.4.1.5923.1.1.1.9 (eduPersonScopedAffiliation)
  - urn:oid:1.3.6.1.4.1.5923.1.1.1.6 (eduPersonPrincipalName)
  - urn:oid:1.3.6.1.4.1.5923.1.1.1.10 (eduPersonTargetedID)
  - urn:oid:1.3.6.1.4.1.25178.1.2.9 (schacHomeOrganization)
- **Za razliku od sustava AAI@EduHr, davatelji elektroničkih identiteta u sustavu eduGAIN nemaju obvezu isporuke svih navedenih atributa;**
- **Posrednički autentikacijski modul i pripadajuće upute bit će objavljeni tijekom travnja;**

Primjer:

Autentikacija putem sustava eduGAIN:

https://edugain-rnd.srce.hr/wayf/

Novosti u 2017. godini

- **Ukida se usluga lokalnog repozitorija SKS PGP ključeva:**
  - http://pks.aaiedu.hr
  - analiza korištenja usluge pokazuje da korištenje već godinama stagnira ili opada - ne isplati se ulagati u novi hardver;
  - podaci neće biti izgubljeni, već će ih biti moguće dohvatiti iz nekog drugog repozitorija PGP ključeva;
- **Obavezna primjena “password policy” funkcionalnosti za sve matične ustanove u sustavu AAI@EduHr:**
  - od ove godine svi davatelji elektroničkih identiteta morat će imati implementiranu funkcionalnost obavezne promjene korisničke zaporke;
  - korisnici zaporku mogu promijeniti preko AOSI web sučelja za administraciju LDAP imenika ili preko web stranice https://login.aaiedu.hr/promjenazaporke/
  - bez implementiranog mehanizma obavezne promjene zaporke matične ustanove **neće moći proći certificiranje** tijekom svibnja i lipnja;
  - mehanizam obavezne promjene zaporke podržan je samo na **Debian Jessie** distribuciji;

Novosti u 2017. godini (2)

- **U suradnji s CARNetom realiziran prototip autentikacijskog servisa za višestupanjsku autentikaciju korisnika:**
  - kombinirana autentikacija uporabom AAI@EduHr elektroničkog identiteta u prvom i CARNetovog token servisa u drugom koraku;
  - za autentikaciju se i dalje koristi standardni SAML SSO profil - nisu potrebne nikakve značajnije tehničke modifikacije na strani davatelja usluga;
  - očekivano uvođenje u produkciju tijekom 2017. godine;
- **Napravljena je programska podrška i upute za uključivanje aplikacija u eduGAIN infrastrukturu:**
  - opisano na nekoliko prethodnih slajdova;
  - već se koristi u produkciji za neke od usluga koje Srce pruža međunarodnoj zajednici: eduroam monitoring servisi i eduroam Configuration Assistant Tool;
  - zbog tehničkih “izazova” (SSL enkripcija) posrednički autentikacijski modul i pripadajuće upute bit će javno objavljeni nakon što migriramo središnje AAI@EduHr servise na novi hardver i operacijski sustav (očekivano tijekom travnja);

Novosti u 2017. godini (3)

- **Povezivanje sustava AAI@EduHr s eIDAS infrastrukturom:**
  - eIDAS - EU regulation on electronic identification and trust services for electronic transactions in the internal market;
  - slično kao Nacionalni Identifikacijski i Autentifikacijski Sustav (NIAS / e-Građani), ali na razini Europske Unije;
  - u sklopu projekta Srce planira ponuditi Home for Homeless uslugu (projekt: “Ubožnica”) za osobe koje imaju pravo na elektronički identitet u sustavu AAI@EduHr, ali nisu zaposleni u sustavu znanosti i visokog obrazovanja u RH. Takvi korisnici elektronički identitet u sustavu AAI@EduHr moći će zatražiti elektroničkim putem, uporabom elektroničkog identiteta dobivenog izvan Hrvatske;
  - očekivano u produkciji do kraja lipnja 2017. godine;

Novosti u 2017. godini (4)

- **Izrada novog Registra resursa u sustavu AAI@EduHr:**
  - tehnologija kojom je realiziran postojeći Registar nije skalabilna - problem prilikom dodavanja novih funkcionalnosti u Registar;
  - za implementaciju postojećih funkcionalnosti nastojat ćemo u najvećoj mjeri zadržati dosadašnji raspored elemenata (osim ako netko nema primjedbi?);
  - (najvjerojatnije) podrška i za CAS autentikacijski protokol;
  - omogućavanje registracije resursa koji žele koristiti vanjske autentikacijske servise (društvene mreže);
  - omogućavanje registracije resursa koji za autentikaciju koriste eduGAIN infrastrukturu;
  - bolja podrška za usluge pristupa mreži (resurse koji koriste RADIUS protokol);
  - očekivano u produkciji tijekom ljeta 2017. godine;

Novosti u 2017. godini (5)

- **Izrada nove aplikacije za upravljanje vanjskim repozitorijima atributa (virtualnim organizacijama):**
  - intuitivnije sučelje za administratore vanjskih repozitorija atributa;
  - bolja podrška za slanje pozivnica za registraciju članova virtualne organizacije;
  - prilikom dizajniranja nastojat ćemo se oslanjati i na iskustva iz drugih AAI federacija;
  - očekivana realizacija do kraja 2017. godine;
- **Anketa o zadovoljstvu korisnika:**
  - nije namijenjena krajnjim korisnicima usluga u sustavu AAI@EduHr, nego administratorima LDAP imenika i davateljima usluga;
  - realizira se u sklopu anketiranja zadovoljstva korisnika ključnih usluga koje Srce pruža akademskoj i istraživačkoj zajednici;
  - svega nekoliko pitanja;
  - što veći odaziv, veće su i šanse da dođe do pozitivnih kvalitativnih promjena u pojedinim segmentima usluge;

Hvala na pažnji!

aai@srce.hr

http://www.aaiedu.hr

srce
Sveučilište u Zagrebu
Sveučilišni računski centar

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-

creativecommons.org/licenses/by-nc/4.0/deed.hr

srce
otvoreni pristup