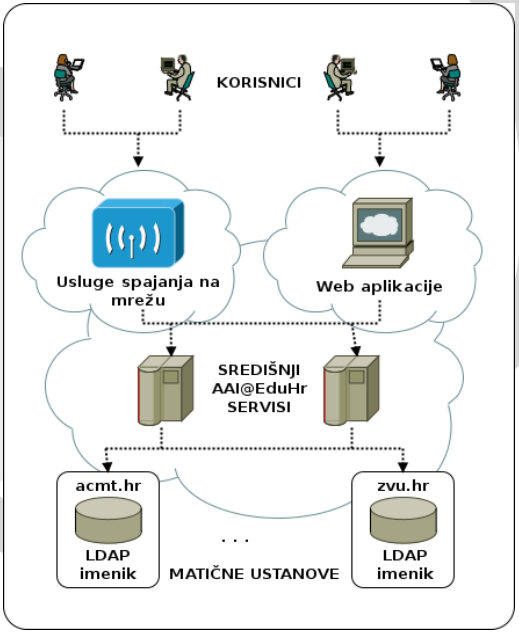
AAI@EduHr SSO rješenje za autentikaciju krajnjih korisnika

Dubravko Vončina, Mijo Đerek

Drugo okupljanje korisnika ISVU REST API-ja, 25. ožujka 2015.

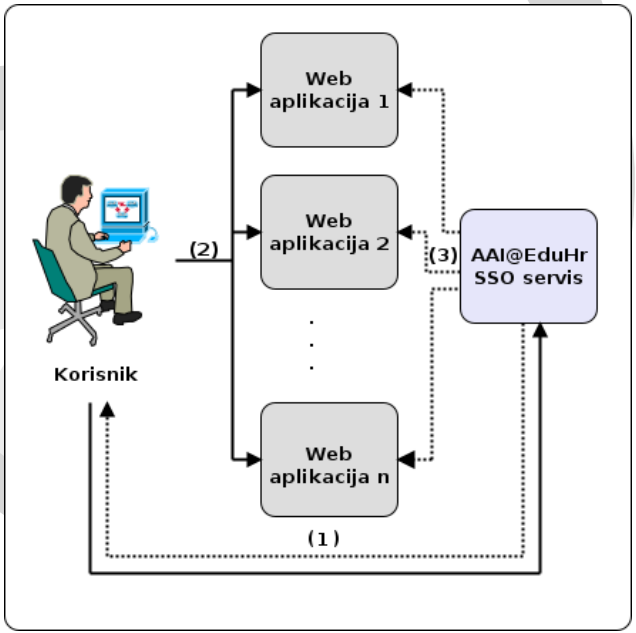
srce
Sveučilište u Zagrebu
Sveučilišni računski centar

Što je AAI@EduHr?



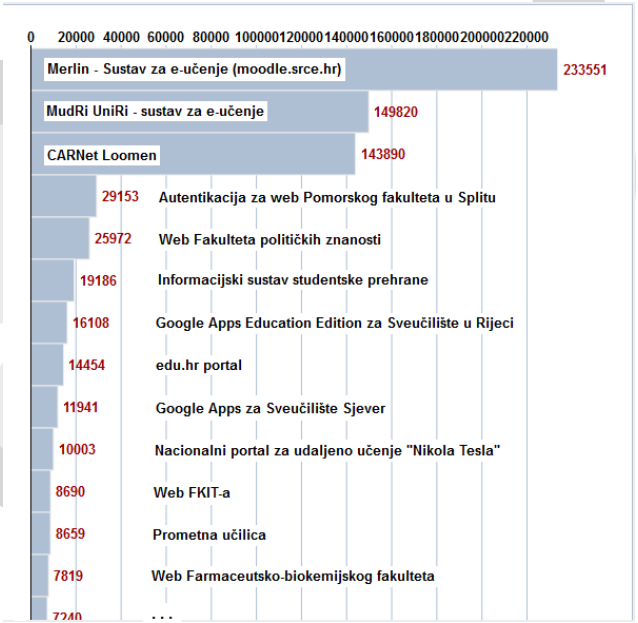
- Autentikacijska i autorizacijska infrastruktura sustava znanosti i (visokog) obrazovanja u Republici Hrvatskoj;
- **228** matičnih ustanova, više od **780000** elektroničkih identiteta;
- **76** davatelja usluga pristupa mreži;
- Više od **250** web aplikacija koje koriste AAI@EduHr SSO servis za autentikaciju korisnika;

Što je Single Sign-On (SSO)?



- 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 SSO 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;

Je li komplicirano implementirati AAI@EduHr SSO u web aplikacijama?



- Na temelju **206** produkcijskih aplikacija za pristup kojima su se tijekom veljače korisnici prijavljivali putem AAI@EduHr SSO servisa (ukupno **827324** autentikacijskih zahtjeva), moglo bi se zaključiti da nije;
- Prilikom implementacije SSO autentikacijskog modula jedan od najvećih izazova je prilagoditi se Single Sign-On konceptu autentikacije - korisnici ne unose korisničku oznaku i zaporku u formu na strani aplikacije, već ih se preusmjerava na središnji AAI@EduHr autentikacijski servis;

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

- Potrebno je prijaviti (registrirati) aplikaciju u sustavu AAI@EduHr putem online registra resursa:
  http://developer.aaiedu.hr/faq/sso_registracija.html
- Davatelji usluga (vlasnici aplikacija) koji nisu u sustavu znanosti i visokog obrazovanja moraju se registrirati kao partneri AAI@EduHr federacije:
  http://www.aaiedu.hr/faq_partneri.html
- Ovisno o programskom jeziku u kojem je aplikacija realizirana potrebno je proučiti dokumentaciju i implementirati odgovarajuću programsku podršku, odnosno autentikacijski modul za autentikaciju putem AAI@EduHr SSO servisa:
  http://developer.aaiedu.hr/faq.html
- I naravno, za odgovore na sva dodatna pitanja i rješavanje eventualnih nedoumica uvijek nas možete kontaktirati slanjem elektroničke pošte na adresu aai@srce.hr

Koje platforme i programski jezici su podržani?

- **PHP** (simpleSAMLphp):
  http://developer.aaiedu.hr/faq/8.html
- **Java** (Spring Security SAML):
  http://projects.spring.io/spring-security-saml/
- **.NET** (OIOSAML.NET):
  http://developer.aaiedu.hr/faq/OIOSAML.html
- **Python / Django**:
  https://gist.github.com/darbula/5003f1d2e1528b089b30
- Aplikacije koje koriste Shibboleth kao autentikacijski modul za implementaciju Single Sign-On autentikacije uporabom **SAML 2.0** protokola;

Je li AAI@EduHr SSO servis siguran?

- Svake godine provodi se certificiranje matičnih ustanova čime se osigurava visoka razina kvalitete korisničkih podataka u imenicima matičnih ustanova;
- AAI@EduHr infrastruktura je prošla certificiranje FINA-e i zadovoljila sve kriterije za uključivanje u sustav e-Građani;
- Koristi se prilikom *online* upisa u srednje škole i na fakultete;
- I velike međunarodne tvrtke omogućavaju prijavu korisnika putem AAI@EduHr SSO servisa za pristup pojedinim svojim uslugama;
- U planu je implementacija mehanizma koji će prisiljavati korisnike da promijene inicijalnu zaporku što će još više povećati razinu sigurnosti;

Koliko je AAI@EduHr Single Sign-On servis pouzdan?

- Već nekoliko godina uspješno ga koristi nekoliko velikih sustava za e-učenje (Merlin, Loomen, MudRi) kod kojih su zbog *online* polaganja ispita pouzdanost i raspoloživost autentikacijskog servisa iznimno važne;
- Sustav jedinstvene autentikacije realiziran je kao klaster poslužitelja s implementiranom *failover* funkcionalnošću;
- Implementiran je kontinuirani nadzor središnjih autentikacijskih servisa i lokalnih imeničkih servisa na matičnim ustanovama;
- Većina matičnih ustanova ima implementiran i sekundarni LDAP imenik - cilj je s vremenom postići da sve matične ustanove imaju uspostavljen i sekundarni imenik;
- Sekundarni SSO servis na dislociranoj lokaciji Srca na Borongaju;

Okruženje za razvoj i testiranje SSO autentikacije

- Da bi se izbjegla mogućnost eventualnog negativnog utjecaja nedovršenih aplikacija na produkcijski SSO servis (npr. nehotično izazivanje *Denial of Service* napada), za aplikacije koje se nalaze u fazi razvoja na raspolaganju je AAI@EduHr Lab okruženje s testnim SSO servisom:
  http://fed-lab.aaiedu.hr/
- U AAI@EduHr Lab okruženju ne mogu se koristiti produkcijski (*pravi*) elektronički identiteti;
- Moguće je zatražiti jedan ili više elektroničkih identiteta za testiranje što u produkcijskom okruženju nije moguće:
  https://fed-lab.aaiedu.hr/zahtjev.php?show=zahtjev_identitet
- Po 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

Dodatne funkcionalnosti SSO servisa

- Virtualne organizacije / vanjski repozitoriji atributa: http://www.aaiedu.hr/virtualne_organizacije.html
- Posrednički autentikacijski servis za društvene mreže: http://www.unizg.hr/authdemo/
- Autentikacija korisnika iz drugih zemalja posredstvom eduGAIN infrastrukture: http://services.geant.net/edugain/Pages/Home.aspx

Pitanja? Prijedlozi? Komentari?

Kontakt: aai@srce.hr

srce
Sveučilište u Zagrebu
Sveučilišni računski centar