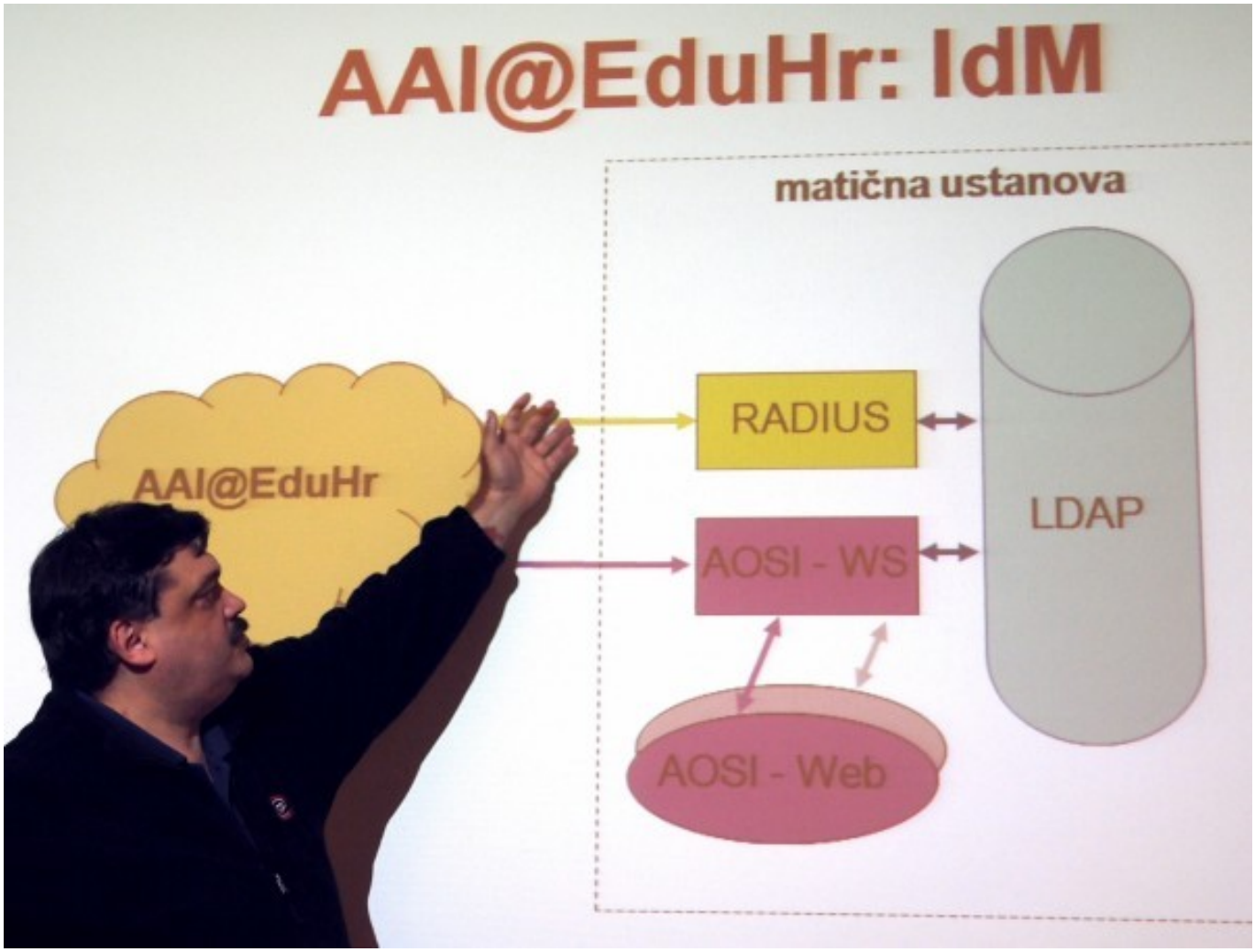
EDU IT PRO: Active Directory i AAI@EduHr

U petak, 18. svibnja 2012. na Srcu je održan osmi susret Microsoftove EDU IT PRO zajednice. Na jednom od prošlih druženja [1] predavač Igor Pavleković iz Algebre spomenuo je teškoće pri integraciji Active Directory-ja i LDAP imenika iz AAI@EduHr sustava, prozvavši izrijekom CARNet, a zapravo Srce, da se AAI@EduHr projekt "ne drži standarda". Da bi se nejasnoće uklonile, Miroslav Milinović, voditelj projekta, pripremio je predavanje pod naslovom "AAI@EduHr: povezivanje aplikacija sa sustavom elektroničkih identiteta".

Ukratko, sustav AAI@EduHr u produkciji je već šest godina i povezuje 220 imenika matičnih ustanova s otprilike 690.000 elektroničkih identiteta. U sustav je povezano i 230 resursa, odnosno usluga, kojima AAI@EduHr sustav služi za identifikaciju i autorizaciju korisnika. Projekt je povezan sa sličnim projektima akademskih zajednica Europske unije, odnosno sa sustavima **eduroam** [2] i GEANT-ovm projektom **eduGAIN** [3]. AAI@EduHr je zapravo federacijski servis koji osigurava SSO (*Single Sign On*) na razini akademskih zajednica EU. Konkretno, to znači da strani predavači mogu koristiti usluge koje se nude u našoj akademskoj zajednici, autenticirajući se pomoću elektroničkog identiteta svoje matične ustanove. Naravno, moguće je i obrnuto, korisnici iz Hrvatske mogu pristupati sadržajima u EU koristeći identitet koji su dobili na svojoj ustanovi.

LDAP imeniku ne pristupa se izravno, nego preko posredničkih protokola, poput RADIUS [4]-a, SAML [5]-a i SOAP [5]-a. Administriranje imenika obavlja se preko AOSI web sučelja. Pri tom se poštuju svi relevantni standardi, poput SAML v.2. Kako neke starije aplikacije podržavaju stariju verziju tog protokola, AAI@EduHr će još neko vrijeme podržavati i SAML 1.1.

AAI@Edu.Hr sustav zamišljen je i realiziran kao centralizirana, hub-and-spoke *[6]* usluga. Prilikom pristupa resursima davatelja usluga obavlja se provjera identiteta korisnika preusmjeravanjem na centralni sustav (*hub*). Davatelj usluga dobija samo potvrdu korisnikova identiteta, bez otkrivanja zaporke i osobnih podataka. Dovoljno je da davatelj usluge dobije potvrdu identiteta i potvrdu prava na korištenje resursa. Ako je tako dogovoreno, korisnik čak može ostati i anoniman. Sustav počiva na povjerenju koje se uspostavlja između davatelja usluge i davatelja identiteta, a davatelji identita, odnosno ustanove članice CARNeta, zadužene su za odgovornu dodjelu elektroničkih identiteta svojim korisnicima.



S druge strane, Microsoft je razvio svoj sustav Active Directory koji je također zasnovan na LDAP-u. Većina ustanova koje koriste Active Directory dodjeljuje korisnicima dvostruke elektroničke identitete, zasebno u AD-u i zatim još u AAI@EduHr imeniku. Razvojni tim AAI@EduHr projekta omogućio je korištenje plugina koji se može iskoristiti za sinhronizaciju oba imenika, tako da se dodavanjem, odnosno brisanjem korisnika ili promjenom zaporke podaci iz AAI sustava prenose u Active Directory. Na taj se način olakšava administriranje korisničkih računa, izbjegava dvostruki unos, a korisnik ne mora pamtiti više različitih zaporki.

Upute su raspoložive na adresi:
http://developer.aaiedu.hr/faq/AOSI-2-Plugins-MSAD.html [7].

Neke od prisutnih sistemaca zanimalo je zašto se administriranje korisnika ne bi obavljalo preko AD-a, pa se onda obavljala sinkronizacija sa AAI@EduHr sustavom? Milinović je odgovorio da je to tehnički moguće, ali bi tada imeničku shemu iz AAI@EduHr projekta trebalo implementirati u Microsoftovom LDAP-u. Ukoliko se netko želi prihvatiti tog posla, razvojni tim je spreman pomoći.

Predavanje je bilo iznadprosječno posjećeno, jer se očigledno radi o temi koja je zajednici zanimljiva. Za neki od narednih susreta polaznici su predložili da se obradi pGina [8], autentikacijski sustav otvorenog koda koji omogućava da se korisnici prijavljuju u Windows domenu koristeći AAI@EduHr sustav.

A što se tiče "nepoštivanja standarda", ispalo je da se radi samo o lošoj komunikaciji. Milinović je sa svoje strane priznao "autističnost" razvojnog tima, koji je informacije o MSAD pluginu objavio na webu projekta, ali tu činjenicu nije dovoljno propagirao u zajednici. S druge strane, sistemci bi trebali češće posjećivati web stranice AAI@EduHr projekta kako bi bili bolje informirani. Nadamo se da će ovo predavanje, a i članci na CARNetovu portalu u kojima pratimo akualna zbivanja, doprinjeti boljem razumjevanju i pomoći kolegama sistemcima u obavljanju njihova posla.

uto, 2012-05-22 10:00 - Aco Dmitrović**Vijesti:** Događanja [9]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1013

Links
[1] https://sysportal.carnet.hr/node/995
[2] http://www.eduroam.hr/
[3] http://www.geant.net/service/edugain/pages/home.aspx
[4] http://en.wikipedia.org/wiki/RADIUS
[5] http://en.wikipedia.org/wiki/Security_Assertion_Markup_Language
[6] http://en.wikipedia.org/wiki/Spoke-hub_distribution_paradigm
[7] http://developer.aaiedu.hr/faq/AOSI-2-Plugins-MSAD.html
[8] http://pgina.org
[9] https://sysportal.carnet.hr/taxonomy/term/43
[10] https://sysportal.carnet.hr/taxonomy/term/28