Analiza koncepta višestrukih repozitorija atributa

SADRŽAJ

ver. 1.0, svibanj 2010

1. UVOD

Autentikacijska i autorizacijska infrastruktura znanosti i visokog obrazovanja u Republici Hrvatskoj (dalje u tekstu: **AAI@EduHr**) je infrastrukturni, posrednički sustav čija je temeljna zadaća omogućiti sigurno, pouzdano i efikasno upravljanje elektroničkim identitetima te njihovu uporabu za pristup mrežnim i mrežom dostupnim resursima.

Zapisi u AAI@EduHr predstavljaju temeljne zapise o elektroničkom identitetu fizičkih osoba iz sustava znanosti i visokog obrazovanja u Republici Hrvatskoj. Navedeni zapisi predstavljaju polazište za ostale informacijske i mrežne sustave koji koriste ili se oslanjaju na elektroničke identitete fizičkih osoba iz sustava znanosti i visokog obrazovanja. Takvi informacijski i mrežni sustavi trebaju uvažiti osnovne tehničke i organizacijske zahtjeve AAI@EduHr, te osigurati potrebnu interoperabilnost.

Ustroj sustava AAI@EduHr određen je Pravilnikom o ustroju Autentikacijske i autorizacijske infrastrukture znanosti i visokog obrazovanja u Republici Hrvatskoj - AAI@EduHr. Detalje organizacijskih, informacijskih i tehničkih normi, sukladno Pravilniku, propisuje Koordinator AAI@EduHr – Srce.

Pravilnik o ustroju AAI@EduHr, sukladno općeprihvaćenom modelu autentikacijske i autorizacijske infrastrukture (AAI) utvrđuje postojanje dvije temeljne uloge koje subjekti u sustavu mogu imati: matična ustanova (davatelj elektroničkog identiteta) i davatelj usluge.

Temeljna je zadaća matične ustanove osigurati informacijsku pouzdanost i potpunost zapisa o elektroničkim identitetima koje je izdala. To međutim ne znači da matična ustanova može i treba uvijek i u svako vrijeme raspolagati svim podacima vezanim uz pojedinu fizičku osobu kojoj je izdala elektronički identitet, a koji bi mogli biti potrebni nekom od davatelja usluga u procesu autorizacije korisnika. Kao rješenje ovoga problema stvoren je koncept dodatnih (višestrukih) repozitorija atributa koji su vezani uz (osnovni) elektronički identitet. Tim se konceptom nastoji osigurati davatelju usluge sve potrebne atribute za proces autorizacije dok se s druge strane održavanje pojedinih podataka (atributa) o nekoj fizičkoj osobi povjerava subjektu koji je siguran i pouzdan izvor tih podataka.

U ovom dokumentu donosimo sažetu analizu koncepta višestrukih repozitorija atributa i virtualnih organizacija i opisujemo neka od mogućih rješenja za njegovu praktičnu implementaciju. Donosimo i prijedlog te opis pilot implementacije koncepta virtualnih organizacija u sustavu AAI@EduHr.

2. VIŠESTRUKI REPOZITORIJI ATRIBUTA I VIRTUALNE ORGANIZACIJE

2.1. Koncepti višestrukih repozitorija atributa i virtualnih organizacija (VO)

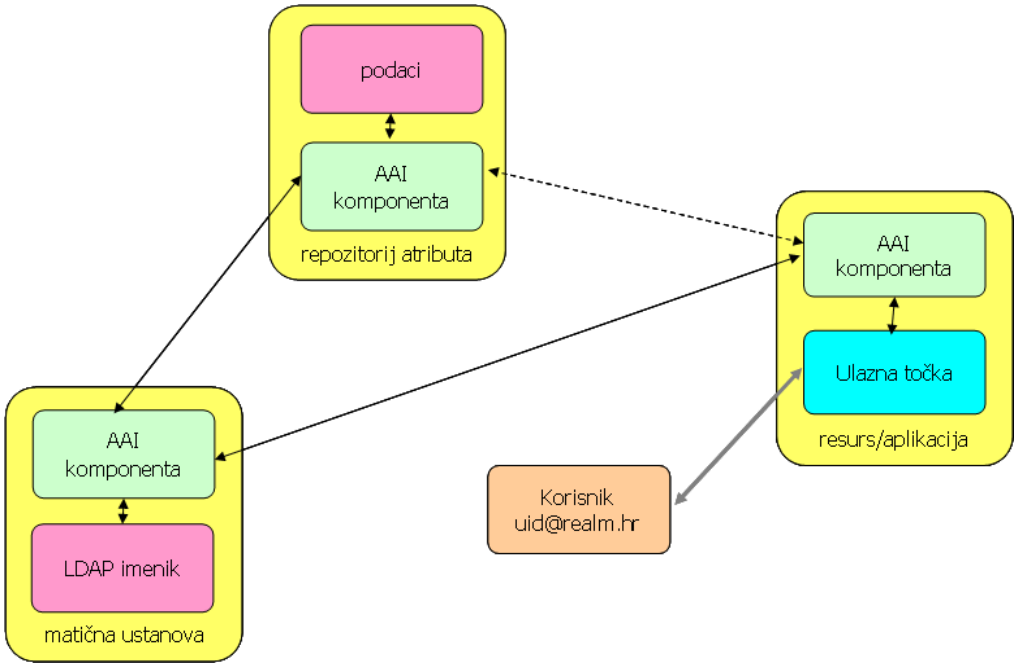
Klasični, općeprihvaćeni model AAI u kojem postoje matična ustanova (davatelj elektroničkog identiteta) i davatelj usluge ne može u potpunosti odgovoriti na sve potrebe davatelja usluga vezane uz podatke (atribute) koji se koriste u procesu autorizacije. Model AAI proširuje se stoga dodatnim izvorima informacija odnosno **repozitorijima atributa** koji su provjereni i pouzdani izvor dodatnih podataka o nekoj fizičkoj osobi – nositelju elektroničkog identiteta. Naravno podaci u takvom dodatnom repozitoriju moraju biti jednoznačno povezani s osnovnim zapisom o elektroničkom identitetu.

Primjeri u kojima je poželjno korištenje takvog proširenog modela AAI s dodatnim repozitorijem atributa u pravilu se odnose na situacije u kojima je jedna ili više usluga namijenjena grupi ljudi koji su međusobno povezani na neki način, npr. radom na zajedničkom projektu ili članstvom u nekom tijelu. Takva grupa može obuhvatiti članove iz više različitih ustanova, regija ili zemalja i naziva se **virtualna organizacija (VO)**. Kao konkretan primjer VO može se npr. navesti GRID zajednica.

Članstvo u pojedinoj VO moguće je dakako evidentirati i u osnovnom zapisu o elektroničkom identitetu pojedinca kroz atribute kao što je *eduPersonEntitlement* ili u hrEduPerson imeničkoj

shemi, *Pripadnost grupi* (*hrEduPersonGroupMember*). Pokazuje se međutim da to rješenje nije dovoljno dobro i skalabilno posebno pri većem broju VO-a i njihovih članova iz većeg broja različitih matičnih ustanova. Problem se dakako povećava ukoliko je uz pripadnost grupi (VO) potrebno ažurnim održavati i dodatne podatke o pojedincu vezane isključivo uz njegov rad i položaj u VO. Kao logično rješenje koje će osigurati izravan i pouzdan izvor tih podataka nudi se uspostava dodatnog repozitorija atributa o kojem će izravno brinuti VO, a koji će na odgovarajući način biti povezan s imenicima matičnih ustanova odnosno elektroničkim identitetima članova VO.

Model AAI s dodatnim repozitorijem atributa prikazan je na slici 1.



Slika 1. – Model AAI s dodatnim repozitorijem atributa

Naravno, nužno je izgraditi odgovarajući **sustav VO**, odnosno platformu koja omogućuje efikasno ažuriranje podataka o članovima VO te povezivanje s odgovarajućim matičnim ustanovama i uslugama.

Informacijski model

Vlasnik elektroničkog identiteta može ili ne mora biti članom neke VO. Njegova registracija može biti izvedena na različite načine:

- izravnim zahtjevom člana putem Web sučelja; administrator te zahtjeve rješava individualno;
- izravnim registriranjem članova (odnosno podataka o njihovom elektroničkom identitetu);
- slanjem pozivnih poruka elektroničkom poštom (poruke mogu i ne moraju sadržavati i personalizirani pozivni kod); ove poruke omogućuju samoregistraciju.

Svaki član VO može imati određeni skup atributa kojima se dopunjuje njegov osnovni elektronički identitet. Ovaj skup atributa određuje svaka VO zasebno te nije ničim propisan. Vrijednost pojedinog atributa može biti:

- postavljena automatski prilikom registracije člana; može biti i izvedena iz vrijednost atributa osnovnog elektroničkog identiteta,
- održavana od strane administratora VO,
- održavana automatski od strane nekog sustava vezanog uz VO,
- održavana od strane samoga člana VO.

Načini registracije članova VO kao i ažuriranja podataka mogu se podešavati ovisno o pojedinoj VO i izravno ovise o konkretnoj implementacija sustava VO.

Web sučelje za upravljanje VO

Kako bi se omogućilo kreiranje VO te efikasno upravljanje podacima o članstvu nužno je postojanje odgovarajućeg Web sučelja. koje, prije svega administratoru VO, olakšava i ubrzava rad.

Komunikacija s uslugom (davateljem usluge)

Kroz komunikaciju s davateljem usluge sustav VO može omogućiti dohvaćanje:

- podataka o grupama (VO),
- popisa svih članova grupe,
- podataka o nekom članu neke grupe.

Ova komunikacija može se realizirati na različite načine, a konačno rješenje u pravilu ovisi o tehnologiji i izvedbi AAI u koju se sustav VO implementira. U svakom slučaju sustav VO mora moći kontrolirati prava pristupa kako podatke ne bi proslijedio neovlaštenoj usluzi.

Sakupljanje atributa

Sakupljanje atributa (*attribute aggregation*) akcija je kojom se prikupljalju korisnikovi atributi iz više izvora (repozitorija). Atributi se prikupljaju ne samo od davatelja (osnovnog) identiteta nego i iz drugih izvora.

Proces sakupljanja atributa može biti:

- vođen od davatelja identiteta (*IdP-centric attribute aggregation*) te se izvodi prilikom procesa prijave korisnika (*login*);
- vođen od davatelja usluge (*SP-centric attribute aggregation*) pa je posve nezavisan od procesa prijave korisnika (*login*);

U procesu sakupljanja atributa razlikujemo:

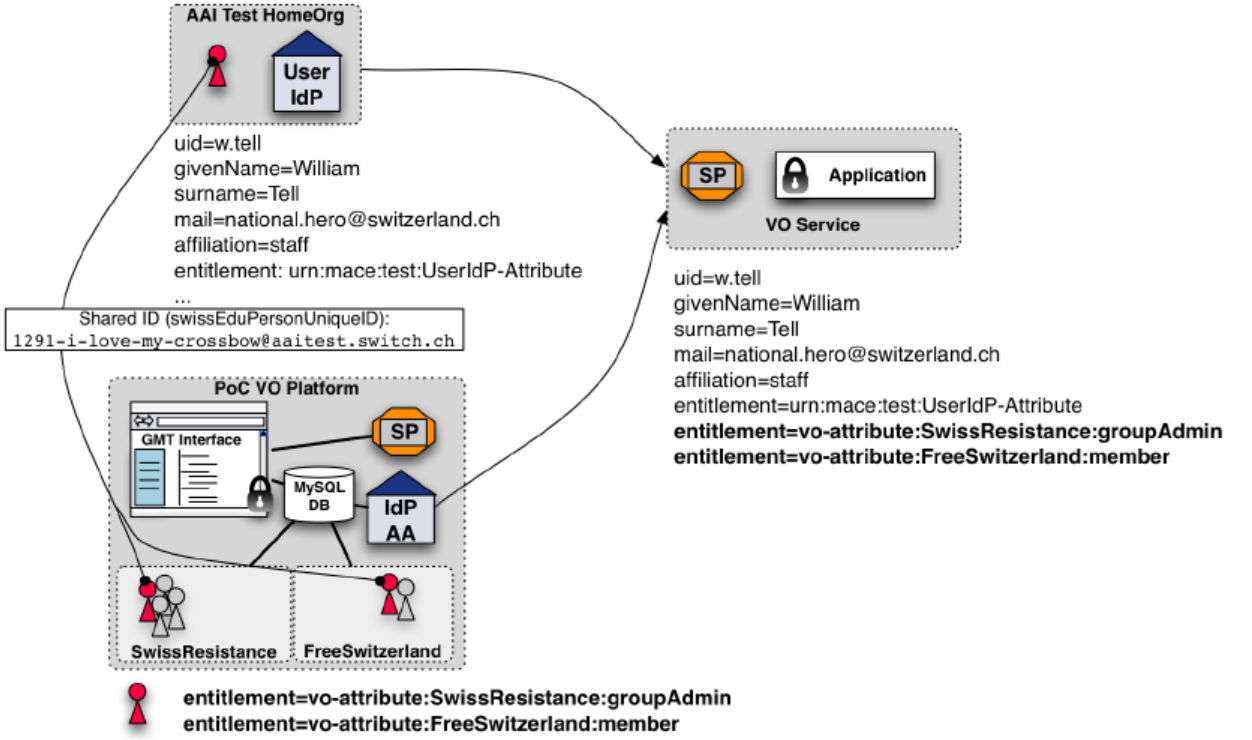
- izvor atributa (a*ttribute authority*) - servis koji daje atribute (podatke)
- potrošač atributa (*attribute consumer*) – klijent, uobičajeno davatelj usluge, koji traži atribute od izvora.

2.2. Načini implementacije koncepta VO u AAI

Kao što je već rečeno načini implementacije koncepta VO u pravilu ovise o tehnologiji i izvedbi AAI u koju se VO implementira. Sustavi VO se stoga mogu bitno razlikovati ne samo po informacijskom modelu već i po korištenim tehnološkim rješenjima.

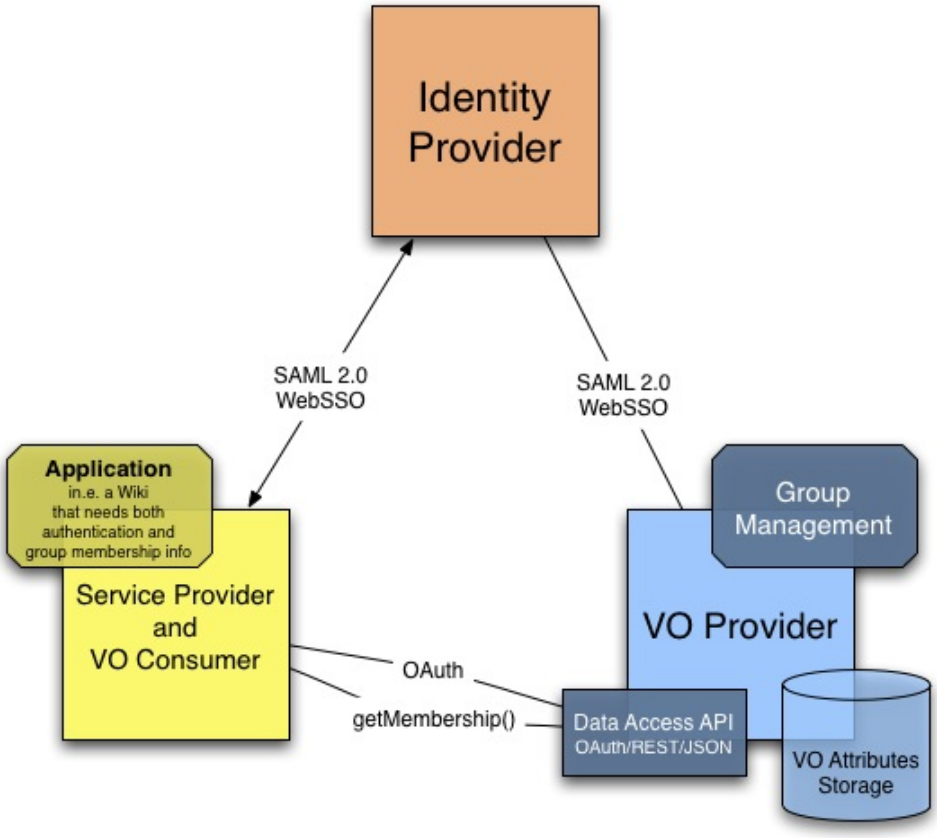
Kao primjer donosimo osnovne informacije o dvije postojeće implementacije sustava VO. Više detalja o obje implementacije moguće je naći u odgovarajućoj dokumentaciji. Izdvajamo dokument pod naslovom *Deliverable DJ3.2.1,1: Identity Federations* koji je nastao kao rezultat projekta GEANT3 kojeg u okviru FP7 programa financira Europska komisija (http://www.geant.net/Media_Centre/Media_Library/Media%20Library/GN3-10-039-DJ3-2-1-1_Identity_Federations-FINAL.pdf).

Implementacija koja je realizirana u švicarskoj AAI (Switch-AAI), a koja temelji na Shibboleth tehnologiji prikazana je na slici 2. koju prenosimo iz izvorne dokumentacije.



Slika 2. – sustav Switch VO

Implementacija simpleSAMLphp VO realizirana u norveškoj AAI (FEIDE) koja se oslanja na simpleSAMLphp programsku podršku prikazana je na slici 3. koju također prenosimo iz izvorne dokumentacije.



Slika 3. – sustav simpleSAMLphp VO

Kako je simpleSAMLphp VO rješenje tehnološki najbliže sustavu AAI@EduHr to je upravo ono odabrano za detaljnije testiranje i uspostavu pilot-sustava VO u AAI@EduHr.

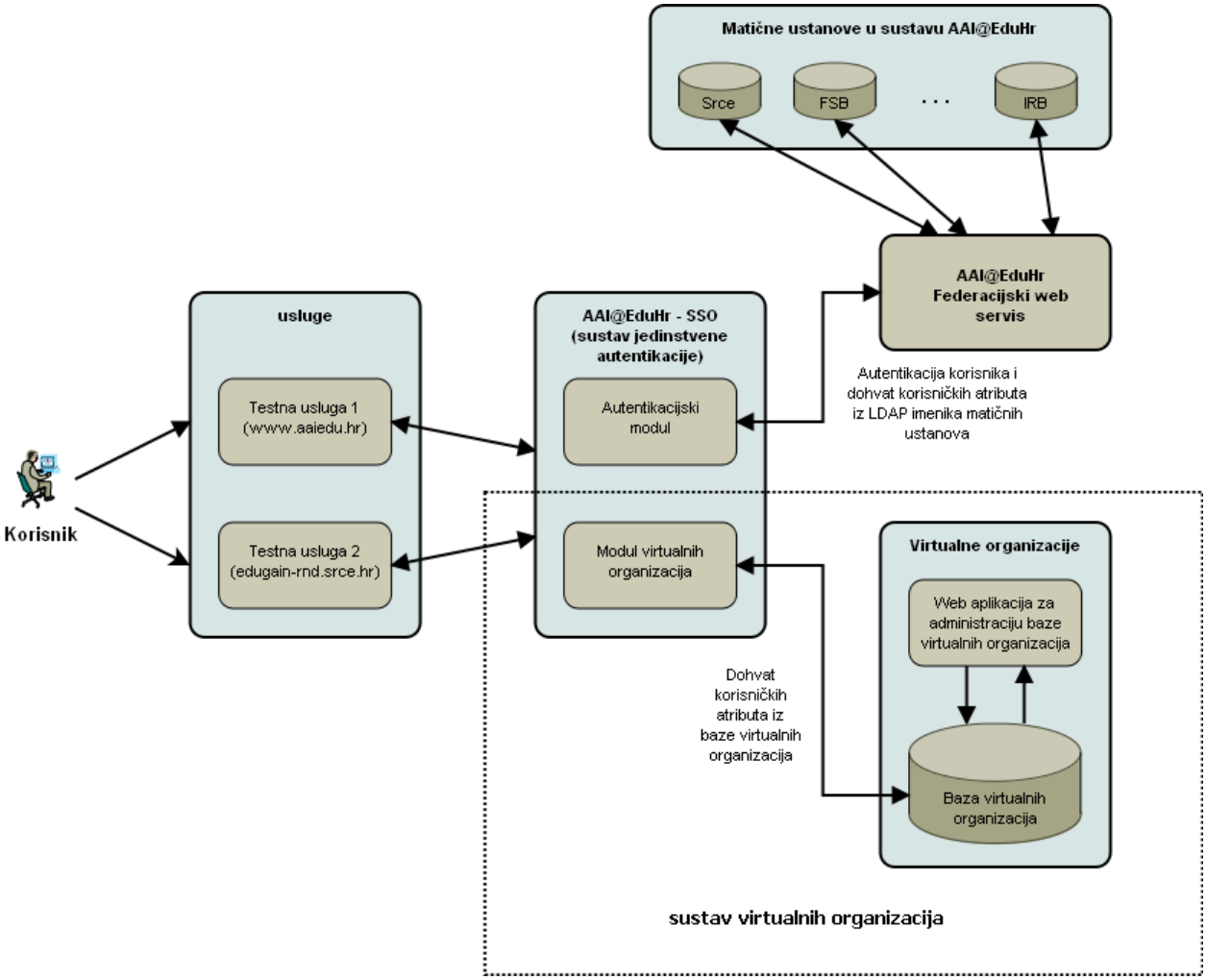
3. IMPLEMENTACIJA KONCEPTA VO U AAI@EDUHR

Sustav AAI@EduHr moguće je i poželjno proširiti konceptom VO. Zajednica korisnika CRO GRID-a, različiti sveučilišni, nacionalni i međunarodni projekti i tijela izvrsni su kandidati za uporabu sustava VO.

U ovom odjeljku donosimo idejno rješenje te kratak opis izvedene pilot-usluge. Izvedeni je modul VO-AAI@EduHr temeljen na iskustvima u testiranju i korištenju rješenja simpleSAMLphp VO.

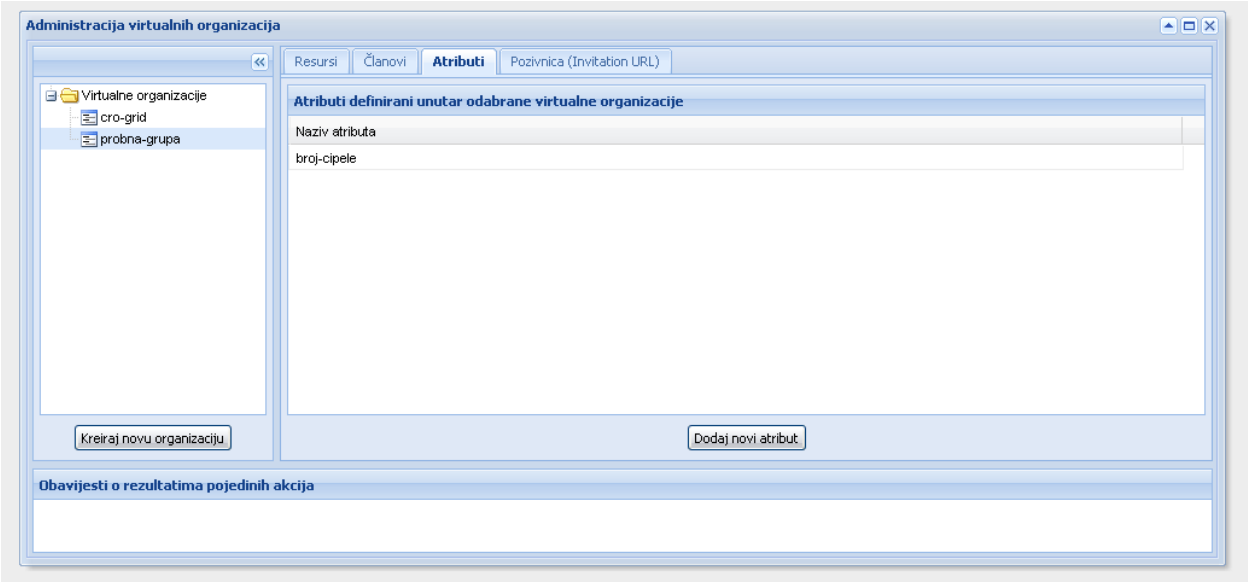
Izvedeni sustav VO u AAI@EduHr je pilot-sustav kojeg je potrebno dodatno testirati te po zahtjevu potencijalnih korisnika (VO) dotjerati prije prelaska u punu produkciju.

Arhitektura AAI@EduHr sa sustavom VO prikazana je na slici 4.



Slika 4. – Arhitektura AAI@EduHr sa sustavom VO

Rješenje se oslanja na postojeće središnje servise sustava AAI@EduHr (FWS i SSO/login). Za povezivanje između VO i matičnog imenika koristi se atribut *korisnička oznaka (hrEduPersonUniqueID)*. Web sučelje za administratora VO dostupno je na adresi http://edugain-rnd.srce.hr/admin/, naravno uz prethodnu autentikaciju i autorizaciju kroz sustav AAI@EduHr. Administrator VO ima na raspolaganju mehanizam slanja pozivnih poruka članovima grupe te može dodati proizvoljan broj atributa vezanih uz grupu za koju je nadležan. Izgled web-sučelja prikazan je na slici 5.



Slika 5. – administratorsko web-sučelje sustava VO u AAI@EduHr