

Virtualne organizacije

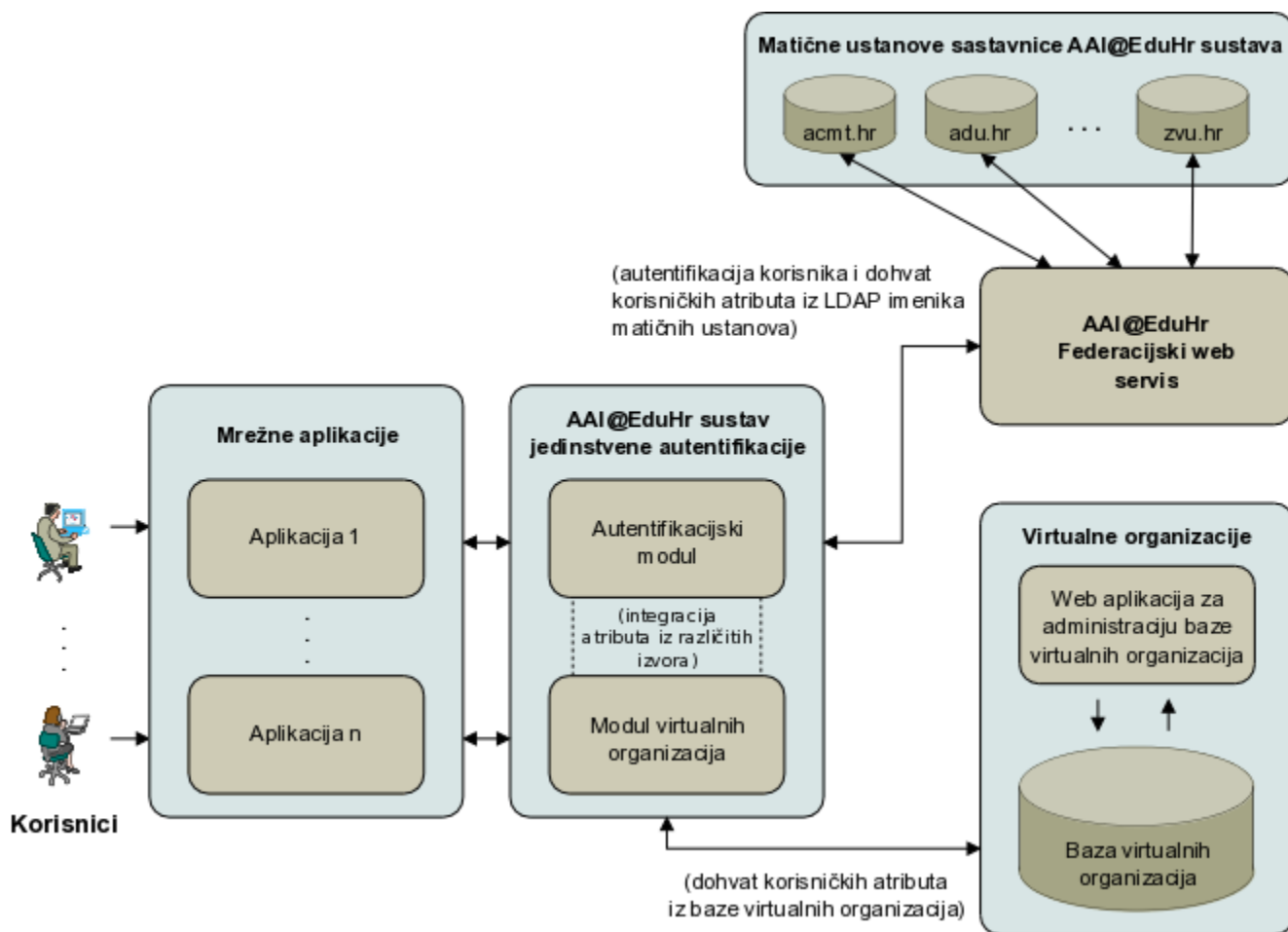
1. Koncept virtualnih organizacija

Klasični model autentikacijsko-autorizacijske infrastrukture (AAI) u kojem postoje matična ustanova (davatelj elektroničkih identiteta) i davatelj usluge ne može u potpunosti odgovoriti na sve potrebe davatelja usluga vezane uz podatke (atribute) koji se koriste u procesu autorizacije prilikom pristupanja nekom mrežnom resursu ili aplikaciji. Model AAI proširuje se stoga dodatnim izvorima informacija, odnosno repozitorijima atributa, koji su provjereni i pouzdani izvor dodatnih podataka o nekoj fizičkoj osobi.

Koncept virtualnih organizacija zamišljen je i realiziran kao vanjski repozitorij atributa koji služe kao nadopuna podacima pohranjenim u LDAP imenicima matičnih ustanova. Tim se konceptom nastoji davatelju usluge osigurati sve potrebne attribute za proces autorizacije, kao i potpunu ili barem djelomičnu kontrolu nad autorizacijskim atributima. Više informacija o konceptu virtualnih organizacija možete pronaći u dokumentu [Analiza koncepta višestrukih repozitorija atributa](#).

U sustavu AAI@EduHr virtualne organizacije su implementirane kao dodatni modul unutar sustava jedinstvene autentikacije korisnika (**Single Sign-On sustava**). Način implementacije virtualnih organizacija prikazan je na slici 1.

- 1. Koncept virtualnih organizacija
- 2. Administracija virtualnih organizacija
 - 2.1. Kreiranje nove virtualne organizacije
 - 2.2. Uređivanje administratora virtualne organizacije
 - 2.3. Resursi
 - 2.4. Članovi virtualne organizacije
 - 2.5. Atributi
 - 2.6. Postavljanje vrijednosti atributa
- 3. Primjer primjene virtualnih organizacija
- 4. Dodatne informacije i odgovori na pitanja



Slika 1. Implementacija virtualnih organizacija u sustavu AAI@EduHr

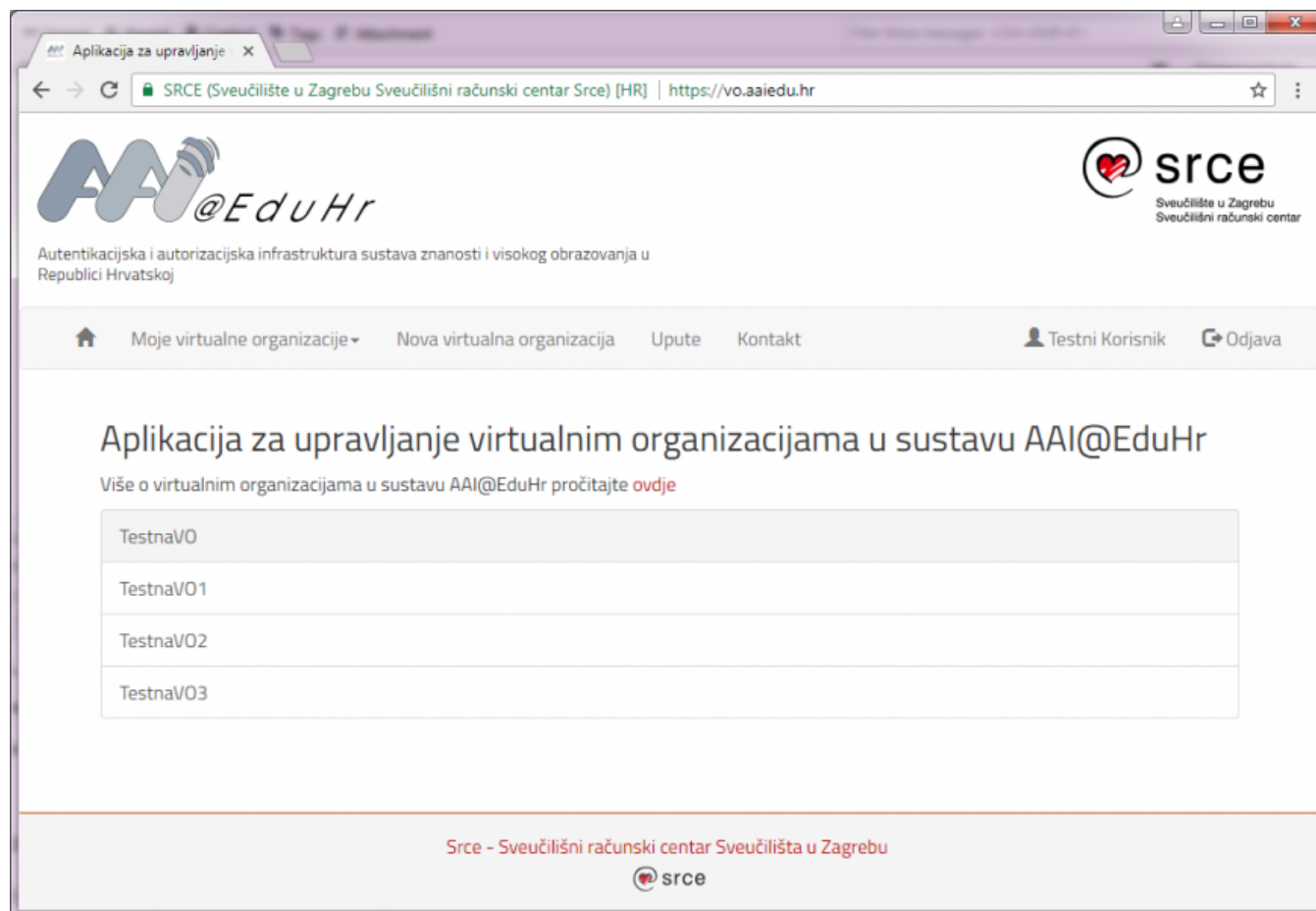
Za isporuku atributa definiranih unutar virtualnih organizacija koristi se SAML 2.0 protokol koji se koristi i za isporuku atributa pohranjenih u LDAP imenicima matičnih ustanova. Prednost ovakvog pristupa je u tome da niti jednu aplikaciju koja koristi Single Sign-on sustav nije potrebno posebno prilagođavati za dohvat atributa iz repozitorija virtualnih organizacija. Određeni nedostatak predstavlja činjenica da virtualne organizacije trenutno mogu koristiti samo resursi koji za autentikaciju i dohvat korisničkih podataka koriste AAI@EduHr Single Sign-On sustav.

Da bi se omogućilo kreiranje virtualnih organizacija te efikasno upravljanje podacima o članstvu, nužno je postojanje odgovarajućeg web sučelja koje administratorima virtualnih organizacija olakšava i ubrzava rad. U nastavku je opisana aplikacija za administraciju virtualnih organizacija u sustavu AAI@EduHr.

2. Administracija virtualnih organizacija

Administracija atributa i članova virtualnih organizacija vrši se putem [aplikacije za upravljanje virtualnim organizacijama u sustavu AAI@EduHr](#).

Za pristup aplikaciji za upravljanje virtualnim organizacijama potrebno se autenticirati elektroničkim identitetom iz sustava AAI@EduHr. Nakon prijave u aplikaciju, administratoru će se prikazati početna stranica kao na slici 2.



Slika 2. Početna stranica aplikacije za administraciju virtualnih organizacija

Na početnoj stranici prikazuje se popis virtualnih organizacije koje imate pravo administrirati. Isti popis Vam je u svakom trenutku dostupan tako da u traci izbornika kliknete na "Moje virtualne organizacije".

Nakon što s popisa odaberete željenu virtualnu organizaciju, u podizborniku možete odabrati želite li uređivati opće podatke o virtualnoj organizaciji, administratore virtualne organizacije, resurse kojima se isporučuju atributi virtualne organizacije, članove virtualne organizacije ili attribute koji se isporučuju odabranim resursima.

2.1. Kreiranje nove virtualne organizacije

U izborniku [aplikacije za upravljanje virtualnim organizacijama u sustavu AAI@EduHr](#) odaberite "Nova virtualna organizacija"

Prilikom kreiranja virtualne organizacije potrebno je unijeti

- **Naziv virtualne organizacije** - može sadržavati najviše 128 znakova. Za naziv je dozvoljeno koristiti slova (bez dijakritičkih znakova), brojeke te znakove '.', '-' i '_'. Poželjno je da naziv bude što kraći i da barem djelomično odgovara nazivu aplikacije kojoj će virtualna organizacija isporučivati attribute;
- **Opis virtualne organizacije** - može sadržavati do 500 znakova;

Važno je napomenuti da virtualna organizacija neće biti kreirana odmah nakon postavljanja zahtjeva, već zahtjev treba odobriti netko od administratora sustava AAI@EduHr. Stranica zahtjeva za otvaranje nove virtualne organizacije prikazana je na sljedećoj slici.

Slika 3. Zahtjev za otvaranjem virtualne organizacije

Nakon što u menuu odaberete željenu virtualnu organizaciju, u podizborniku odavrane virtualne organizacije kliknite na "Administratori".

Na stranici za uređivanje administratora prikazat će Vam se popis svih administratora odabrane virtualne organizacije kao na slici ispod. Ako želite nekom administratoru ukinuti pravo administriranja virtualne organizacije, kliknite na ikonicu kante za smeće.

The screenshot shows a web browser window with the URL `https://vo.aai.edu.hr/?show=vo_admins&id_vo=76`. The page header includes the AAI@EduHr logo and the SRCE logo (Sveučilište u Zagrebu, Sveučilišni računski centar). The main navigation bar contains links for 'Moje virtualne organizacije', 'Nova virtualna organizacija', 'Upute', and 'Kontakt'. The user is logged in as 'Testni Korisnik'.

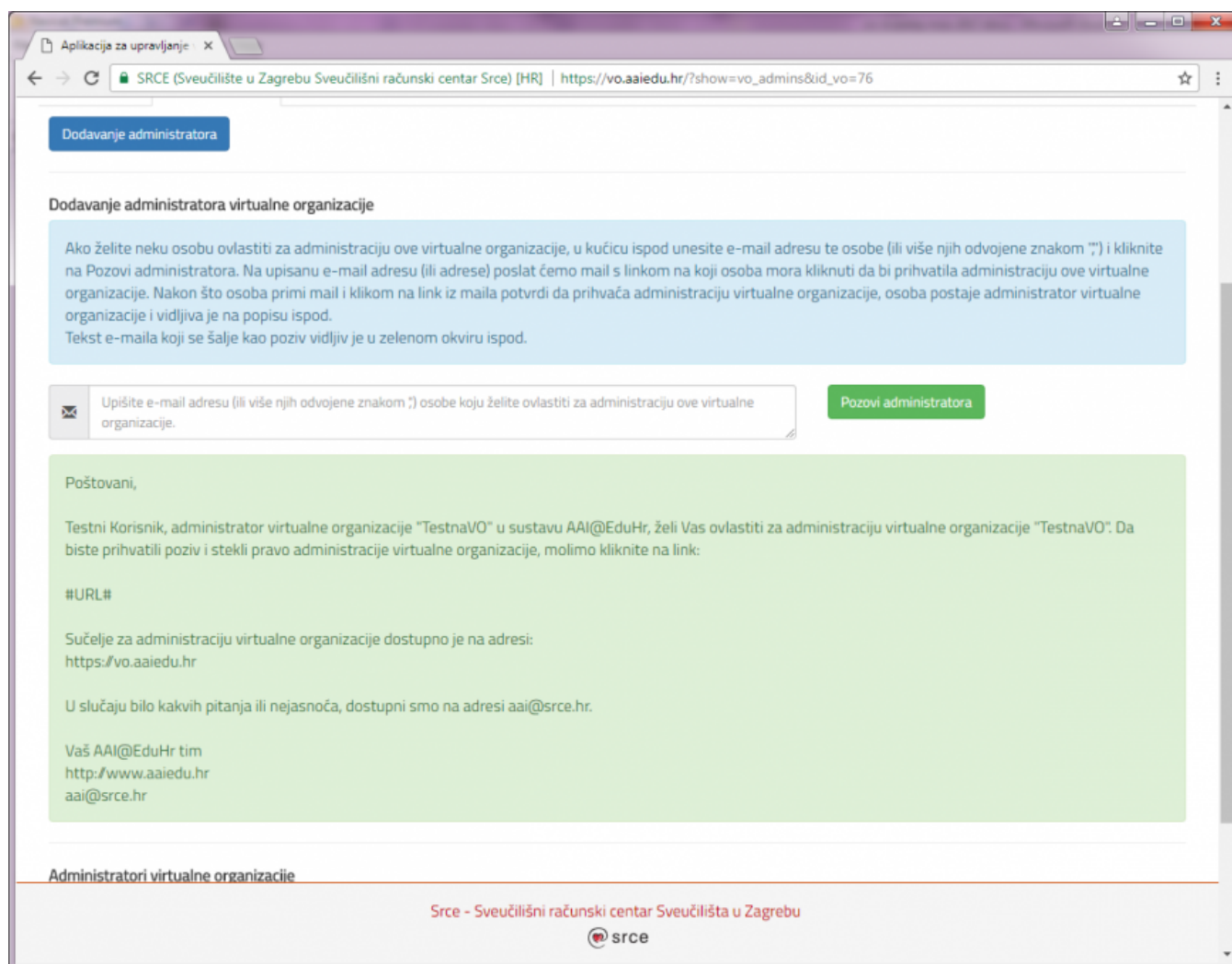
The 'Administrators' tab is selected, showing a list of administrators for the 'TestnaVO' organization. A blue button 'Dodavanje administratora' is visible. The table below lists the administrators:

Ime	Prezime	Korisnička oznaka	
Testni	Korisnik	testko@test.hr	
Testni1	Korisnik1	test@test.hr	
Testni2	Korisnik2	test2@test.hr	

Below the table, it says 'Prikazano 1 do 3 od 3 zapisa'. Navigation buttons 'Prethodna', '1', and 'Sljedeća' are present. The footer contains the text 'Srce - Sveučilišni računski centar Sveučilišta u Zagrebu' and the SRCE logo.

Slika 4. Uređivanje administratora virtualne organizacije

Za administriranje virtualne organizacije možete ovlastiti bilo koga tko ima elektronički identitet u sustavu AAI@EduHr i to na sljedeći način: nakon što kliknete na gumb Dodavanje administratora, prikazat će se obrazac kao na slici dolje:





Slika 5. Dodavanje administratora virtualne organizacije

U za to predviđenu kućicu upišite e-mail adresu (ili više njih odvojenih znakom ";") osoba koje želite ovlastiti za administraciju virtualne organizacije. Na upisane adrese poslat će se mail čiji je tekst prikazan u zelenom okviru. Po primitku poruke, osoba koju želite ovlastiti za administraciju virtualne organizacije treba kliknuti na link iz maila i otvorit će joj se SSO servis sustava AAI@EduHr. Nakon što unese svoju korisničku oznaku i zaporku iz sustava AAI@EduHr, osoba će steći pravo administracije virtualne organizacije.

2.3. Resursi

Odabirom ove opcije administrator dobiva mogućnost odabrati resurse kojima će se isporučivati atributi virtualne organizacije. Na stranici su prikazana dva popisa. Gornji popis je popis onih resursa kojima se isporučuju atributi odabrane virtualne organizacije, a na donjem popisu su svi ostali resursi dostupni kroz sustav AAI@EduHr. Ako želite omogućiti isporuku atributa virtualne organizacije nekom resursu, pronađite ga na donjem popisu i kliknite na ikonicu +. Resur će se tada pojaviti na gornjem popisu, što znači da je odabran za isporuku atributa virtualne organizacije. Ako želite onemogućiti isporuku atributa virtualne organizacije nekom od resursa s gornjeg popisa, kliknite na ikonicu kante za smeće.

Aplikacija za upravljanje
SRCE (Sveučilište u Zagrebu Sveučilišni računski centar Srce) [HR]
https://vo.aaiedu.hr/?show=vo_resources&id_vo=76


Autentikacijska i autorizacijska infrastruktura sustava znanosti i visokog obrazovanja u Republici Hrvatskoj

Moje virtualne organizacije
Nova virtualna organizacija
Upute
Kontakt
Testni Korisnik
Odjava

Opći podaci
Administratori
Resursi
Članovi
Atributi
TestnaVO

Resursi kojima se isporučuju atributi virtualne organizacije

Prikaži 10 zapisa po stranici
Pretraži:




Naziv	EntityId	
AAI Dev	161.53.0.184	


Prikazano 1 do 1 od 1 zapisa
Prethodna
1
Sljedeća

U gornjoj tablici prikazan je popis resursa kojima se isporučuju atributi ove virtualne organizacije. Želite li dodati neki resurs na taj popis, pronađite ga u donjoj tablici i kliknite na ikonicu +.

Ostali resursi

Prikaži 10 zapisa po stranici
Pretraži:

Naziv	EntityId	
12tesla DokuWiki HomePage	https://12tesla.phy.pmf.unizg.hr/ssphp/module.php/saml/sp/metadata.php/default-sp	
AAI@EduHr autentifikacija za vsmti.hr intranet	http://new.vsmi.hr/simplesamlphp/www/module.php/saml/sp/metadata.php/default-sp	
AAI@EduHr Lab	https://fed-lab.aaiedu.hr/sp/module.php/saml/sp/metadata.php/default-sp	

Srce - Sveučilišni računski centar Sveučilišta u Zagrebu


Slika 6. Administracija resursa kojima se isporučuju atributi virtualne organizacije

2.4. Članovi virtualne organizacije

U tablici su prikazani su svi postojeći članovi odabrane virtualne organizacije. Da biste nekog člana isčlanili iz virtualne organizacije, kliknite na ikonicu kante za smeće u njegovom retku u tablici. Ako želite **upisati vrijednosti atributa** koje se za nekog člana šalju resursima, kliknite na ikonicu uredi atributa. VAŽNO: da biste mogli unijeti vrijednost pojedinog atributa virtualne organizacije za odabranog člana, prvo morate odrediti attribute virtualne organizacije u tabu [Atributi](#).

Aplikacija za upravljanje

SRCE (Sveučilište u Zagrebu Sveučilišni računski centar Srce) [HR] | https://vo.aai.edu.hr/?show=vo_members&id_vo=76

AAI@EduHr
Autentikacijska i autorizacijska infrastruktura sustava znanosti i visokog obrazovanja u Republici Hrvatskoj

srce
Sveučilište u Zagrebu
Sveučilišni računski centar

Moje virtualne organizacije Nova virtualna organizacija Upute Kontakt

Mijo Derek Odjava

Opći podaci Administratori Resursi **Članovi** Atributi

TestnaVO

Dodavanje članova

Članovi virtualne organizacije

Prikaži 10 zapisa po stranici Pretraži:

Ime	Prezime	Korisnička oznaka	
Testni1	Korisnik1	test@test.hr	
Testni2	Korisnik2	test2@test.hr	

Prikazano 1 do 2 od 2 zapisa

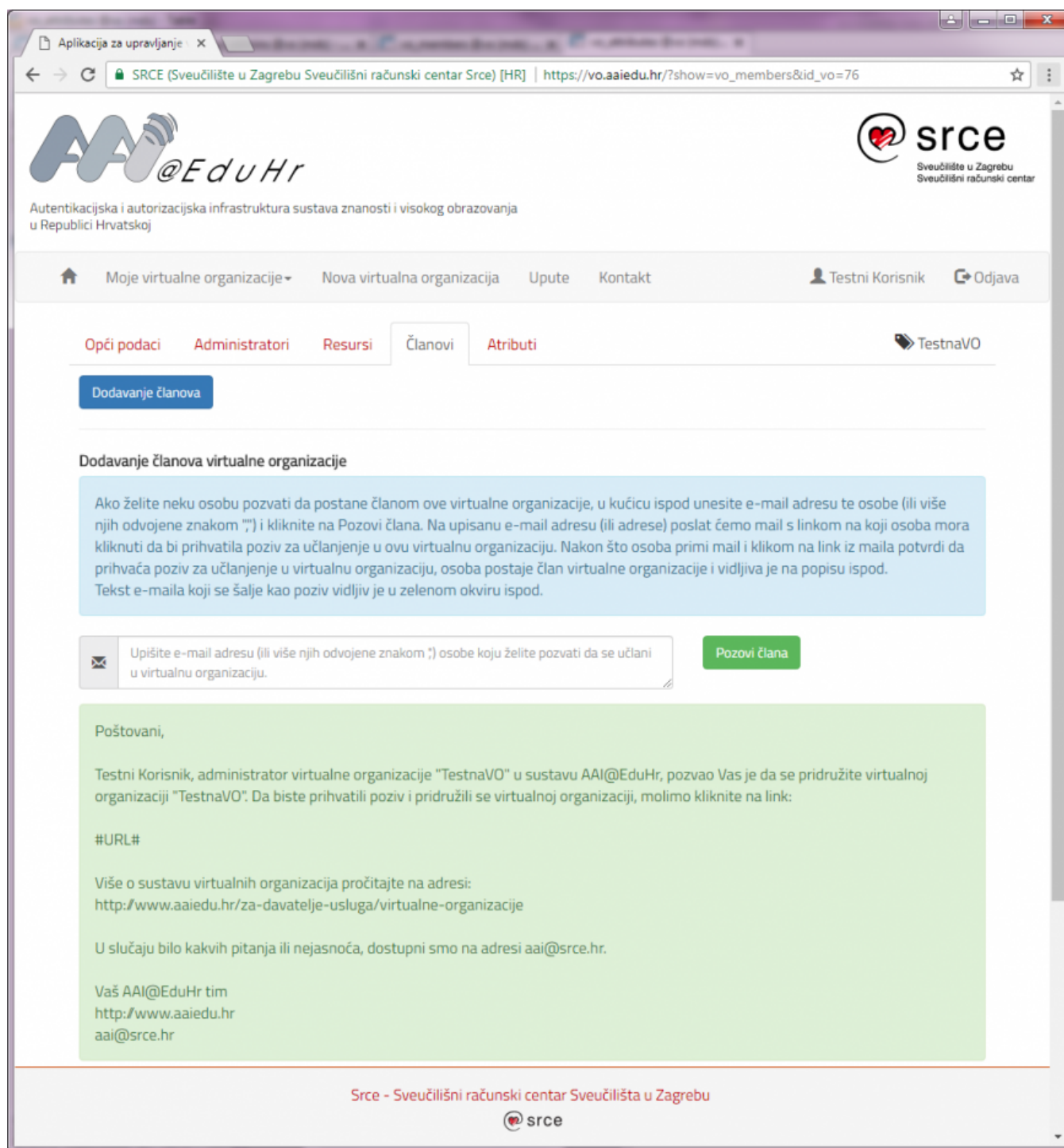
Prethodna 1 Sljedeća

Srce - Sveučilišni računski centar Sveučilišta u Zagrebu

srce

Slika 7. Sučelje za administraciju članova odabrane virtualne organizacije

Novi članovi u virtualnu organizaciju ulaze na način da prihvate pozivnicu koju im je e-mailom uputio administrator virtualne organizacije. Kod prihvata pozivnice pozvana osoba se mora autentificirati ili elektroničkim identitetom iz sustava AAI@EduHr ili vjerodajnicama neke od podržanih društvenih mreža (trenutno su to Google, Facebook, Twitter i LinkedIn). Administrator pozivnicu za učlanjenje može poslati na sljedeći način: nakon što kliknete na gumb Dodavanje članova, prikazat će se obrazac kao na slici dolje:

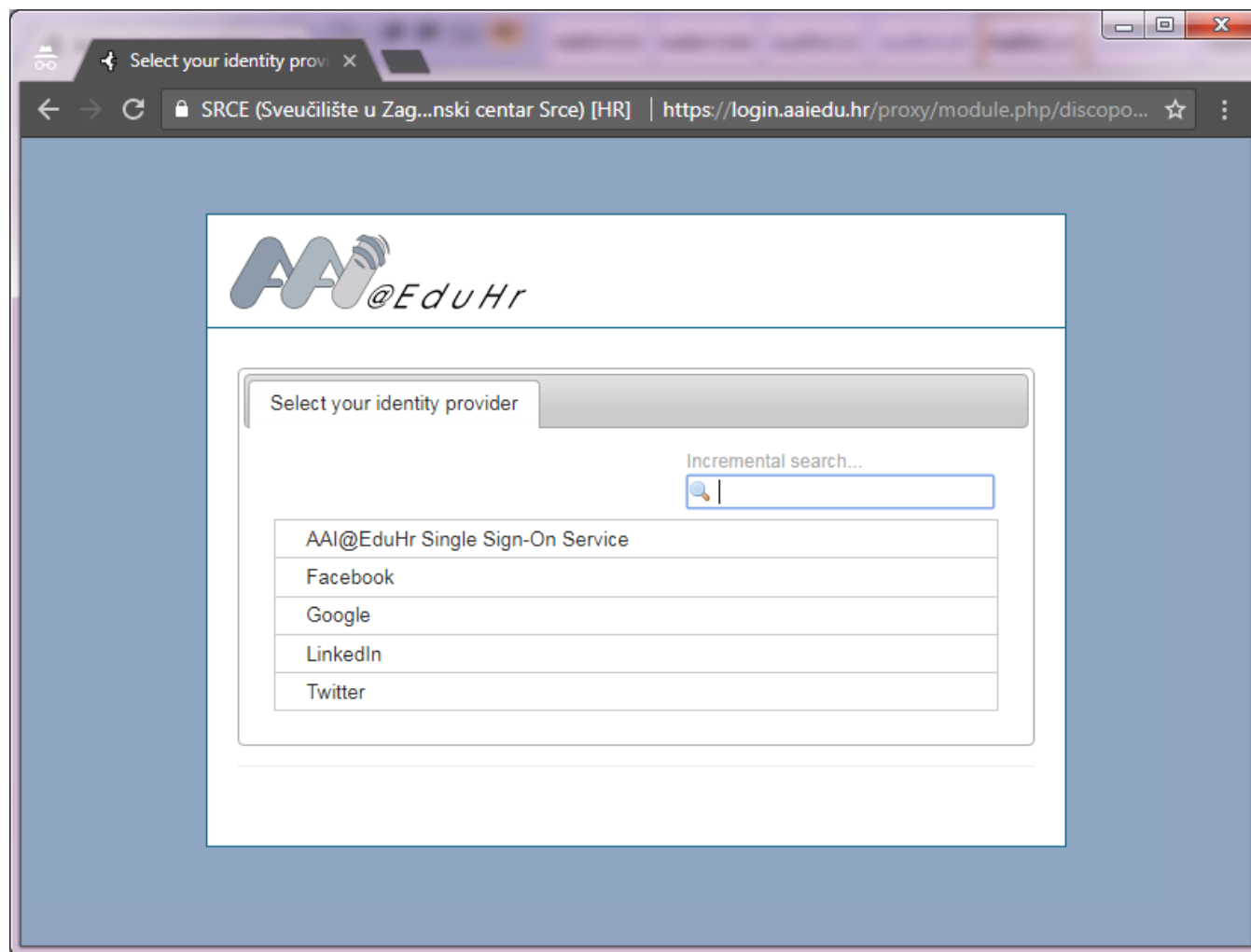


Slika 8. Sučelje za pozivanje članova virtualne organizacije

U za to predviđenu kućicu upišite e-mail adresu (ili više njih odvojenih znakom ,) osoba koje želite ovlastiti za pozvati da se učlane u virtualnu organizaciju. Na upisane adrese poslat će se mail čiji je tekst prikazan u zelenom okviru. Po primitku poruke, osoba koju pozvati u članstvo virtualne organizacije treba kliknuti na link iz maila i otvoriti će joj se izbornik u kojem izabire kojim vjerodajnicama se želi autentificirati za članstvo u virtualnoj organizaciji (slika 9). Nakon što unese svoje vjerodajnice iz odabranog sustava, osoba će postati član virtualne organizacije.

VAŽNO: ako se član prilikom učlanjenja predstavi vjerodajnicom neke od podržanih društvenih mreža, da bi resurs primio atribute njegove virtualne organizacije, i sam resurs treba podržavati prijavu tim vjerodajnicama, a korisnik se prilikom pristupa resursu treba autentificirati istim. Npr: ako korisnik A prihvati članstvo u virtualnoj organizaciji B predstavljajući se vjerodajnicama Googlea, a administrator virtualne organizacije B je odabrao resurs C da mu se isporučuju atributi virtualne organizacije, da bi resurs C mogao dohvatiti atribute korisnika A u virtualnoj organizaciji B, resurs C mora podržavati autentikaciju putem društvenih mreža preko SSO servisa sustava AAI@EduHr i korisnik A se prilikom pristupa resursu C mora predstaviti istim (Google) vjerodajnicama kojima se autentificirao prilikom učlanjenja u virtualnu organizaciju B.

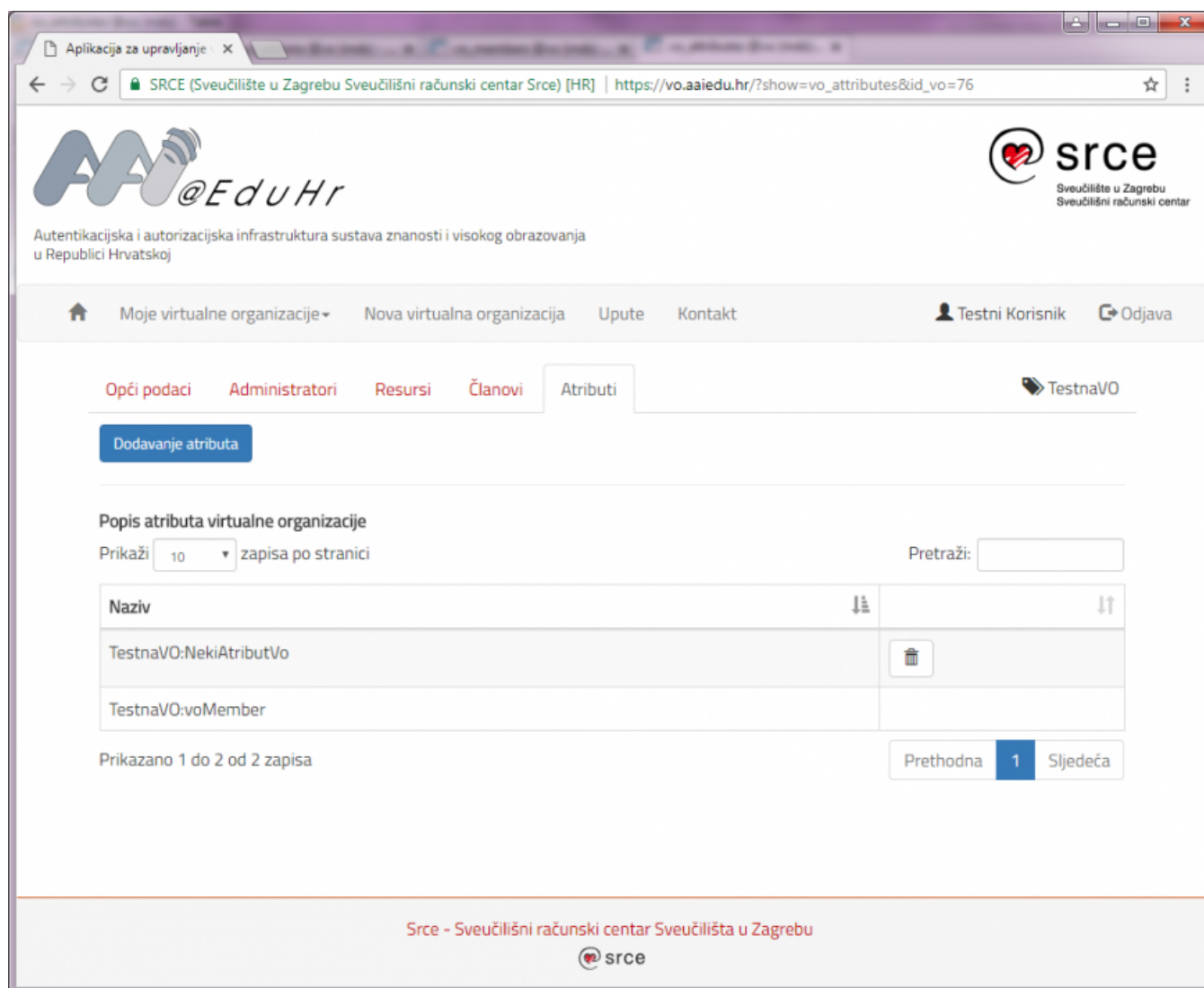
Također je važno naglasiti da članovi virtualne organizacije ne moraju pripadati matičnoj ustanovi kojoj pripada administrator. Bilo koja osoba koja posjeduje elektronički identitet u sustavu AAI@EduHr može biti član bilo koje virtualne organizacije.



Slika 9. Odabir kojim će se vjerodajnicama korisnik autentificirati prilikom prihvatanja poziva za učlanjenje u virtualnu organizaciju

2.5. Atributi

Odabirom Opcije **Atributi** prikazat će se tablica s popisom svih atributa definiranih unutar pojedine virtualne organizacije.



Slika 10. Sučelje za dodavanje i brisanje atributa

Sustav AAI@EduHr attribute definirane unutar virtualnih organizacija isporučuje u slijedećem obliku:

naziv_virtualne_organizacije:naziv_atributa = vrijednost_atributa

Isporuka atributa u takvom obliku omogućuje da unutar različitih virtualnih organizacija budu definirani atributi istog naziva.

Želite li dodati atribut, kliknite na gumb Dodavanje atributa, u odgovarajuću kućicu upišite naziv atributa i kliknite na Dodaj atribut. Važno je napomenuti da je atribut **voMember** unaprijed definiran za svakog člana bilo koje virtualne organizacije. Taj atribut označava da je osoba član neke virtualne organizacije i njegova vrijednost je uvijek **true**.

2.6. Postavljanje vrijednosti atributa

Kroz ovo sučelje administrator može za svakog člana virtualne organizacije postavljati vrijednosti **atributa definiranih unutar te virtualne organizacije**. U gornjem dijelu stranice prikazani su podaci koje aplikacija pamti o pojedinom članu odabrane virtualne organizacije. Nakon toga slijedi tablica s popisom atributa (i njihovih vrijednosti) definiranih za pojedinog člana virtualne organizacije. Kako se uvijek za svakog člana svakom resursu šalje atribut **NazivVO:voMember** s vrijednošću **true**, ova će tablica uvijek imati barem jedan redak. U tablici na dnu stranice je popis atributa definiranih za odabranu virtualnu organizaciju, a kojima nije postavljena vrijednost za odabranog člana. Vrijednost tih atributa možete postaviti tako da u odgovarajuću kućicu upišete vrijednost i kliknete na gumb Dodaj. Nakon što se postavi vrijednost atributa, on se seli u gornju tablicu. Vrijednost nekog atributa za odabranog člana možete izbrisati klikom na ikonicu kante za smeće.

Aplikacija za upravljanje

SRCE (Sveučilište u Zagrebu Sveučilišni računski centar Srce) [HR] | https://vo.aai.edu.hr/?show=vo_member_attributes&id_vo=71&id_member=1079

AAI@EduHr
Autentikacijska i autorizacijska infrastruktura sustava znanosti i visokog obrazovanja u Republici Hrvatskoj

srce
Sveučilište u Zagrebu
Sveučilišni računski centar

Moje virtualne organizacije Nova virtualna organizacija Upute Kontakt Testni Korisnik Odjava

Opći podaci Administratori Resursi Članovi **Atributi** TestnaVO

Podaci o članu virtualne organizacije

Ime Tetni

Prezime Korisnik

E-Mail test@test.hr

Korisnička oznaka test@test.hr

Aplikacija za upravljanje virtualnim organizacijama u sustavu AAI@EduHr prilikom pridruživanja korisnika virtualnoj organizaciji dohvaća i pamti gore navedene osobne podatke. Navedeni osobni podaci se koriste isključivo u svrhu omogućavanja upravljanja virtualnim organizacijama i ne dijele se trećim stranama.

Popis atributa koji se isporučuju resursima

Naziv	Vrijednost
TestnaVO:voMember	true

Atributi definirani za virtualnu organizaciju kojima nisu postavljene vrijednosti za odabranog korisnika

Naziv	Vrijednost
TestnaVO:testniAtribut	<input type="text" value="Upišite vrijednost atributa."/> <input type="button" value="Dodaj"/>

Da biste članu virtualne organizacije mogli upisati vrijednost nekog atributa, prvo morate virtualnoj organizaciji pridružiti željeni atribut. To možete učiniti u tabu **Atributi**.

Srce - Sveučilišni računski centar Sveučilišta u Zagrebu

srce

Slika 11. Sučelje za postavljanje vrijednosti atributa

Aktualna verzija aplikacije za administraciju virtualnih organizacija za svakog korisnika dozvoljava unos samo jedne vrijednosti za svaki atribut. Atributi koji nemaju definiranu vrijednost (prikazani su u donjoj tablici) se ne isporučuju aplikacijama.

3. Primjer primjene virtualnih organizacija

Radi lakšeg razumijevanja koncepta virtualnih organizacija, u nastavku je opisana jedna od mogućih primjena virtualnih organizacija. Pretpostavimo da određenoj aplikaciji, npr. Internim web stranicama nekog sveučilišta, smiju pristupiti samo ovlaštene osobe s pojedinih fakulteta. U standardno iskonfiguriranim LDAP imenicima matičnih ustanova ne postoji atribut koji bi označavao da netko treba imati pristup internom webu Sveučilišta.

Osim toga, čak i kad bi takav atribut postojao, s obzirom na to da osobe koje pristupaju internim web stranicama sveučilišta dolaze s velikog broja različitih fakulteta, ne bi bilo jednostavno osigurati da u LDAP imenicima svih fakulteta atributi koji se odnose na navedenu aplikaciju budu ažurni. Da bi se eliminirali prethodno navedeni nedostaci, za kontrolu pristupa internom webu moglo bi se definirati virtualnu organizaciju "interni_web_sveucilista" i u nju dodati sve osobe koje trebaju imati pristup internom webu. Prilikom prijavljivanja u aplikaciju, AAI@EduHr sustav će za svakog takvog korisnika aplikaciji isporučiti atribut:

```
interni_web_sveucilista:voMember=true
```

na temelju kojega će korisniku biti omogućen pristup aplikaciji. Ovo je najjednostavniji primjer primjene virtualnih organizacija jer je za potrebe autorizacije dovoljno kreirati virtualnu organizaciju i u nju dodati korisnike koji trebaju imati pristup aplikaciji.

U nešto kompliciranijem slučaju možemo pretpostaviti da svi korisnici koji imaju pristup internom webu smiju dohvaćati sve sadržaje s tog weba, ali samo određeni korisnici (administratori) smiju stavljati nove sadržaje na web. Za takvu, finiju, kontrolu pristupa potrebno je unutar virtualne organizacije definirati novi atribut, npr. *status*, koji će imati dvije vrijednosti:

```
interni_web_sveucilista:status=korisnik
```

ili:

```
interni_web_sveucilista:status=administrator
```

i na temelju kojega će aplikacija odlučivati smije li korisnik stavljati nove sadržaje na web ili ima samo ovlasti dohvaćanti postojeće sadržaje s internog weba sveučilišta.

4. Dodatne informacije i odgovori na pitanja

Za sve dodatne informacije i odgovore na eventualna pitanja kontaktirajte nas elektroničkom poštom na aai@srce.hr