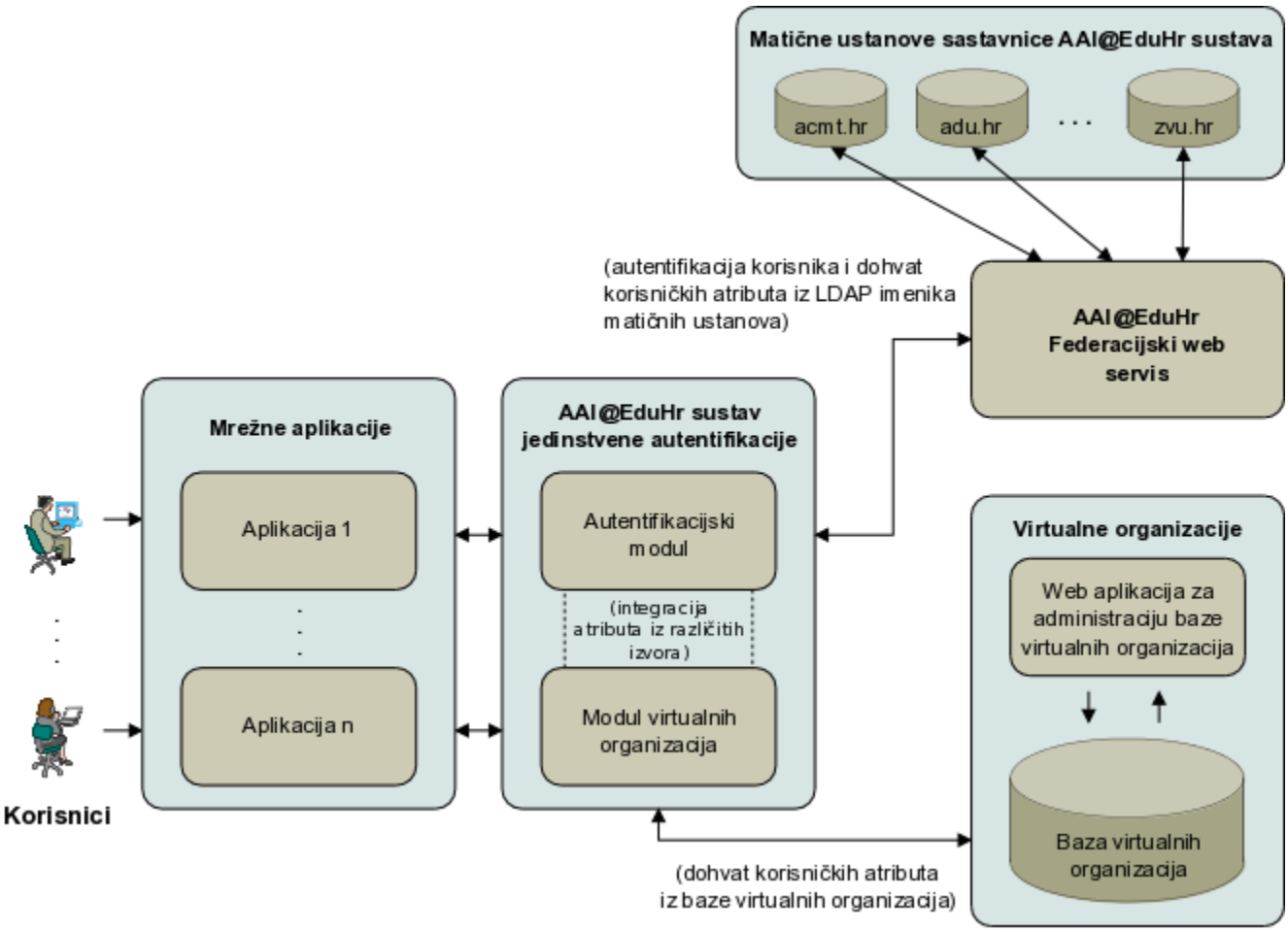
Virtualne organizacije

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 atribute 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.



Slika 1. Implementacija virtualnih organizacija u sustavu AAI@EduHr

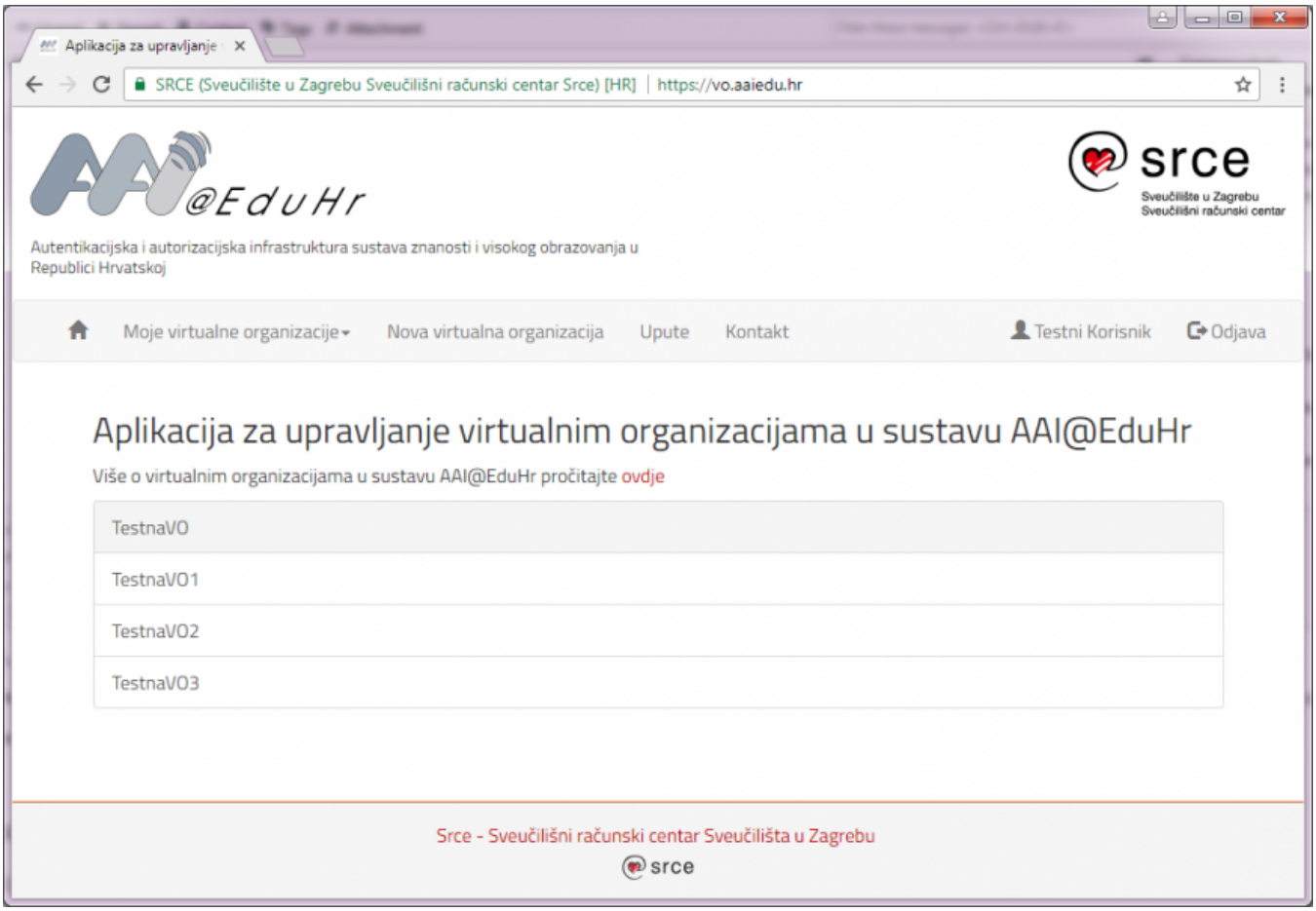
Za isporuku atributa definiranih unutar virtualnih organizacija koristi se SAML 2.0 protokol koji se koristi i za isporuku atributa pohranjenih u LDAP imenicima matičnih ustanova. Prednost ovakvog pristupa je u tome da niti jednu aplikaciju koja koristi Single Sign-on sustav nije potrebno posebno prilagođavati 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 prikazje 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 atribute koji se isporučuju odabranim resursima.

2.1. Kreiranje nove virtualne organizacije

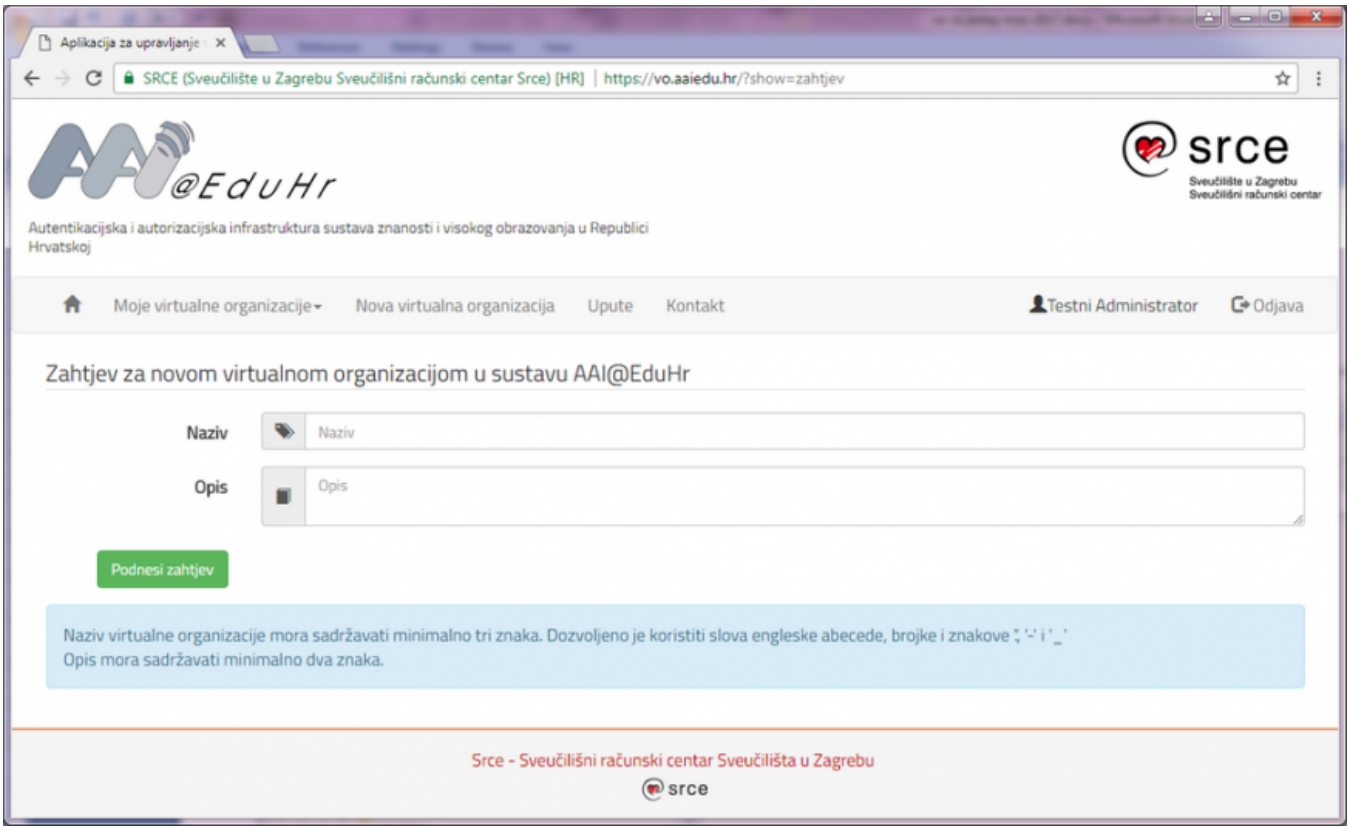
U izborniku aplikacije za upravljanje virtualnim organizacijama u sustavu AAI@EduHr odaberite "Nova virtualna organizacija"

Prilikom kreiranja virtualne organizacije potrebno je unijeti

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

U pravilu bi za jedan proizvod, projekt ili grupu korisnika trebala biti dovoljna jedna virtualna organizacija. Naravno, za različite proizvode ili projekte jedna osoba može zatražiti kreiranje više različitih virtualnih organizacija.

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.

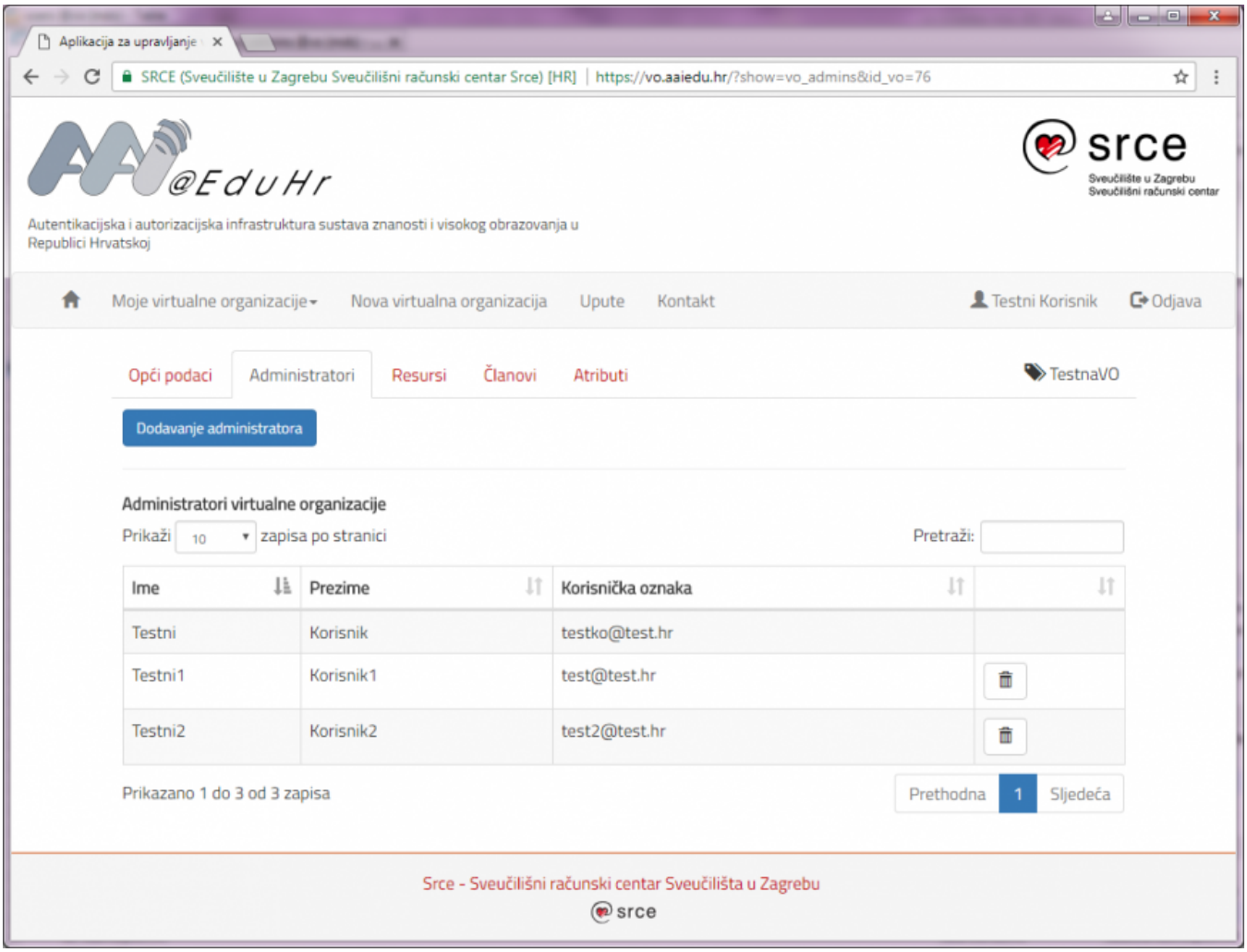


Slika 3. Zahtjev za otvaranjem virtualne organizacije

2.2. Uređivanje administratora virtualne organizacije

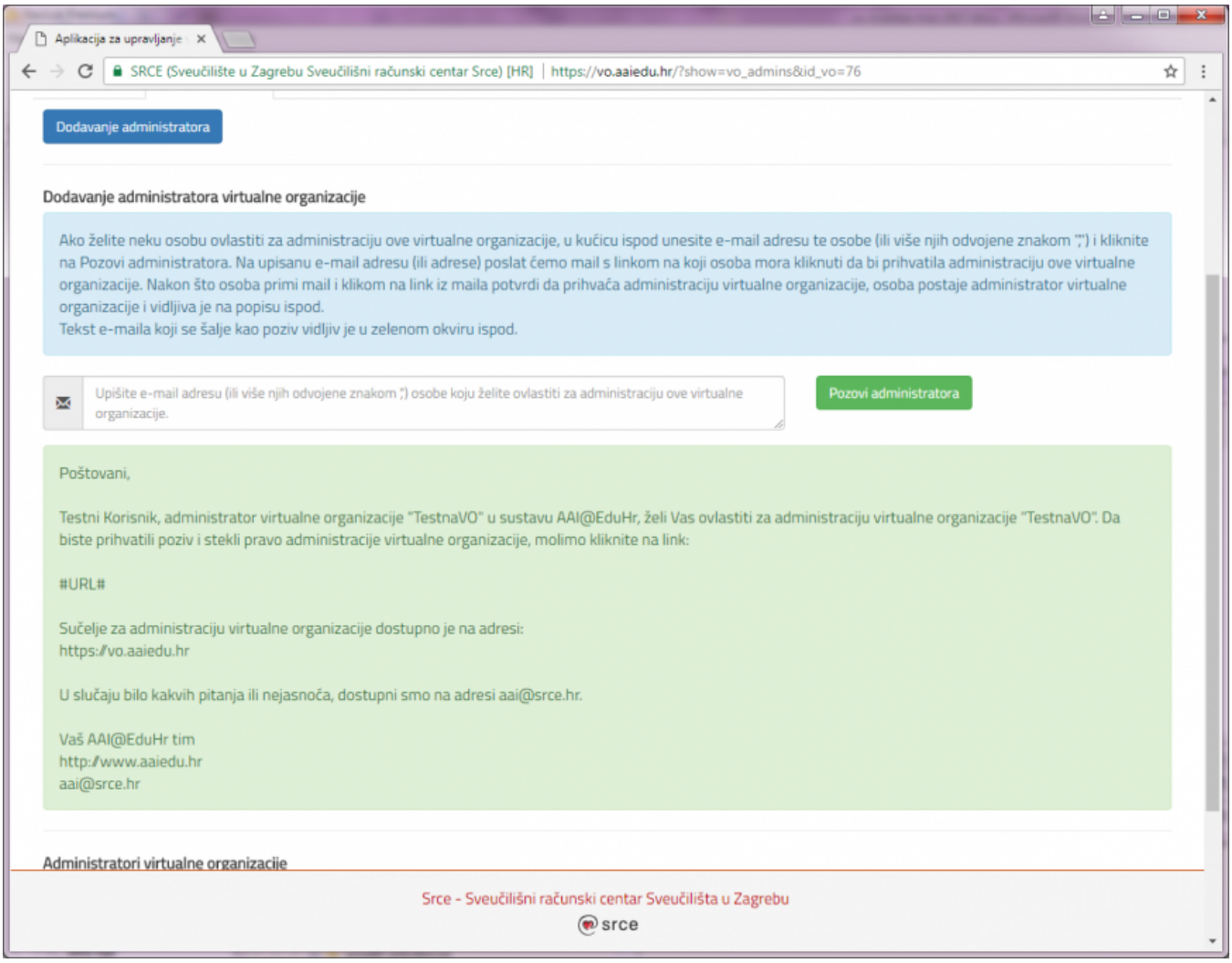
Nakon što u menuu odaberete željenu virtualnu organizaciju, u podizborniku odavrane virtualne organizacije kliknite na "Administratori".

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.



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:

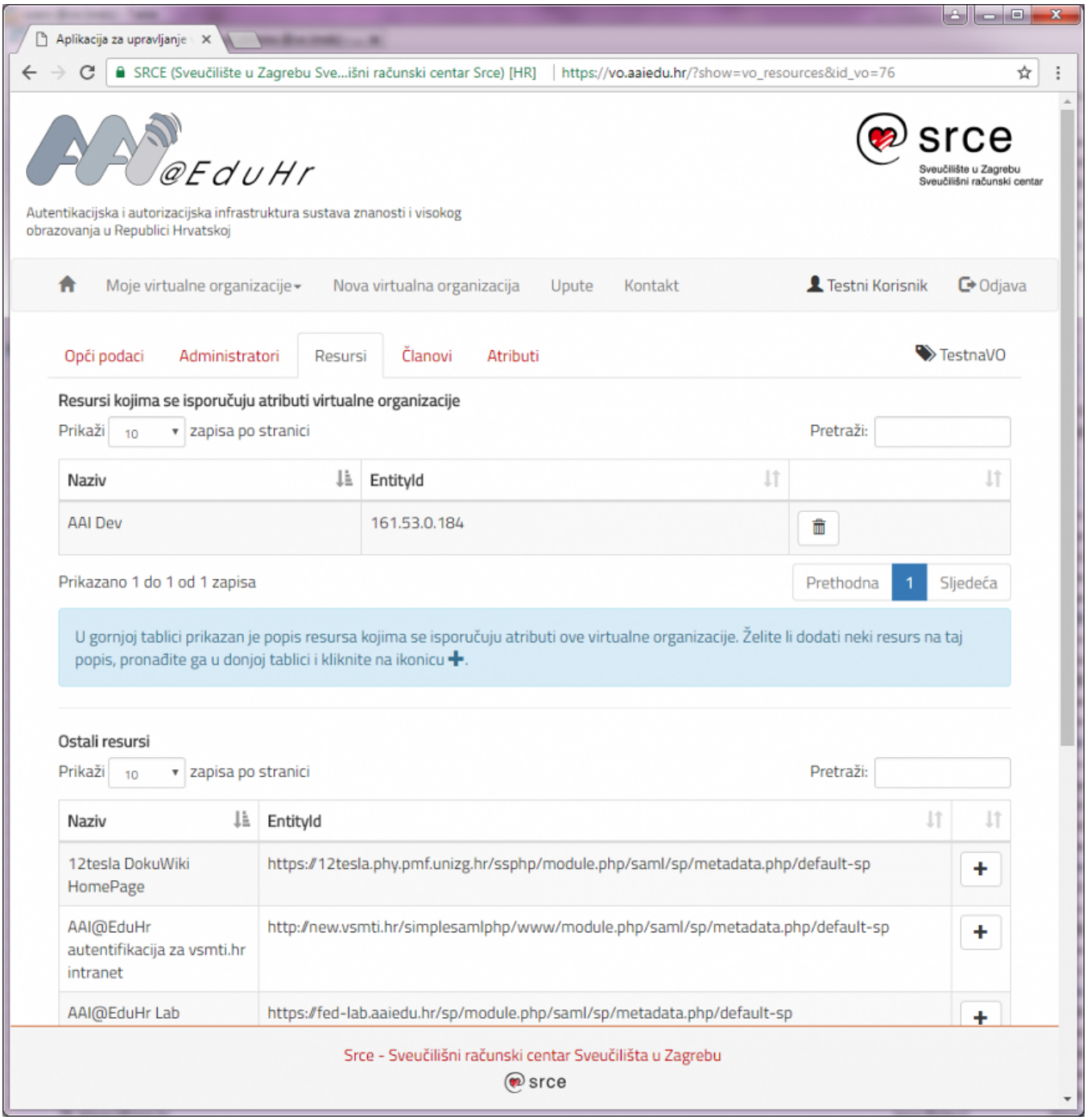


Slika 5. Dodavanje administratora virtualne organizacije

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

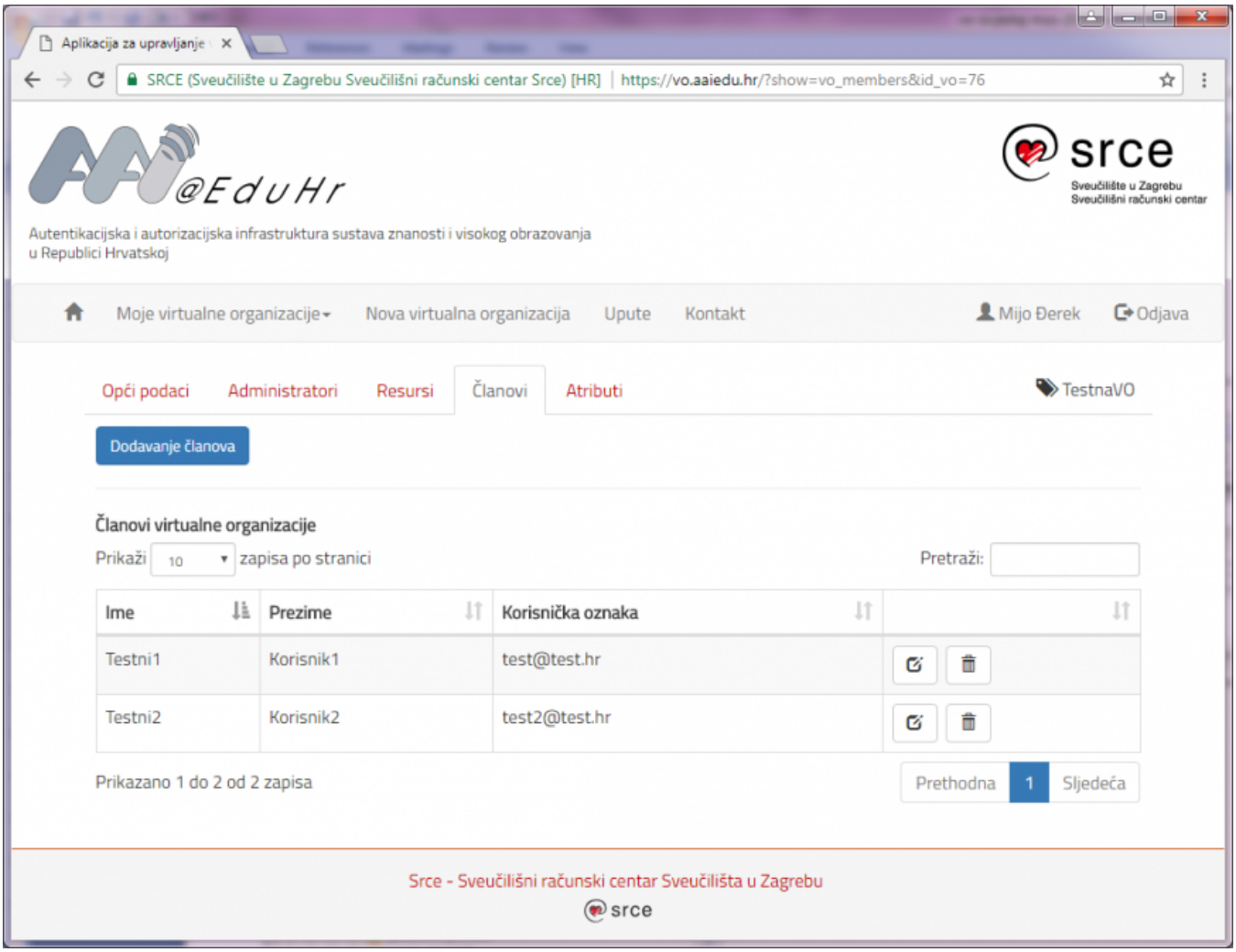
Odabirom ove opcije adminsitrator dobiva mogućnost odabrati resurse kojima će se isporučivati atributi virtualne organizacije. Na stranici su prikazana dva popisa. Gornji popis je popis onih resursa kojima se isporučuju atributi odabrane virtualne organizacije, a na donjem popisu su svi ostali resursi 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.



Slika 6. Administracija resursa kojima se isporučuju atributi virtualne organizacije

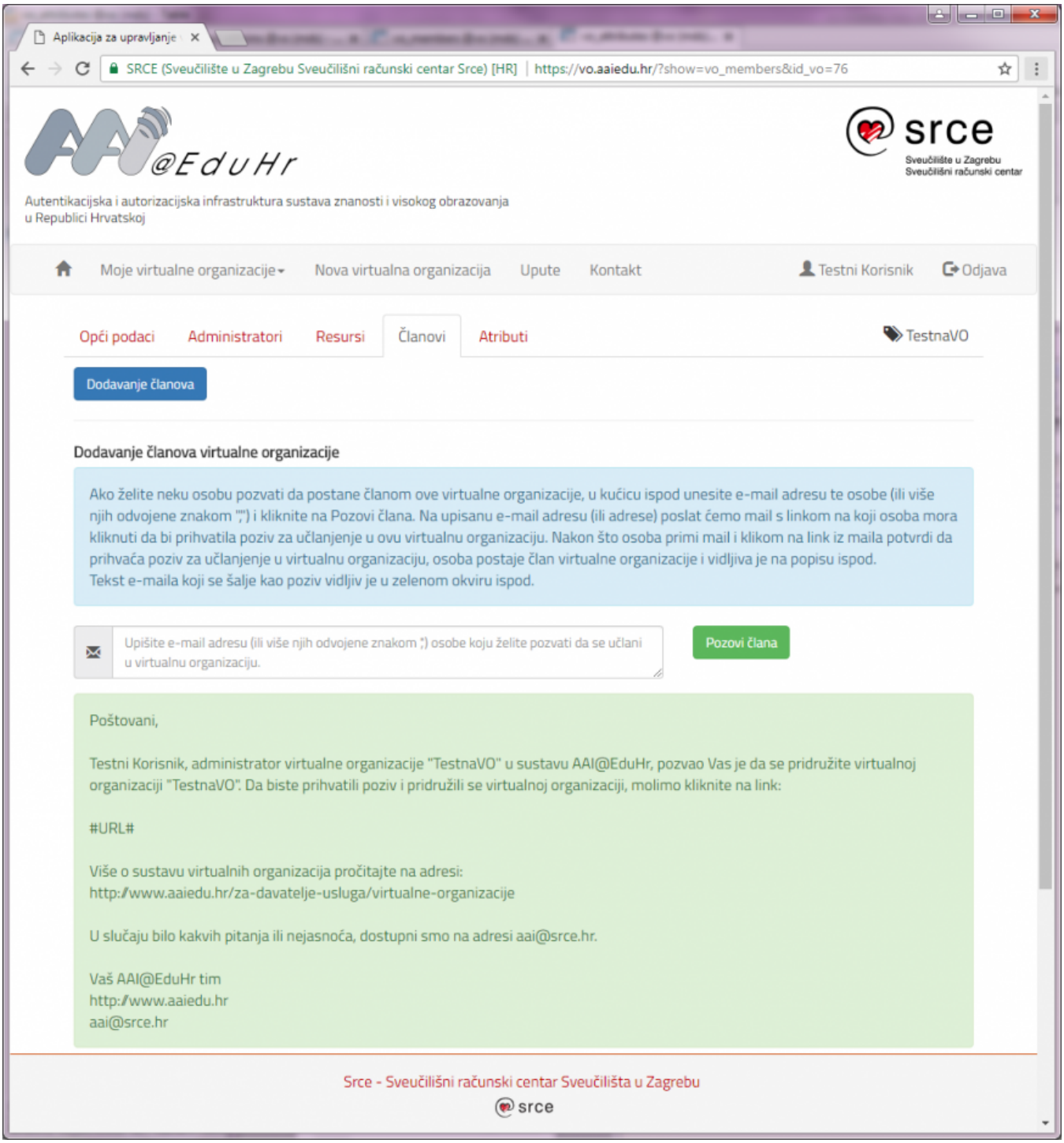
2.4. Članovi virtualne organizacije

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 atribute. VAŽNO: da biste mogli unijeti vrijednost pojedinog atributa virtualne organizacije za odabranog člana, prvo morate odrediti atribute virtualne organizacije u tabu Atributi.



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 autenticirati 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:

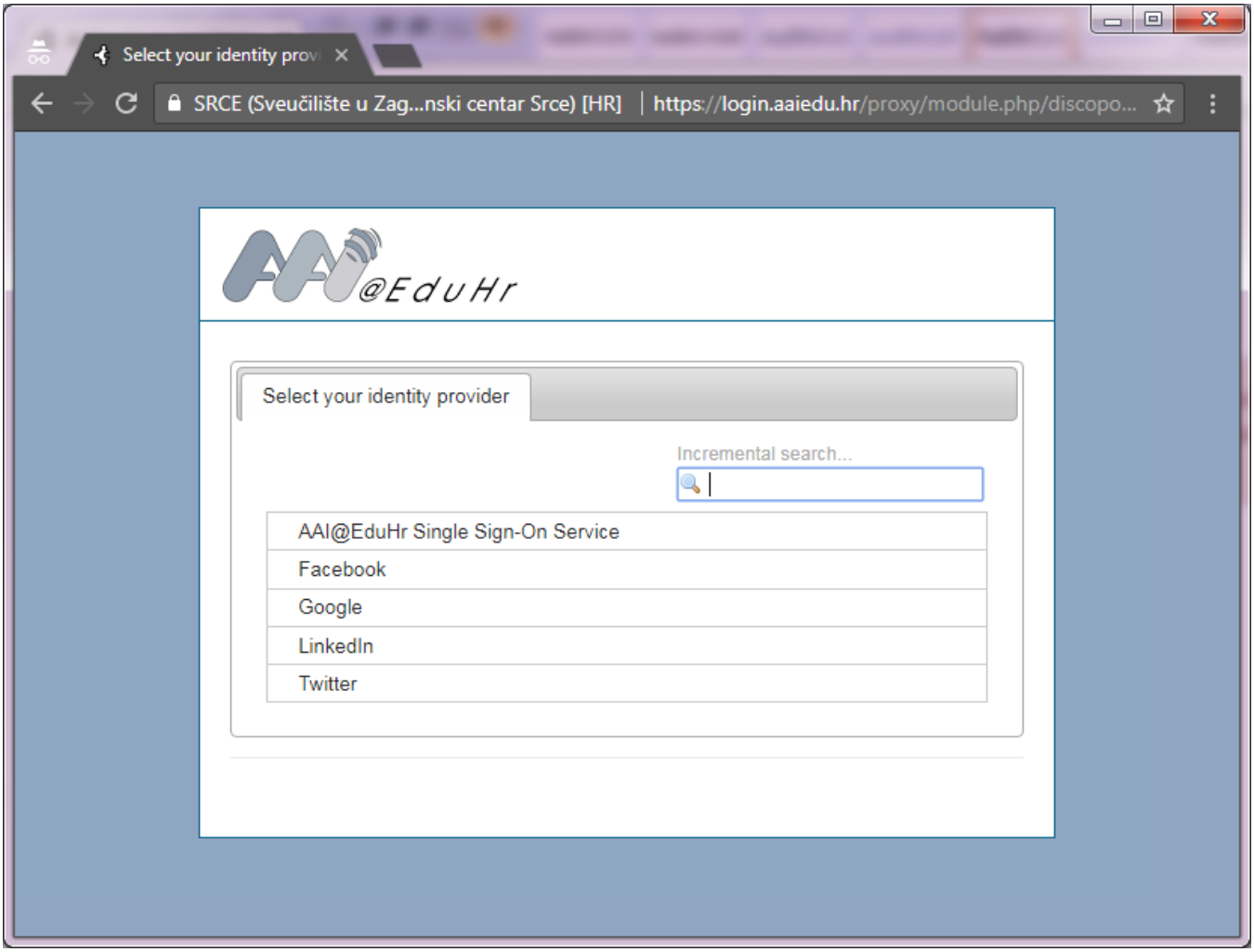


Slika 8. Sučelje za pozivanje članova virtualne organizacije

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 otvorit će joj se izbornik u kojem izabire kojim vjerodajnicama se želi autenticirati 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 autenticirati 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 društevnih mreža preko SSO servisa sustava AAI@EduHr i korisnik A se prilikom pristupa resursu C mora predstaviti istim (Google) vjerodajnicama kojima se autenticirao prilikom učlanjenja u virtualnu organizaciju B.

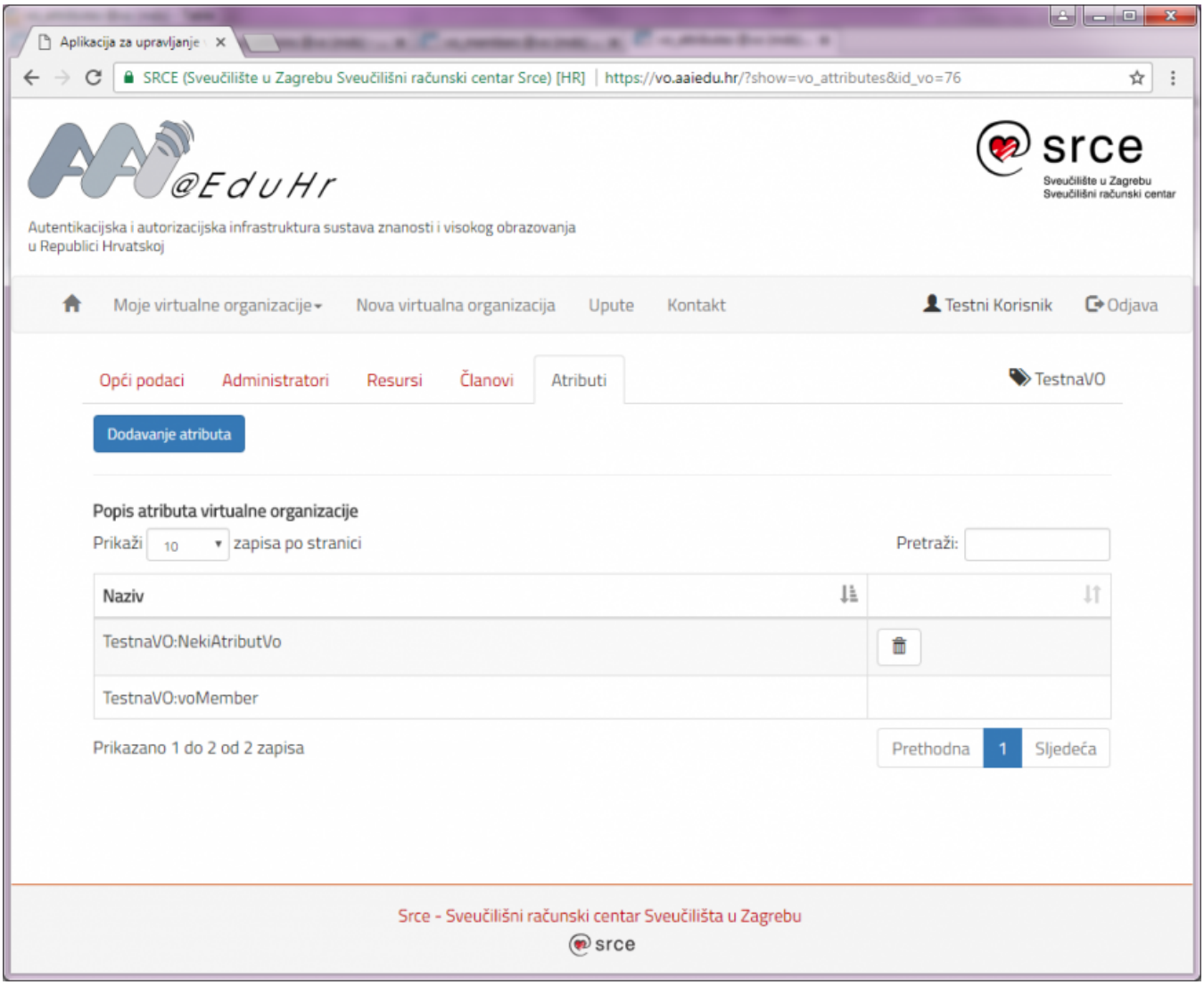
Također ja važno naglasiti da članovi virtualne organizacije ne moraju pripadati matičnoj ustanovi kojoj pripada administrator. Bilo koja osoba koja posjeduje elektronički identitet u sustavu AAI@EduHr može biti član bilo koje virtualne organizacije.



Slika 9. Odabir kojim će se vjerodajnicama korisnik autenticirati prilikom prihvaćanja 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 atribute definirane unutar virtualnih organizacija isporučuje u slijedećem obliku:

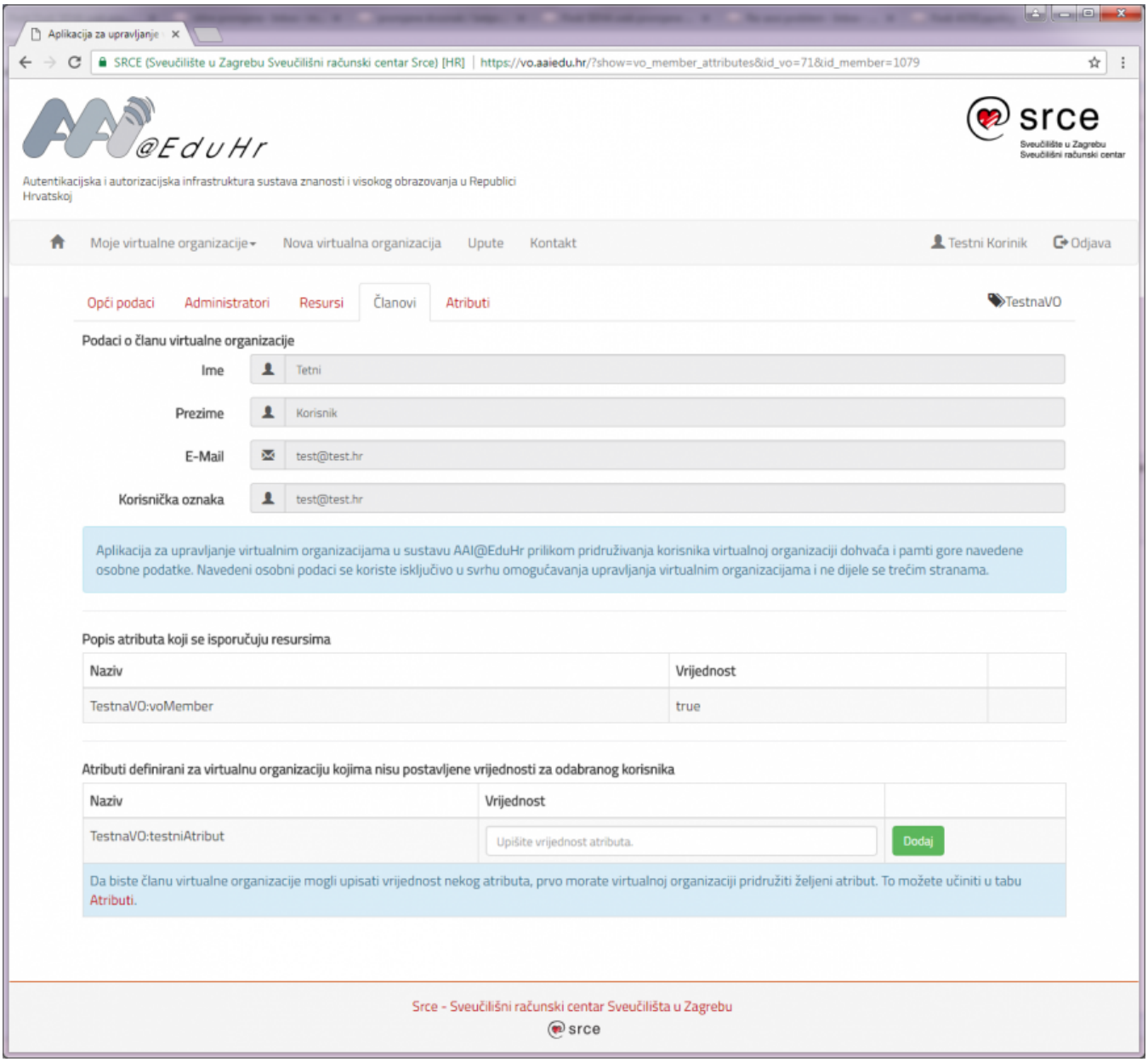
naziv_virtualne_organizacije:naziv_atributa = vrijednost_atributa

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

Želite li dodati atribut, klinkite 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 kliknite 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.



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 inormacije i odgovori na pitanja

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