Registar resursa

Registracija novog resursa, ažuriranje podataka o resursu i brisanje resursa u sustavu AAI@EduHr vrši se putem Registra resursa, središnjeg mjesta za pohranu konfiguracijskih postavki i općih podataka vezanih uz usluge koje za autentikaciju korisnika koriste sustav AAI@EduHr. Registar resursa dostupan je na poveznici:

https://registar.aaiedu.hr/

Pristup Registru resursa omogućava se isključivo ovlaštenim predstavnicima davatelja usluga koje za autentikaciju korisnika koriste sustav AAI@EduHr kako bi mogli registrirati nove usluge ili ažurirati postavke već registriranih usluga.

Davatelji usluga koje koriste sustav AAI@EduHr mogu biti matične ustanove u sustavu AAI@Eduhr ili partneri AAI@EduHr federacije.

Ako želite ponuditi uslugu za koju se korisnici trebaju autenticirati putem sustava AAI@EduHr, a vaša ustanova ili tvrtka nema pravo biti sastavnica AAI@EduHr infrastrukture, u sustav AAI@EduHr možete se uključiti kao partner AAI@EduHr federacije.

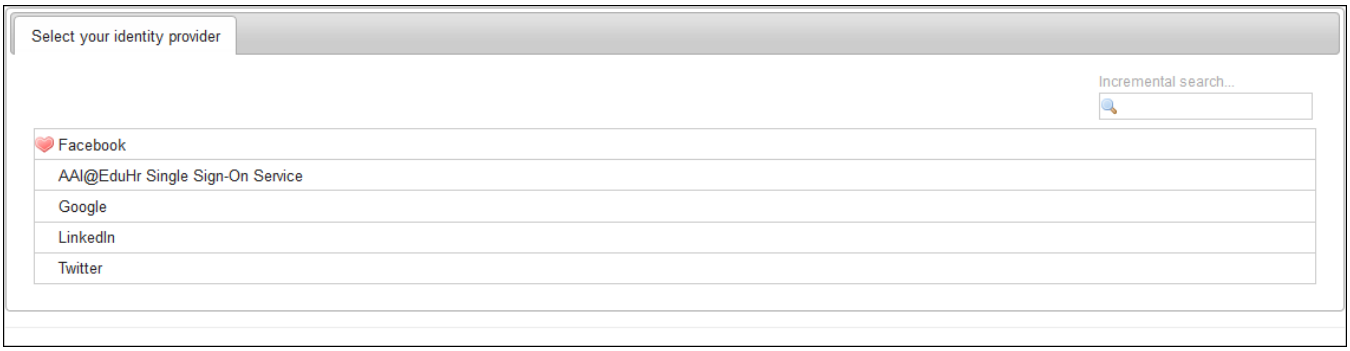
- Otvaranje korisničkog računa u Registru resursa
- Što je resurs?
- Postavljanje zahtjeva za registraciju resursa
- Opći podaci resursa
- Odabir autentikacijskog modula
- CAS konfiguracija
- SAML konfiguracija
    - Opće postavke
    - Adrese
    - Atributi
    - Namjene atributa
    - Vanjski autentikacijski mehanizmi
    - Konfiguracija za višestupanjsku autentikaciju
    - Konfiguracija za eduGAIN resurse
    - Automatsko dohvaćanje postavki
- OIDC konfiguracija
- RADIUS konfiguracija
- Postupak odobravanja i obrade zahtjeva
    - Direktne akcije nad testnim resursima za koje nisu potrebni zahtjevi i odobrenja
- Objašnjenje boja i indikatora statusa resursa

Otvaranje korisničkog računa u Registru resursa

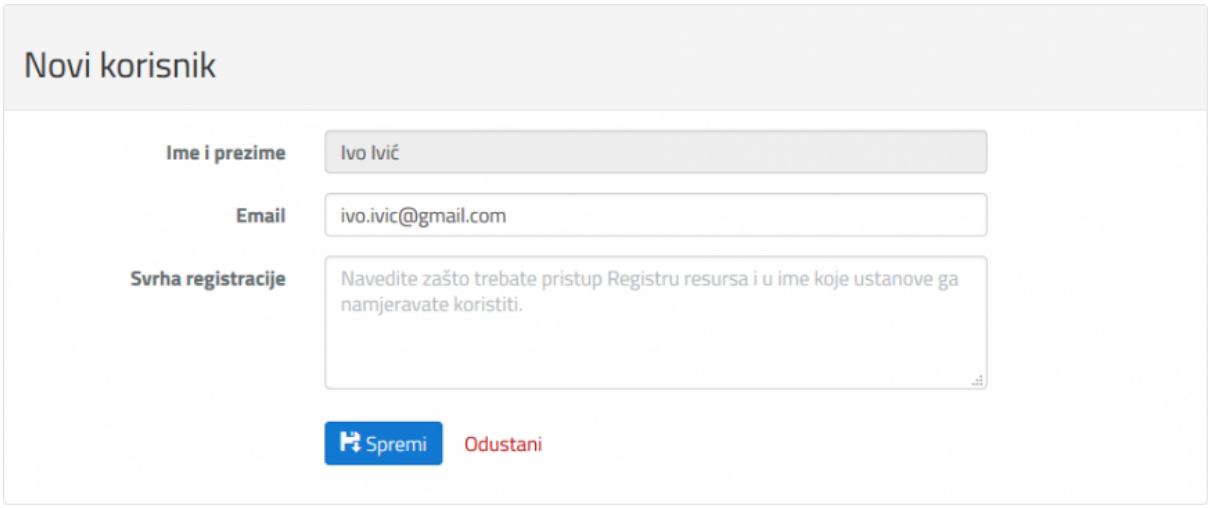
Pristup Registru resursa dozvoljen je isključivo ovlaštenim predstavnicima davatelja usluga u sustavu AAI@EduHr. Davatelji usluga u sustavu AAI@EduHr mogu biti matične ustanove u sustavu AAI@EduHr ili partneri AAI@EduHr federacije.

Ako ste ovlašteni predstavnik davatelja usluge, trebate se registrirati (otvoriti korisnički račun) u Registru resursa nakon čega će administrator AAI@EduHr autorizirati vaš korisnički račun za puni pristup aplikaciji. Prvi korak je prijava u Registar resursa korištenjem AAI@EduHr elektroničkog identiteta ili neke od vjerodajnica kreiranih na društvenim mrežama (Facebook, Google, LinkedIn, Twitter). Gumb za prijavu nalazi se na desnom kraju navigacijske trake:

Na sljedećoj stranici potrebno je odabrati vjerodajnicu za prijavu:



Sljedeći korak registracije korisnika je popunjavanje postavki korisničkog profila. U polju **Svrha registracije** važno je navesti opravdan razlog potrebe korištenja Registra kako bi administrator sustava AAI@EduHr bio siguran da je korisnik dobro upoznat sa svrhom i namjenom Registra resursa te ga namjerava koristiti u smislene svrhe.



Po kliku na gumb "Spremi", vaš korisnički profil će biti zapamćen i postupak registracije dovršen, o čemu će biti obaviješteni administratori sustava AAI@EduHr. Na temelju informacija iz vašeg profila vašem će korisničkom računu naknadno biti omogućena (ili odbijena) autorizacija za puni pristup i korištenje Registra, o čemu ćete biti obaviješteni elektroničkom poštom.

Što je resurs?

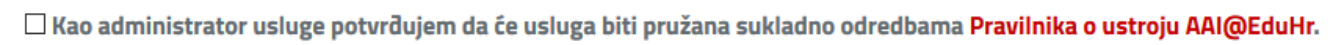
Resurs je entitet u sustavu AAI@EduHr koji, osim što sadrži osnovne podatke o aplikaciji/usluzi koja koristi sustav AAI@EduHr, obuhvaća i aktivne konfiguracije svih autentikacijskih mehanizama kojima se navedena aplikacija/usluga služi u sustavu. Resurs se dakle sastoji od **Općih podataka** i **autentikacijskih modula**. U prvu skupinu spadaju općenite informacije poput naziva, opisa i vrste resursa skupa s nazivom ustanove s kojom je resurs povezan i pripadajućim kontaktima za podršku. Svaki resurs, da bi bio aktivan i funkcionalan, mora imati pridružen najmanje jedan od dostupnih autentikacijskih modula. Autentikacijski modul je segment koji sadrži skup konfiguracijskih parametara za CAS, SAML, OIDC, FWS ili RADIUS protokol. Svaki resurs može imati najviše po jedan aut. modul za pojedinačnu vrstu autentikacije putem jednog od navedenih protokola, no autentikacijski mehanizmi time nisu ograničeni svaki na samo jedan poslužitelj. U svakom modulu može se uključiti više autentikacijskih poslužitelja s kojima aplikacija/usluga komunicira koristeći iste konfiguracijske parametre koje taj modul definira.

Postavljanje zahtjeva za registraciju resursa

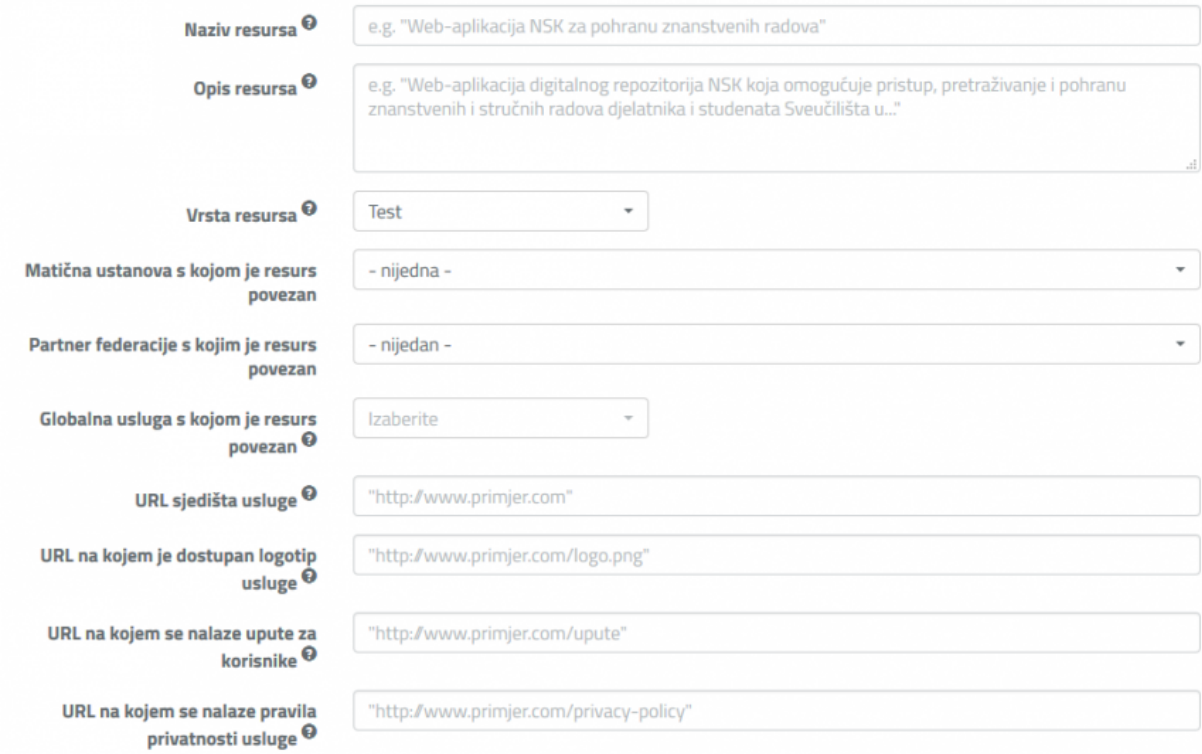
S autoriziranim pristupom u Registar resursa imate pravo kreirati zahtjeve za registraciju novih, te mijenjanje ili brisanje postojećih resursa čiji ste administrator. Na navigacijskoj traci nalazi se poveznica za pregled postojećih resursa (**Resursi**) te poveznica do forme zahtjeva za registraciju novog resursa (**Registracija resursa**). Ako još za nijedan resurs niste navedeni kao administrator, popis sa prve poveznice bit će prazan. Kliknite na poveznicu Registracija resursa i otvorit će se forma za unos općih podataka. Detaljniji opis te forme nalazi se u nastavku.

Opći podaci resursa

Na vrhu forme za unos općih podataka o novom resursu nalazi se kvadratić s naslovom "**Kao administrator usluge potvrđujem da će usluga biti pružana sukladno odredbama Pravilnika o ustroju AAI@EduHr**". U kvadratić trebate staviti kvačicu kako biste potvrdili da prihvaćate uvjete korištenja AAI@EduHr infrastrukture definirane Pravilnikom o ustroju autentikacijske i autorizacijske infrastrukture sustava znanosti i visokog obrazovanja u Republici Hrvatskoj.



U sljedećem nizu polja potrebno je unijeti podatke koji će u najvećoj mjeri biti javno dostupni korisnicima na stranici Aplikacije koje koriste sustav AAI@EduHr te je stoga bitno da podaci budu što jasniji i informativniji.



Naziv resursa i **opis resursa** mogu biti proizvoljni, no bitno je da krajnji korisnici iz naziva i opisa mogu nedvojbeno shvatiti koja je točna namjena resursa.

Osim ako se ne radi o nekoj već isprobanoj aplikaciji, za svaki novi resurs u sustavu AAI@EduHr koji je u fazi razvoja i testiranja u polju **Vrsta resursa** treba postaviti vrijednost "Test". Autentikacija za resurse koji su u fazi razvoja vrši se putem testne AAI@EduHr SSO infrastrukture čiji parametri su dostupni na web stranici AAI@EduHr Lab. Naknadne izmjene postavki u testnim resursima ne podilaze kreiranju zahtjeva i čekanju na odobrenje istih kao što je slučaj kod produkcijskih resursa; izmjene se umjesto toga prihvaćaju odmah, o čemu više možete pročitati u poglavlju "Postupak odobravanja i obrade zahtjeva".

U padajućem izborniku **Matična ustanova s kojom je resurs povezan** potrebno je odabrati odgovarajuću matičnu ustanovu, osim u slučaju kad je resurs vezan za Partnera federacije. Tada je umjesto prvog obavezan drugi padajući izbornik: **Partner federacije s kojim je resurs povezan**. Izbor **Globalne usluge s kojom je resurs povezan** nije obavezan.

U polje **URL sjedišta usluge** treba unijeti adresu početne stranice aplikacije na kojoj se nalazi gumb/poveznica za prijavu korisnika potem sustava AAI@EduHr.

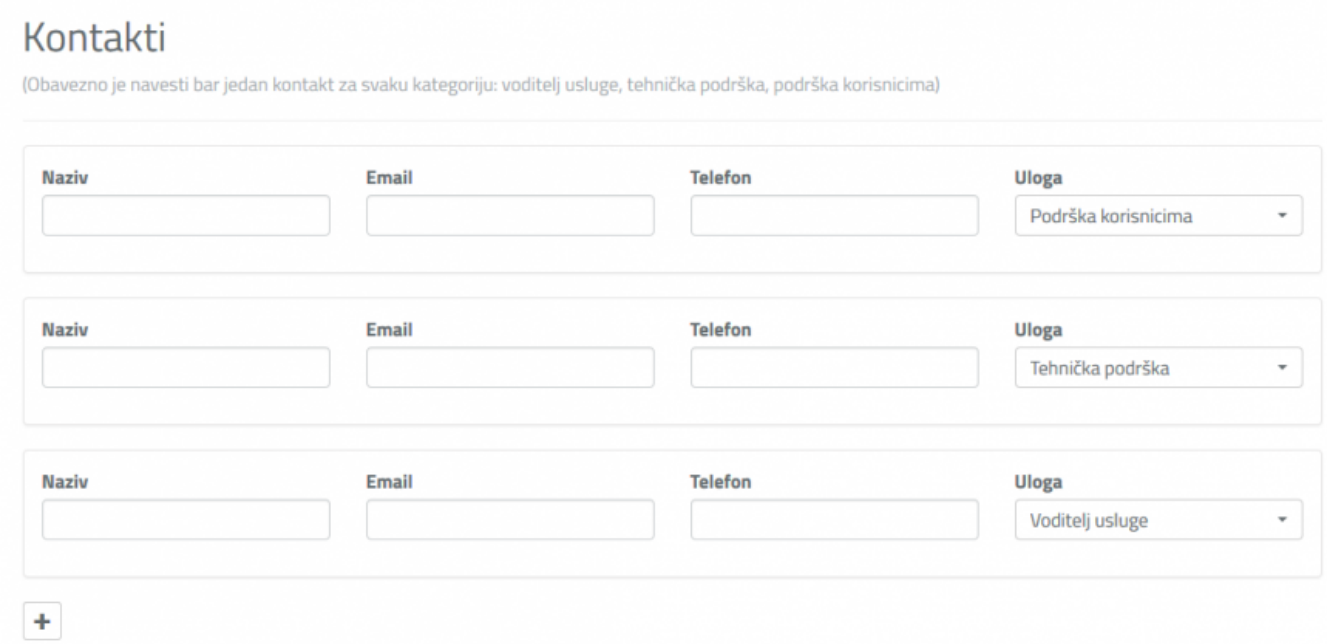
Ako postoji **URL na kojem je dostupan logotip usluge**, u polje treba unijeti direktan URL do datoteke logotipa. Preostala dva polja je potrebno popuniti ako postoje traženi podaci.

U odjeljku **Kontakti** trebate unijeti podatke najmanje po jednog kontakta za svaku od sljedeće tri kategorije:

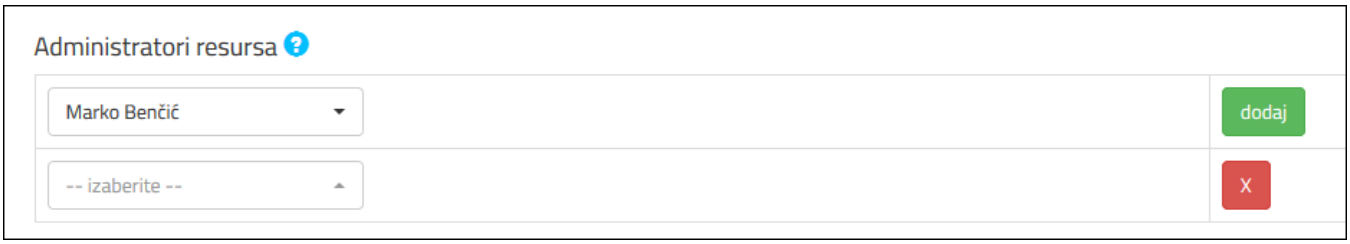
- Podrška korisnicima
- Tehnička podrška
- Voditelj usluge

Podaci o voditelju proizvoda i tehničkoj podršci koriste se isključivo interno, tj. služe AAI@EduHr timu kao kontakt podaci u slučaju da se pojavi nekakav problem s aplikacijom.

Podaci o službi koja bi trebala pružati podršku krajnjim korisnicima dostupni su javno, tj. prikazuju se nakon što korisnik odabere odgovarajući resurs na popisu produkcijskih resursa dostupnom na web stranici Aplikacije koje koriste sustav AAI@EduHr.



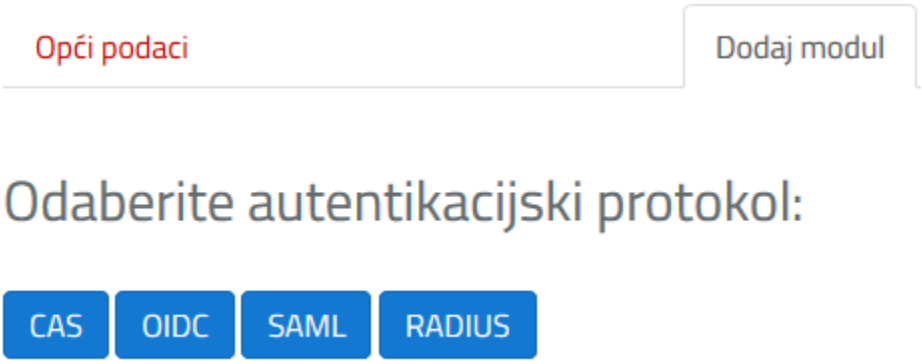
Pri dnu forme za unos općih podataka nalazi se tablica s popisom svih osoba koje su evidentirane u bazi Registra resursa. Ako želite da još netko osim vas ima mogućnost ažuriranja podataka o resursu, označite te osobe dodavanjem polja i odabirom tih osoba s liste.



Klikom na gumb **Zatraži registraciju** na dnu forme poslat ćete zahtjev. Čim to učinite trebate nastaviti i odabrati odgovarajući autentikacijski modul novoga resursa. Upute za taj dio slijede u nastavku.

Odabir autentikacijskog modula

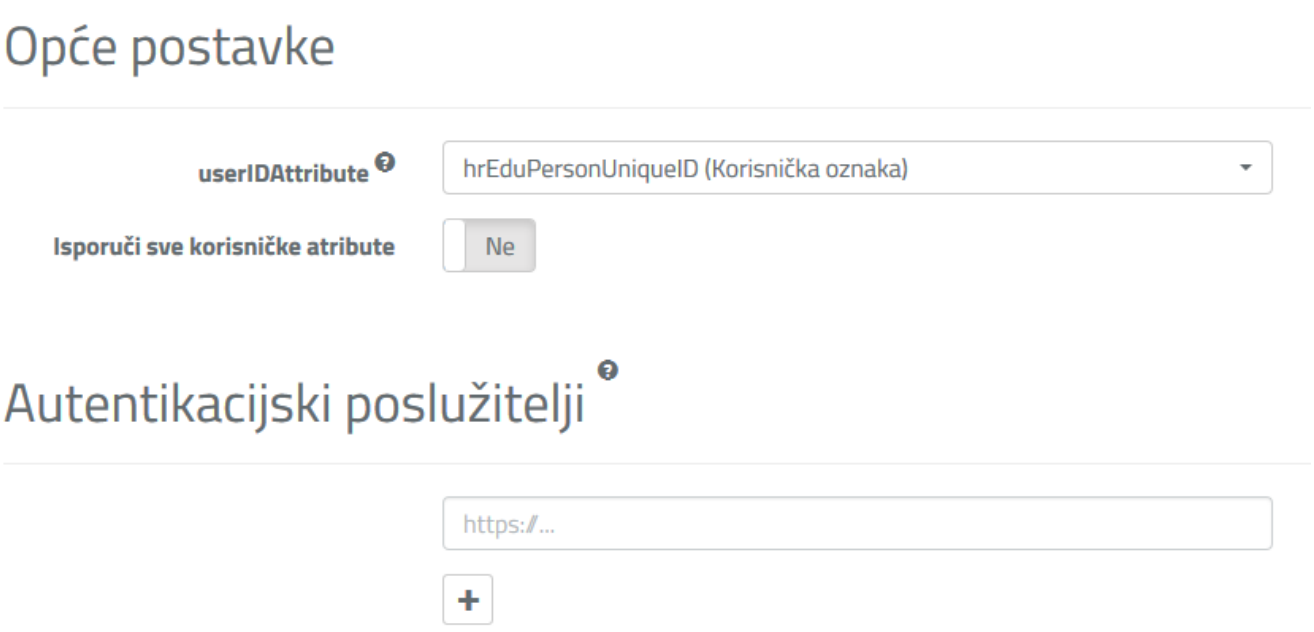
Svaki funkcionalan resurs mora imati najmanje jedan pridruženi autentikacijski modul. Ako se radi o novom resursu za kojega je netom kreiran zahtjev s općim podacima za registraciju, na stranici resursa će se, uz karticu "Opći podaci" nalaziti nova kartica **Odabir autentikacijskog modula**.



U slučaju da se radi o resursu s pridruženim nekim autentikacijskim modulom, a koji nema već pridružene sve vrste aut. modula, kartica **Dodaj modul** n alazit će se izdvojena uz desni rub stranice.

CAS konfiguracija

Ako odaberete modul za CAS autentikaciju, dobit ćete sljedeću formu:



Parametri CAS konfiguracije obuhvaćaju:

- Atribut koji će se isporučuje kao jedinstveni identifikator korisnika
- Izbor isporuke svih korisničkih atributa

- Popis URL-ova poslužitelja s kojeg stižu autentikacijski zahtjevi - moguće je dodavanje polja te **višestruki unos URL-ova** klikanjem na gumb '**+**'

SAML konfiguracija

Forma za unos SAML konfiguracije dijeli se na četiri cjeline: Opće postavke, Adrese, Atributi i Vanjski autentikacijski mehanizmi. Na vrhu stranice nalazi se polje za automatsko dohvaćanje postavki putem priloženih metapodataka davatelja usluge u XML formatu. Više o ovoj mogućnosti naći ćete na dnu ovih uputa za SAML konfiguraciju.

Opće postavke

Skup s naslovom "Opće postavke" sadrži parametre s jednostrukim vrijednostima za resurs u cjelini (za razliku od Adresa koje mogu biti višestruke, ovisno o broju krajnjih točaka koje predstavljaju). Opće postavke su:

Auth Service - Autentikacijski servis koji aplikacija koristi

Name Format - Kako se trebaju interpretirati nazivi atributa

NameID Format - Određuje način na koji se generira parametar NameID, odnosno njegov oblik. Ako je u ovom izborniku odabrana opcija "transient", za svaku novu prijavu NameID će biti nasumce generiran.

NameID Attribute - Naziv atributa čija se vrijednost koristi za generiranje parametra NameID u SAML porukama. Koristi se samo u slučaju kad je za NameID Format odabrana opcija "email" ili "persistent". Mora biti jedan od atributa koje davatelj usluge može primiti.

NameID Encryption - Kriptira li se parametar NameID u SAML porukama davatelju usluge

Encrypt Assertion - Kriptiraju li se *assertioni* (elementi tipa <saml:Assertion> - dio autentikacijskog odgovora koji sadrži korisničke podatke) u SAML poruci davatelju usluge

Sign Assertion - Da li se digitalno potpisuju *assertioni* (elementi tipa <saml:Assertion> - dio autentikacijskog odgovora koji sadrži korisničke podatke) u SAML poruci davatelju usluge

Sign Response - Da li se digitalno potpisuju autentikacijski odgovori (elementi tipa <saml:Response>) u SAML poruci davatelju usluge

Sign Logout - Da li se digitalno potpisuju zahtjevi za odjavu davatelju usluge

SP Encryption Certificate - Enkripcijski certifikat (s javnim ključem) davatelja usluge

SP Signing Certificate - Potpisni certifikat (s javnim ključem) davatelja usluge

Validate Authn Request - Odbacuju li se nepotpisani odnosno nevažeće potpisani zahtjevi za autentikaciju koje šalje davatelj usluge

Validate Logout Request - Odbacuju li se nepotpisani odnosno nevažeće potpisani zahtjevi za odjavu koje šalje davatelj usluge

Redirect Validate - Ovjeravaju li se potpisi zahtjeva za autentikacijom i zahtjeva za odjavom koje šalje davatelj usluge

Force Authn - Zahtijeva li se reautentikacija prilikom svakog pristupa korisnika davatelju usluge (ignoriranje SSO sjednice)

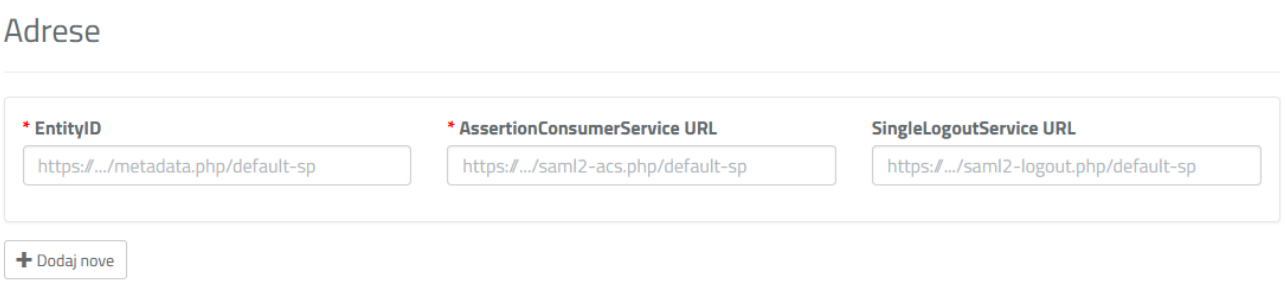
IdP Certificate - (samo za Office 365 resurse) Ime datoteke koja sadrži certifikat davatelja identiteta

Adrese

Odjeljak pod nazivom **Adrese** sadrži jedan ili više skupova s po tri parametra:

1. **EntityID** - Jedinstveni identifikator (instance) vaše aplikacije na razini AAI@EduHr federacije.
2. **AssertionConsumerService URL** - Adresa na koju sustav jedinstvene autentikacije preusmjerava korisnikov web-preglednik nakon uspješne autentikacije.
3. **SingleLogoutService URL** - Adresa za odjavu (poništavanje SSO sjednice aplikacije) na koju sustav jedinstvene autentikacije preusmjerava korisnikov web-preglednik tijekom izvođenja procesa jedinstvene odjave (Sigle Logout).

Iako se resurs u sustavu AAI@EduHr predstavlja jednu aplikaciju, ta aplikacija u praksi može imati **više instanci**. Gornja tri parametra su jedini parametri resursa koji mogu zauzimati različite vrijednosti ovisno o lokaciji svake instance iste aplikacije. Stoga nije uobičajeno otvarati novi, zasebni resurs za svaku instancu aplikacije koja je već registrirana u sustavu AAI@EduHr, već sve se sve one okupljaju i vode pod istim resursom. Da biste uvrstili novu instancu kao jednu od krajnjih točaka koje koriste ovaj resurs, kliknite gumb "**Dodaj nove**". Pojavit će se novi set praznih polja EntityID, AssertionConsumerService URL i SingleLogoutService URL u koje možete upisati podatke.

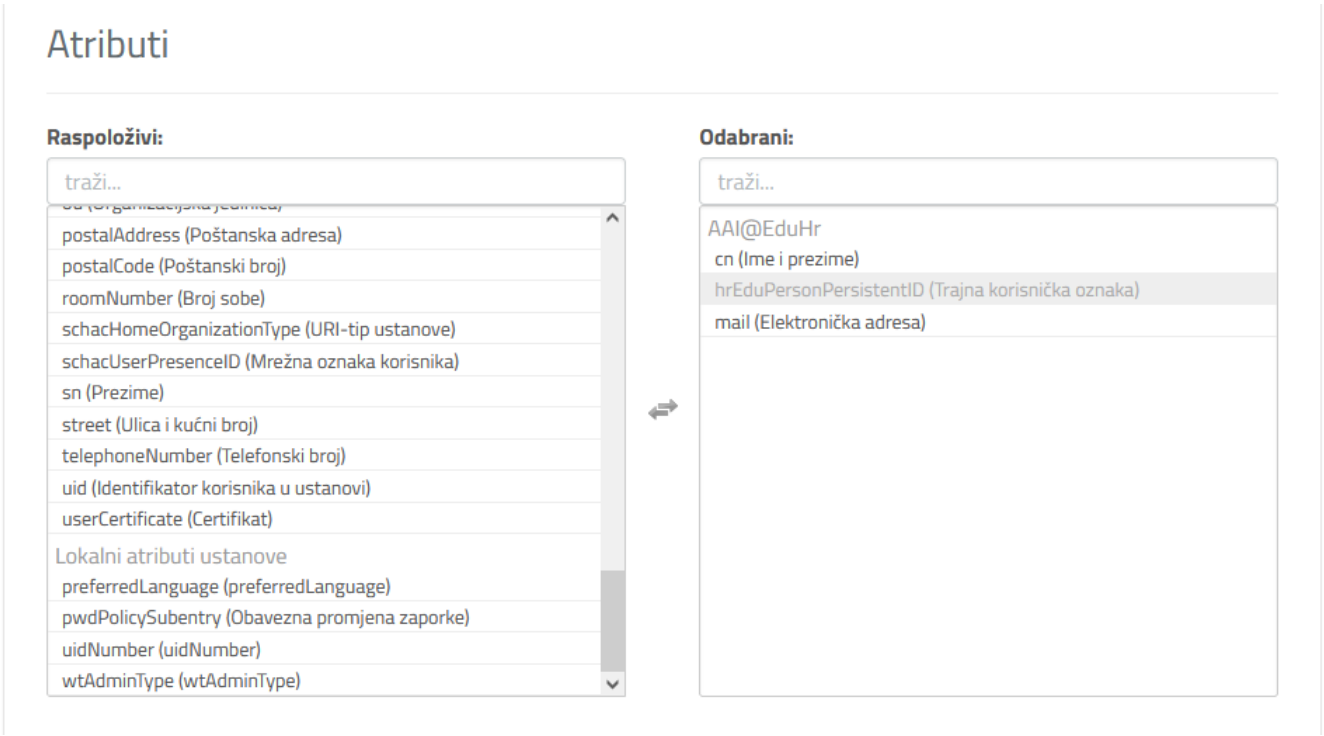


Ovisno o programskom jeziku u kojem je vaša aplikacija napisana, vrijednosti navedenih parametara za SAML metapodatke možete pronaći u odgovarajućoj konfiguracijskoj datoteci ili na određenoj web adresi:

- Ako je vaša aplikacija napisana u programskom jeziku PHP, tj. ako kao autentikacijski modul koristite simpleSAMLphp instaliran i iskonfiguriran prema uputama za implementaciju AAI@EduHr SSO mehanizma u PHP ailikacijama, vrijednosti parametara **entityID**, **assertion ConsumerService** i **singleLogoutService** možete pronaći preko simpleSAMLphp administratorskog sučelja kao što je opisano u odjeljku Regist racija novog resursa u sustavu AAI@EduHr;
- Ako vaša aplikacija kao autentikacijski modul koristi OIOSAML.NET instaliran i iskonfiguriran sukladno uputama za implementaciju AAI@EduHr SSO mehanizma u .NET ailikacijama, parametre **entityID**, **AssertionConsumerService Location** i **SingleLogoutService Location** možete pronaći u datoteci **metadata.ashx** koja se spominje u 13. koraku;
- Ako koristite Python/Django i SSO autentikaciju ste implementirali prema uputama na web stranici https://gist.github.com/darbula/5003f1d2e1528b089b30, vrijednosti parametara **entityid**, **assertion_consumer_service**, **single_logout_service** navedene su u datoteci **setting s.py**;

Atributi

Pod odjeljak **Atributi** spada izbornik za odabir Atributa i polja za upisivanje njihove namjene. Izbornik za biranje atributa podijeljen je na dva segmenta: lijevi - koji predstavlja skup raspoloživih atributa koji još nisu odabrani - i desni u kojem se nalaze svi odabrani atributi. Klikanjem po nazivima atributa u lijevom popisu selite taj atribut u desni popis i obrnuto; klikom na atribut u popisu odabranih vraćate ga na popis raspoloživih, tj. poništavate njegov odabir. Svaki od dva popisa moguće je pretraživati (filtrirati) pomoću polja "traži…" na vrhu svakog od njih.



Ako se na popisu odabranih pojavi atribut s posivljenim nazivom i onemogućen za klikanje, to je atribut za tvorbu parametra NameID koji je na popis automatski uvrstio izbornik "NameID Attribute". Budući da tvorba NameID-ja ovisi o spomenutom atributu, njega nije moguće ručno ukloniti s popisa odabranih. To možete učiniti tako da promijenite izbor "NameID Attribute" ili da za NameID Format odaberete "transient". Potom će se spomenuti atribut otključati za klikanje i moći ćete ga maknuti s popisa.

Svaki ručno odabrani atribut donosi sa sobom polje za upis njegove namjene. Iznimka je jedino atribut rezerviran za tvorbu parametra NameID (iz čega je razvidna njegova namjena). Više o obaveznom upisu namjena atributa pročitajte u poglavlju "Namjene atributa".

Skup odabranih atributa mora biti minimalan; dozvoljava se označiti isključivo one atribute koji su potrebni za ispravno funkcioniranje vaše aplikacije. U slučaju da se u budućnosti pokaže potreba za proširivanjem tog skupa, to se može učiniti novim zahtjevom za ažuriranje konfiguracije.

Važno je napomenuti da su pojedini atributi u sustavu AAI@EduHr opcionalni. Ovisno o tome je li za neki atribut unesena vrijednost ili ne, sustav AAI@EduHr može ili ne mora isporučiti te atribute. Također, atributi u podskupini **Lokalni atributi ustanove** su specifični za domenu **skole.hr** i druge ustanove u sustavu AAI@EduHr ih ne koriste. Više informacija o standardnim atributima koje sustav AAI@EduHr može isporučiti vašoj aplikaciji možete pronaći na web stranici hrEdu imeničke sheme.

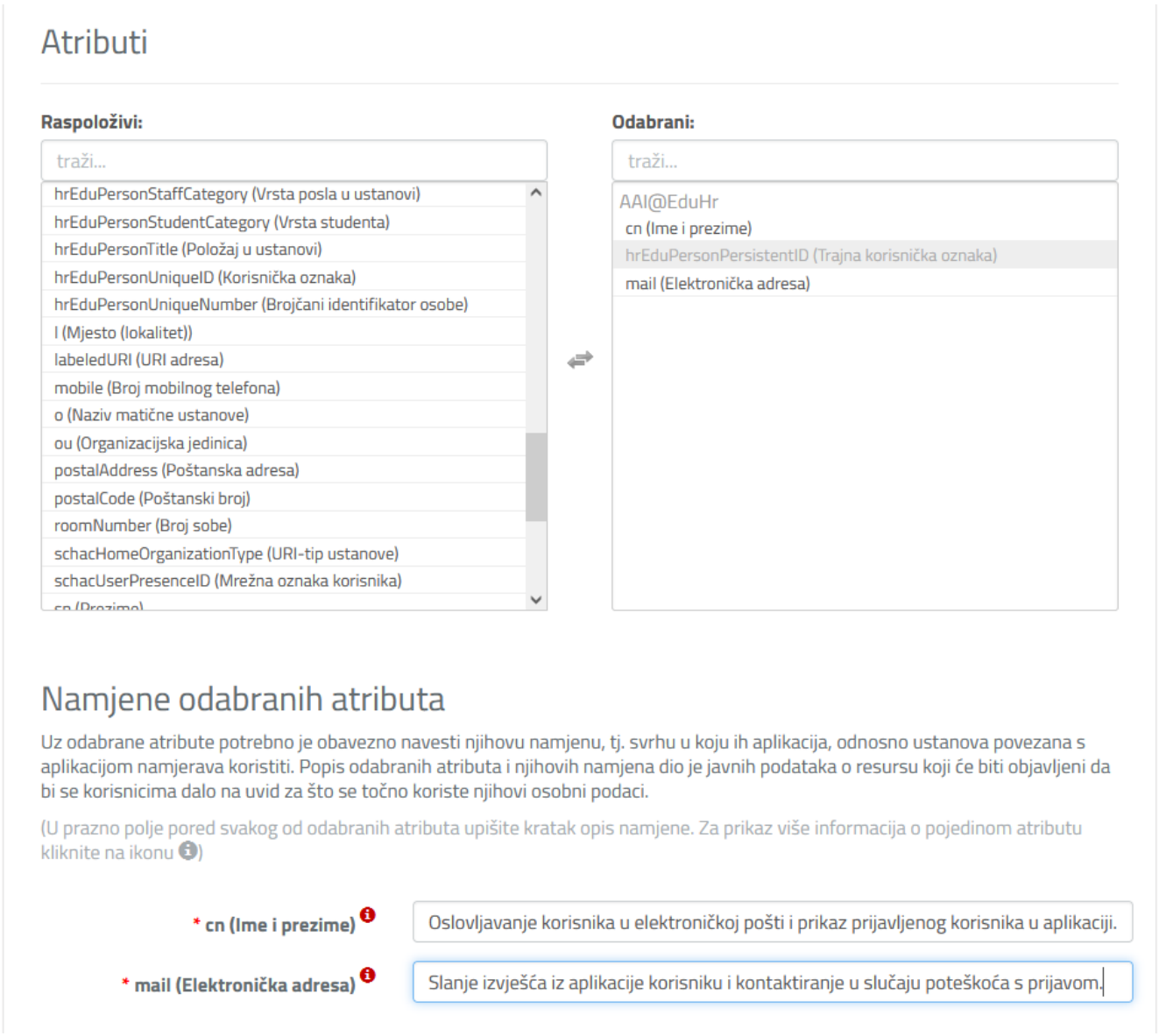
Namjene atributa

Sa svakim ručnim odabirom pojedinog atributa, u nizu ispod izbornika atributa naslovljenom "**Namjene odabranih atributa**" pojavljuje se polje za upis njegove namjene u vašoj aplikaciji ili sustavu. Ova polja su obavezna i služe za navođenje svih razloga posezanja za informacijom u sadržanom u tom atributu, tj. objašnjenja **zašto vaša aplikacija ili sustav treba upravo tu informaciju o prijavljenom korisniku** te što s njom namjerava činiti.

Pravilnik sustava AAI@EduHr nalaže da davatelj usluge mora obrazložiti odabir svakog atributa koji želi koristiti za pristup svojim uslugama. To je nužno ne samo radi poštivanja Opće uredbe o zaštiti podataka (GDPR), već i radi kontrole sigurnosti i pouzdanosti sustava AAI@EduHr. Upravo zbog toga se te informacije (namjene atributa) objavljuju javno na našim stranicama. Kroz navedene opise namjena davatelj usluge mora **potvrditi i jasno dati do znanja korisnicima da se njihovi podaci ne zlorabe i ne prosljeđuju trećoj strani** (što je zabranjeno pravilnikom AAI@EduHr), već da ih se koristi samo i isključivo za potrebe ispravnog funkcioniranja aplikacije odnosno sustava.

Osnovni naputci za pisanje obrazloženja namjena:

1. Obrazloženja trebaju biti jasna i nedvosmislena te po mogućnosti što kraća.
2. Ako se atribut koristi u više svrha, svaka od njih treba biti navedena.
3. Ako aplikacija ili sustav pohranjuje podatke sadržane u atributu, to je potrebno navesti i iz tog navoda mora biti jasno zašto je pohranjivanje tih podataka neophodno za funkcioniranje aplikacije odnosno sustava.
4. Ako se podaci iz atributa u nekom trenutku prosljeđuju van aplikacije u širi sustav ili u neku drugu aplikaciju na daljnju obradu, to također treba biti navedeno i opravdano.



Vanjski autentikacijski mehanizmi

U ovom odjeljku moguće je pored prijave putem sustava AAI@EduHr uključiti i neke od vanjskih autentikacijskih opcija za prijavu u vašu aplikaciju:

- Google
- Facebook
- LinkedIn
- Twitter
- ba (Autentikacijska i autorizacijska infrastruktura obrazovnih institucija u BiH)
- ASSECO TWIN

Vanjski autentikacijski servisi imaju vlastite politike isporuke atributa, stoga su njihova vrsta i količina nešto nad čime sustav AAI@EduHr nema kontrolu.

Konfiguracija za višestupanjsku autentikaciju

U sustavu AAI@EduHr moguće je registrirati uslugu koja će za prijavu korisnika koristiti višestupanjsku autentikaciju, gdje prvi stupanj predstavlja korištenje korisničke oznake i zaporke iz sustava AAI@EduHr, a drugi stupanj korištenje jednokratnih tokena.

Trenutačno podržani sustavi koji generiraju jednokratne tokene su:

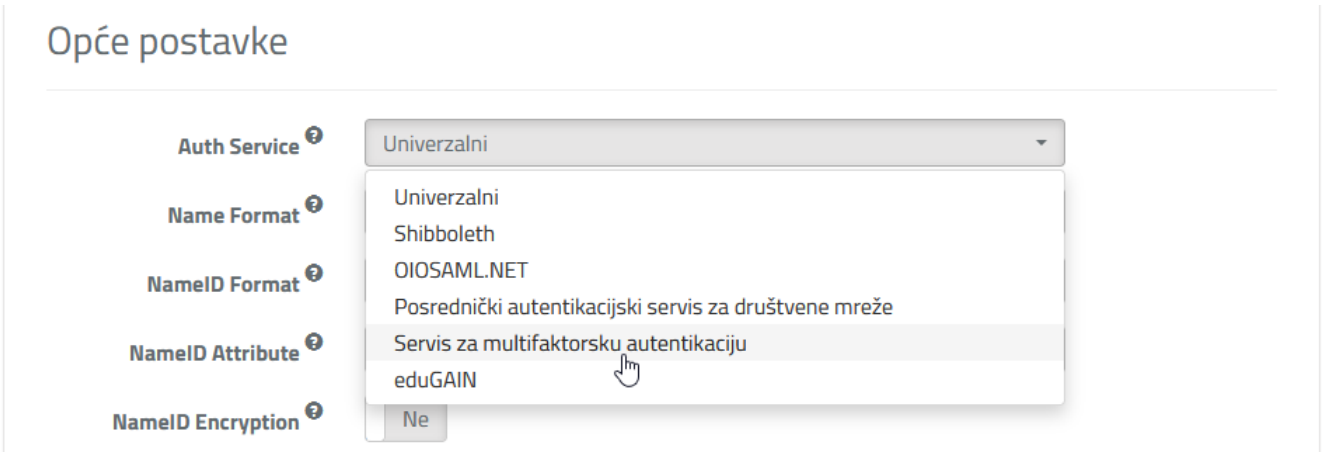
- OTP (One Time Password) via SMS (uz korištenje mobilnog telefona korisnika) - korisnik upisuje token kojeg dobiva putem SMS-a na registirani telefonski broj
- Yubico Yubikey (https://www.yubico.com) uređaj (kojeg korisnik mora posjedovati) - korisnik prenosi token putem Yubikey uređaja
- TOTP (Time-based One Time Password) uz korištenje posebne aplikacije (npr. Google Authenticator, FreeOTP ili OpenOTP) koju korisnik mora instalirati na svoje računalo - korisnik upisuje token koji mu je izgenerirala aplikacija (temeljem registriranog tajnog ključa).

Napominjemo kako autentikaciju putem tokena poslanog SMS-om (OTP via SMS) smatramo namanje sigurnom (u odnosu na ostale raspoložive sustave odnosno metode). Osim toga, za potrebe produkcijskog rada, usluga treba osigurati odgovarajući SMS gateway odnosno podmiriti troškove njegovog rada.

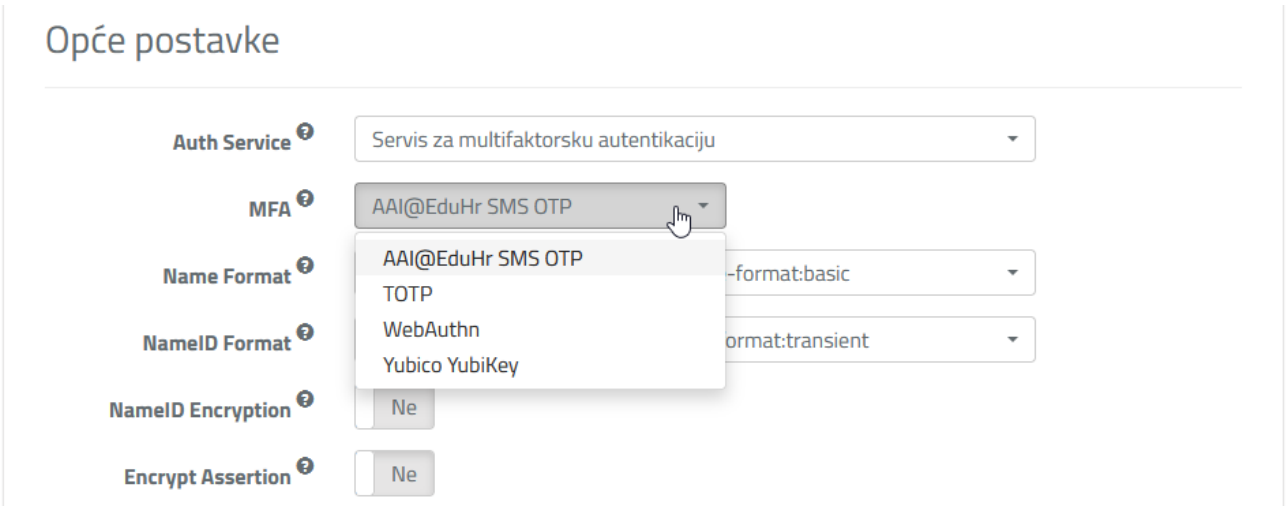
U svrhu registracije usluge koja će za prijavu korisnika koristiti višestupanjsku autentikaciju potrebno je slijediti poveznice u nastavku:

1. Postavljanje zahtjeva za registracijom novog resursa (Aplikacija koja će za prijavu korisnika koristiti višestupanjsku autentikaciju treba biti registrirana u Registru resursa isključivo kao nova usluga u sustavu AAI@EduHr)
2. Opći podaci
3. Odabir autentikacijskog modula (SAML).

Kod odabira konfiguracije za SAML modul dobivamo formu u čijem je izborniku za Auth Service (Autentikacijski servis) potrebno odabrati opciju ***Servis za multifaktorsku autentikaciju.***



Potom se pojavljuje novi izbornik "MFA" u kojem možemo odabrati tip višestupanjske autentikacije.

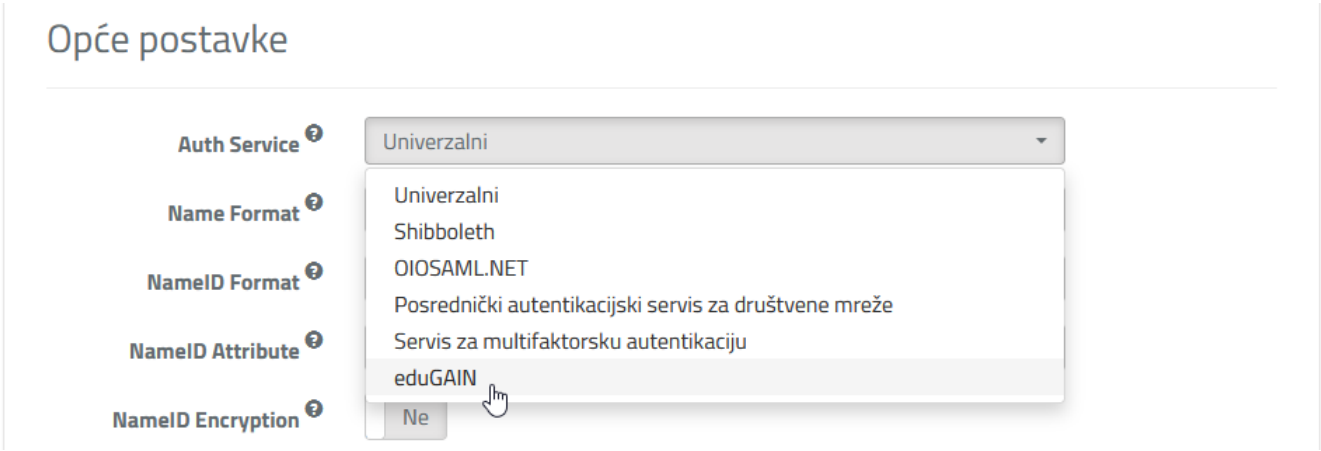


Sustav višestupanjske autentikacije putem atributa ***mfa_type*** vraća informaciju o vrsti drugog stupnja koji je korišten za autentikaciju.

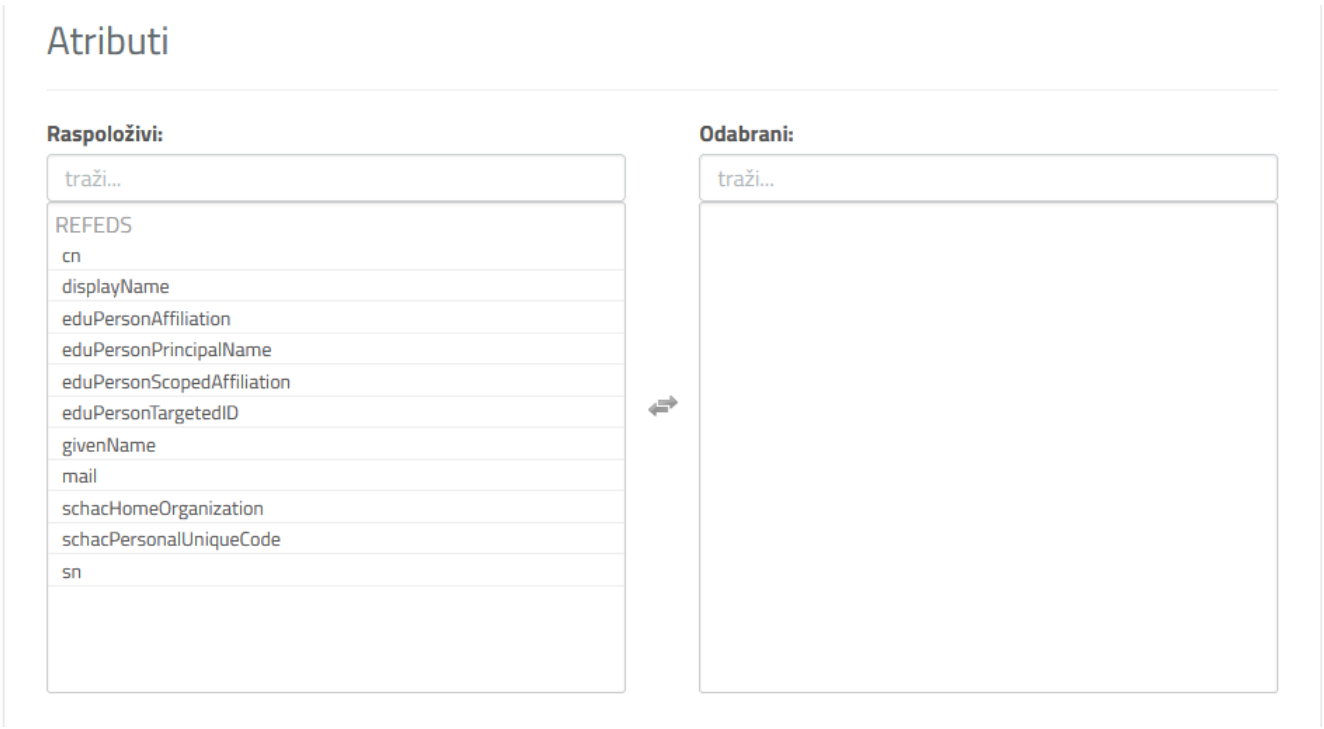
Kao zadnji korak preostaje ispunjavanje SAML metapodataka prema uputama na poveznici SAML konfiguracija, odjeljak Adrese.

Konfiguracija za eduGAIN resurse

Ako želite omogućiti da vaša aplikacija bude dostupna široj, internacionalnoj zajednici putem infrastrukture eduGAIN, to možete učiniti tako da u izborniku **Auth Service** kao autentikacijski servis odaberete "eduGAIN".



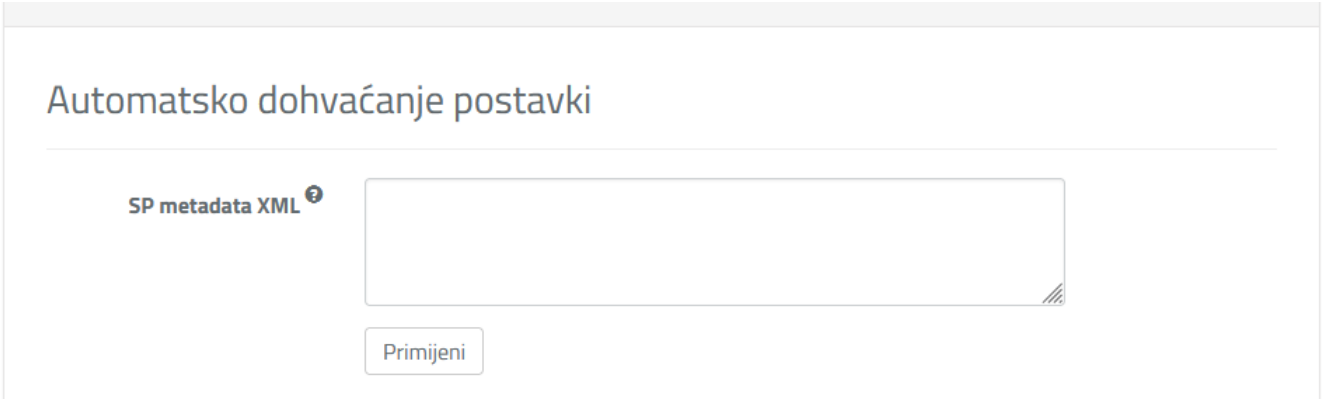
Stranica će se potom ponovo učitati s popisom atributa iz eduGAIN profila koje sustav AAI@EduHr može isporučiti.



Nakon toga dovršite postavljanje konfiguracije na standardan način.

Automatsko dohvaćanje postavki

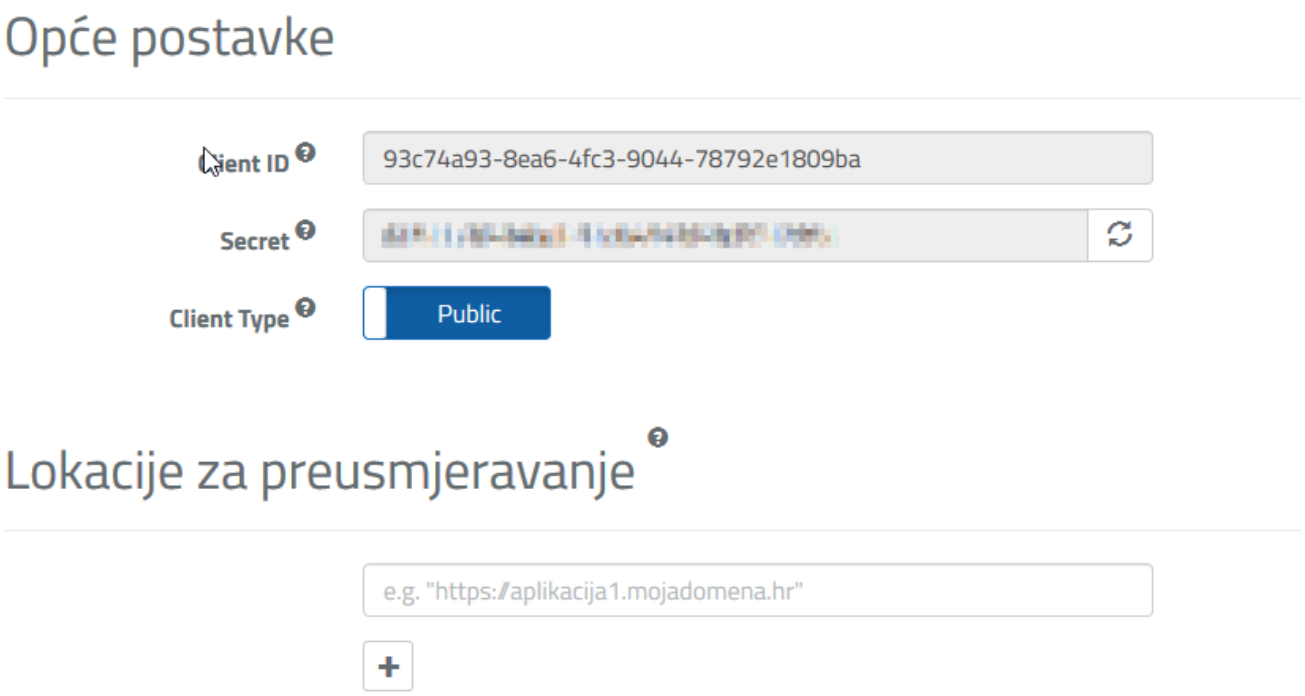
Neke od postavki SAML konfiguracije resursa moguće je automatski popuniti na temelju metapodataka koji opisuju davatelja usluge (vašu aplikaciju) u XML formatu. Dovoljno je kopirati i zalijepiti metapodatke u polje **SP metadata XML** u odjeljku naslovljenom "**Automatsko dohvaćanje postavki**" i kliknuti gumb "Primijeni". Treba imati na umu da je, ako se radi o metapodacima eduGAIN SP-a, potrebno najprije u izborniku autentikacijskih servisa "Auth Service" odabrati opciju "eduGAIN". U protivnom bi moglo doći do biranja pogrešnih atributa koji su dio AAI@EduHr shema hrEduPerson i hrEduOrg.



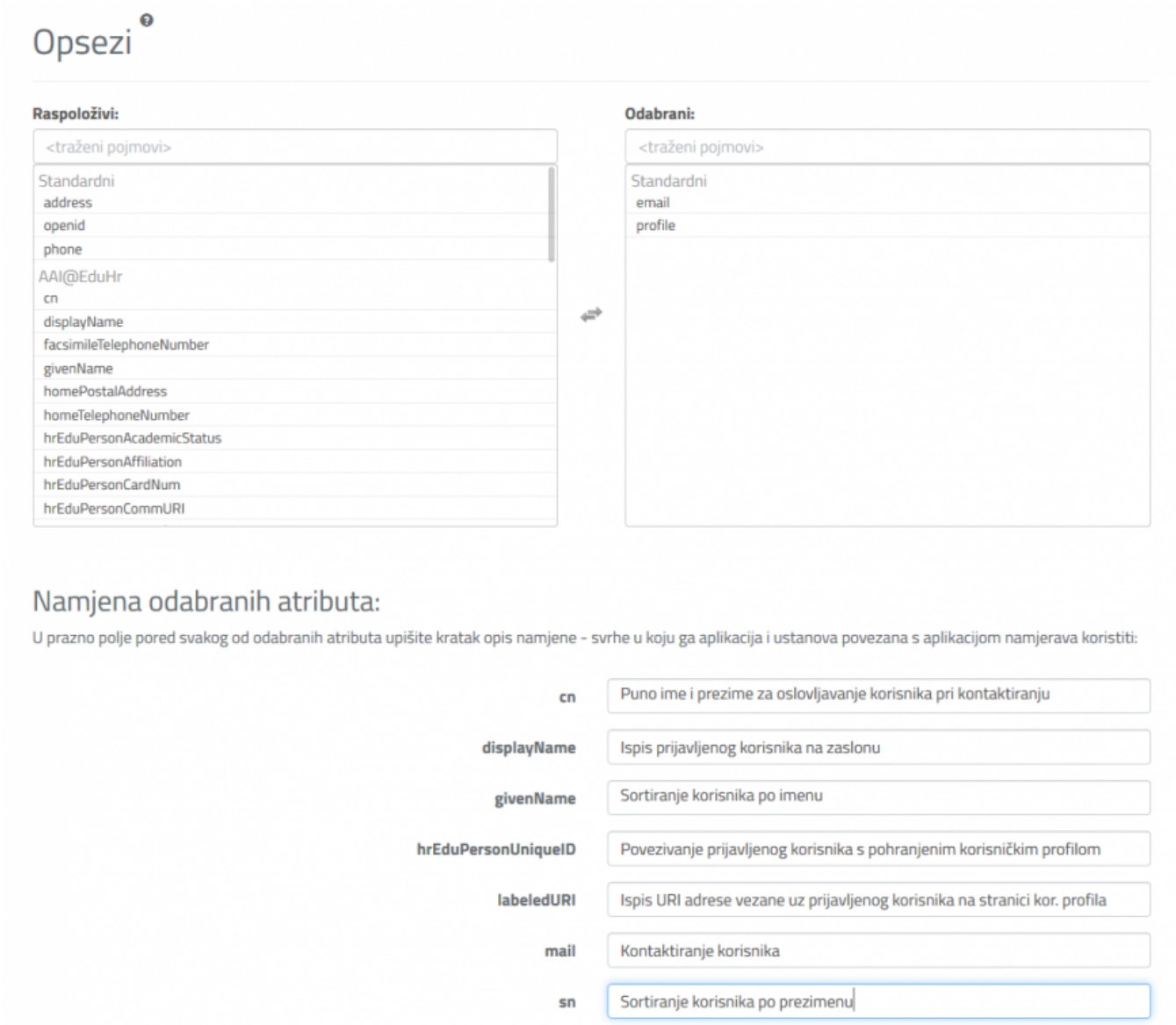
OIDC konfiguracija

Forma za unos OIDC konfiguracije podijeljena je na:

- Opće postavke:
  - **Client ID**
  - **Secret** - Tajni ključ klijenta
  - **Client Type** - Naznaka je li klijent povjerljiv (eng. *confidential*) ili javan (eng. *public*)
- Lokacije za preusmjeravanje (redirectURI) - popis lokacija u URI formatu (moguće je dodavanje polja te **višestruki unos URI-jeva** klikanjem na gumb '**+**')



- Popis za odabir opsega (eng. *scope*s), tj. skupova tvrdnji (eng. *claims*) koje u sustavu AAI@EduHr predstavljaju korisnički atributi. Atribute po uspješnoj prijavi korisnika sustav AAI@EduHr prosljeđuje aplikaciji koja koristi resurs. Željene opsege je potrebno kliknuti kako bi se preselili iz lijevog u desni popis odabranih.



Slično kao kod SAML konfiguracije, pri svakom odabiru novog opsega, u nižem se odjeljku naslovljenom "Namjena odabranih atributa" pojavljuju polja za upis namjene atributa. Svaki opseg obuhvaća jednu ili više tvrdnji od kojih se svaka u sustavu AAI@EduHr predstavlja odgovarajućim korisničkim atributom. Kao i kod SAML konfiguracije, polja za opis namjena atributa su obavezna. Potrebno je dakle kratko i precizno opisati na koji način web-aplikacija, odnosno ustanova namjerava koristiti svaki odabrani atribut. Ove definicije namjena moraju biti točne jer će se dati na javni uvid korisnicima da ih se informira o tome na koji način se koriste njihovi osobni podaci.

Podrobniji opisi svih parametara iz OIDC konfiguracije nalaze se u uputama za implementiranje OIDC autentikacije, u poglavlju "Registar resursa":

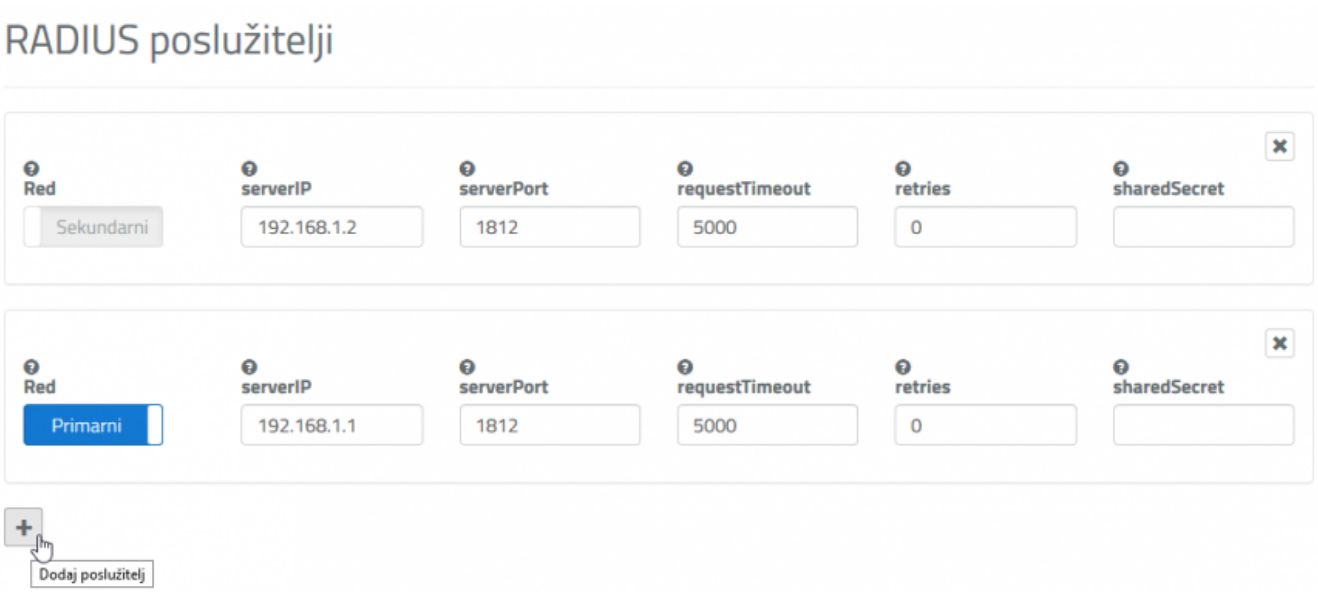
https://wiki.srce.hr/pages/viewpage.action?pageId=59867172#Autentikacijapomo%C4%87uprotokolaOpenIDConnect(OIDC)-Registarresursa

Objašnjenje opsega i tvrdnji nalaze se na istoj stranici u poglavlju "Opsezi i tvrdnje":

https://wiki.srce.hr/pages/viewpage.action?pageId=59867172#Autentikacijapomo%C4%87uprotokolaOpenIDConnect(OIDC)-Opseziitvrdnje(eng.ScopesandClaims)

RADIUS konfiguracija

Kod odabira konfiguracije za RADIUS modul dobivamo sljedeću formu za unos postavki RADIUS poslužitelja:



- **Red** - Red poslužitelja: primarni ili sekundarni
- **serverIP** - IP adresa RADIUS poslužitelja koji šalje upite
- **serverPort** - Port RADIUS poslužitelja (zadano: 1812)
- **requestTimeout** - Maksimalno vrijeme čekanja na odgovor (zadano: 5000)
- **retries** - Maksimalan broj ponavljanja upita (zadano: 0)
- **sharedSecret** - Javni ključ (ostavite neispunjeno)

Moguće je dodati **više RADIUS poslužitelja** za resurs klikanjem na gumb '**+**'. Na popisu se mora uvijek nalaziti jedan primarni poslužitelj, dok su svi ostali sekundarni.

Postupak odobravanja i obrade zahtjeva

U Registru resursa postoji nekoliko vrsta zahtjeva koji korisnik može postavljati nad pojedinim produkcijskim resursom. To su:

1. Zahtjev za registraciju resursa
2. Zahtjev za brisanje resursa
3. Zahtjev za izmjenu Općih podataka resursa
4. Zahtjev za dodavanje nekog od dostupnih autentikacijskih modula resursu
5. Zahtjev za izmjenu konfiguracije nekog od pripadajućih autentikacijskih modula
6. Zahtjev za brisanje nekog od pripadajućih autentikacijskih modula resursa

Prva dva tipa zahtjeva odnose se na resurs kao cjelinu skupa sa aut. modulima, ako postoje. Primjerice, zahtjev za brisanje resursa podrazumijeva automatsko brisanje i svih njegovih modula. Ostale vrste zahtjeva odnose se na dijelove resursa; konkretno na njegove Opće podatke ili autentikacijske module pojedinačno.

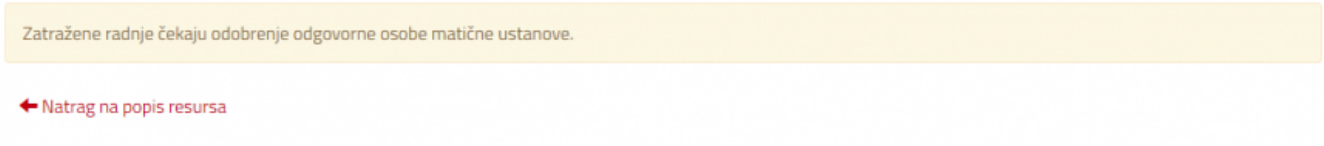
Kad autorizirani korisnik (odnosno administrator resursa) postavi neki od navedenih zahtjeva, o njegovom postavljanju obaviještavaju se **odgovorne osobe ustanove ili partnera** za koju/kojeg je resurs vezan (postavka "Matična ustanova s kojom je resurs povezan" odnosno "Partner federacije s kojim je resurs povezan" u Općim podacima) te **administratori sustava AAI@EduHr**. Svaki se zahtjev dakle šalje na uvid odgovornoj osobi matične ustanove/partnera te na razmatranje administratoru AAI@EduHr. Da bi administrator AAI@EduHr prihvatio i proveo zahtjev nad resursom, zahtjev mora:

1. biti ispravan
2. imati odobrenje odgovorne osobe

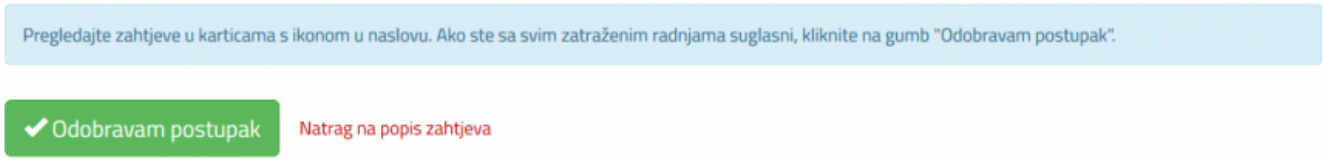
Opis postupka odobravanja i provedbe zahtjeva za registraciju resursa s pripadajućim aut. modulom koje ste kreirali u prethodnim koracima ovih uputa slijedi u nastavku.

Napomena: U slučaju da je autorizirani korisnik (administrator resursa) ujedno i odgovorna osoba mat. ustanove/partnera, dodatne intervencije odgovornih osoba kao i slanje obavijesti u tu svrhu se **ne izvode** u postupku provedbe zahtjeva nad resursom.

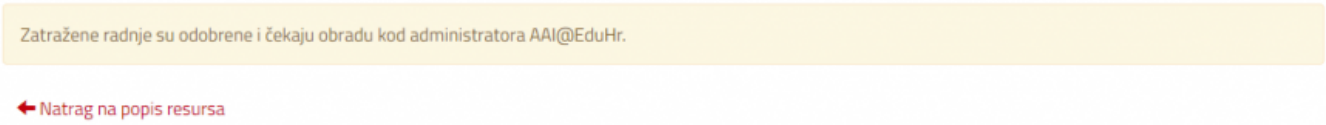
Ako ste ispunili odgovarajuće forme za registraciju resursa i dodavanje aut. modula te poslali zahtjeve klikom na gumb **Zatraži...** na svakoj od njih, obavijesti o pojedinom zahtjevu poslane su putem elektroničke pošte na adrese odgovornih osoba i administratora AAI@EduHr. Na dnu stranice s prikazom resursa za administratora stoji obavijest "Zatražene radnje čekaju odobrenje odgovorne osobe matične ustanove" odnosno "Zatražene radnje čekaju odobrenje odgovorne osobe ustanove-partnera".



Kad se odgovorna osoba prijavi u Registar resursa i otvori istu stranicu, na dnu će joj stajati prikazana kratka uputa i gumb **Odobravam postupak**.



Ako je pregledala sve zatražene radnje nad resursom te je sa svima njima suglasna, odgovorna osoba treba kliknuti na spomenuti gumb i time će odobriti sve zahtjeve. Nakon toga, na stranici se administratoru resursa prikazuje obavijest "Zatražene radnje su odobrene i čekaju obradu kod administratora AAI@EduHr."



Sad na red dolazi administrator AAI@EduHr koji još jednom provjerava unesene podatke. Ako je sve u redu, administrator AAI@EduHr će prihvatiti zahtjeve i provesti kompletan postupak (sve zatražene radnje) nad resursom. U slučaju da postoje neki nedostaci, administrator će ispravne zahtjeve provesti, a one s greškom odbiti uz obrazloženje koje će biti prikazano na stranici kako biste nedostatke mogli otkloniti. O uspješnom zaključenju postupka, odnosno o odbijenim zahtjevima bit ćete obaviješteni putem elektroničke pošte.

Napomena: autentikacija s novounesenim postavkama proradit će u roku od najviše pet minuta od trenutka provedbe zatraženih zahtjeva.

Direktne akcije nad testnim resursima za koje nisu potrebni zahtjevi i odobrenja

Za većinu zahvata u testnim resursima, odnosno resursima koji koriste testno okruženje sustava AAI@EduHr, ne otvaraju se zahtjevi te nije potrebno čekanje na odobrenja odgovornih osoba i administratora AAI@EduHr. Ti su zahvati sljedeći:

1. Brisanje resursa
2. Izmjena Općih podataka resursa
3. Dodavanje nekog od dostupnih autentikacijskih modula resursu
4. Izmjena konfiguracije nekog od pripadajućih autentikacijskih modula
5. Brisanje nekog od pripadajućih autentikacijskih modula resursa

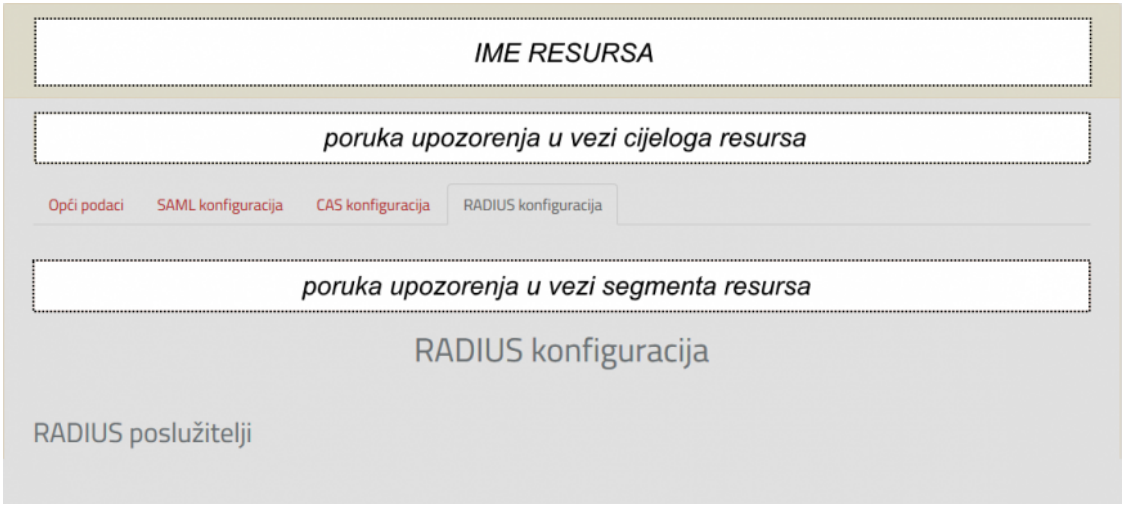
Jedine akcije koje otvaraju zahtjeve jesu:

1. registracija novog testnog resursa - traži ručnu provedbu od administratora AAI@EduHr te
2. prelazak u produkcijsku okolinu - traži odobrenje odgovorne osobe ustanove/partnera i zatim provedbu od administratora AAI@EduHr

Nakon odobrene i provedene registracije testnog resursa administratori istog mogu bilo što mijenjati (čak i obrisati testni resurs) odmah i bez čekanja na odobrenje - pod uvjetom da resurs i dalje ostaje u testnoj okolini.

Objašnjenje boja i indikatora statusa resursa

Aplikacija Registra resursa na više mjesta koristi kombinacije ikona, boja i specifičnih izraza kako bi korisniku prenijela bitne informacije kroz što jednostavnije sučelje. Stranica s prikazom resursa sastoji se od nekoliko cjelina koje svojim izgledom i sadržajem upućuju na određeno stanje u kojem se resurs nalazi. Na samom vrhu je glavni naslov s imenom resursa ispisanim velikim tekstom. Ispod njega je pozicija rezervirana za poruke koje se odnose na resurs u cjelini, dok je niže, u prostoru za sadržaj otvorene kartice pozicija na kojoj se pojavljuju upozorenja vezana uz segment koji prikazuje otvorena kartica (Opći podaci ili neki od autentikacijskih modula).



Pozadinska boja oko imena resursa upućuje na to je li resurs aktivan i postoji li neki otvoreni zahtjev nad njime ili ne. Ako je pozadina siva, resurs je neaktivan. U tom slučaju uobičajeno na stranici stoji i dodatna obavijest zašto je to tako te što treba napraviti da bi se problem riješio. Žuta pozadina upozorava da je nad resursom otvoren jedan ili više zahtjeva, tj. da se nad njime vodi neki postupak. Tamnoplava pak znači da je resurs aktivan te da nema otvorenih zahtjeva nad njime; to je dakle stanje u kojem nikakva akcija nije potrebna. Primjer prikaza aktivnog resursa bez otvorenih zahtjeva nalazi se na slici:

U slučaju da nad resursom postoje **otvoreni zahtjevi**, kartica segmenta na koji se pojedini zahtjev odnosi prikazuje poruku s opisom zatražene radnje. Također, uz naslov te kartice je i ikona vezana uz vrstu radnje:

1. zvjezdica (*): registracija/dodavanje
2. ključ (🔧): modifikacija
3. minus (−): brisanje

Kad administrator AAI@EduHr zbog uočene pogreške **odbije zahtjev**, resurs zadržava žutu boju jer taj zahtjev i dalje postoji, tj. čeka da korisnik koji ga je kreirao ispravi grešku. Poruka na razini cijelog resursa upozorava da je odbijen jedan ili više zahtjeva. Da bismo ga lakše pronašli, njegova kartica ima ikonu uskličnika ( ) u naslovu. Kad je otvorimo, u njoj ćemo uočiti upozorenje narančaste boje koje uz radnju koja je odbijena navodi i obrazloženje (ako ga je administrator naveo prilikom odbijanja):

Napomena: upozorenja narančaste boje upućuju na pogrešku ili propust korisnika.

U **popisu resursa** izlistani su svi resursi kojima je korisnik administrator ili su vezani za matičnu ustanovu/partnera federacije za koju je korisnik odgovorna osoba u sustavu AAI@EduHr. Popis resursa podijeljen je na dvije kartice od kojih jedna prikazuje **aktivne**, a druga **neaktivne** resurse. Resurs je aktivan ako je registriran te ima najmanje jedan pridružen autentikacijski mehanizam (modul) koji je u funkciji.

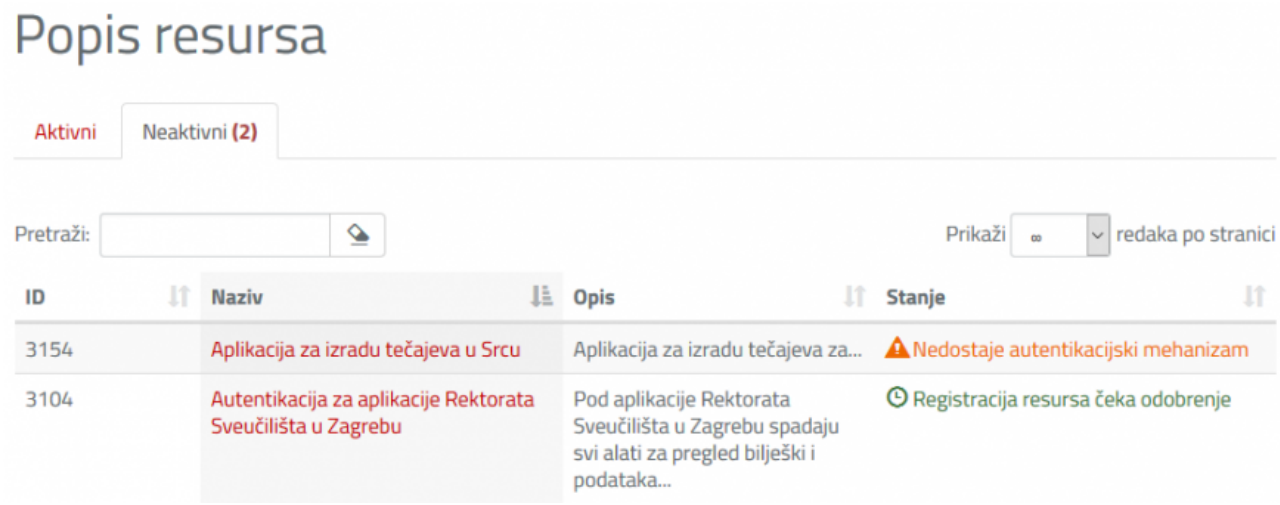
U svakom od stupaca koji predstavljaju autentikacijske module trenutno dostupne u Registru resursa nalazi se ikona-indikator njihovog statusa. Postoje četiri vrste indikatora:

1. zelena kvačica ( ): označava da je modul aktivan
2. smeđa kvačica ( ): označava da je modul aktivan, no nad njim je otvoren zahtjev
3. sivi križić ( ): označava da nema aktivnog modula
4. smeđi križić ( ): označava da nema aktivnog modula, no otvoren je zahtjev za njegovo dodavanje

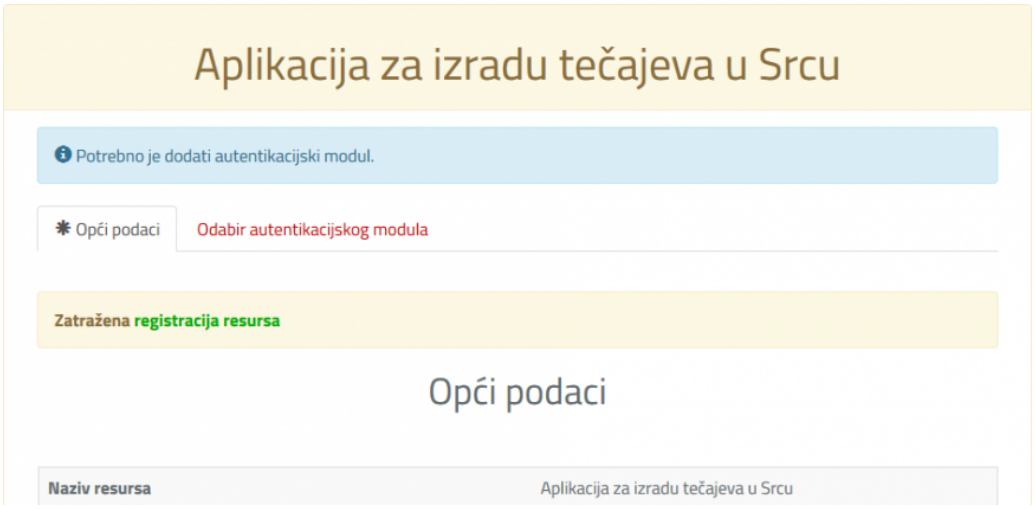
Klikanje bilo gdje u retku otvorit će stranicu s prikazom pojedinosti o resursu i pripadajućim modulima.

Kao što je već spomenuto, resurs je neaktivan ako još nije registriran ili ako nema pridružen funkcionalni autentikacijski modul. U stupcu **Stanje** u kartici s **neaktivnim** resursima evidentiramo tri tipa statusa u kojim resurs vodimo kao neaktivan:

1. nedostaje autentikacijski mehanizam - zatražena je registracija resursa, no uz nju još nije zatražen autentikacijski modul
2. registracija resursa čeka odobrenje - zatražena je registracija resursa skupa s aut. modulom, no postupak još nije odobren i proveden
3. autentikacijski modul čeka aktivaciju - resurs je registriran, no postojeći zahtjev za dodavanje aut. modula još nije odobren i proveden



Ako kliknemo na resurs koji čeka registraciju, ali mu nedostaje zahtjev za dodavanje aut. modula, otvorit će se prikaz sličan ovome:



Odmah ispod imena resursa stoji obavijest da je uz zahtjev za registraciju potrebno dodati još i zahtjev za autentikacijski modul.