

# Davatelji usluga

Sustav AAI@EduHr davateljima usluga (vlasnicima resursa) omogućuje veću dostupnost i vidljivost usluge uz pojednostavljenu administraciju i standardiziran proces autentikacije i autorizacije korisnika.

Informacije o tome koje vrste usluga (resursa) mogu koristiti sustav AAI@EduHr za autentikaciju korisnika te kako omogućiti autentikaciju korisnika za pristup vašoj usluzi putem sustava AAI@EduHr možete pronaći u nastavku.

## Usluga, resurs, aplikacija, servis... koji naziv je ispravan?

Gledajući iz konteksta sustava AAI@EduHr (i prema AAI@EduHr pravilniku), usluga može biti autenticirani pristup mreži (npr. eduroam), ili autenticirani pristup aplikacijama. Davatelji tih usluga mogu biti matične ustanove ili partneri sustava AAI@EduHr. Gledajući iz konteksta autentikacijskih protokola koje sustav AAI@EduHr podržava, u različitim protokolima se za iste stvari koriste različiti nazivi. Na primjer, u protokolu SAML, naziv za davatelja usluge je "Service Provider (SP)", u protokolu OpenID Connect je "Relying Party (RP)", u protokolu CAS je to tipično "Protected Application", u protokolu RADIUS je to "Access Client"... Zbog toga, u sustavu AAI@EduHr, prilikom registracije usluge koristimo termin 'resurs' kao objedinjeni termin za spomenute nazive iz samih protokola.

## Implementacija autentikacije putem sustava AAI@EduHr

Da biste mogli registrirati aplikaciju koja za autentikaciju korisnika koristi sustav AAI@EduHr, vaša ustanova / tvrtka mora imati status [partnera sustava AAI@EduHr](#) ili [matične ustanove u sustavu AAI@EduHr](#).

Ako se radi o usluzi pristupa mreži, naša je preporuka korištenje RADIUS protokola i eduroam standarda, a upute su dostupne [ovdje](#).

Ako se radi o aplikaciji, naša je preporuka korištenje [SAML protokola](#) (alternativno je moguće koristiti [CAS](#) ili [OIDC](#) protokol) putem [sustava jedinstvene autentikacije korisnika](#).

Koraci u omogućavanju autentikacije korisnika aplikacije putem sustava AAI@EduHr:

1. Osigurajte da ustanova / tvrtka davatelj usluge ima status [partnera sustava AAI@EduHr](#) ili [matične ustanove u sustavu AAI@EduHr](#)
2. Pročitajte [upute za omogućavanje autentikacije za aplikacije](#).
3. Razmislite koji će protokol aplikacija koristiti. Naša je preporuka [SAML protokol](#), a alternativno su dostupni [CAS](#) i [OIDC](#) protokol.
  - Ako želite da vaša usluga bude globalno dostupna kroz sustav [eduGAIN](#), usluga mora koristiti SAML protokol i biti dostupna i na engleskom jeziku, a za više informacija javite se na adresu [aai@srce.hr](mailto:aai@srce.hr)
4. Registrirajte svoju uslugu kroz [Registar resursa](#). Upute su dostupne [ovdje](#).
  - Za usluge u fazi razvoja / testiranja preporučamo korištenje [AAI@EduHr Lab-a](#).
  - Podaci o korisniku koje možete dohvatiti kroz sustav AAI@EduHr propisani su [hrEdu imeničkim shemama](#). Popis i opis atributa možete pronaći [ovdje](#).
    - Pri izboru atributa / podataka koje želite dohvatiti kroz svoju aplikaciju vodite računa o tome da je riječ (i) o osobnim podacima korisnika, te da Zakon o zaštiti osobnih podataka i GDPR propisuju da obrada osobnih podataka treba biti takva da se koristi minimalno potreban set podataka, te da korisnik mora biti informiran o točnoj namjeni za koju se koristi pojedini podatak što je potrebno uz svaki odabrani atribut unijeti prilikom registracije resursa.
    - Unos vrijednosti nekih atributa nije obavezan. Kod takvih atributa aplikacija treba očekivati da možda neće dobiti vrijednost atributa.
5. Ovisno o platformi koju koristite za razvoj usluge i samom autentikacijskom protokolu, preuzmite odgovarajuće metapodatke središnjih AAI@EduHr servisa te podesite "klijenta" sukladno autentikacijskom protokolu na strani same usluge. Upute su dostupne [ovdje](#).
6. Kad je usluga spremna za produkciju, kroz [Registar resursa](#) je potrebno zatražiti produkcijski status za uslugu, te uslugu podesiti da koristi produkcijski a ne testni SSO servis sustava AAI@EduHr.

- [Sustav jedinstvene autentikacije korisnika \(SSO\)](#)
- [Registar resursa](#)
- [Autentikacija u aplikacijama](#)
  - [Autentikacija pomoću protokola SAML](#)
    - [SAML metapodaci SSO servisa](#)
    - [SAML u PHP aplikacijama](#)
    - [SAML u .NET aplikacijama](#)
    - [SAML u JAVA aplikacijama](#)
    - [SAML u okruženju Django / Python](#)
  - [Autentikacija pomoću protokola CAS](#)
  - [Autentikacija pomoću protokola OpenID Connect \(OIDC\)](#)
- [Virtualne organizacije](#)
- [Usluge spajanja na mrežu](#)
  - [Spajanje na mrežu po eduroam standardu](#)
  - [Autentikacija korisnika iz tekstualne datoteke za FreeRADIUS](#)

- Kako napraviti jednostavnu black-listu za FreeRADIUS
- AAI@EduHr Lab (testno okruženje)
  - Pravila korištenja AAI@EduHr Lab usluge
  - Upute za korištenje AAI@EduHr Laba
- Prilagođene aplikacije i servisi
  - G Suite (Google Apps) for Education
  - Microsoft Office 365
    - o365connect - AOSI plugin za sinkronizaciju Azure AD i LDAP imenika
  - Adobe Acrobat Connect Pro
  - e-portfolio sustav Mahara
  - Joomla 2.5.x
  - LimeSurvey
  - MediaWiki (upute na engleskom jeziku)
  - MediaWiki - autorizacija pristupa korištenjem virtualnih organizacija
  - Moodle
  - OTRS (upute na engleskom jeziku)
  - phpBB3 forum
  - Skype for Business
  - WordPress
  - SAML autentikacija za Laravel 8.x
- Često postavljena pitanja
  - Kako izvršiti zamjenu certifikata za provjeru SSO autentikacije za uslugu Office 365?
  - Kako postati partner AAI@EduHr federacije?
  - Kako prilagoditi SameSite atribut kolačića
  - Ne mogu omogućiti jedinstvenu odjavu (Single Logout) iz svoje aplikacije. Što mi je činiti?