srce | Sveučilište u Zagrebu Sveučilišni računski centar

Izrada jedinstvenog autentikacijskog dodatka za prijavu putem AAI@EduHr i eduGAIN identitetima

Zvonko Martinović
Sveučilišni računski centar Sveučilišta u Zagrebu (Srce)
6. lipnja 2024.

moodlemoot™ HRVATSKA 2024

Prijava u sustav Merlin

- do 2023. godine prijava isključivo putem AAI@EduHr elektroničkog identiteta korištenjem SAML 2.0 protokola
- od 2023. umjesto prijave putem AAI@EdHr elektroničkog identiteta omogućena prijava putem eduGAIN elektroničkog identiteta
- uvođenje eduGAIN prijave dovelo i do dodatnog koraka prilikom prijave

AAI@eduHr vs eduGAIN

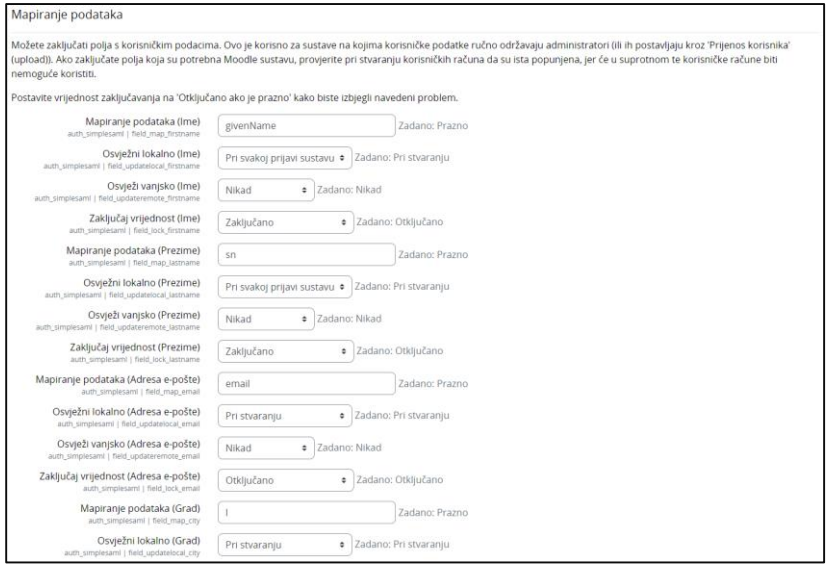
- imenička shema AAI@eduHr-a i eduGAIN-a, odnosno nazivi atributa, se razlikuje:
  - hrEduPersonUniqueID naspram urn:oid:1.3.6.1.4.1.5923.1.1.1.6 za korisničku oznaku
  - givenName naspram urn:oid:2.5.4.42 za ime
  - sn naspram urn:oid:2.5.4.4 za prezime
  - AAI@EduHr isporučuje OIB, dok on nije dostupan u sklopu eduGAIN-a (od nedavno edugainproxy.srce.hr isporučuje OIB prilokom eduGAIN prijave)
- kategorija atributa se razlikuje između imeničkih shema AAI@eduHr-a i eduGAIN-a
  - ime i prezime su atributi koji se obavezno isporučuju u sklopu AAI@EduHr-a, ali nisu obavezni u sklopu eduGAIN-a

Izrada novog jedinstvenog autentikacijskog dodatka

- cilj je izrada jedinstvenog autentikacijskog dodatka koji će se moći koristiti na svim Moodle sustavima Srca, a koji će pokriti sve specifične potrebe pojedinih sustava:
  - mogućnost prijave bilo putem AAI@eduHr identiteta ili putem eduGAIN identiteta u isti korisnički profil na sustavu (npr. sustav Merlin)
  - prijava samo putem AAI@eduHr/eduGAIN identiteta (npr. isključivo AAI@eduHr identiteta prijava za lms.srce.hr ili isključivo prijava putem eduGAIN identiteta za mod.srce.hr)
  - u slučaju korištenja eduGAIN prijave omogućiti ili zabraniti prijavu u sustav ako IDP ne isporuči sve osobne podatke, odnosno ime i prezime (npr. na sustavu Merlin onemogućena prijava, dok na sustavu MoD omogućena)
  - u slučaju korištenja eduGAIN prijave kada dopuštamo da IDP ne isporuči sve osobne podatke, odnosno ime i prezime, otključati odgovarajuća profilna polja kako bi ih korisnik sam mogao upisati te zaključati ako IDP isporuči tražene atribute

Izazovi prilikom izrade autentikacijskog dodatka

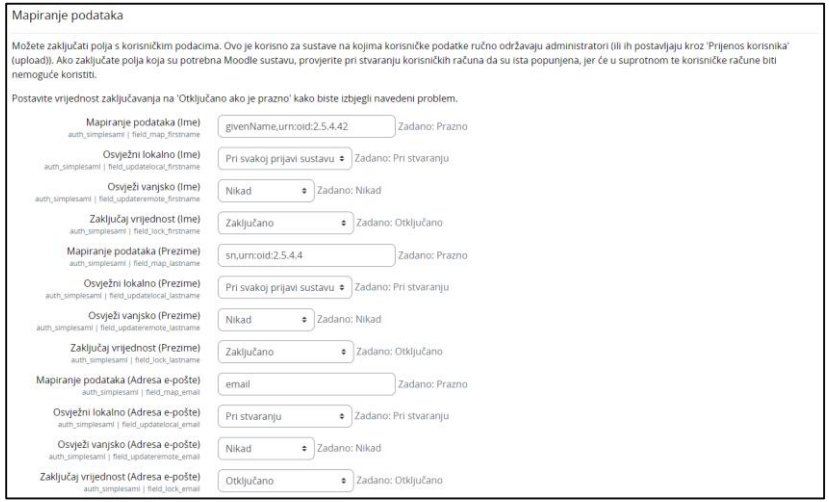
- autentikacijski dodaci za sustav Moodle su zamišljeni da mapiraju jedno polje korisničkog profila u sustavu Moodle s jednim atributom metapodataka korisnika koji se autenticira
- zaključavanje korisničkih profila je zamišljeno na razini cijelog autentikacijskog dodatka



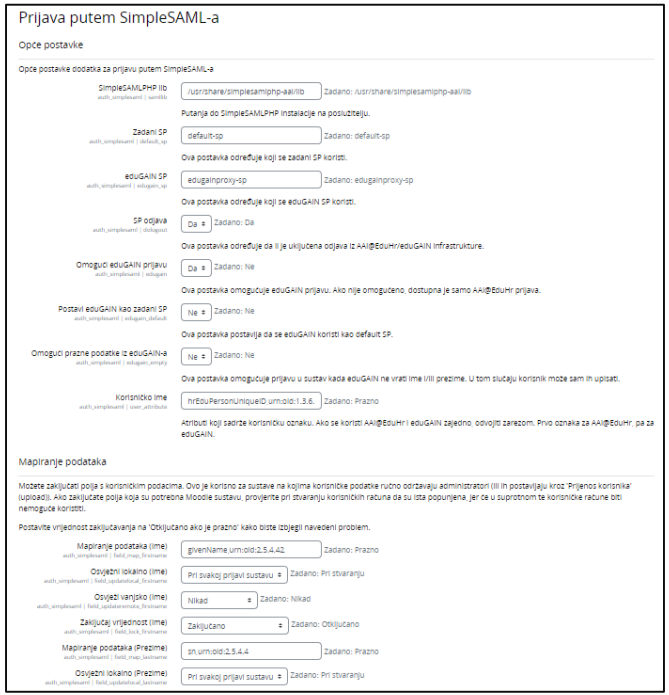
Kako smo otklonili navedene izazove?

- za mapiranje više različitih IDP atributa u jedan korisnički profil na sustavu Moodle iskorištena zadana Moodle polja, a atributi odvojeni zarezom – programska logika bira odgovarajući atribut ovisno o odabranom IDP-u

- zaključavanje/otključavanje polja korisničkog profila u Moodle-u izvedeno putem korisničkih postavki, funkcija set_user_preferences(), pošto ona omogućava postavljanje postavki za vrijeme trajanja sesije



Postavke novog autentikacijskog dodatka



Prijava putem SimpleSAML-a

Opće postavke

Opće postavke dodatka za prijavu putem SimpleSAML-a

SimpleSAMLPHP lib
auth_simplesaml | samllib
/usr/share/simplesamlphp-aai/lib
Zadano: /usr/share/simplesamlphp-aai/lib
Putanja do SimpleSAMLPHP instalacije na posluzitelju.

Zadani SP
auth_simplesaml | default_sp
default-sp
Zadano: default-sp
Ova postavka određuje koji se zadani SP koristi.

eduGAIN SP
auth_simplesaml | edugain_sp
edugainproxy-sp
Zadano: edugainproxy-sp
Ova postavka određuje koji se eduGAIN SP koristi.

SP odjava
auth_simplesaml | dologout
Da
Zadano: Da
Ova postavka određuje da li je uključena odjava iz AAI@EduHr/eduGAIN infrastrukture.

Omogući eduGAIN prijavu
auth_simplesaml | edugain
Da
Zadano: Ne
Ova postavka omogućuje eduGAIN prijavu. Ako nije omogućeno, dostupna je samo AAI@EduHr prijava.

Postavi eduGAIN kao zadani SP
auth_simplesaml | edugain_default
Ne
Zadano: Ne
Ova postavka postavlja da se eduGAIN koristi kao default SP.

Omogući prazne podatke iz eduGAIN-a
auth_simplesaml | edugain_empty
Ne
Zadano: Ne
Ova postavka omogućuje prijavu u sustav kada eduGAIN ne vrati Ime i/ili prezime. U tom slučaju korisnik može sam ih upisati.

Korisničko Ime
auth_simplesaml | user_attribute
hrEduPersonUniqueID urn:oid:1.3.6.
Zadano: Prazno
Atributi koji sadrže korisničku oznaku. Ako se koristi AAI@EduHr i eduGAIN zajedno, odvojiti zarezom. Prvo oznaka za AAI@EduHr, pa za eduGAIN.

Mapiranje podataka

Možete zaključati polja s korisničkim podacima. Ovo je korisno za sustave na kojima korisničke podatke ručno održavaju administratori (ili ih postavljaju kroz 'Prijenos korisnika' (upload)). Ako zaključate polja koja su potrebna Moodle sustavu, provjerite pri stvaranju korisničkih računa da su ista popunjena, jer će u suprotnom te korisničke račune biti nemoguće koristiti.

Postavite vrijednost zaključavanja na 'Otključano ako je prazno' kako biste izbjegli navedeni problem.

Mapiranje podataka (Ime)
auth_simplesaml | field_map_firstname
givenName urn:oid:2.5.4.42
Zadano: Prazno

Osvježni lokalno (Ime)
auth_simplesaml | field_updatelocal_firstname
Pri svakoj prijavi sustavu
Zadano: Pri stvaranju

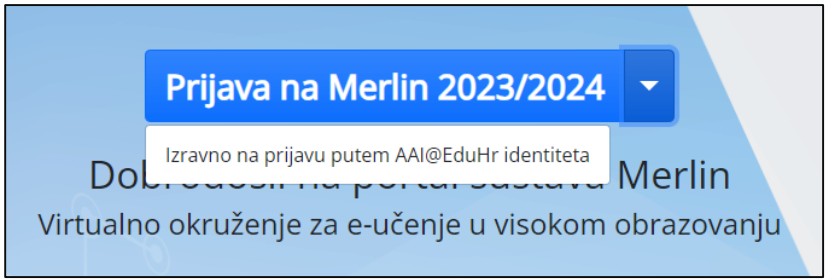
Osvježi vanjsko (Ime)
auth_simplesaml | field_updateremote_firstname
Nikad
Zadano: Nikad

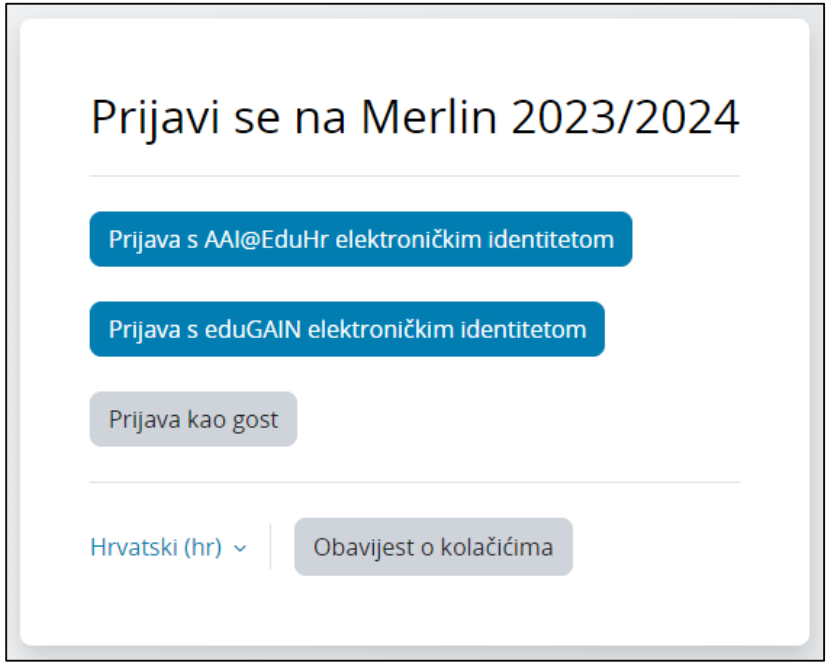
Zaključaj vrijednost (Ime)
auth_simplesaml | field_lock_firstname
Zaključano
Zadano: Otključano

Mapiranje podataka (Prezime)
auth_simplesaml | field_map_lastname
sn urn:oid:2.5.4.4
Zadano: Prazno

Osvježni lokalno (Prezime)
auth_simplesaml | field_updatelocal_lastname
Pri svakoj prijavi sustavu
Zadano: Pri stvaranju

Mogućnosti prijave u sustavu Merlin





Hvala na pažnji !

zvonko.martinovic@srce.hr

ceu@srce.hr

srce
Sveučilište u Zagrebu
Sveučilišni računski centar

Srce politikom otvorenog pristupa široj javnosti osigurava dostupnost i korištenje svih rezultata rada Srca, a prvenstveno obrazovnih i stručnih informacija i sadržaja nastalih djelovanjem i radom Srca.

www.srce.unizg.hr

creativecommons.org/licenses/by/4.0/deed.hr

www.srce.unizg.hr/otvoreni-pristup

srce
otvoreni pristup