OpenID Connect (OIDC)

Ožujak 2021., Zagreb, AAI@EduHr tim
Mijo Đerek, Marko Ivančić, Matija Lovrić, Miro Mačinković, Miroslav Milinović

Sadržaj

- Osnovni pojmovi
- OIDC
  - Metapodaci i povjerenje
  - Opsezi i tvrdnje (eng. scopes and claims)
  - ID token
  - Podržani autentikacijski tijekovi
    - Tijek autorizacijskog koda (eng. authorization code flow)
    - OAuth2 implicitni tijek (eng. OAuth2 implicit flow)

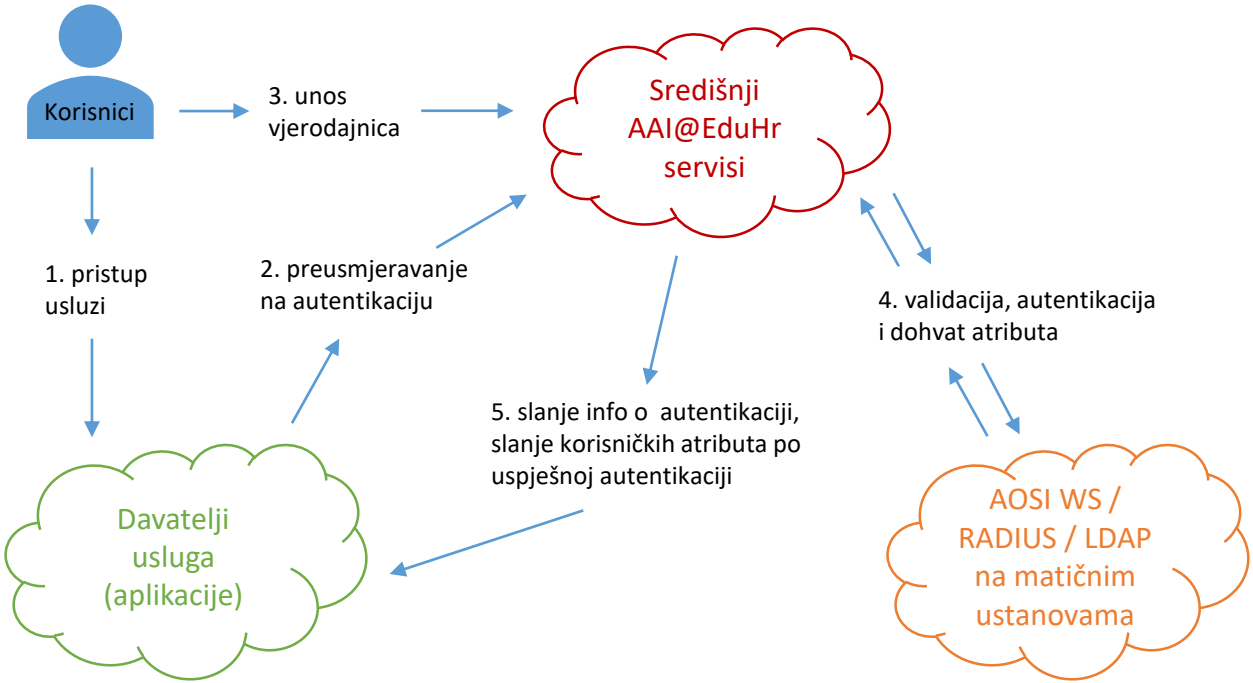
Preporuča se poznavanje…

- osnove HTTP protokola
  - metode GET, POST
  - kolačići (eng. cookies)
  - preusmjeravanje (eng. redirection, HTTP 3** odgovori)
- JSON
- Koncept asimetrične kriptografije (eng. asymetric cryptography)
- Koncept funkcija za raspršivanje (eng. hash function)
- Koncept kodiranja / dekodiranja (eng. encoding / decoding)

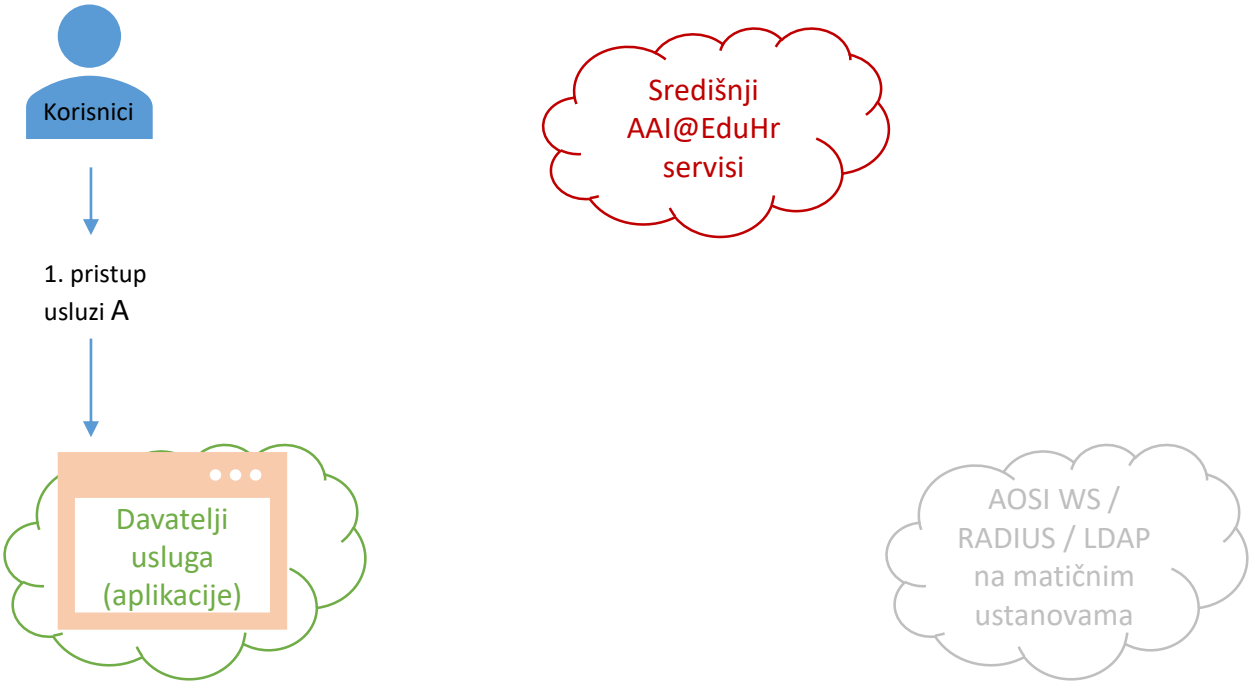
Osnovni elementi AAI@EduHr

- Elektronički identitet
  - skup podataka (atributa) o pojedincu koji se koristi za potrebe provjere identiteta (autentikacija) i prava pristupa (autorizacija)
- Matične ustanove
  - davatelji elektroničkih identiteta
  - npr. sveučilišta, fakulteti, visoke škole, škole
- Krajnji korisnici
  - vlasnici elektroničkog identiteta
  - npr. profesori, studenti, učenici, zaposlenici na ustanovi
- Davatelji usluga (resursa)
  - matične ustanove ili partneri AAI@EduHr
  - daju usluge kroz (web) aplikacije na koje se krajnji korisnici mogu autenticirati svojim elektroničkim identitetom
- Središnji AAI@EduHr servisi
  - posrednički sustav između korisnika, usluge i matične ustanove koji se koristi prilikom postupka autentikacije

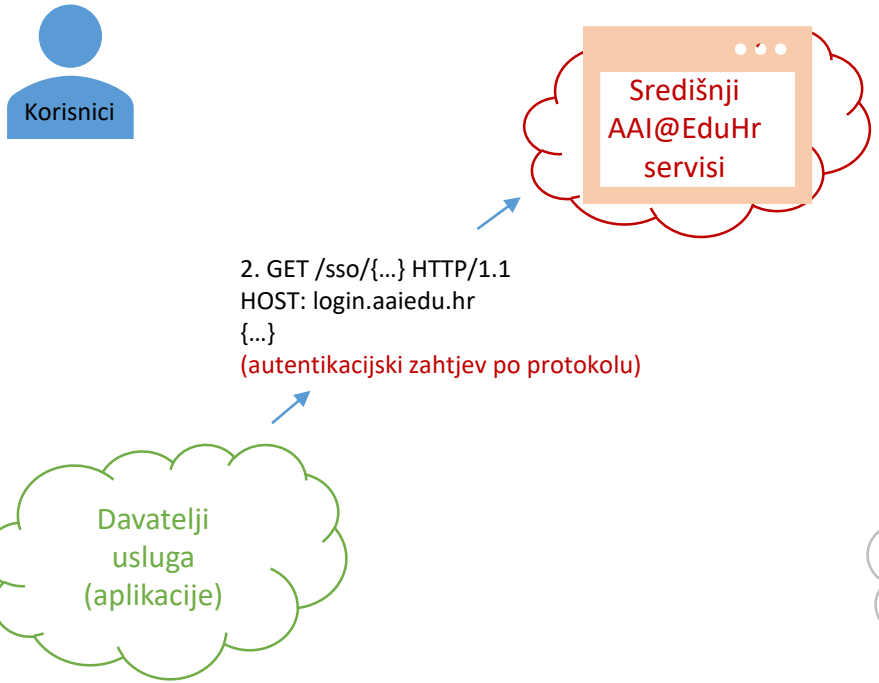
Pojednostavljen autentikacijski tijek



Autentikacijski tijek u Single Sign-On (SSO) kontekstu (1)

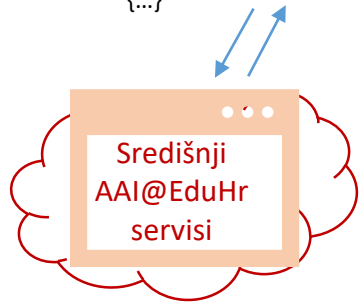


Autentikacijski tijek u Single Sign-On (SSO) kontekstu (2)

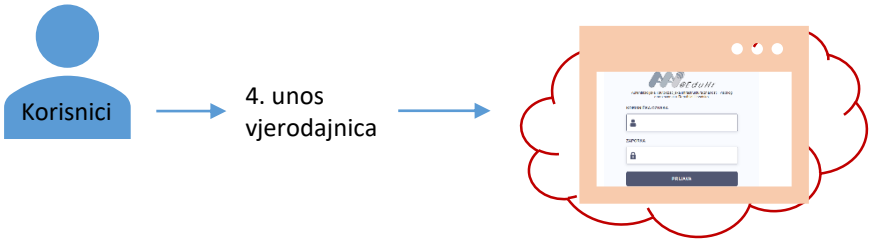


Autentikacijski tijek u Si kontekstu (3)

3. HTTP/1.1 302 Found
LOCATION: https://login.aaiedu.hr/sso/auth
SET-COOKIE: ssoID=123abc; path=/; secure; SameSite=None
{…}



Autentikacijski tijek u Single Sign-On (SSO) kontekstu (4)



Davatelji usluga (aplikacije)

AOSI WS / RADIUS / LDAP na matičnim ustanovama

Autentikacijski tijek u Single Sign-On (SSO) kontekstu (5)

5. validacija, autentikacija i dohvat atributa

Davatelji usluga (aplikacije)

AOSI WS / RADIUS / LDAP na matičnim ustanovama

Autentikacijski tijek u Single Sign-On (SSO) kontekstu (6)

6. GET|POST /callback/{…} HTTP/1.1
HOST: neka-usluga.hr
{…}
(autentikacijski odgovor po protokolu)

Autentikacijski tijek u Single Sign-On (SSO) kontekstu (7)

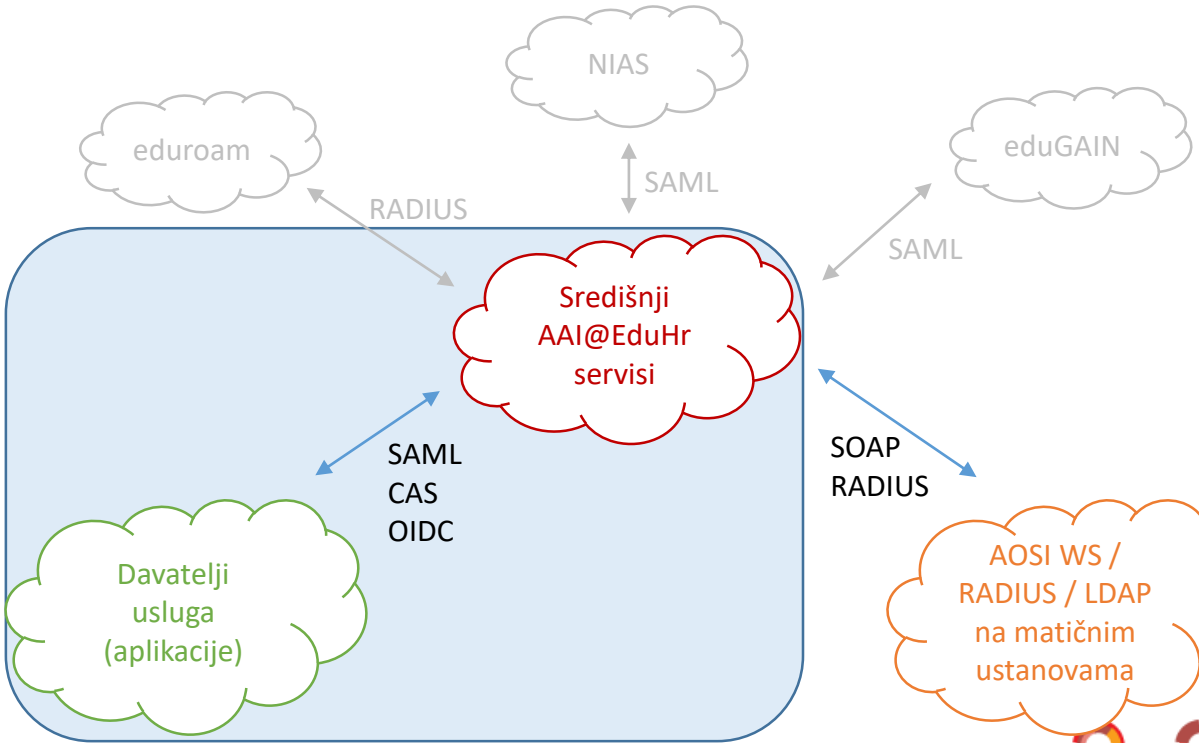
Autentikacijski tijek u Single Sign-On (SSO) kontekstu (8)

8. GET /sso/{…} HTTP/1.1
HOST: login.aaiedu.hr
COOKIE: ssoID=abc123; {…}
{…}
(autentikacijski zahtjev po protokolu)

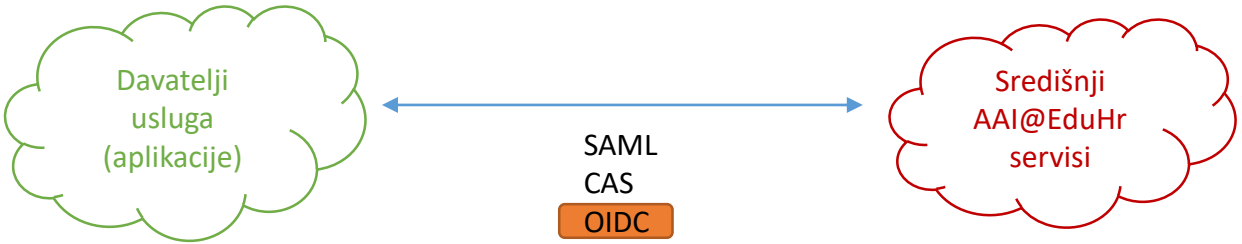
Autentikacijski tijek u Single Sign-On (SSO) kontekstu (9)

9. GET|POST /callback/{…} HTTP/1.1
HOST: neka-usluga.hr
{…}
(autentikacijski odgovor po protokolu)

Pregled korištenih protokola



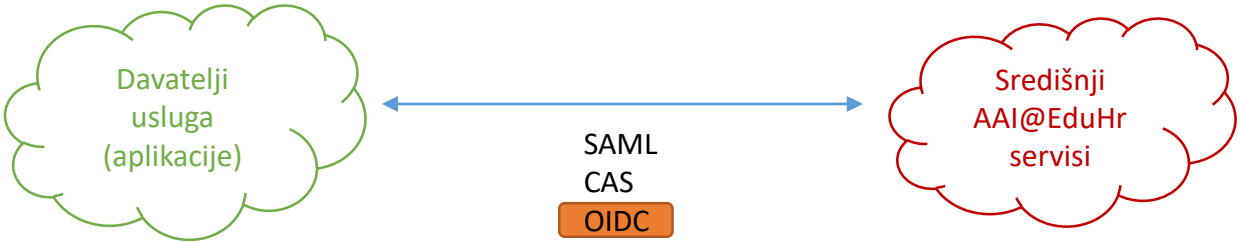
Podržani autentikacijski protokoli za usluge realizirane kao aplikacije



- SAML (Security Assertion Markup Language) - od početka rada AAI@EduHr 2006. godine
- CAS (Central Authentication Service) - od veljače 2010. godine
- OIDC (OpenID Connect) - od prosinca 2020. godine

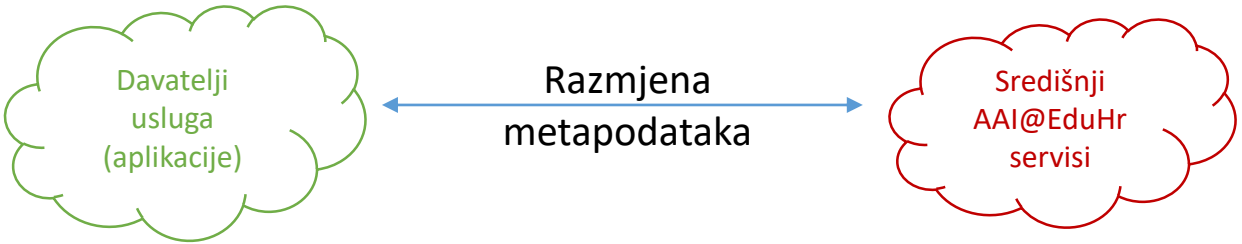
- Koji odabrati?
- 1. SAML
  - Veza s nacionalnim, europskim i globalnim autentikacijskim i autorizacijskim sustavima (NIAS, eduGAIN)
  - Virtualne organizacije (VO) - https://www.aaiedu.hr/za-davatelje-usluga/virtualne-organizacije
- 2. Alternativno
  - OIDC
  - CAS

Nazivi entiteta prema autentikacijskom protokolu



Davatelj usluge	Protokol	Središnji AAI@EduHr servis
Service Provider (SP)	SAML	Identity Provider (IdP)
Protected Application, CAS Client	CAS	CAS Server
Relying Party (RP), OIDC Client	OIDC	OpenID Provider (OP), OIDC Server

Uspostava povjerenja (na primjeru OIDC-a)



- Davatelj usluga (Relying Party - RP)
  - registrira OIDC resurs u Registru resursa (https://registar.aaiedu.hr/), čime efektivno "javlja" svoje metapodatke OpenID Provider-u
  - preuzima metapodatke od središnjeg AAI@EduHr OIDC servisa (OpenID Provider-a - OP) sa URL-a: https://login.aaiedu.hr/.well-known/openid-configuration
- Središnji AAI@EduHr OIDC servis (OpenID Provider - OP)
  - po prihvaćanju registracije OIDC resursa davatelja usluge, omogućuje slanje autentikacijskih odgovora na novoregistrirani OIDC resurs

Registracija OIDC resursa

- https://registar.aaiedu.hr/
- Definira se
  - ID klijenta (Client ID) - definira ga AAI@EduHr, nepromjenjiv je
  - Tajni ključ (Secret) - definira ga AAI@EduHr, može se resetirati
  - Tip klijenta (Client Type) - povjerljiv ili javan, definira ga davatelj usluge
    - povjerljiv klijent je onaj koji može na siguran način čuvati klijentske vjerodajnice
  - Lokacije za preusmjeravanje (Redirect URIs) - definira ih davatelj usluge
  - Opsezi (Scopes), a kroz njih i tvrdnje (Claims) tj. korisničke atribute - bira ih davatelj usluge
- Detaljne upute za registraciju resursa: https://www.aaiedu.hr/za-davatelje-usluga/za-web-aplikacije/sustav-jedinstvene-autentikacije-korisnika

OpenID Provider (OP) metapodaci

- https://login.aaiedu.hr/.well-known/openid-configuration
- JSON objekt
- Definira:
  - izdavatelja (eng. issuer): "https://login.aaiedu.hr/"
  - krajnje točke (eng. endpoints) koje se koriste za autentikaciju krajnjeg korisnika - svojstva 'authorization_endpoint', 'token_endpoint' i 'userinfo_endpoint'
  - URL na JSON web skup ključeva (eng. JSON Web Key Set - JWKS) pomoću kojih se može provjeravati potpis u ID tokenu - svojstvo 'jwks_uri'
  - podržani opsezi - svojstvo 'scopes_supported'
  - podržani autentikacijski tijekovi - svojstvo 'response_types_supported'
  - podržani tipovi identifikatora subjekta (eng. subject identifier) - svojstvo 'subject_types_supported'
  - podržani algoritmi za potpisivanje ID tokena - svojstvo 'id_token_signing_alg_values_supported'
  - podržane metode za generiranje parametra 'code_challenge' - svojstvo 'code_challenge_methods_supported'

OpenID Provider (OP) metapodaci (2) - JWKS

- JWKS se trenutno nalazi na URL-u: https://login.aaiedu.hr/sso/module.php/oidc/jwks.php (točan URL će uvijek biti naveden u OP metapodacima)
- JSON objekt
- Pod svojstvom 'keys' sadrži polje ključeva, dakle jedan ili više ključeva formatu JWK (JSON Web Key - JWK). To su ključevi među kojima će se nalaziti i onaj javni ključ koji se može koristiti za provjeru potpisa.
- U slučaju nemogućnosti korištenja ključeva u formatu JWK, javni ključ u formatu PEM je dostupan na poveznici: https://login.aaiedu.hr/sso/module.php/saml/idp/certs.php/idp.crt

Opsezi i tvrdnje (eng. scopes and claims)

- Opsezi definiraju koje tvrdnje o korisniku će se isporučivati klijentu.
- Tvrdnje su informacije o autentikacijskom događaju ili o autenticiranom korisniku.
- AAI@EduHr koristi tri vrste opsega i tvrdnji:
  - standardni opsezi i tvrdnje (definirano specifikacijom)
  - AAI@EduHr opsege i tvrdnje
  - stalne tvrdnje (informacije o autentikacijskom događaju)

Standardni opsezi i tvrdnje

Opseg	Podržane tvrdnje (standardna tvrdnja / AAI@EduHr korisnički atribut)	Nepodržane tvrdnje
openid - naznačuje isporuku ID tokena	/	/
profile	name / cn, given_name / givenName, nickname / displayName, preferred_username / hrEduPersonUniqueID, profile / labeledURI	middle_name, picture, website, gender, birthdate, zoneinfo, locale, updated_at
email	email / mail	email_verified
address	/	address
phone	phone_number / mobile, telephoneNumber	phone_number_verified

Dodatni, AAI@EduHr opsezi i tvrdnje

- AAI@EduHr OIDC opsezi su definirani tako da svaki opseg sadrži jednu tvrdnju.
- Naziv opsega odgovara nazivu tvrdnje koju sadrži, a naziv tvrdnje odgovara nazivu AAI@EduHr korisničkog atributa kojeg tvrdnja predstavlja.
- Svaka AAI@EduHr tvrdnja će biti u obliku JSON polja (eng. array), neovisno o tome može li AAI@EduHr korisnički atribut kojeg predstavlja imati višestruke vrijednosti ili ne.
- Na primjer, odabirom opsega 'uid', isporučivat će se tvrdnja 'uid' (u obliku polja) koja će za vrijednost imati vrijednost AAI@EduHr korisničkog atributa 'uid'.
- AAI@EduHr shema atributa: https://www.aaiedu.hr/o-sustavu/imenicke-sheme/shema

Stalne tvrdnje

Tvrdnja	Opis
iss	Identifikator izdavatelja (eng. issuer). Sadrži vrijednost AAI@EduHr identifikatora izdavatelja koji je inače dostupan na OIDC konfiguracijskom URL-u.
sub	Identifikator subjekta (eng. subject identifier). Sadrži jedinstveni identifikator krajnjeg korisnika tj. korisnika koji se autenticirao. Sadrži vrijednost AAI@EduHr korisničkog atributa 'hrEduPersonPersistentID'.
aud	Publika (eng. audience) kojoj je ID token namijenjen. Sadrži ID klijenta kojem je ID token namijenjen.
jti	JWT ID, jedinstveni identifikator samog ID tokena. Može se koristiti za sprječavanje ponovnog korištenja već iskorištenog ID tokena.
iat	Tvrdnja 'izdan u' (eng. issued at). Sadrži vremensku oznaku** kada je ID token izdan.
exp	Vrijeme isteka (eng. expiration time). Sadrži vremensku oznaku** nakon koje ID token ne smije biti prihvaćen.
nbf	Tvrdnja 'ne prije' (eng. not before). Sadrži vremensku oznaku** (eng. timestamp) prije koje ID token ne smije biti prihvaćen.
nonce	Vrijednost parametra 'nonce' kojeg klijent koristi tijekom autentikacije krajnjeg korisnika će biti proslijeđena u ID token. Nakon što klijent dobije ID token, mora provjeriti je li vrijednost 'nonce' u ID tokenu ista kao i ona korištena tijekom autentikacije.

ID token

- Primarni način isporuke tvrdnji
- Sadrži tvrdnje o korisniku (korisničke atribute), te tvrdnje o samom autentikacijskom događaju
- JWT (JSON Web Token)
- Primjer:
  - eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IjY5ZDhjNDY1NzQifQ.eyJpc3MiOiJodHRwczovL2xvZ2luLmFhaWVkdS5ociIsImF1ZCI6IjZlNTUyOTUyMDk3ODJiN2IyIiwianRpIjoiYzQ0ZjRjZmZjYzg0Zjc5OTBmN2ExZDViMmMiLCJuYmYiOjE2MDI2NzQ0NzAsImV4cCI6MTYwMjY3NTA3MCwic3ViIjoiYmZhMTYwNWJlNDRhNTBhN2MiLCJpYXQiOjE2MDI2NzQ0NzAsIm5vbmNlIjoiZHRubWVCTDVIVm5oUWtJUiIsIm5hbWUiOiJJdmFuIEhvcnZhdCIsImZhbWlseV9uYW1lIjoiSG9ydmF0IiwiZ2l2ZW5fbmFtZSI6Ikl2YW4iLCJwcmVmZXJyZWRfdXNlcm5hbWUiOiJpaG9ydmF0QHByaW1qZXIuaHIiLCJlbWFpbCI6Iml2YW4uaG9ydmF0QHByaW1qZXIuaHIiLCJockVkdVBlcnNvblVuaXF1ZU51bWJlciI6WyJMT0NBTF9OTzogMTIzNCIsIk9JQjogMTIzNDU2Nzg5MTIiLCJKTUJBRzogMTIzNDU2Nzg5MSJdfQ.c5q4W3bmcxQepAHj9n7xxj8WaH0wqIaiFkOFB9UE3joeVUyU9hWuNsDfPJ_BZ7WfYnhyMrv29Ys-dHs1oKqagvqFdk157IEwLnW1Dd5vNXvgGhMBhCTtseeQBDFS_DHN6KaksFDnGtFyWh3GXq-dWEBO86fpgSB3OuV9CD-AQAAbjXsN4Mz9MyaajMkhxWgxh_7HTZMlg5hACv3Xn-wiI8N3IGDqWrgdB87Vo6n0T5TfVaUZQ8mw5ca5fKy-aH5BP940LBb3bt6CvhZqxK0XFmD_M8hh-2MyRuPf2u6_P9HUORo1f8x8ZI30J2arhghPRcqEK9Sv_hdPxMy7WJJupg

ID token (2) - sastav

- Sastoji od tri dijela odvojenih točkom:
  - zaglavlje (eng. header)
  - korisni podaci (eng. payload)
  - potpis (eng. signature)
- Zaglavlje i korisni podaci su Base64 URL kodirani JSON objekti
- Potpis je generiran nad kodiranim zaglavljem i korisnim podacima koristeći privatni ključ i algoritam naznačen u zaglavlju, također Base64 URL kodiran
- zzzzz.kkkkk.ppppp

ID token (3) - zaglavlje i korisni podaci

- Primjer zaglavlja:


```
{
 "typ": "JWT",
 "alg": "RS256",
 "kid": "69d8c46574"
}
```


- Primjer korisnih podataka:


```
{
 "iss": "https://login.aaiedu.hr",
 "aud": "6e55295209782b7b2",
 "jti": "c44f4cffcc84f7990f7a1d5b2c",
 "nbf": 1602674470,
 "exp": 1602675070,
 "sub": "bfa1605be44a50a7c",
 "iat": 1602674470,
 "nonce": "dtnmeBL5HVnhQkIR",
 "family_name": "Horvat",
 "given_name": "Ivan",
 "preferred_username": "ihorvat@primjer.hr",
 "email": "ivan.horvat@primjer.hr",
 "hrEduPersonUniqueNumber": [
  "LOCAL_NO: 1234",
  "OIB: 12345678912",
  "JMBAG: 1234567891"
 ]
}
```

ID token (4) - provjera potpisa

- Algoritam 'RS256'.
- U postupku kreiranja potpisa koristi se privatni ključ iz para javnog i privatnog RSA ključa.
- Za provjeru tog potpisa potrebno je iskoristiti javni ključ koji je dostupan u JSON web skupu ključeva (JWKS URI).
- Odgovarajući javni ključ se može pronaći preko ID ključa ('kid') koji je naznačen u zaglavlju ID tokena te u pojedinom ključu u JSON web skupu ključeva.

Podržani autentikacijski tijekovi (eng. authentication flows)

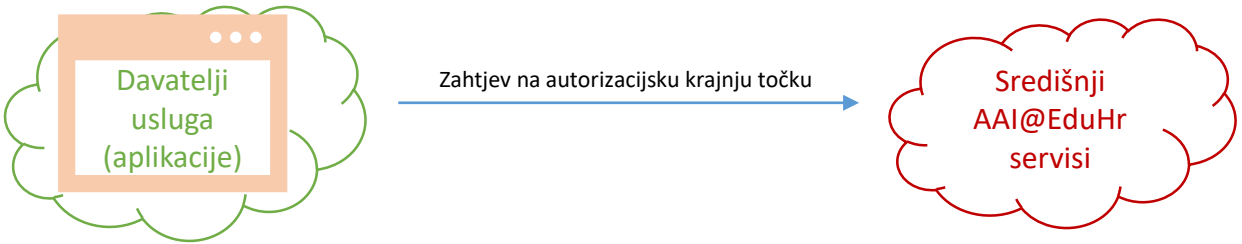
- Podržani autentikacijski tijekovi su:
  - Tijek autorizacijskog koda (eng. Authorization Code Flow) - OIDC ili OAuth2 tijek autorizacijskog koda
  - OAuth2 implicitni tijek (eng. Implicit Flow)
- Niz HTTP zahtjeva i preusmjeravanja (eng. redirections) između aplikacije (resursa) i autentikacijskog poslužitelja.
- Različiti autentikacijski tijekovi znače različit način slanja HTTP zahtjeva i različit način dohvata korisničkih podataka nakon autentikacije.
- Različiti tijekovi donose i različite razine sigurnosti autentikacijskog postupka. Na primjer, od trenutno podržana dva tijeka, tijek autorizacijskog koda ima veću razinu sigurnosti od implicitnog tijeka.
- AAI@EduHr preporuča korištenje tijeka autorizacijskog koda za autentikaciju korisnika, neovisno tome koji tip klijenta se koristi ili u kojem programskom jeziku je klijent implementiran.

Tijek autorizacijskog koda (eng. authorization code flow)

- Tijek autorizacijskog koda je glavni i preporučeni način autenticiranja krajnjih korisnika koristeći protokol OIDC.
- Tijek autorizacijskog koda u protokolu OIDC je nadogradnja postojećeg tijeka autorizacijskog koda u protokolu OAuth2. Glavne promjene koje u ovaj tijek donosi protokol OIDC u odnosu na OAuth2 su predefinirani OIDC opsezi i mogućnost izdavanja ID tokena.
- Ukratko, tijek autorizacijskog koda se obavlja na način:
  - klijent napravi autorizacijski HTTP zahtjev na autorizacijsku krajnju točku pomoću web preglednika
  - krajnji korisnik se autenticira
  - autentikacijski poslužitelj preusmjeravanjem na registriranu lokaciju za preusmjeravanje (eng. redirect URI) šalje klijentu kratkotrajni (eng. short-lived) autorizacijski kod (kao GET parametar 'code')
  - klijent u pozadini (bez web preglednika) napravi HTTP zahtjev na token krajnju točku koristeći dobiveni autorizacijski kod, a u HTTP odgovoru dobije pristupni token (eng. access token), te ID token ako je korišten opseg 'openid' (što je preporučeno)
- Dakle, klijent dobije autorizacijski kod kojeg onda u pozadinskom kanalu (eng. back channel) direktno zamjeni za pristupni token i ID token.
- Ako se ne koristi opseg 'openid' (ako se ID token ne izdaje), korisničke podatke je moguće dohvatiti sa krajnje točke za korisničke podatke (eng. userinfo endpoint).

Tijek autorizacijskog koda (2)

- Primjer za povjerljivog klijenta




```
GET {Authorization Endpoint}
  ?response_type=code
  &client_id=client123
  &redirect_uri=https://neka-usluga.hr/callback
  &scope=openid hrEduPersonUniqueNumber
  &state=state123
  &nonce=nonce123
  HTTP/1.1
Host: {Authorization Server}
```

Tijek autorizacijskog koda (3)

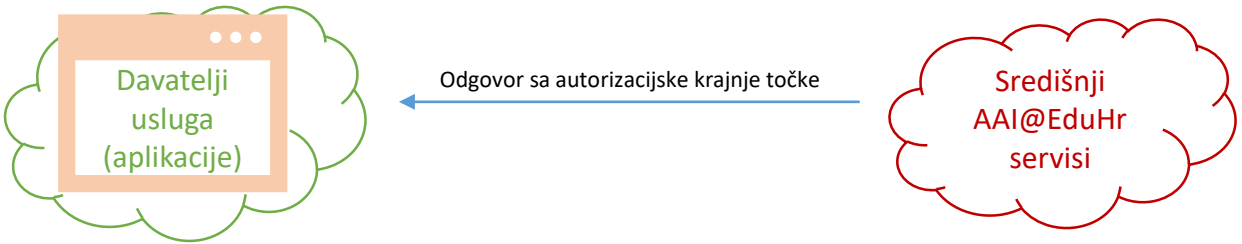
- Primjer za povjerljivog klijenta

Kreiranje sjednice,
prijava korisnika

HTTP/1.1 302 Found
Set-Cookie: ssoID=abc123; {…}
Location: {Login Endpoint}

Tijek autorizacijskog koda (4)

- Primjer za povjerljivog klijenta




```
GET /callback
  ?code=authcode123
  &state=state123
  HTTP/1.1
Host: neka-usluga.hr
```

Tijek autorizacijskog koda (5)

- Primjer za povjerljivog klijenta

BACK CHANNEL

Zahtjev na token krajnju točku

```
POST {Token Endpoint} HTTP/1.1
Host: {Authorization Server}
Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code
&client_id=client123
&client_secret=secret123
&code=authcode123
&redirect_uri=https://neka-usluga.hr/callback
```

Tijek autorizacijskog koda (6)

- Primjer za povjerljivog klijenta


```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
  "id_token": "{ID Token}",
  "access_token": "{Access Token}",
  "token_type": "{Token Type}",
  "expires_in": {Lifetime In Seconds},
  "refresh_token": "{Refresh Token}",
}
```

Odgovor sa token krajnje točke

Tijek autorizacijskog koda (7)

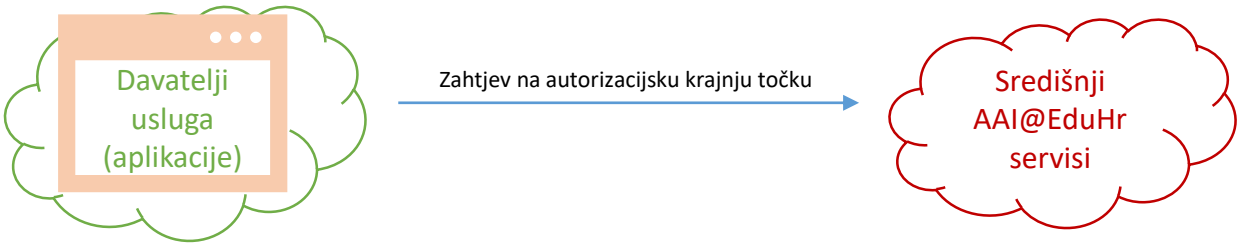
- Razlike za javnog klijenta:
  - ne koristi tajni ključ klijenta (eng. Client Secret)
  - koristi dodatne parametre prema standardu 'Proof Key for Code Exchange by OAuth Public Clients - PKCE' ('code_verifier', 'code_challenge' i 'code_challenge_method')

- Parametri 'code_verifier', 'code_challenge' i 'code_challenge_method' su dio dodatnog standarda 'Proof Key for Code Exchange by OAuth Public Clients - PKCE' kojim se želi poboljšati sigurnost za javne klijente. Upravo zbog tog standarda, javnim klijentima se omogućuje i preporučuje korištenje tijeka autorizacijskog koda za autentikaciju, umjesto da se koristi implicitni tijek. Vrijednosti koje mogu poprimiti parametri 'code_verifier', 'code_challenge' i 'code_challenge_method' detaljno su opisan su u specifikaciji PKCE u poglavlju https://tools.ietf.org/html/rfc7636#section-4.

OAuth2 implicitni tijek (eng. Oauth2 implicit flow)

- Izdaje se samo pristupni token (eng. access token); ID token se ne izdaje
- Za dohvat podataka o korisniku koristi se krajnja točka za korisničke podatke (eng. userinfo endpoint)
- Ukratko, implicitni tijek se obavlja na način:
  - klijent napravi autorizacijski HTTP zahtjev na autorizacijsku krajnju točku
  - krajnji korisnik se autenticira
  - klijent dobije natrag pristupni token kao fragment u URL-u (dio nakon znaka #)
  - klijent napravi HTTP zahtjev na krajnju točku za korisničke podatke pomoću pristupnog tokena
- Zbog veće razine sigurnosti, AAI@EduHr preporuča korištenje tijeka autorizacijskog koda umjesto implicitnog tijeka.
  - pristupni token (eng. access token) je vidljiv u URL-u

OAuth2 implicitni tijek (2)




```
GET {Authorization Endpoint}
  ?response_type=token
  &client_id=client123
  &redirect_uri=https://neka-usluga.hr/callback
  &scope=openid hrEduPersonUniqueNumber
  &state=state123
  HTTP/1.1
Host: {Authorization Server}
```

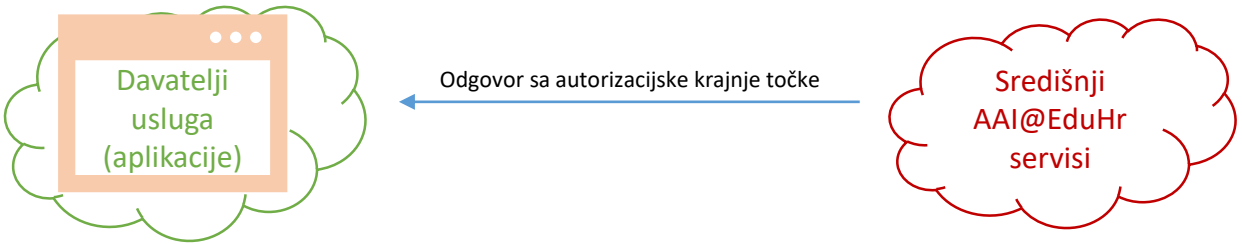
OAuth2 implicitni tijek (3)

Davatelji usluga (aplikacije)

Kreiranje sjednice, prijava korisnika

HTTP/1.1 302 Found
Set-Cookie: ssoID=abc123; {…}
Location: {Login Endpoint}

OAuth2 implicitni tijek (4)




```
GET /callback
  #access_token=accesstoken123
  &token_type=Bearer
  &expires_in=3600
  &state=state123
  HTTP/1.1
Host: neka-usluga.hr
```

OAuth2 implicitni tijek (5)

BACK CHANNEL

Zahtjev na userinfo krajnju točku

```
GET {Userinfo Endpoint} HTTP/1.1
Authorization: Bearer accesstoken123
Host: {Authorization Server}
```

OAuth2 implicitni tijek (6)

HTTP/1.1 200 OK
Content-Length: 25
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json

Odgovor sa userinfo krajnje točke

{"sub":"bfa1605be44a50a7c","family_name":"Horvat
","given_name":"Ivan","preferred_username":"ihorv
at@primjer.hr","email":"ivan.horvat@primjer.hr","h
rEduPersonUniqueNumber":["LOCAL_NO:
1234","OIB: 12345678912","JMBAG: 1234567891"]}

Rezime

- OIDC (kao niti ostali autentikacijski protokoli) ne definira na koji način autenticirati korisnika, nego na koji način isporučiti korisničke podatke već autenticiranog korisnika.
- RP i OP uspostavljaju povjerenje razmjenom metapodataka, čime se definira
  - na koje URI-e će se slati autentikacijski zahtjevi i vraćati autentikacijski odgovori
  - koji podaci o korisniku će se isporučivati RP-u (definirajući listu opsega, a time i tvrdnji)
- Nakon autentikacije korisnika, RP dobiva ID token iz kojeg "čita" korisničke podatke, ili ih dohvaća sa 'userinfo' endpoint-a (ako ne podržava čitanje ID tokena)
- Detaljnije upute: https://wiki.srce.hr/pages/viewpage.action?pageId=59867172

Povijest OIDC-a

- objavljen 2014. godine
- OpenID 1.0 i 2.0. su prethodne verzije protokola (ne miješati ih sa OIDC)

Aerodrom – analogija

povjerenje

- Izvori slika:
- https://www.shutterstock.com/image-photo/bangkok-feb-9-unidentified-passengers-arrive-95935672
- https://www.shutterstock.com/image-photo/hong-kong-november-12-2017-passenger-768349297
- https://www.shutterstock.com/image-vector/pattern-airline-boarding-pass-ticket-qr2-375639601
- https://www.shutterstock.com/image-illustration/biometric-blue-passport-cover-template-identity-1571214127

Pitanja

- U vezi OIDC?
- U vezi AAI@EduHr?
- Prijedlozi tema za webinar?