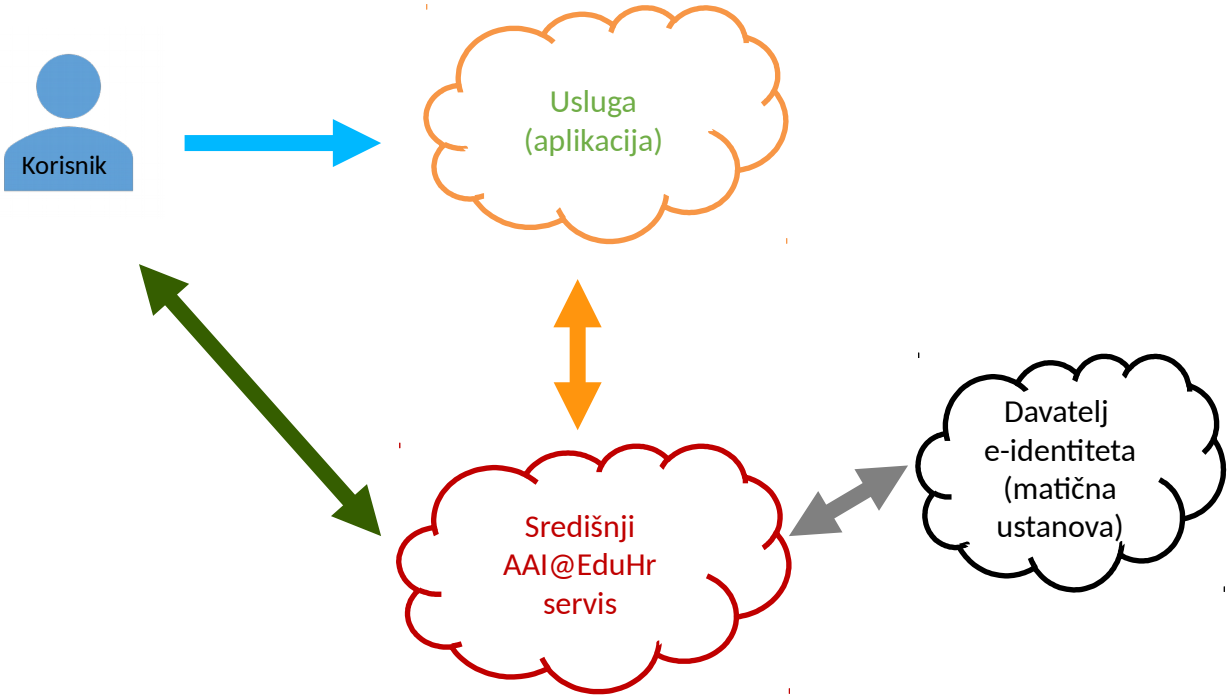
Višestupanjska autentikacija u AAI@EduHr

Mijo Đerek, Dubravko Penezić,
Sveučilište u Zagrebu, Sveučilišni računski centar (Srce)

Dani e-infrastrukture – Srce DEI 2021
Konferencija projekta HR-ZOO

28. i 29. travnja 2021.

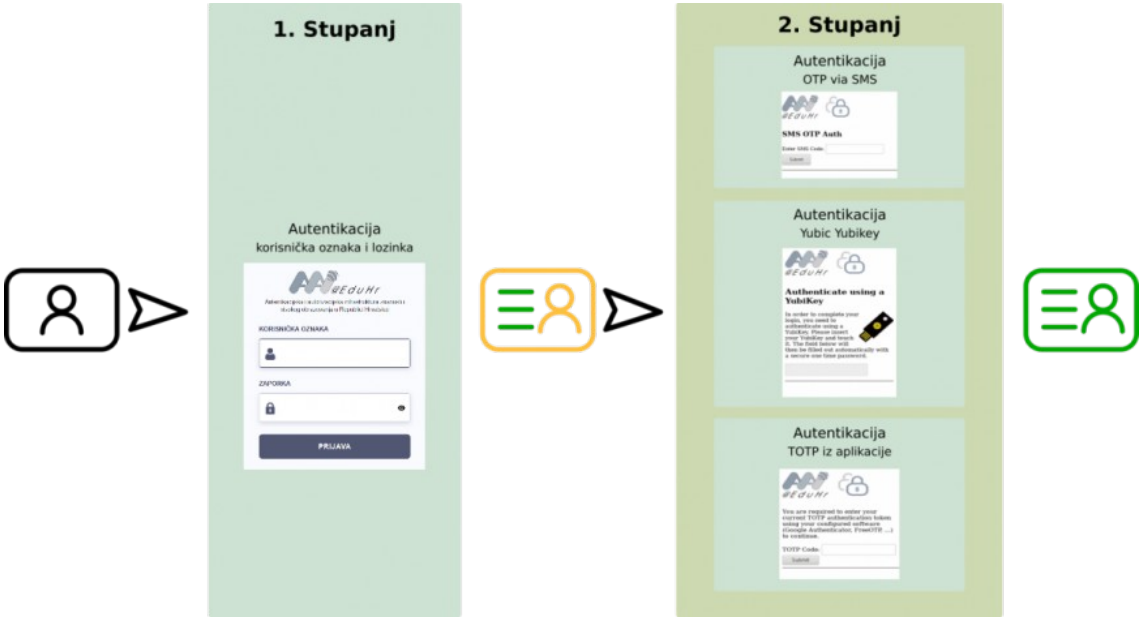
AAI@EduHr - tijek autentikacije



Višestupanjska autentikacija (MFA)

- Definicija
  - Višestupanjska autentikacija (MFA) vrsta je autentikacije u kojoj je korisnik autenticiran nakon što se uspješno autenticira kombinacijom dvije ili više različitih metoda autentikacije.
  - Kombinira se autentikacija onim što korisnik zna (npr. korisnička oznaka i lozinka) s autentikacijom onim što korisnik ima (npr. neki uređaj, pametna kartica) i/ili s autentikacijom korisnikovim biometrijskim podacima (npr. otisak prsta).
- Prednost
  - Podizanje razine sigurnosti dodavanjem dodatnih autentikacijskih metoda
  - Smanjenje utjecaja kompromitacije neke od vjerodajnica

Dvostupanjska autentikacija (2FA) u sustavu AAI@EduHr



Dvostupanjska autentikacija (2FA) u sustavu AAI@EduHr (2)

- Dvije različita metode autentikacije
- Prvi stupanj: autentikacija korisničkom oznakom i lozinkom
  - Imenici članica sustava AAI@EduHr
- Mogući drugi stupanj: za autentikaciju se koristi OTP, TOTP, certifikati
  - Yubico TOTP (Yubikey),
  - TOTP (Google Authenticator, Open OTP, Free OTP),
  - SMS OTP (SimpleSMS, infobip)
  - WebAuthn (u pripremi)
- Autentikacijski proces provodi središnji AAI@EduHr servis
- Dvostupanjsku autentikaciju odabire davatelj usluge
  - opcija pri registraciji usluge
  - treba voditi brigu o sigurnosti pojedine metode i cijeni implementacije

2FA - davatelji usluga

- Odabir ispravnog autentikacijskog mehanizma u registru resursa https://registar.aaiedu.hr/
- Obavijestiti korisnike o 2FA (davatelj usluge i/ili sami korisnici osiguravaju potrebne uređaje, programsku podršku, ...)
- Dodatni atribut u autentikacijskom odgovoru ***`mfa_type`***
- SMS Gateway se posebno dogovara (troškove snosi davatelj usluge)
- Nužna registracija korisnika prije korištenja usluge
  - prilikom prve prijave korisnika
  - aplikacija na strani davatelja usluge
  - aplikacija na strani matične ustanove

2FA - korisnici

- Registracija za svaku uslugu posebno prije korištenja usluge
- Registracija kod prvog korištenja usluge se obavlja u tri koraka:
  - Korisnik se autenticira korištenjem korisničke oznake i lozinke
  - Korisnik unosi podatke za drugi izvor autentikacije
  - AAI@EduHr servis šalje aktivacijski kod na e-mail adresu korisnika iz e-identiteta
  - Odabirom linka iz e-maila korisnik potvrđuje svoju registraciju, te može koristiti 2FA za odabranu uslugu
- Brisanje registiranih podataka za 2FA:
  - https://moj.aaiedu.hr/ web aplikacija
  - Brišu ili mjenjaju se podaci za sve usluge koje koriste istu metodu autentikacije za drugi stupanj autentikacije

Demo usluga

- Demonstracija 2FA za podržane autentikacijske metode
- Demo aplikacija obuhvaća procese registracije korisnika i autentikacije
- https://registar.aaiedu.hr/mfa-demo/

Planovi za budućnost

- Uvođenje WebAUTHN (FIDO2), te drugih autentikacijskih metoda
- Registracija 2FA kao vjerodajnica značajne razine sigurnosti u NIAS-u
- Unapređenje rješenja za registraciju korisnika za 2FA

Imate li pitanja?

Hvala na pažnji!

aai@srce.hr

https://www.aaiedu.hr

srce
Sveučilište u Zagrebu
Sveučilišni računski centar

www.srce.unizg.hr

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/otvoreni-pristup

srce otvoreni pristup