Višestupanjska autentikacija (MFA) u sustavu AAI@EduHr

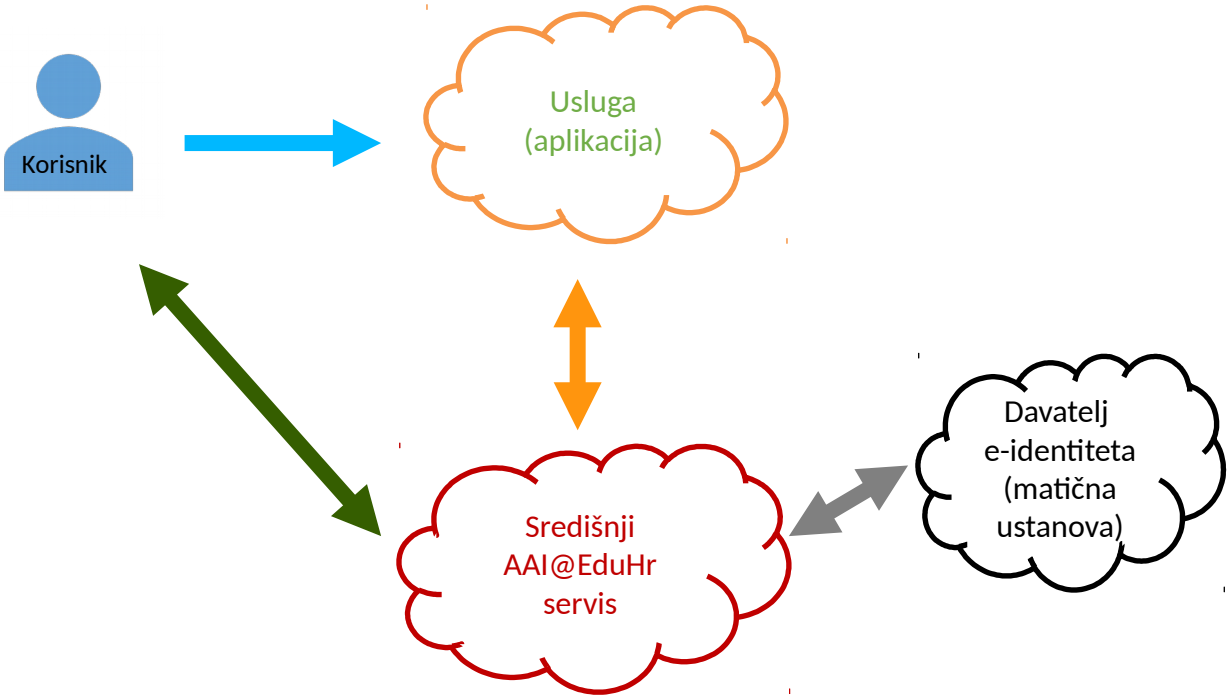
15. travnja, 2021.

Dubravko.Penezić@srce.hr

Sadržaj

- Autentikacijska struktura AAI@EduHr
- Višestupanjska autentikacija (MFA)
- Dvostupanjska autentikacija u sustavu AAI@EduHr
  - Osnovni podaci
  - Davatelji usluga
  - Korisnici
  - Demo usluga
- Opisi pojedinih elemenata 2FA u sustavu AAI@EduHr
  - Izvor autentikacije za drugi stupanj autentikacije
  - Registracija usluge za dvostupanjsku autentikaciju
  - Registracija korisnika za dvostupanjsku autentikaciju
- Prikaz rada (demo)
- Pitanja i odgovori

Tijek autentikacije



Tijek autentikacije – pogled korisnika

- Korisnik pristupa usluzi/aplikaciji registriranog davatelja usluge
- Usluga/aplikacija inicira proces autentikacije putem središnjeg AAI@EduHr servisa
- Središnji AAI@EduHr servis pokreće odgovarajući proces autentikacije
- Informacije vezane uz autentikaciju središnji AAI@EduHr servis i usluga razmjenjuju posredstvom korisnikovog web-preglednika (klijenta)
- Nakon uspješne autentikacije središnji AAI@EduHr servis obavještava uslugu/aplikaciju o uspješnosti autentikacije te proslijeđuje dogovoreni set podataka o korisniku
- Dokumentacija: https://www.aaiedu.hr/o-sustavu/sto-je-aaieduhr

Protokoli i izvori autentikacijskih podataka

- Podržani autentikacijski protokoli:
  - SAML (preporučen)
  - CAS
  - OIDC
  - RADIUS (samo za pristup mreži)

- Mogući izvori autentikacijskih podataka
  - Imenici članica sustava AAI@EduHr
  - Društvene mreže (Google, Facebook, LinkedIn, Twiter)
  - Vanjski izvori (eduID.ba, eduGAIN, NIAS)
  - Pod kontrolom korisnika (YubiKey, TOTP, SMS OTP, WebAuthn)

Načini autentikacije u AAI@EduHr

- Vrste vjerodajnica:
  - Korisnička oznaka i lozinka
  - Yubico Keys (multifunkcijski)
  - TOTP (uz odgovarajuću programsku podršku)
  - OTP via SMS
  - FIDO2/WebAuthn NFC/USB ključevi (u planu)
- Oblici autentikacije
  - Autentikacije putem korisničke oznake i lozinke
  - Dvostupanjska autentikacija
    (putem korisničke oznake i lozinke i jedne od ostalih vrsta vjerodajnica)

Višestupanjska autentikacija (MFA)

- Definicija
  - Višestupanjska autentikacija (MFA) vrsta je autentikacije u kojoj je korisnik autenticiran nakon što se uspješno autenticira kombinacijom dva ili više različita izvora 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 izvora
  - Smanjenje utjecaja kompromitacije neke od vjerodajnica

2FA u sustavu AAI@EduHr

- Dva različita izvora autentikacije
- Izvor prvog stupnja autentikacije: korisnička oznaka i lozinka
  - Imenici članica sustava AAI@EduHr
- Mogući izvori drugog stupnja autentikacije: OTP, TOTP, certifikati
  - Yubico TOTP, TOTP, SMS OTP, uskoro WebAuthn
- Autentikacijski proces obavlja središnji AAI@EduHr servis

2FA - davatelji usluga

- Odabir ispravnog autentikacijskog mehanizma u registru resursa
- 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)
- Moguće obaviti registraciju korisnika prije korištenja usluge
  (aplikacija na strani davatelja usluge)

2FA - korisnici

- Registracija za svaku uslugu posebno (automatska po prvom korištenju usluge) prije korištenja usluge
- Registracija 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 podataka za drugi izvor autentikacije:
  - https://moj.aaiedu.hr/ web aplikacija
  - Brišu ili mjenjaju se podaci za sve usluge koje koriste istu vrstu izvora za drugi stupanj autentikacije

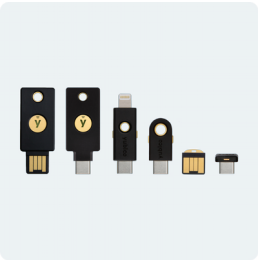
Demo usluga

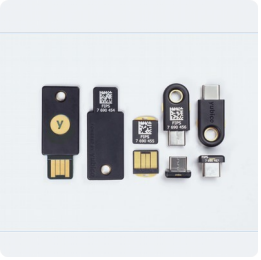
- Demonstracija 2FA za podržane autentikacijske izvore
- Demo aplikacija obuhvaća procese registracije korisnika i autentikacije
- https://registar.aaiedu.hr/mfa-demo/

Izvori autentikacije za drugi stupanj

- Yubico YubiKey
- SMS Gateway OTP
- TOTP – programska podrška

Yubico Yubikey





- USB/NFC autentikacijski ključevi
- Višestruki protokoli autentikacije (FIDO2, U2F, Smart card, OTP, OpenPGP 3)
- Trenutno podržan OTP (https://developers.yubico.com/OTP/OTPs_Explained.html), u planu FIDO2
- Autentikacija se obavlja umetanjem ključa u USB port ili korištenjem NFC-a, te pritiskom na tipku na samom uređaju
- Više o ključevima na https://www.yubico.com/
- Okvirna cijena oko 45 Eura

OTP putem SMS-a

- Generiranje jednokratnog ključa lokalno ili putem API-a
- Proslijeđivanje teksta poruke sustavu koji se brine o slanju SMS poruke (SMS Gateway)
- Korisnik na registrirani mobitel dobiva jednokratni ključ i unosi ga putem web-forme
- Trenutno implementirana podrška za infobip API (https://www.infobip.com/) i playSMS API (https://github.com/playsms/)
- Okvirna cijena oko 25 lipa po poruci

TOTP

- Vremenski ograničeni jednokratni ključevi
- Generiranje jednokratnog ključa temeljem registriranog serijskog broja generatora ključeva (najčešće je to aplikacija npr. Google Authenticator na korisnikovom uređaju)
- Ključ (kojeg prikaže aplikacija) se unosi putem web-forme
- Važno je imati sinkronizirano točno vrijeme na uređaju na kojem se nalazi aplikacija
- Cijena - besplatno

Registracija usluge za 2FA

- Precizne upute mogu se pronaći na adresi: https://www.aaiedu.hr/za-davatelje-usluga/za-web-aplikacije/sustav-jedinstvene-autentikacije-korisnika

  (poglavlje ***SAML konfiguracija za višestupanjsku autentikaciju***)
- Postupak kao za standardni SAML resurs, samo se odabire dodatni korak autentikacije

Registracija korisnika za 2FA

- Preciznu uputu moguće je pronaći na adresi:

  https://www.aaiedu.hr/za-krajnje-korisnike/cesto-postavljana-pitanja/registracija-korisnika-za-visestupanjsku-autentikaciju

- Korisnik prolazi kroz tri koraka:
  - Autentikacija prvim stupnjem
  - Registracija parametra za drugi stupanj (broj mobitela, YubiKey, secret/pin/code TOTP programske podrške)
  - Potvrda registriranog parametra za drugi stupanj autentikacije (klikom na link u dobivenom e-mailu)
- Na istoj stranici nalazi se uputa za web aplikaciju https://moj.aaiedu.hr/ putem koje je moguće vidjeti koji su parametri registrirani, te iste obrisati ako je potrebno

Demo: prikaz rada 2FA

- Registracija podataka za drugi stupanj (https://registar.aaiedu.hr/mfa-demo/) prvi prolaz kroz autentikaciju
- Autentikacija korisnika (https://registar.aaiedu.hr/mfa-demo/) standardni prolaz kroz autentikaciju
- Podaci o drugom faktoru (https://moj.aaiedu.hr/)
- Brisanje podatak o drugom faktoru (https://moj.aaiedu.hr/)

Pitanja

- U vezi MFA/2FA?
- U vezi AAI@EduHr?
- Prijedlozi tema za webinar?

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