MUNI

Novinky v Jednotném přihlášení MUNI

Pavel Břoušek
brousek@ics.muni.cz

Masarykova univerzita

2. září 2021

Osnova

Více-faktorová autentizace

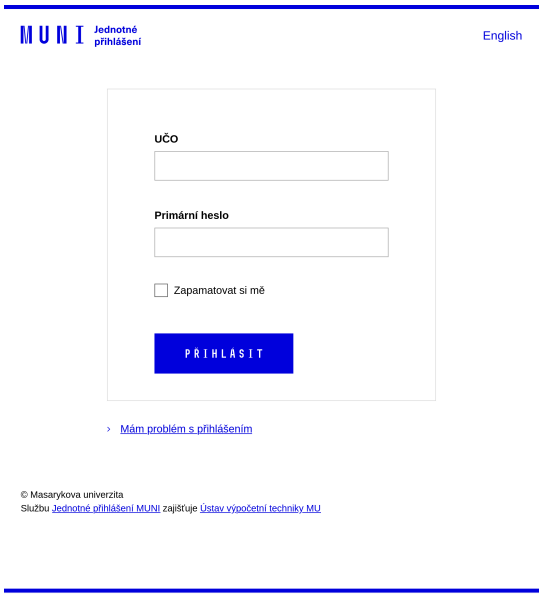
Bezpečnostní obrázky

Správa připojených služeb

Bezpečná konfigurace OIDC pro front-end aplikace

Jednotné přihlášení MUNI

- poskytovatel identit Masarykovy univerzity
- připojení
  - Security Assertion Markup Language V2.0 (SAML2)
  - OpenID Connect (OIDC)



Obrázek: Přihlašovací obrazovka

Osnova

Obecně k více-faktorové autentizaci

- metody autentizace uživatelů
  - tajemství (heslo, PIN)
  - vlastnictví (TOTP, certifikát, fyzické tokeny)
  - biometriky (otisk prstu)
  - chování
- kombinace dvou nebo více metod
  - zvýšit bezpečnost
  - minimalizovat nárůst komplexity pro uživatele
- ochrana proti krádeži jednoho faktoru autentizace (hesla)
  - útoky hrubou silou (online i offline)
  - lámání hashů hesel
  - offline phishingu

Time-based One-Time Password (TOTP)[1]

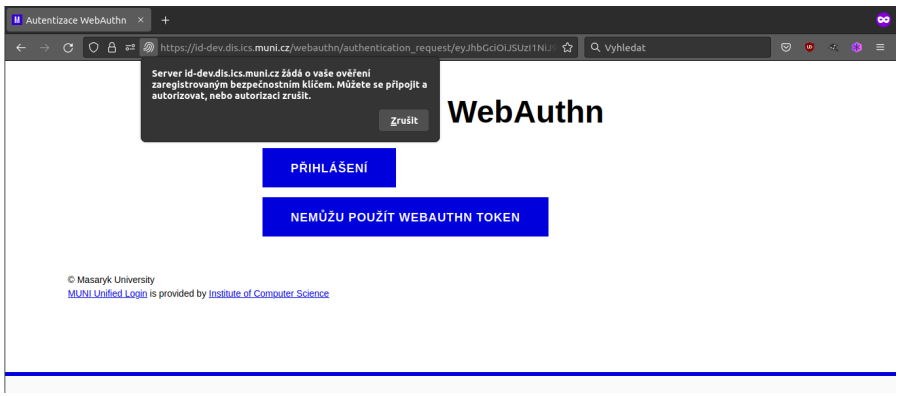
- 6místný číselný kód vygenerovaný TOTP aplikací
- podpora napříč platformami
- časové okno platnosti kódu
- negativní důsledky kompromitace serveru (databáze)

Obrázek: TOTP

[1] RFC 6238

Web Authentication (WebAuthn)[3]

- jednoduché použití
- ochrana proti MitM a phishingu[2]
- podpora ve většině webových prohlížečů
- omezené možnosti připojení fyzických klíčenek



Obrázek: WebAuthn

[2] developers.yubico.com/U2F/Protocol_details/Overview.html
[3] w3.org/TR/webauthn-2/

Implementace v Jednotném přihlášení

- aktivace na žádost služby (REFEDS MFA Profile[4])
- SAML
  - AuthnContextClassRef s hodnotou `https://refeds.org/profile/mfa`

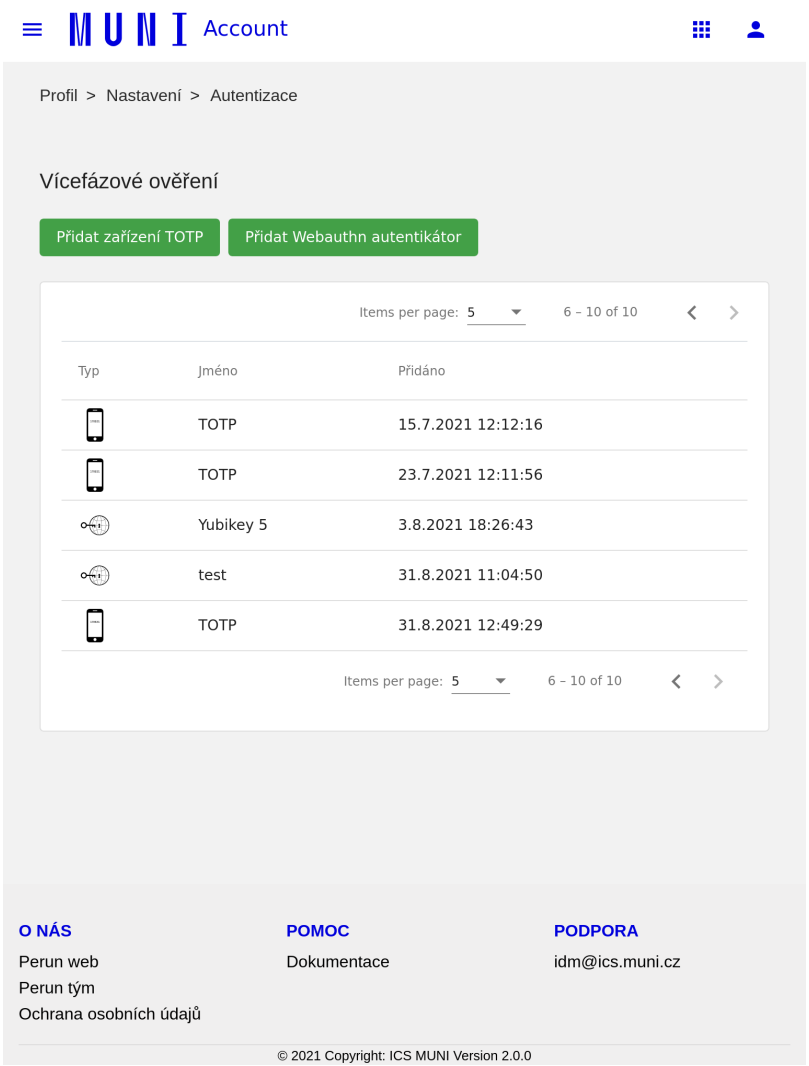
```
$auth->login([
  'saml:AuthnContextClassRef'
    => 'https://refeds.org/profile/mfa',
]);
```

- OIDC
  - parametr acr_values s hodnotou `https://refeds.org/profile/mfa`

```
customQueryParams: {
  acr_values: 'https://refeds.org/profile/mfa'
}
```

[4] `https://refeds.org/profile/mfa`

Uživatelský profil



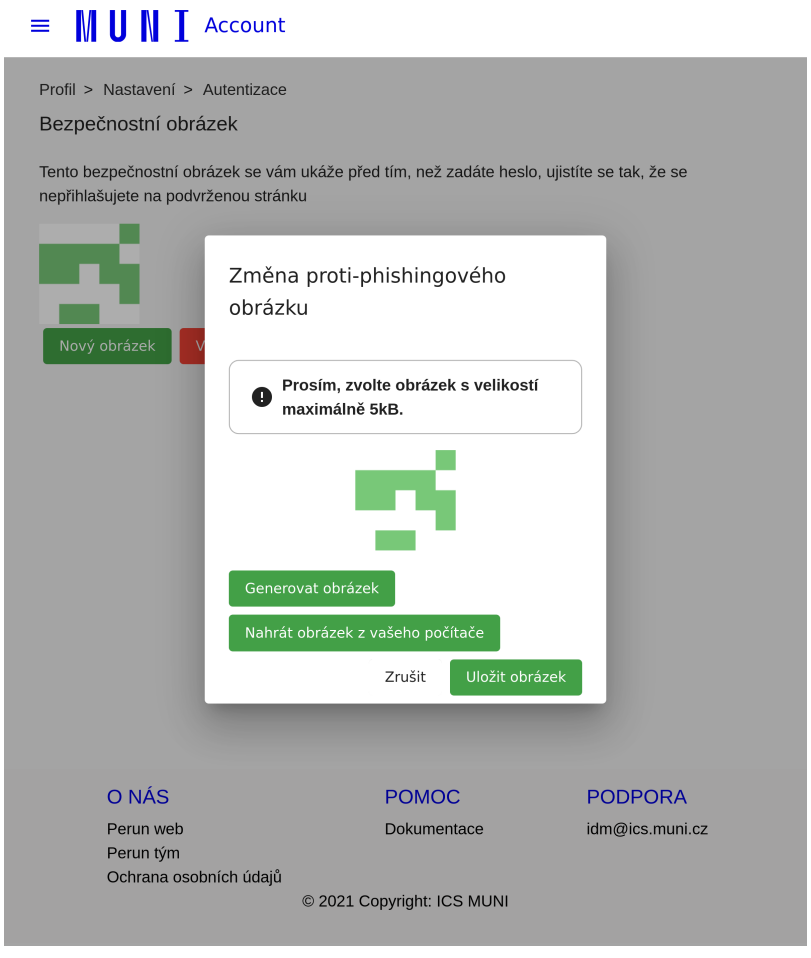
Obrázek: account.muni.cz

Osnova

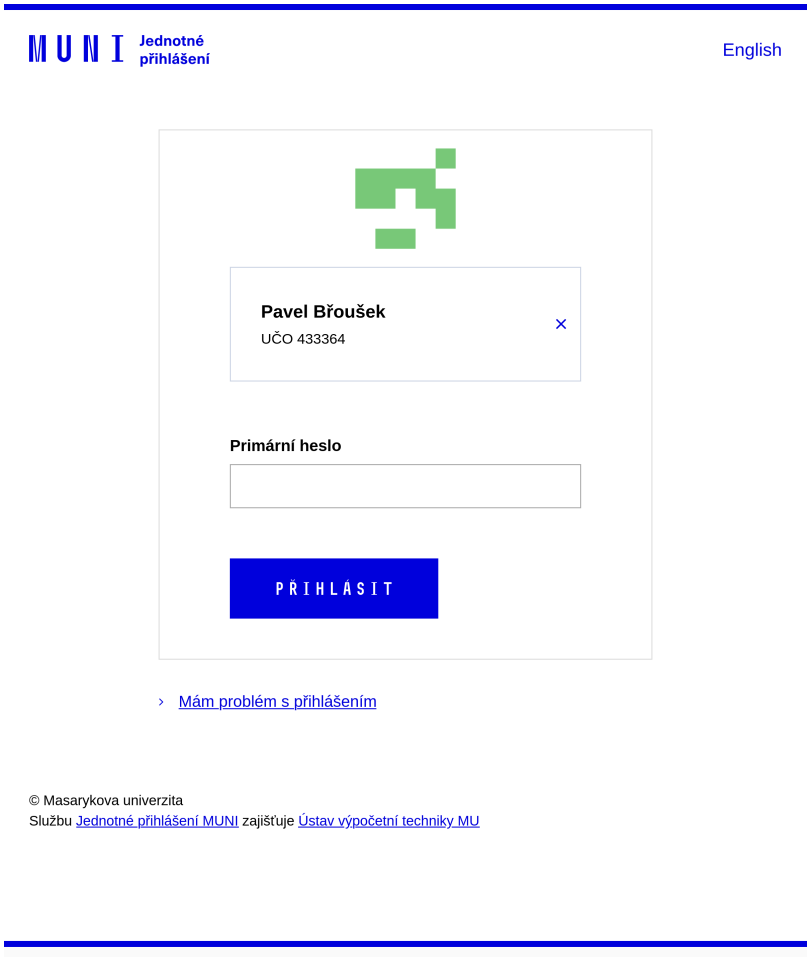
Ochrana proti phishingu

- různé variace (např. SiteKey)
- personalizovaný obrázek/text/barva na přihlašovací stránce
- chybějící obrázek může znamenat phishing
- výhody
  - jednoduchá implementace
  - jednoduché použití uživatelem
- nevýhody
  - obecně velmi malá účinnost
- alternativy
  - školení uživatelů
  - doplněk do prohlížeče
  - více-faktorová autentizace

Implementace v Jednotném přihlášení



(a) account.muni.cz

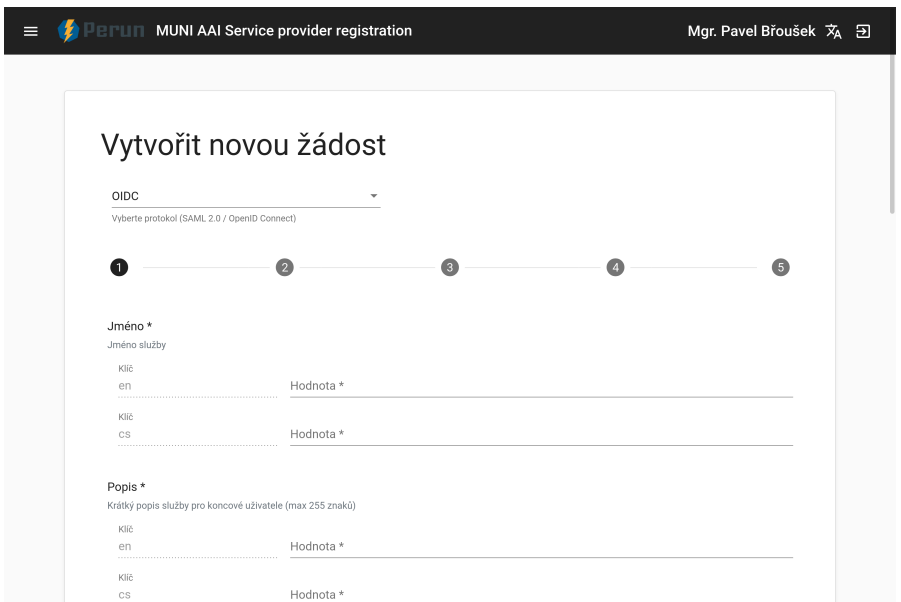


(b) přihlašovací obrazovka

Osnova

Aplikace SP reg

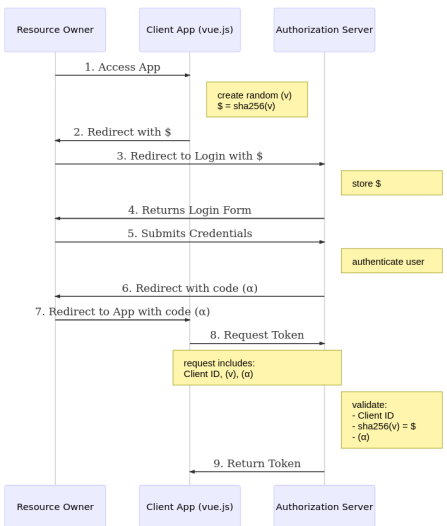
- spreg.aai.muni.cz
- přihlášky nových služeb
- správa připojených služeb a jejich parametrů
- přidávání/odebírání dalších správců



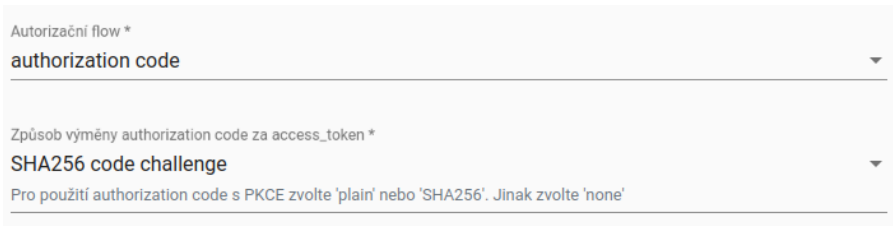
Osnova

Authorization code flow + PKCE

- Proof Key for Code Exchange[5]
- náhrada implicit flow
- určeno pro front-endové nebo mobilní aplikace (bez client secret)



zdroj: okta.com




```
{
   responseType:  'code'
}
```

[5] RFC 7636

Děkuji za pozornost.

idp@ics.muni.cz

MASARYKOVA
UNIVERZITA