

MUNI

Novinky v Jednotném přihlášení MUNI

Pavel Broušek

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)

MUNI Jednotné přihlášení English

uCo

Přihlašovací heslo

 Zapamatovat si mě

PŘIHLÁSIT

[Mám problémy s přihlášením](#)

© Masarykova univerzita
06.05.2021 [Jednotné přihlášení s SAML2](#) [zapřístup](#) [uživatel](#) [přihlášení](#) [masarykova.univzita.cz](#)

Obrázek: Přihlašovací obrazovka

Osnova

Více-faktorová autentizace

Bezpečnostní obrázky

Správa připojených služeb

Bezpečná konfigurace OIDC pro front-end aplikace

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)

MUNI Jednotné přihlášení

Vyžadována dvoufaktorová autentizace

Opište kód z TOTP aplikace na svém zařízení.

Pokud nevíte, co to znamená, nebo nemáte své zařízení, kontaktujte IT helpdesk.

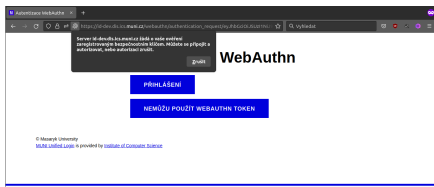
© Masarykova univerzita
Službu [Jednotné přihlášení MUNI](#) zajišťuje Ústav výpočetní techniky MU

Obrázek: TOTP

¹RFC 6238

Web Authentication (WebAuthn)³

- jednoduché použití
- ochrana proti MitM a phishingu²
- podpora ve většině webových prohlížečů
- omezené možnosti připojení fyzických klíčenek



Obrázek: WebAuthn

²developers.yubico.com/U2F/Protocol_details/Overview.html

³w3.org/TR/webauthn-2/

Implementace v Jednotném přihlášení

- aktivace na žádost služby (REFEDS MFA Profile⁴)
- 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'
}
```

⁴https://refeds.org/profile/mfa

Uživatelský profil








Profil > Nastavení > Autentizace

Vícefázové ověření

[Přidat zařízení TOTP](#)
[Přidat Webauthn autentifikátor](#)

Typ	Jméno	Přidáno
	TOTP	15.7.2021 12:12:16
	TOTP	23.7.2021 12:11:56
	Yubikey 5	3.8.2021 18:26:43
	test	31.8.2021 11:04:50
	TOTP	31.8.2021 12:49:29

Items per page: 5 | 6 - 10 of 10 | < >

O NÁS
 Perun web
 Perun tým
 Ochrana osobních údajů

POMOC
 Dokumentace

PODPORA
 idm@ics.muni.cz

© 2021 Copyright: ICS MUNI Version 2.0.0

Obrázek: account.muni.cz

Osnova

Více-faktorová autentizace

Bezpečnostní obrázky

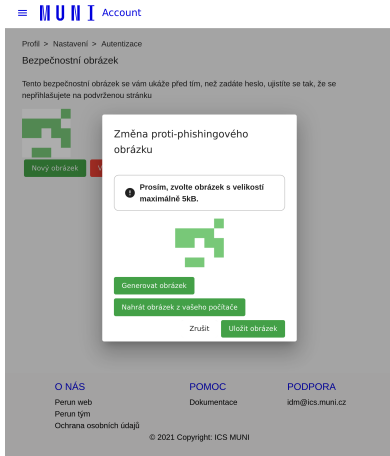
Správa připojených služeb

Bezpečná konfigurace OIDC pro front-end aplikace

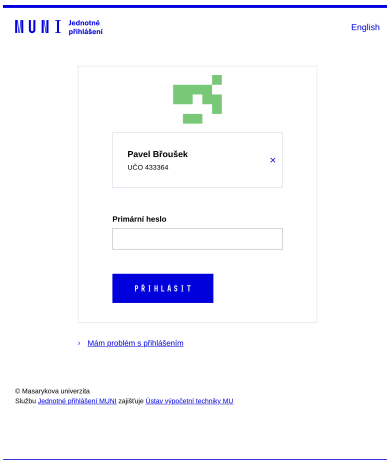
Ochrana proti phishingu

- 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

Více-faktorová autentizace

Bezpečnostní obrázky

Správa připojených služeb

Bezpečná konfigurace OIDC pro front-end aplikace

Aplikace SP reg

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

The screenshot shows a web browser window with the title "MUNI AAI Service provider registration" and the user "Mgr. Pavel Břoušek". The main heading is "Vytvořit novou žádost". Below it, there is a dropdown menu for "ODC" with the text "Vybírejte protokol (SAML, SSO / OpenID Connect)". A progress bar with five steps is shown, with the first step being active. The form contains three sections, each with a label and a description:

- Jméno ***
Jedná se o název
ODC: _____
en: _____ Hodnota *
ODC: _____
cs: _____ Hodnota *
- Popis ***
Krátký popis služby pro koncové uživatele (max 255 znaků)
ODC: _____
en: _____ Hodnota *
ODC: _____
cs: _____ Hodnota *

Osnova

Více-faktorová autentizace

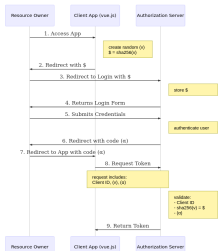
Bezpečnostní obrázky

Správa připojených služeb

Bezpečná konfigurace OIDC pro front-end aplikace

Authorization code flow + PKCE

- Proof Key for Code Exchange⁵
- náhrada implicit flow
- určeno pro front-endové nebo mobilní aplikace (bez client secret)



zdroj: okta.com

Autizační flow *

authorization code

Způsob výměny authorization code za access_token *

SHA256 code challenge

Pro použití authorization code s PKCE zvolte 'plain' nebo 'SHA256'. Jinak zvolte 'none'

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

⁵RFC 7636

Děkuji za pozornost.

idp@ics.muni.cz

**MASARYKOVA
UNIVERZITA**