MUNI
ICS

Multi-Factor Authentication (MFA)

Mgr. Dominik František Bučík
bucik@ics.muni.cz

Viacfázová autentizácia

- “Authentication” = proces overenia proklamovanej identity
- metódy
  - tajná informácia (heslo, PIN)
  - vlastníctvo (TOTP, certifikát, kľúčenky) = token
  - biometrika (odtlačok prsta)
  - správanie
- terminológia
  - Multi-Factor Authentication (MFA)
  - Two-Factor Authentication (2FA)
  - Two-Step Authentication
  - Step-up Authentication
  - Three-Factor Authentication (3FA)

Heslá

- reťazce znakov, tajná informácia
- jednoduchá implementácia, jednoduché použitie
- útoky eliminovateľné na strane serveru
- problém na strane užívateľov
  - správca hesiel?

Prečo MFA?

- jeden faktor môže byť málo
  - kompromitácia faktoru - heslá sú večný problém

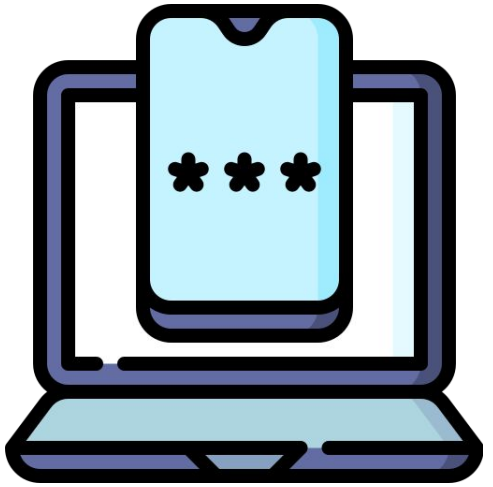
- kombinácia viacero faktorov (aspoň 2)
  - zvýšenie zabezpečenia
  - nenáročné pre užívateľov
  - väčšinou tajná informácia + token

- ochrana proti kompromitácii jedného prostriedku
  - token + heslo
    - brute-force, hash-cracking, offline phishing
  - PIN + token
    - lokálna kompromitácia

PrivacyIDEA

- open-source projekt
- ľahká integrácia, rozšíriteľnosť
- pomerne široká komunita
- nezávislé na IdP SW
- nasadenie na JP MUNI
  - modul do SimpleSAMLphp (privacyIDEA)
  - modul spracovania AuthN kontextov (authswitcher)
  - v budúcnosti integrácia do SaToSa

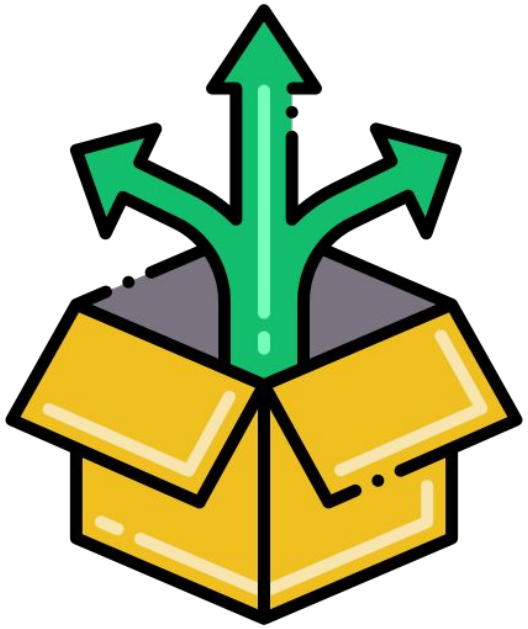
Podporované faktory



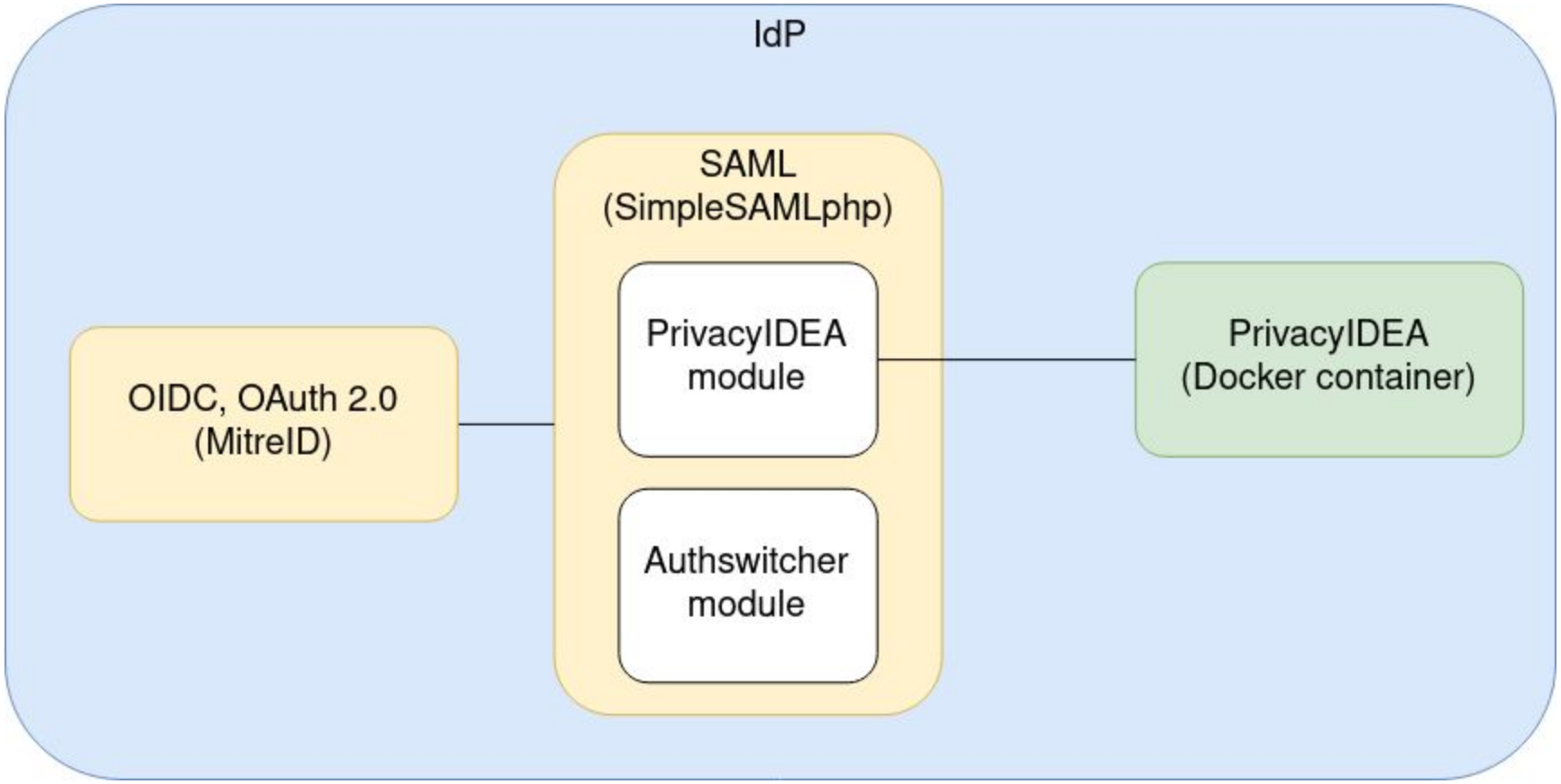
- Podporované
  - TOTP, WebAuthn, PaperCodes
  - SMS, e-mail OTP, TiQR, YubiKey, …
- Používané
  - TOTP
    - 6 číselný kód generovaný v smartphone aplikácii
  - WebAuthn
    - WebAuthn schopný device (FaceID, Windows Hello, YubiKey, …)
  - PaperCodes
    - Záložné kódy vytlačené na papier

Integrácia s IdP

- SimpleSAMLphp
  - docker kontajner (PrivacyIDEA)
  - integrácia cez SSP moduly
    - simplesamlphp-module-privacyidea
    - simplesamlphp-module-authswitcher
- SaToSa
  - docker kontajner (PrivacyIDEA)
  - integrácia ako microservice (vo vývoji)
- Shibboleth (untested)
  - docker kontajner (PrivacyIDEA)
  - library pre integráciu (GitHub repo)



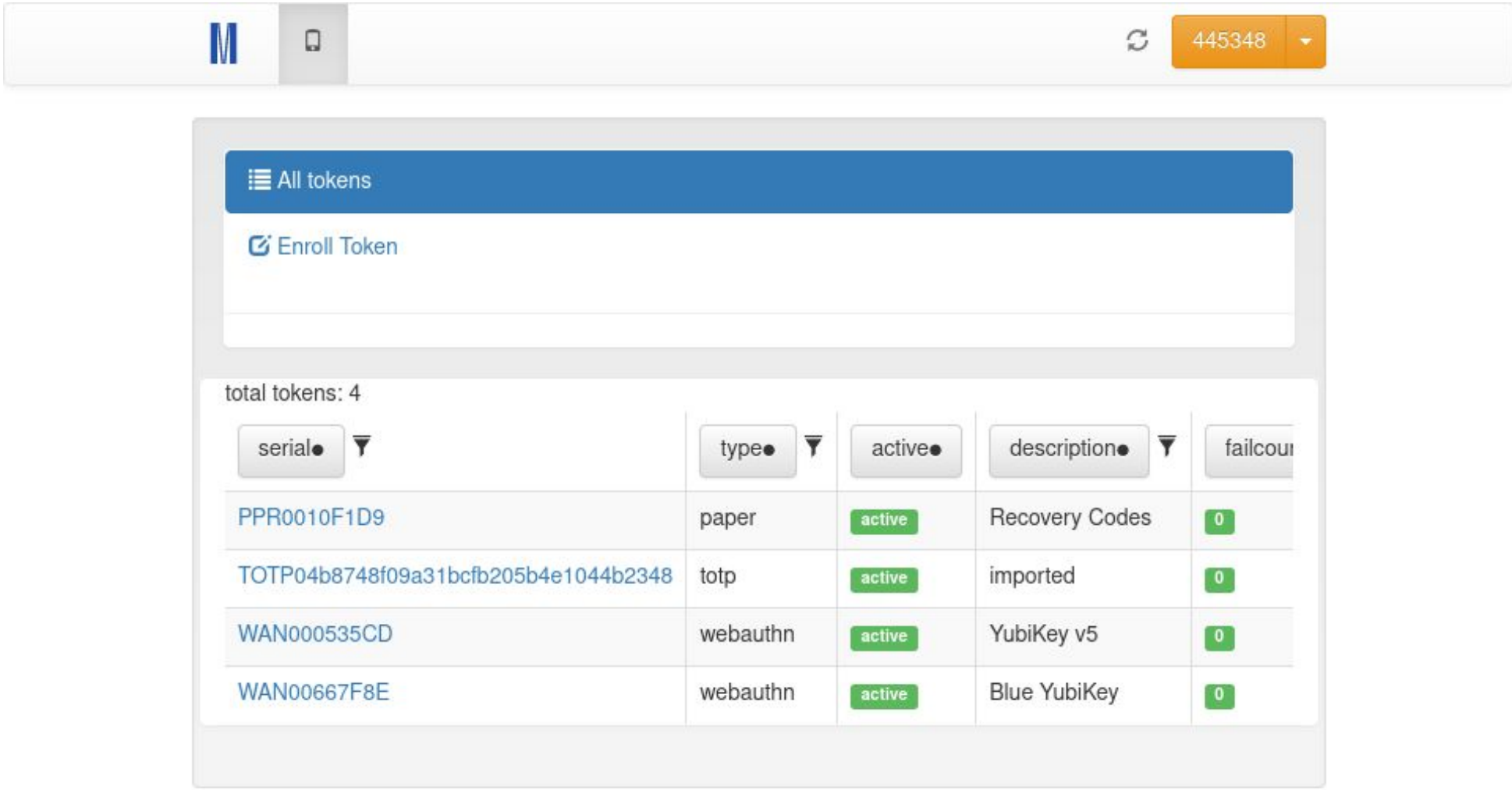
Príklad architektúry s IdP/ProxyIdP



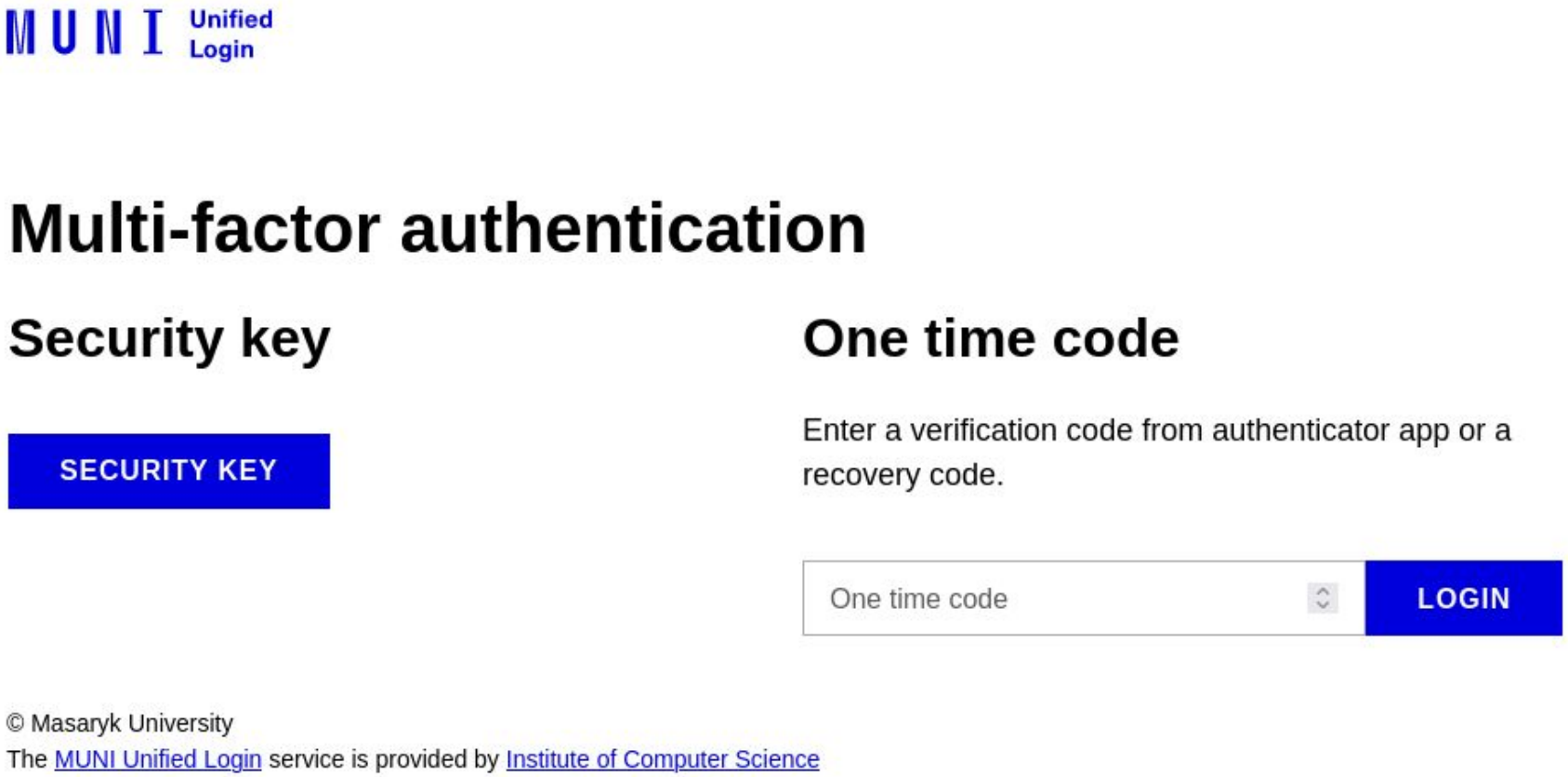
Technikality

- postavené okolo REFEDS MFA
- SP posiela AuthenticationContextClassRef
  - https://refeds.org/profile/mfa - MFA
  - resp. acr_values=... v prípade OIDC
- API pre komunikáciu s PrivacyIDEA serverom
  - Má tokeny? Aké? Sú tokeny validné?
  - execute MFA flow (overenie TOTP, WebAuthn flow, …)
- UI pre registráciu a správu “faktorov”

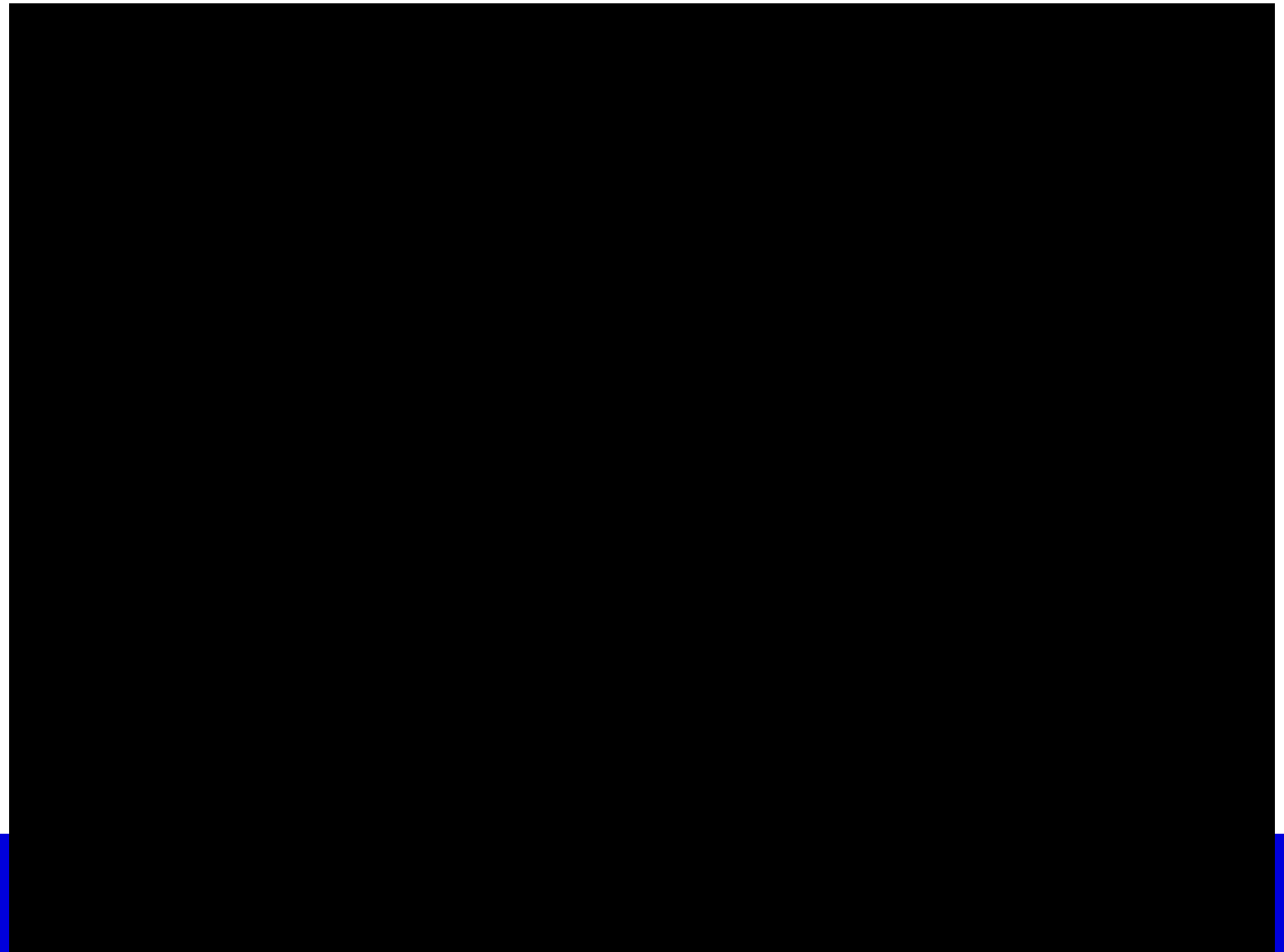
UI - správa tokenov



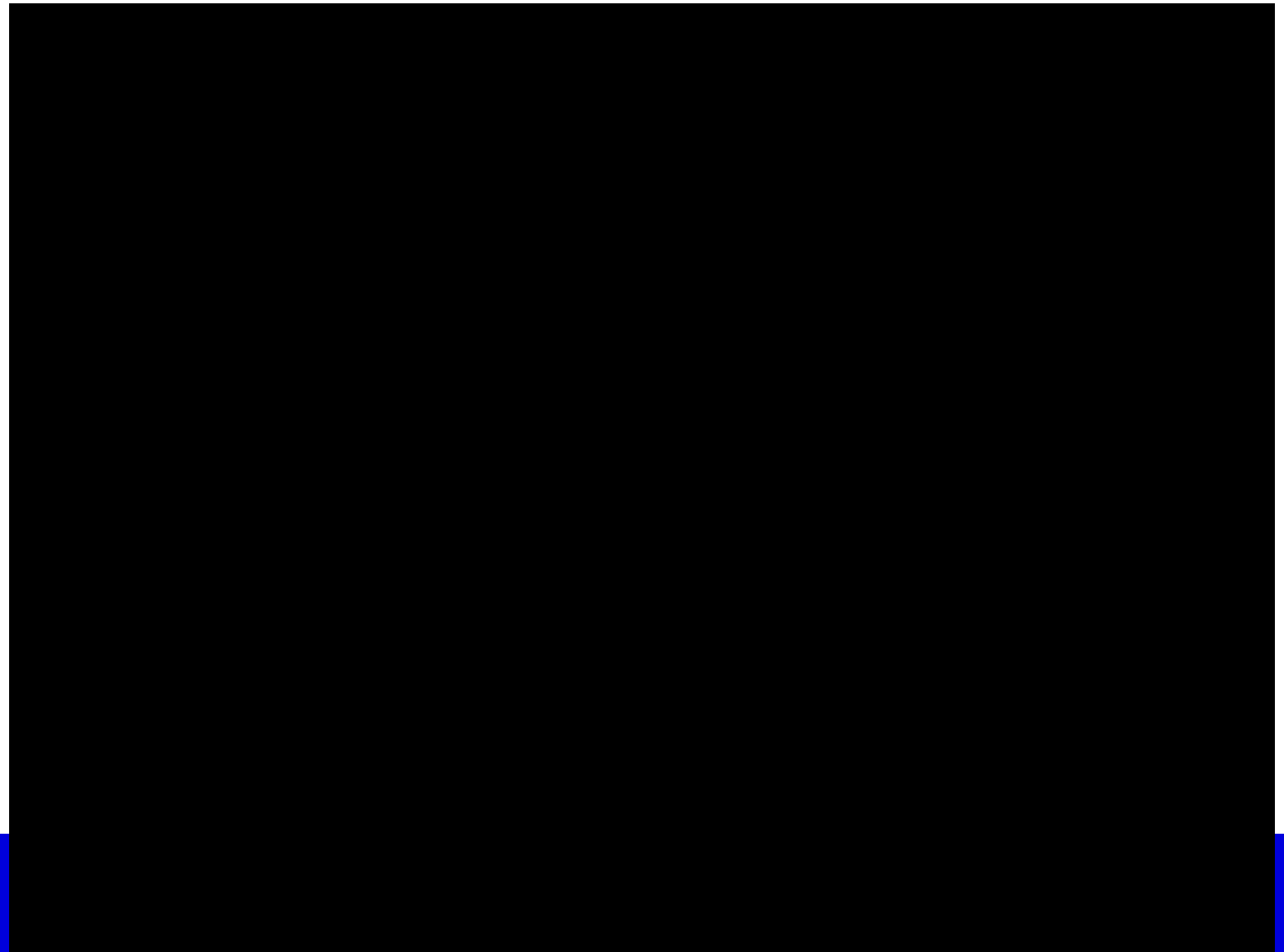
UI - použitie


MUNI Unified Login
Multi-factor authentication
Security key
SECURITY KEY
One time code
Enter a verification code from authenticator app or a recovery code.
One time code
LOGIN
© Masaryk University
The MUNI Unified Login service is provided by Institute of Computer Science

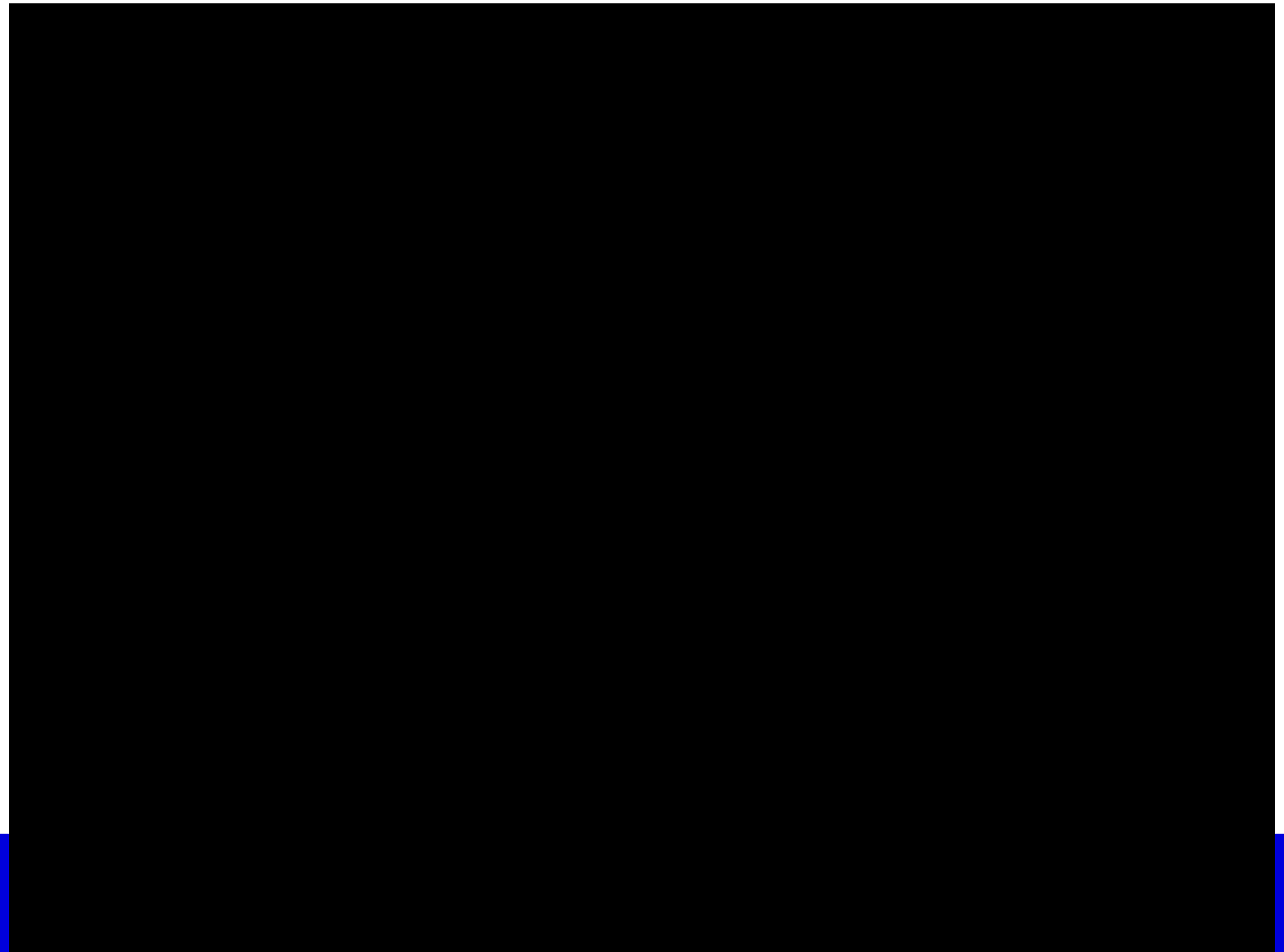
Užívateľská flow (IdP)



Užívateľská flow (ProxyIdP) - MFA IdP



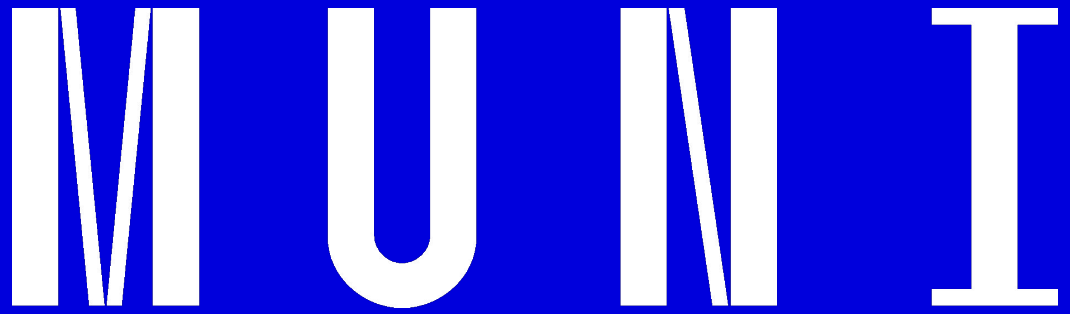
Užívateľská flow (ProxyIdP) - fallback



Použitie, projekty

- Nasadenie
  - Jednotné přihlášení MUNI
  - e-INFRA CZ
  - LifeScience AAI (ELIXIR AAI)

- FR CESNET
  - Link
  - Implementace vícefaktorové autentizace v akademickém prostředí
  - “Úkolem tohoto projektu je sestavení generické komponenty pro realizaci MFA v prostředí Identity Providerů provozovaných akademickými subjekty.”
  - Dôraz na UX



Otázky?

Dominik F. Bučík <bucik@ics.muni.cz>
it@muni.cz