

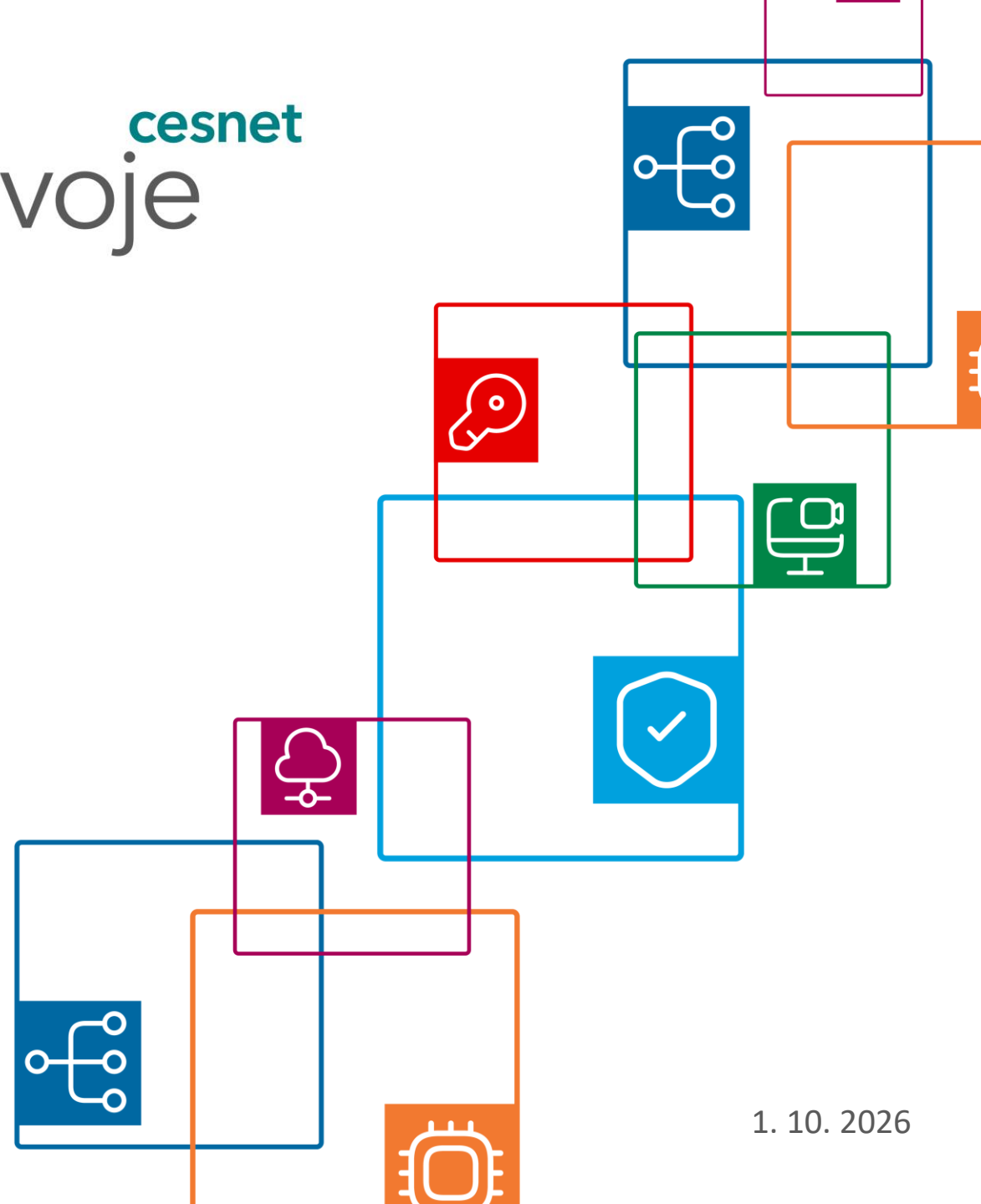


Bezheslová autentizace v prostředí IS ZČU

Pavel Jindra, Petr Schacherl

Konference e-infrastruktury CESNET

Západočeská univerzita v Plzni,
Centrum informatizace a výpočetní techniky (CIV)



1. 10. 2026

- Passwordless autentizace odstraňuje hesla, omezuje phishing a zjednodušuje přihlášení
- Splňuje moderní bezpečnostní standardy (MFA)
- Přináší lepší uživatelský zážitek
- Využívá systémové funkce clientského zařízení pro ochranu klíčů
 - Privátní klíč neopouští zabezpečené prostředí autentizátoru (TPM, HW token, Bitwarden, apod..)
 - Podporují ji Windows Hello, Face ID , TouchID, Yubikey, ...
 - Uživatel využívá známý systémový dialog

- Řešení snadno implementovatelné do stávající SSO Shibboleth
 - Zúročení předchozího úsilí o sjednocení služeb pod SSO
- Snadná správa a klíčů
- Podpora více autentizačních metod
 - Z důvodu kompatibility a uživatelského komfortu (možnost výběru)
 - **TOTP, push notifikace a passkeys**
- Přijatelné pořizovací a provozní náklady
 - Open-source

- **Cisco Duo Security**
 - Komerční řešení založené na CISCO Duo Security
 - Kromě MFA poskytuje i dodatečnou ochranu stanice
 - Komerčně nedostupné
- **WebAuthn plugin do IdP**
 - Podporuje pouze autentizaci FIDO2/WebAuthn
 - Neposkytuje TOTP ani push notifikace
 - Limituje uživatele k určitému technologickému vybavení
- **IdP + Authn-Plugin fudiscr + eduMFA – vybrané řešení**
 - Plugin fudiscr implementuje MFA a passkey do Shibboleth IdP
 - eduMFA doplňuje TOTP, eduPUSH a další typy tokenů
 - eduMFA lze využít také pro služby mimo Shibboleth
 - Navázaná spolupráce s vývojáři

- **Shibboleth Identity Provider (IdP) (v. 5.2.3)**
 - Protokoly SAML 2.0 a OpenID Connect (OIDC)
 - Zajišťuje jednotné přihlášení (SSO) pro interní i federované webové služby
- **fudiscr plugin do IdP**
 - Implementuje MFA i passkey (FIDO2/Webauthn)
 - Vyvíjen na „Freie Universität Berlin“
 - Flexibilní konfigurace autentizačních toků (flow)
- **eduMFA – správce klíčů**
 - Open-source systém pro správu autentizačních tokenů
 - Podporuje passkeys, TOTP, eduPUSH a další metody
 - Vychází z privacyIDEA a rozvíjí funkce pro akademické prostředí

- **Aplikace pro správu klíčů**

- Zjednodušuje registraci a správu tokenů
- S eduMFA komunikuje prostřednictvím API
- Umožňuje jednoduchou a přehlednou správu klíčů

- **Heslo.zcu.cz přes BankID**

- Umožní zneplatnit registrace tokenů uložené v eduMFA
- Po ověření pomocí Bank iD lze zneplatnit registrace tokenů uložené v eduMFA
- Spolehlivé ověření totožnosti

Podpůrné komponenty – vlastní vývoj

■ Aplikace pro správu klíčů

TOKENY

Moje tokeny

Aktivní: 4 Neaktivní: 0

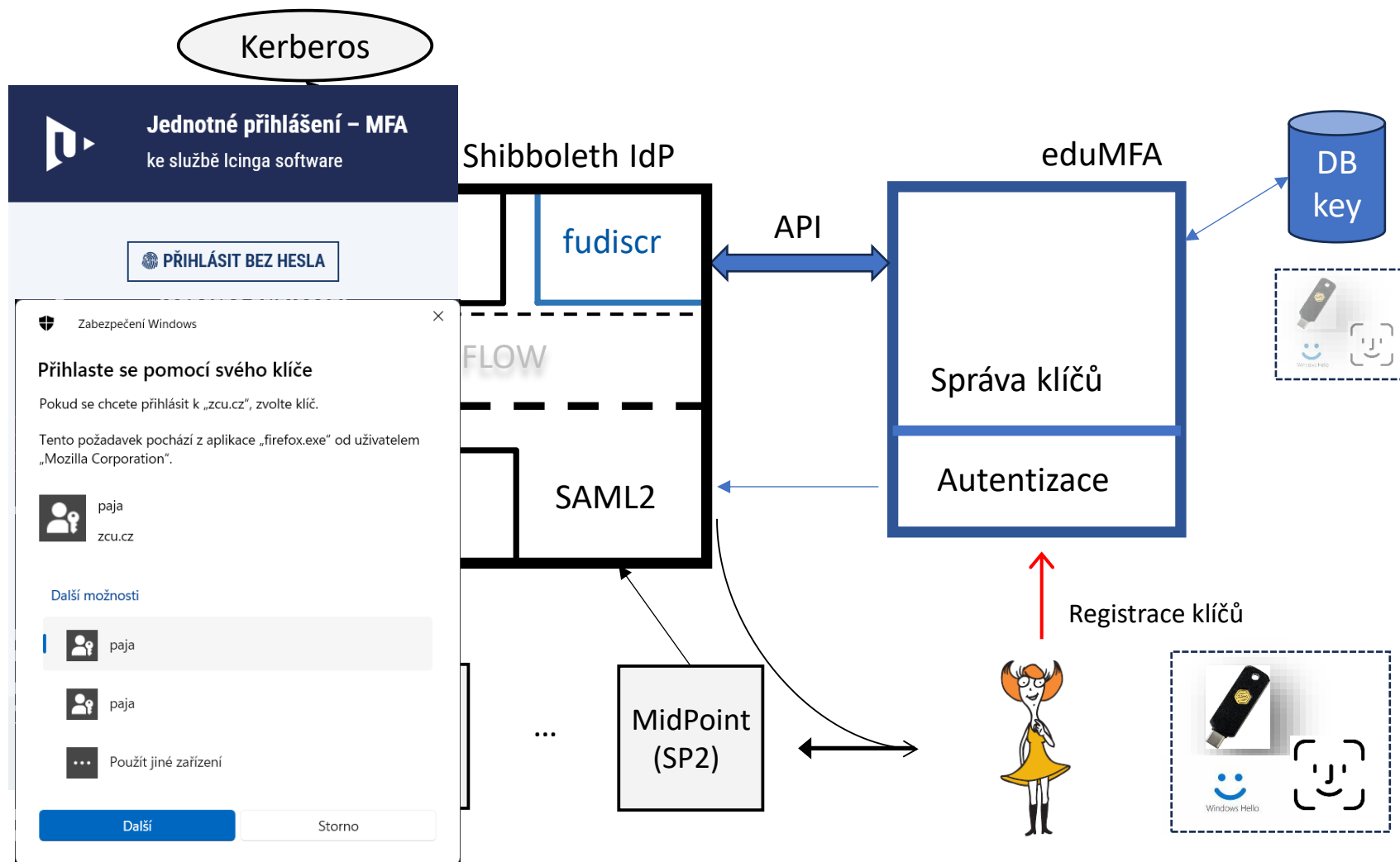
Na jednom místě vidíte své aktivní i neaktivní tokeny a můžete je spravovat bez přechodu do administrace eduMFA.

4
celkem tokenů

4
aktivní

DALŠÍ KROK
Přidat nový token
Vytvoříte TOTP, PPR nebo WebAuthn token.
Registrovat nový token

SERIAL	TYP	POPISEK	STAV	AKCE
EDUP0005C448	• edupush	A55 	Aktivní	Deaktivovat Smazat
TOTP000345C1	• totp	Google Authenticator 	Aktivní	Deaktivovat Smazat
WAN0010DAF9	• webauthn	Win Hello paja dell windowsy 	Aktivní	Deaktivovat Smazat
WAN002214AE	• webauthn	Cerny Idemkey 	Aktivní	Deaktivovat Smazat



- Možnost kombinace password, MFA i usernameless
- Využití systémového autentizačního dialogu (WinHello, FaceID)
- Konfigurovatelné FLOW může dyn. měnit auth. proces
- Podle politiky lze kombinovat heslo, TOTP, push notifikace a passkeys
 - Uživatel s registrovaným tokenem má jeho použití povinné
 - Uživatel bez tokenu může získat přístup pouze k registračnímu portálu
 - Pro vybrané služby lze vyžadovat hardwarový bezpečnostní klíč
- Řešení umožňuje postupný přechod k MFA a bezheslovému přihlášení



Obnova přístupu po ztrátě nebo kompromitaci klíčů

■ Trvalá obnova přístupu - ztráta zařízení



- Po ověření identity pomocí Bank iD systém zneplatní původní registrace tokenů
- Uživatel si následně zaregistruje nové autentizační prostředky
- Proces zajišťuje portál heslo.zcu.cz

■ Dočasná obnova přístupu – zapomenutí

- Administrátor může aktivovat přechodný autentizační prostředek
- Původní tokeny se dočasně zablokuji
- API eduMFA umožňuje jejich řízenou deaktivaci a opětovnou aktivaci



- Passkeys přinášejí přihlášení odolné proti phishingu a odstraňují nutnost zadávat heslo
- Vybrané řešení využívá stávající infrastrukturu Shibboleth SSO
- Kombinace fudiscr a eduMFA podporuje passkeys, TOTP, push notifikace a další tokeny
- Řešení umožňuje postupnou migraci uživatelů bez jednorázového zrušení současných metod
- Pilotní implementace ověřila technickou použitelnost řešení v prostředí ZČU – uživateli vesměs pozitivně přijímáno
- Navrhované řešení je využíváno také na UJEP v Ústí nad Labem

Děkuji za pozornost a podporu



Zdroje:

<https://edumfa.io/>

https://doku.tid.dfn.de/en:shibidp:plugin-fudiscr#idp-authn-plugin_fudiscr

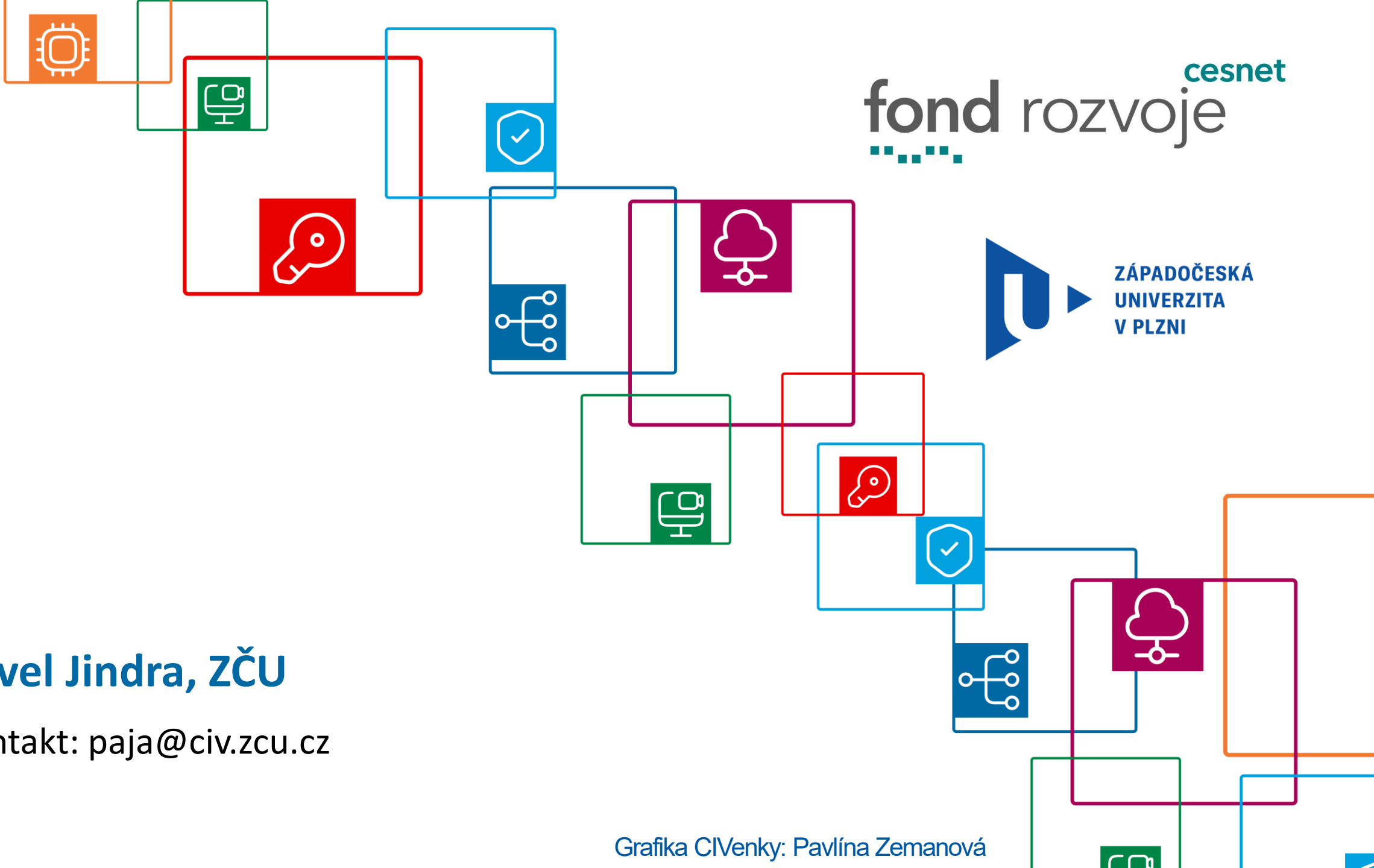
<https://fidoalliance.org/>

Závěrečná zpráva projektu FR Cesnet č. 736/2023.

Projekt byl podpořen z Fondu rozvoje CESNET.

Kontakt:

Pavel Jindra, paja@civ.zcu.cz



fond rozvoje cesnet



**ZÁPADOČESKÁ
UNIVERZITA
V PLZNI**

Pavel Jindra, ZČU

Kontakt: paja@civ.zcu.cz

Grafika CIVenky: Pavlína Zemanová