

mojeID

10 let budování eID v České republice
sdružením CZ.NIC

Jaromír Talíř • jaromir.talir@nic.cz • 06. 11. 2020

Představení CZ.NIC

- Správce domény CZ
- Zájmové sdružení právnických osob (ISP, registrátoři, držitelé domén) – neutrální, otevřené, zisk se nerozděluje.
- 1.3 mil. domén, **800 000+** kontaktů
- Strategie: „...hledání nových technologických výzev a reagovat na ně novými inovativními projekty.... podpora eGovernmentu...“
- Další projekty: Software (FRED, BIRD, Knot DNS, Knot Resolver), Hardware (Turris)



Kyberkriminalita na internetu

```
domain:      myfakedomain.cz
registrant:  XYZ1
registrar:   REG-FRED_A
registered:  16.10.2019 11:41:09
expire:      16.10.2020

contact:     XYZ1
name:        Mickey Mouse
address:     Disneyland
address:     Paris
address:     12345
address:     FR
registrar:   REG-FRED_A
created:     16.10.2019 11:40:51
```

- Obvykle spojeno s falešnou totožností držitele
- Doménové registry jsou často zatahovány do sporů
- Je možné zrušit registraci v případě zjištění nepravdivých údajů

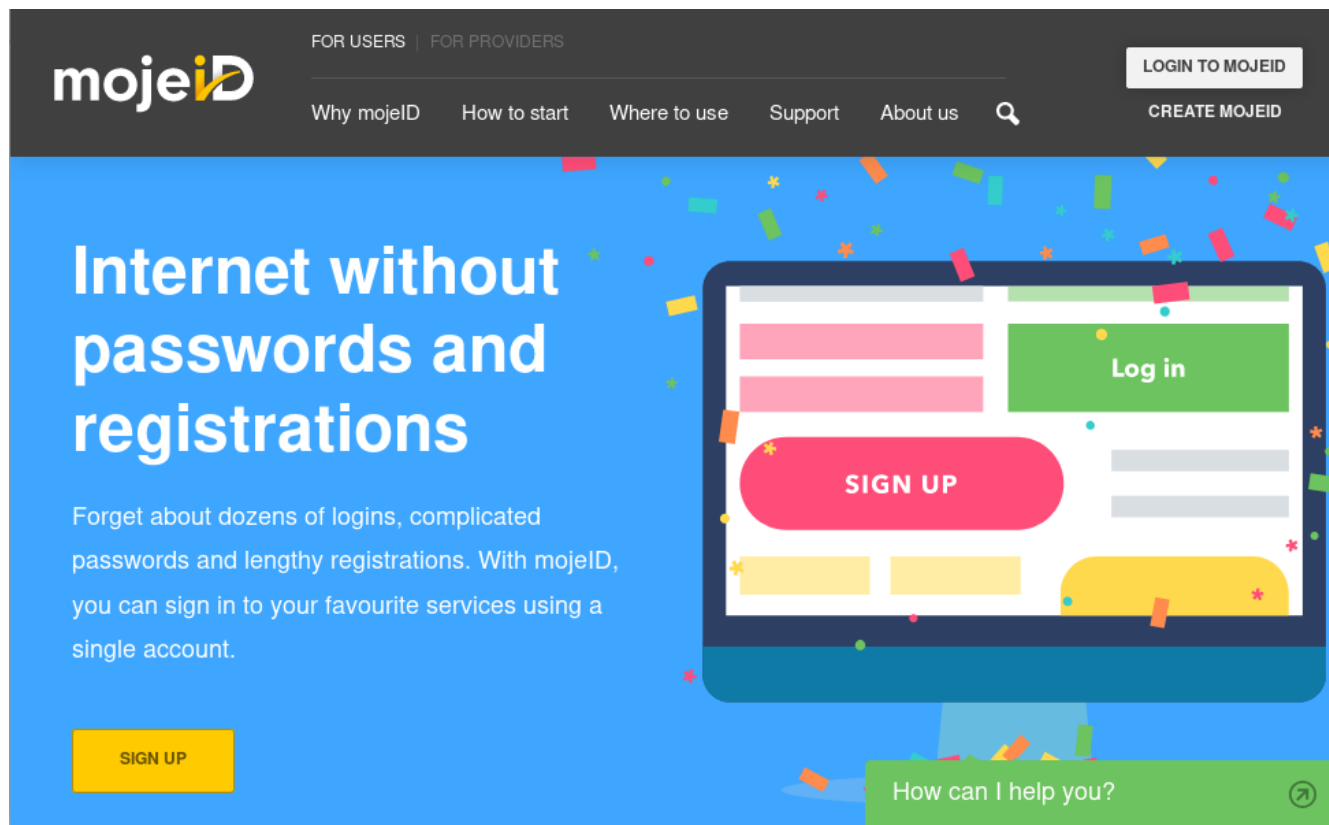


Služba mojeID

- Přímá propojená s registrem domén
 - Uživatelský účet je možné (nikoliv nutné) přímo propojit s doménou
 - Autentizace pro služby registru
 - Motivace udržovat si kontaktní údaje u registru ověřené
- Ověření údajů a „single sign-on“
- První obecně použitelná ověřená digitální identita
- Zdarma pro všechny uživatele
- Spuštěno v říjnu 2010



Jak přesvědčit uživatele



Jak přesvědčit služby

mojeiD

FOR USERS | FOR PROVIDERS

Why MojeiD Options and prices Getting started About us

LOGIN TO MOJEID

CREATE MOJEID

Verified users for your site

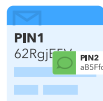
Say goodbye to fake accounts, wrong telephone numbers and non-existent addresses. MojeiD users are verified by us, so you always know who's on the other side.

SET UP MOJEID

How can I help you?



Ověření údajů



- Povinná kontrola e-mailu a telefonu
- Volitelná kontrola korespondenční adresy
- Volitelná plná kontrola totožnosti:
 - Osobní návštěva na pobočkách nebo validačních místech
 - Notářská doložka na zaslaném dopisu
 - Datové schránky
 - Osobní návštěva na CzechPointu

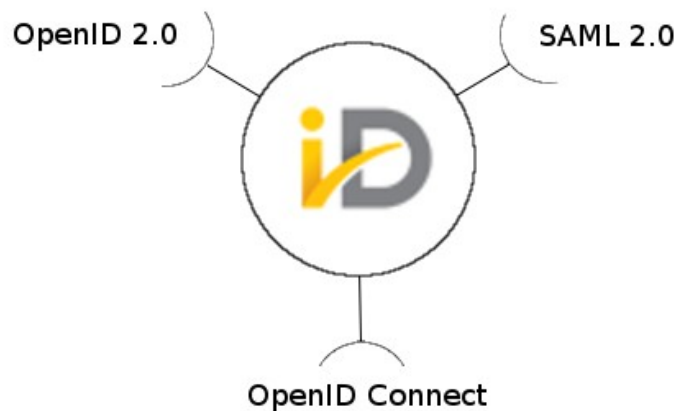


Dvoufaktorová autentizace

- Na začátku bylo jméno a heslo nebo přihlášení TLS klientským certifikátem
- Postupně vzniklo několik alternativ pro druhý faktor:
 - 2013 – TOTP (RFC 6248) – Google Authenticator
 - 2016 – Push notifikace do mobilní aplikace (mojeID Autentikátor)
 - 2019 – FIDO2/WebAuthn – Možnost několik bezpečnostních klíčů
- Možnost kombinace nebo i všech možností najednou



Autentizační protokoly



- **OpenID 2.0 - 2010**
 - Stále velká většina služeb
- **SAML 2.0 - 2014**
 - Akademická sféra
 - eGovernment
- **OpenID Connect - 2015**
 - Nové služby

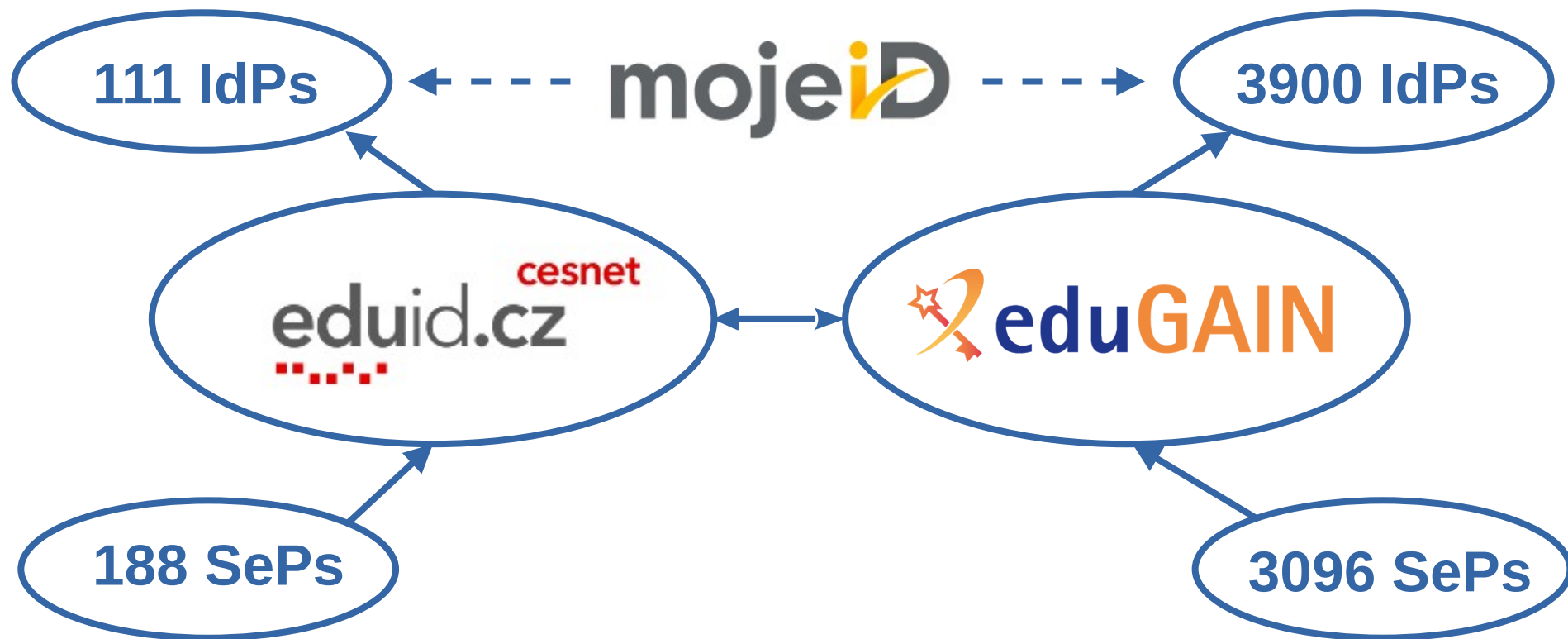


Katalog služeb - <https://www.mojeid.cz/cs/kde-pouzit/kde-pouzit-katalog/>



Akademické federace



Spolupráce se státem

- Rozsáhlé pilotní projekty STORK (**S**ecure **i**den**T**ity **a**cr**O**ss **b**o**R**der **l**in**K**ed) - 2009-2012 a 2012-2015
 - Síť propojených bran napojených na lokální IdP
 - Za ČR účast MVCR a CZ.NIC – provoz autentizační brány napojené na mojeID
 - Možnost využívat mojeID pro přihlášení do portálů evropských institucí
- Nařízení eIDAS
 - Provoz mezinárodní brány (eIDAS uzel) na základě výběrového řízení (2018-2020 a 2020-2024)
 - Zapojení do rozvíjení eIDAS v rámci Cooperation Network a Technical SubGroup
 - Napojení mezinárodní brány na NIA v roli SeP a IdP



mojeID jako kvalifikovaný systém eID

- Hlavní práce během 2019
 - <https://github.com/CZ-NIC/python-cz-nia>
- Akreditace v průběhu 2020
 - Posouzení shody EZU (březen-duben)
 - Vlastní akreditace MVCR (květen-srpen)
 - Produkční spuštění (září)
- Jakýkoliv **FIDO klíč certifikovaný v rámci FIDO certifikačního programu na L1** a ověření totožnosti přes **CzechPoint** nebo **NIA**



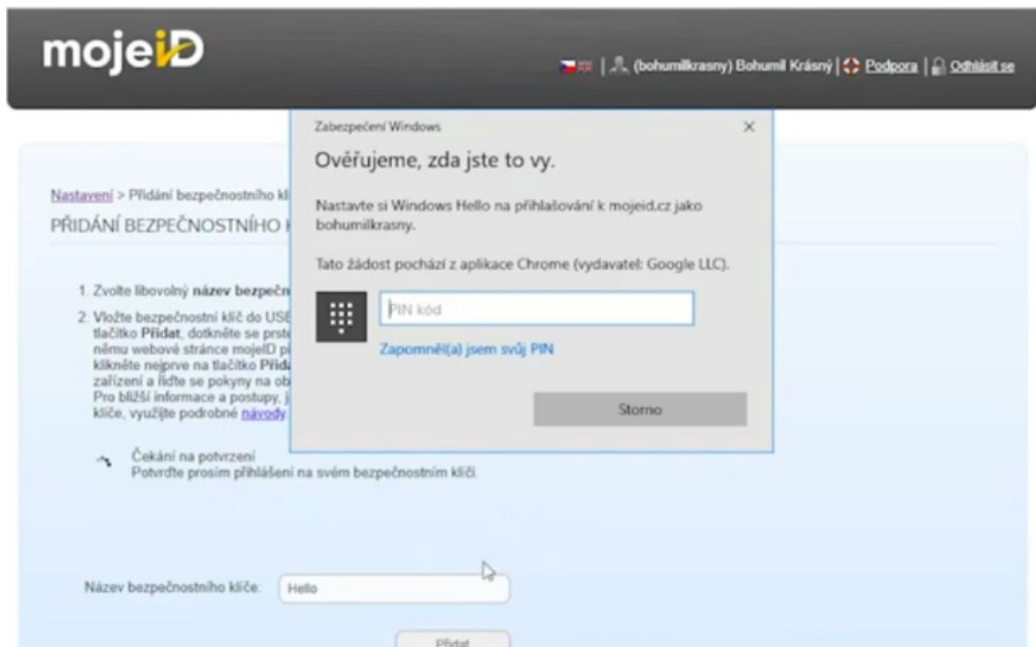
FIDO – Fast IDentity Online



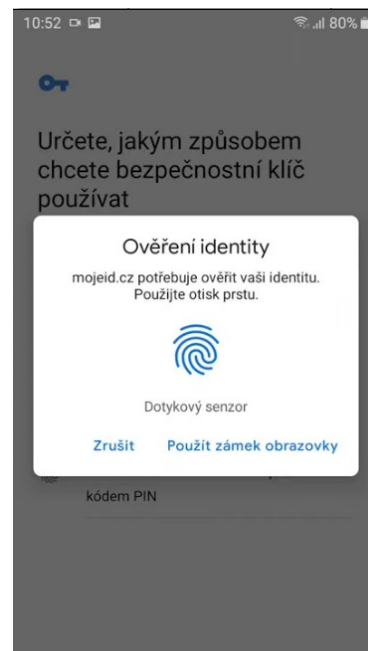
- **Bezpečnost**
 - Kryptografie, Anti-phishing
- **Otevřenost**
 - Desítky výrobců
- **Jednoduchost**
 - Žádné čtečky (USB, NFC, BLE)
 - Žádné aplikace



FIDO – systémové klíče (Win10, Android7, iOS14)



Video návod pro Windows Hello



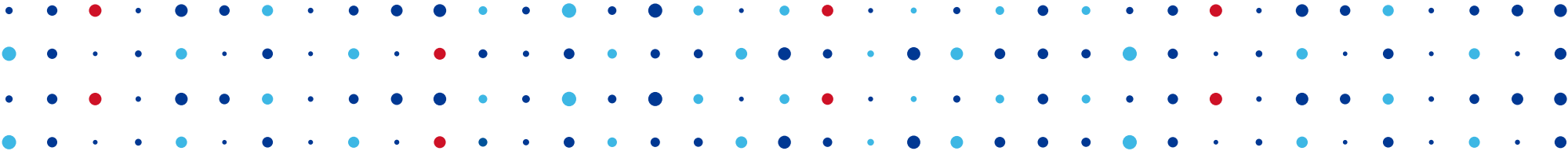
Video návod pro Android



Co dál?

- Ověření totožnosti přes ISDS
- Dokončení akreditace FIDO na úroveň záruky vysoká
- Notifikace mojeID do EU
 - FIDO Alliance bedlivě sleduje první použití FIDO pro eGovernment
- Koordinujeme spolupráci evropských doménových registrů (CZ, EE, DK, NL)
 - <https://regeid.eu>
- Akreditace dalších prostředků (nízká, značná)
- Otevřenost pro spolupráci s dalšími partnery





Děkuji za pozornost

Jaromír Talíř • jaromir.talir@nic.cz