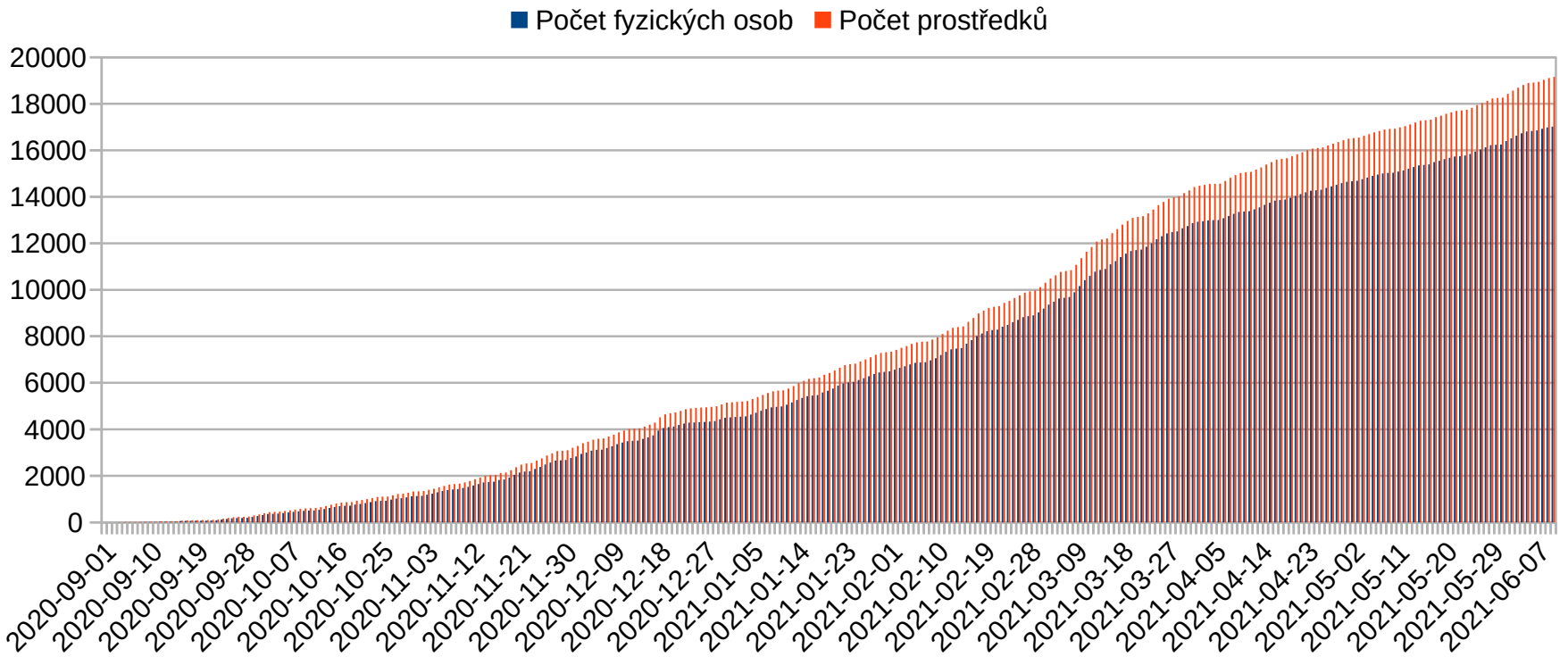
Novinky v mojeID

Co se událo od listopadu

Jaromír Talíř • jaromir.talir@nic.cz • 10. 6. 2021

Propojení se systémy veřejné správy



mojeID

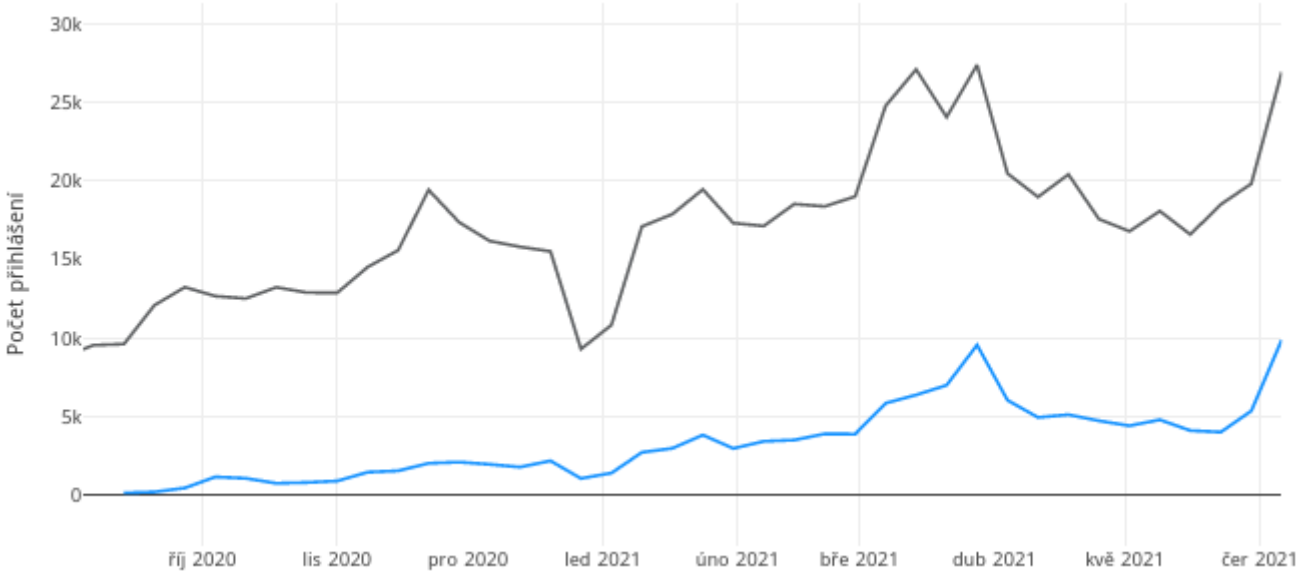
Týdenní počty přihlášení celkem a přes NIA

132 754

ušetřených cest na úřad

25 868

ušetřených cest na úřad za poslední měsíc



mojeID

Další statistiky

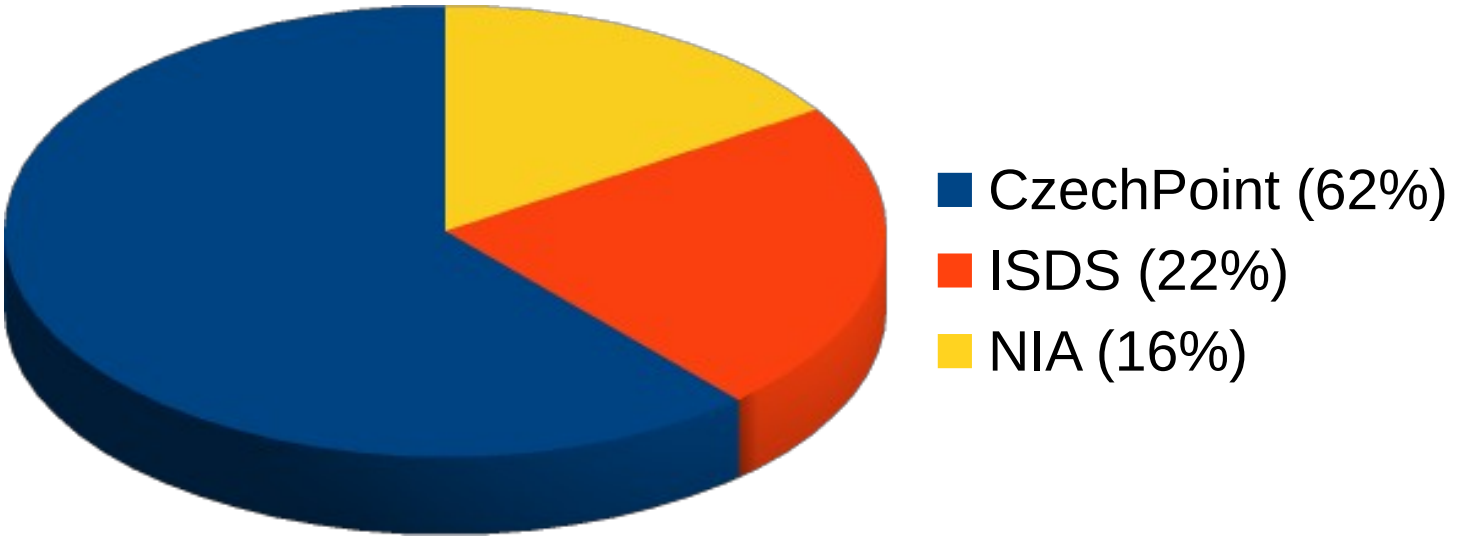
- Počet aktualizací z NIA – **962**
- Počet zrušených účtů z NIA – **12**
- Počet FIDO bezpečnostních klíčů celkem – **29 190**
- Počet účtů mající nastavený FIDO klíč – **25 660**
- Počet účtu aktivních od začátku roku – **100 313**

Ověřování totožnosti přes ISDS

- Při spuštění v září 2020 byly pouze dvě možnosti:
  - Nějaký existující prostředek v rámci kv. systému
  - Návštěva CzechPoint
- Následovala spousta dotazů, proč ne datové schránky
- Cesta existovala – založit NIA-ID z DS a pak použít NIA-ID
- Od prosince 2020 je možno použít DS napřímo
  - Technicky se jedná o stejný koncept jako CzechPoint
  - Z toho pramení omezení na DS fyzické osoby

mojeID

Ověřování totožnosti podle typu



Cesta k elektronické identitě pro cizince

- Služba mojeID nevyžaduje mít průkaz totožnosti ČR
  - Na rozdíl od ostatních komerčních elektronických identit
- Podmínkou je existence záznamu v Registru obyvatel
  - Ten mají např. i cizinci s trvalým pobytem
- Na CzechPointu je možné se prokázat potvrzením vydaným ČR
- Podle údajů ČSÚ se jedná o statisíce cizinců

mojeID

Systémové bezpečnostní klíče FIDO

- Plusy
  - Jednoznačně nejpohodlnější autentizační prostředek
  - Nejpoužívanější prostředky - Windows Hello a Android
  - Zdarma a nabízející anti-phishing vlastnosti technologie FIDO
- Mínusy
  - Chybějící potřebná FIDO certifikace u iOS a Chromebooku
  - Svázanost s konkrétním zařízením
  - Některé problematické verze OS

mojeID

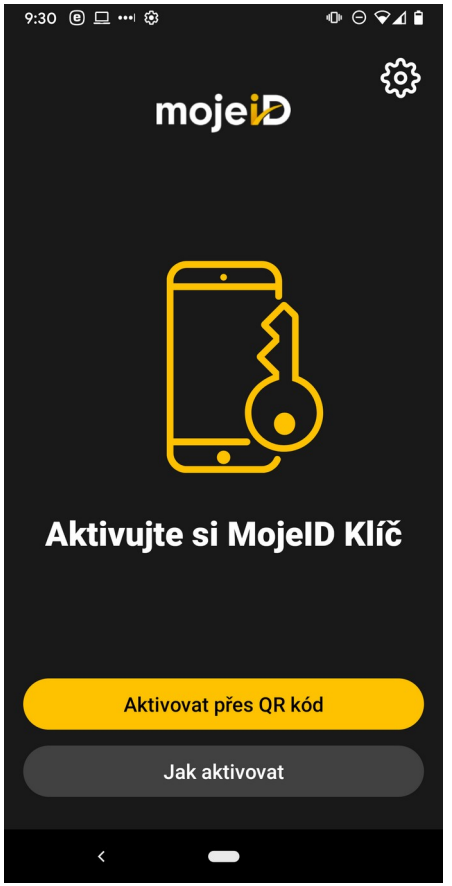
Mobilní autentizační aplikace

- MojeID Autentikátor spuštěn v březnu 2016 jako alternativa k opisování jednorázových kódů (OTP)
  - 3 měsíce před „Výzvou od Google“
- Přes 13 000 aktivních instancí
- Sdílený klíč se vyměňuje naskenováním QR kódu
- Podpis jednorázového kódu přes HMAC

mojeID

MojeID Klíč

- Mobilní aplikace pro Android a iOS vyvinutá společností Wultra
- PowerAuth protokol – open source jádro
- Plně dvoufaktorový prostředek (PIN, otisk prstu, FaceID)
- Zatím jako další faktor vedle hesla
- Jedna instance na účet
- Možno používat souběžně s bezpečnostními klíči
- MojeID Autentikátor již není možné přidat – je stále možné ho používat



Další úrovně záruky

- Doposud máme všechny prostředky na úrovni záruky „Značná“
  - mojeID je jako jedno tlačítko
- Koncept NIA aktuálně počítá s přístupem co úroveň záruky, to jedno tlačítko
- Tři tlačítka mojeID nám přijde moc

Úroveň záruky „Nízká“

- Základní účet s vyplněným heslem a ověřenou totožností přes jednu z možností CzechPoint, ISDS, NIA
- V zásadě má potenciál nahradit existující validaci účtu mojeID, která nikdy nebyla vázána na dvoufaktorový prostředek
- Aktuálně analyzujeme „užitečnost“ takového účtu
  - Zatím máme jen slabé signály, že by toho někdo využil (knihovny)
  - Uživatel může být spíš motivován přejít na vyšší úroveň

Úroveň záruky „Vysoká“ - podmínky

- Bezpečnostní klíč splňující FIDO L2 certifikaci
- Musí mít certifikovaný „Secure Element“
  - FIPS 140-2 Level 3 nebo Common criteria EAL4 + AVA_VAN5
- Ověření totožnosti pouze fyzicky na CzechPointu nebo minimálně stejně silným prostředkem přes NIA
- Musí být nastaven PIN a ten je vyžadován při přihlášení
- Není možné obejít PIN biometrikou

mojeID

Úroveň záruky „Vysoká“

- Jediný klíč aktuálně splňující podmínky je GoTrust IdemKey
  - Verze s USB-C v prodeji snad již koncem měsíce
- Možnost upgrade existujícího prostředku na úroveň záruky „Vysoká“ po přidání PIN a zaslání dopisu s kódem
- První existující služba => motivace pro nás na zrychlení

Ostatní prostředky

- V mojeID jsou další dva prostředky, které nelze použít v souvislosti s propojením na služby veřejné správy
  - Klientský TLS certifikát
  - OTP (Google Authenticator)
- U těchto prostředků nelze nijak vynutit ochranu klíče – základní předpoklad, že prostředek je ve vlastnictví dané osoby
- Přestože tyto prostředky jsou stále používané, s největší pravděpodobností dojde k jejich postupnému utlumení

mojeID

Přechod na „DevOps“

- Migrace provozního prostředí na Docker kontejnery
- Nasazování přímo z CI platformy Gitlab
- Zrychlení vývoje
- Rychlejší integrace nových verzí závislých komponent
- Potenciál pro „white label“ nasazení v zahraničí

mojeID

Co dál?

- Revize adres
  - korespondenční adresa vs. adresa trvalého pobytu
- Spuštění podpory pro další úrovně záruky
- Možnost více instancí MojeID Klíče?

Děkuji za pozornost

Jaromír Talíř • jaromir.talir@nic.cz • https://www.mojeid.cz