mojeID a NIA

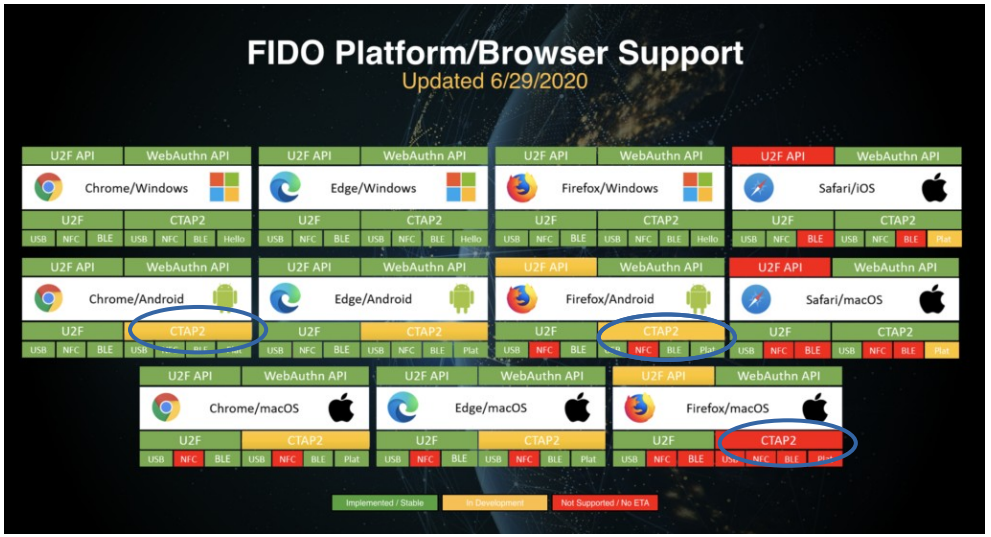
Záludnosti použitých technologií

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

Implementace FIDO

- Vysoká bezpečnost
  - Kryptografie s veřejným klíčem
  - Odolnost proti phishingu
- Dvě verze protokolu
  - **U2F** – U2F JS + CTAP1
  - **FIDO2** – WebAuthn + CTAP1/CTAP2
    - „Passwordless“ (PIN, Biometrika)
- Aplikace implementuje WebAuthn a nemá možnost volit CTAP

Proč ne „Paswordless“?

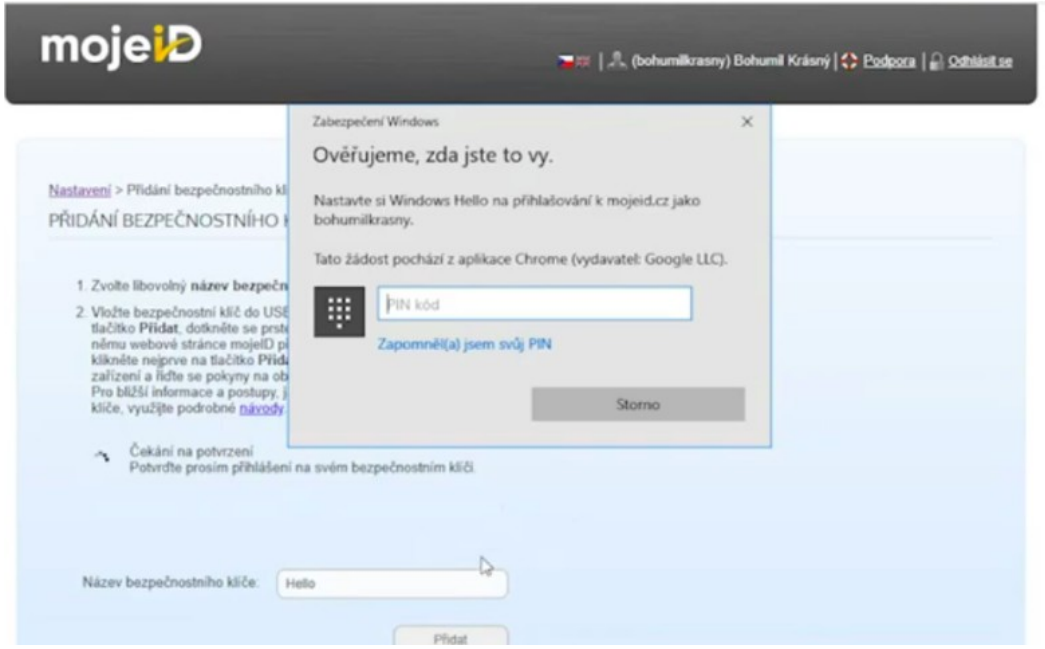


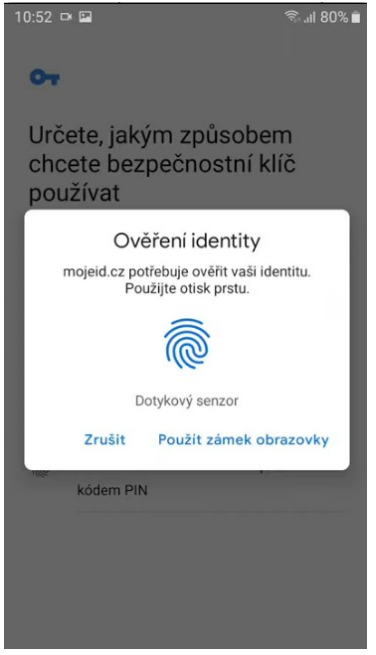
- Konzistentní s ostatními 2FA prostředky
- Jednodušší akreditace díky kontrole nad zadáváním hesel
- Chybějící podpora CTAP2 na některých široce používaných platformách
- Netriviální nastavování PINů

FIDO certifikace a Metadata Service

- Certifikace na L1 jako podmínka akreditace
- Oddělená certifikace pro U2F a FIDO2
  - Jiný typ certifikace zjištěný přes CTAP1 a CTAP2
- FIDO MDS2
  - Řetěz důvěry od kořenového certifikátu až do atestačního certifikátu
  - Publikace certifikace není povinná
  - Měsíční publikační cyklus
- Chybějící certifikace v MDS2 (bude řešit MDS3)

FIDO – systémové klíče (Win10, Android7, iOS14)

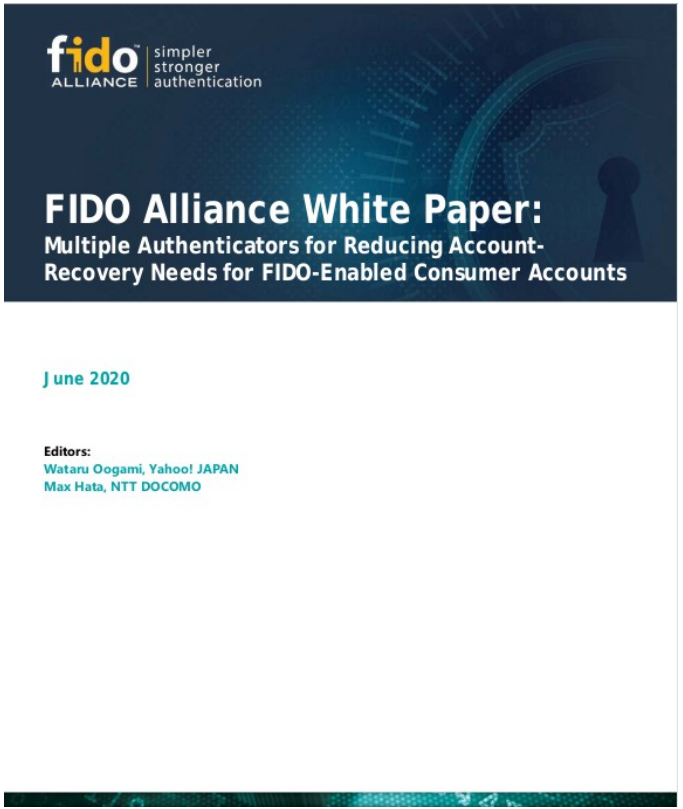




Video návod pro Windows Hello

Video návod pro Android

Přenesení systémového klíče



- Systémové klíče jsou vázané na zařízení!
- Google pracuje na propojení Android zařízení s počítačem přes USB a BLE.
- White Paper od FIDO Alliance
  - Doporučuje implementovat podporu pro více klíčů
  - Doporučuje externí klíč jako zálohu a pro přenos mezi zařízeními

GoTrustID IdemKey

USB/NFC bezpečnostní klíč
GoTrust Idem Key

548 Kč

Cena je včetně DPH 86,60 Kč a poštovného 49 Kč.
Doprava doporučeně prostřednictvím České pošty
s místem dodání v ČR.

Souhlasím se Všeobecnými obchodními podmínkami a prohlašuji, že jsem se seznámil se Zásadami zpracování osobních údajů.

PayPal

Debetní nebo kreditní karta

Využívá službu PayPal

- Součást kampaně
- Možnost přímo objednat
- Umožňuje PIV
  - Personal Identity Verification
  - Obdobně jako u YubiKey 5
  - PKCS11 rozhraní
  - Kerberos? DNSSEC?

Statistika připojených FIDO klíčů

Windows Hello	1345	YubiKey Series 5Ci	8
GoTrustID IdemKey	702	Feitian ePass	6
Android	696	Solo	4
Neznámý	191	TrustKey G310	2
YubiKey Series 5 with NFC	176	Hyper Fido	2
Yubico Security Key with NFC	56	YubiKey NEO	1
Yubico Security Key	50	Feitian BioPass	1
YK4 Series Key by Yubico	50	Feitian MultiPass	1
YubiKey Series 5	48		

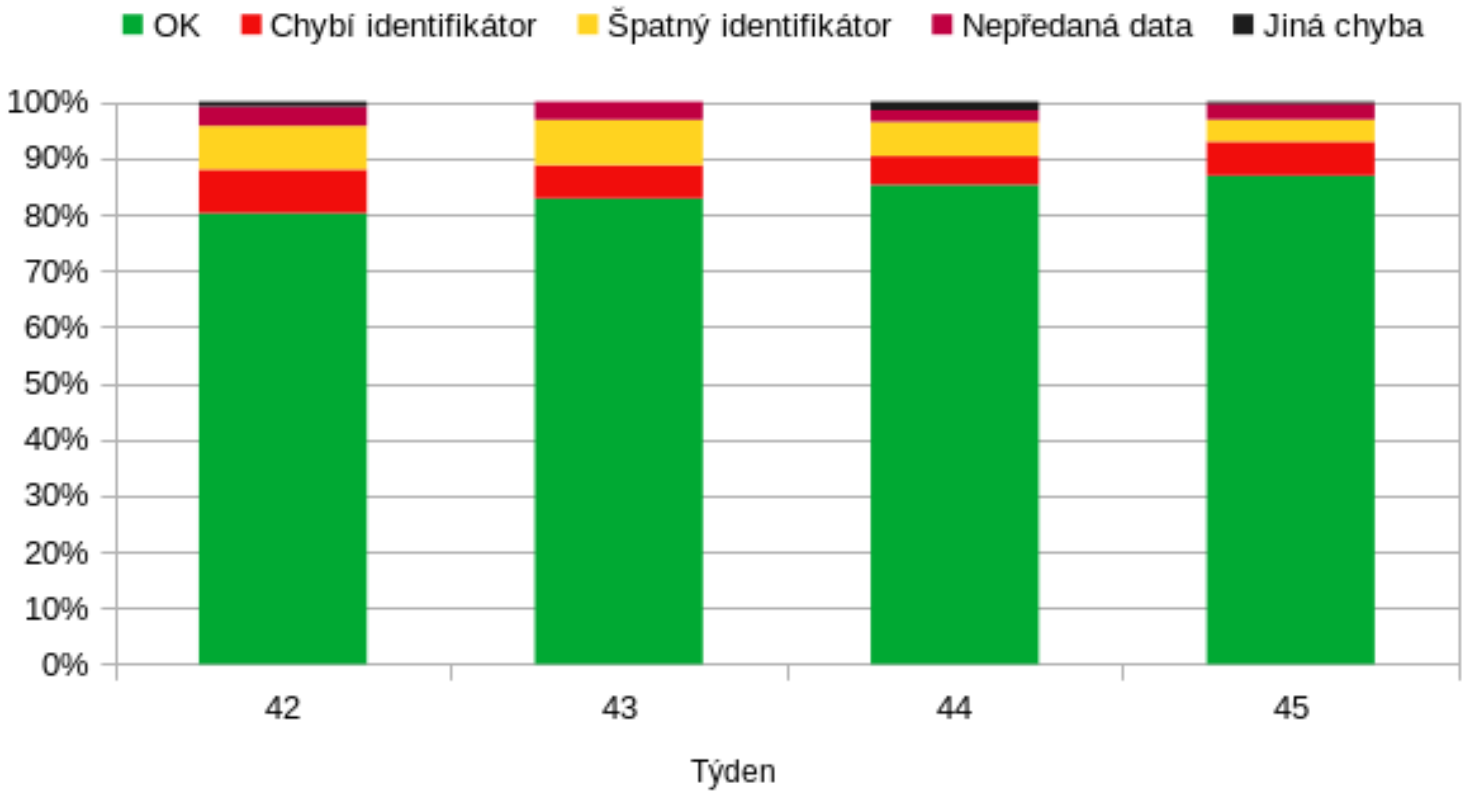
Software

- Postaveno na knihovně od Yubico - https://github.com/Yubico/python-fido2
  - Obsahuje zpracování atestace (kromě formátu Apple)
- Naše vlastní open source rozšíření - https://github.com/CZ-NIC/django-fido/
  - Přímá podpora frameworku Django
  - Hlavní vlastnost je zpracování FIDO MDS2 a detekce certifikace na základě atestace

Ověřování totožnosti na CzechPointech

- Poskytnutí údajů z ROB jiné osobě
  - Podle zákona č 111/2009 Sb. O základních registrech
  - Zdarma na 7000 CzechPointech
- Problém ISDS jako komunikačního kanálu
  - Sdílená datová schránka z běžnou agendou
  - Při stahování zpráv se označují jako doručené všechny
  - Systém nepodporuje více schránek
- Chyby lidského faktoru na pracovištích CzechPoint

Statistika chybovosti na CzechPointech



Možnosti zlepšení na straně státu

- Možnost zasílat do dedikované datové schránky
- Možnost připravit dopředu formulář pro uživatele
  - Uživatel by přišel s číslem žádosti a obsluha by našla v systému vyplněný formulář
- Možnost vyplnit formulář přes QR kód
  - Obsah formuláře by se z QR kódu přenesl do formuláře obsluhy

Zpracování adresy z NIA

- Problém získání údaje město při implementaci napojení na NIA v roli SeP – „Obec, část obce“
- Kompletní přechod na kód adresního místa přes RUIAN
- REST API - http://ags.cuzk.cz/arcgis/rest/services/RUIAN/Prohlizeci_sluzba_nad_daty_RUIAN/MapServer
- Komplikovaná pravidla pro skládání adresy na základě kódu adresního místa

Co dál?

- Ověření totožnosti přes ISDS
- Dokončení akreditace FIDO na úroveň záruky vysoká
- Notifikace mojeID do EU
- Akreditace dalších prostředků (nízká, značná)

Děkuji za pozornost

Jaromír Talíř • jaromir.talir@nic.cz

CZ.NIC | SPRÁVCE DOMÉNY CZ