

# mojeID update

Jaromír Talíř • [jaromir.talir@nic.cz](mailto:jaromir.talir@nic.cz) • 10. 11. 2021



# Obsah

- Implementace úrovně záruky Vysoká
- Proces oznámení (“notifikace”) mojeID do EU

# Akreditace na úroveň záruky Vysoká

- **Zažádáno** - 12. května 2020
  - První žádost o akreditace spolu s úrovní Značná
- **Přerušeno** – srpen 2020
  - Získání času na prodiskutování detailů
- **Obnoveno** – březen 2021
  - Vyjasněny podrobné podmínky
- **Uděleno** – 8. března 2021
  - Formální uzavření procesu

# Dluhopis republiky - <https://pssd.sporicidluhopisycr.cz/pssd-war/>

Ministerstvo financí  
Česká republika



## Přihlášení



Přihlášení prostřednictvím portálu eidentita.cz.

Přihlásit se



Přihlášení pomocí Osobního čísla a PIN zaslaných na mobilní telefon a poštou.

Přihlásit se

Pro registraci nového uživatele, který dosud nemá zřízen majetkový účet v samostatné evidenci státních dluhopisů vedené Ministerstvem financí, zvolte přihlášení eidentita.cz (portál národního bodu pro identifikaci a autentizaci), kde se následně přihlaste s využitím prostředku s úrovní záruky vysoká (např. eObčanka).

Pro přihlášení k elektronickému přístupu ke správě majetkového účtu je možné využít již přidělené Osobní číslo a PIN. Pokud tyto údaje nemáte k dispozici nebo Vám nebyly přiděleny, je možné rovněž využít přihlášení prostřednictvím eidentita.cz, a to prostředkem s úrovní záruky vysoká nebo značná (např. eObčanka, NIA ID, Mobilní klíč eGovernmentu).

Podrobnější informace o přihlášení a registraci naleznete na [www.dluhopisrepubliky.cz](http://www.dluhopisrepubliky.cz).

Více informací o elektronické identifikaci naleznete na internetových stránkách [info.eidentita.cz](http://info.eidentita.cz).







# L2 certifikovaný klíč - GoTrust IdemKey

- Stále jediný klíč splňující parametry
  - L2 certifikace
  - Secure Element s CC/FIPS certifikací
- Dostupný na CZC ve variantách USB-A/NFC i USB-C/NFC



# FIDO MDS3

- Změna způsobu zjišťování certifikací
- Online prohlížeč na <https://opotonniee.github.io/fido-mds-explorer/>

FIDO MDS Explorer <span>?</span>									
List of registered authenticators									
Click on authenticator name to view details									
#	Name	Protocol	Icon	Certification	User Verif.	Attachment	Key Protection	Updated	
22	<a href="#">GoTrust Idem Key FIDO2 Authenticator</a>	fido2		FIDO_CERTIFIED_L2 FIDO_CERTIFIED_L1	presence_internal passcode_internal	external	hardware secure_element	2021-03-05	
34	<a href="#">GoTrust Idem Card U2F Authenticator</a>	u2f		FIDO_CERTIFIED	presence_internal	external wireless nfc bluetooth	hardware secure_element remote_handle	2020-09-02	
55	<a href="#">GoTrust Idem Card FIDO2 Authenticator</a>	fido2		FIDO_CERTIFIED_L1	passcode_internal presence_internal	external	hardware secure_element	2019-12-04	
82	<a href="#">GoTrust Idem Key U2F Authenticator</a>	u2f		FIDO_CERTIFIED FIDO_CERTIFIED_L1 FIDO_CERTIFIED_L2	presence_internal	external wired wireless nfc	hardware secure_element remote_handle	2021-03-09	

Next MDS update is planned on 2021-12-01 - Retrieval and use of this BLOB indicates acceptance of the appropriate agreement located at <https://fidoalliance.org/metadata/metadata-legal-terms/>

# Vynucení PIN – podpora CTAP2 v prohlížeči

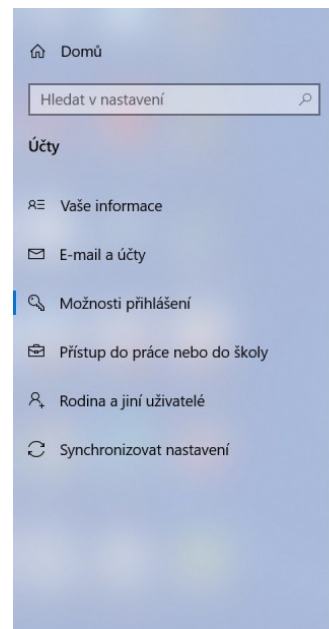
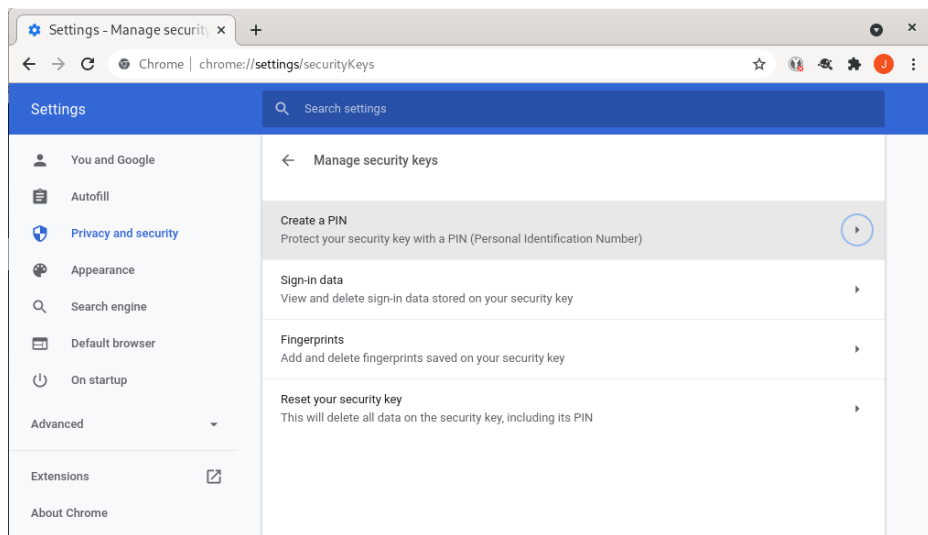
- Nebude možné použít Firefox na Linuxu a MacOS

**FIDO Platform/Browser Support**  
Updated 6/29/2020

U2F API		WebAuthn API		U2F API		WebAuthn API		U2F API		WebAuthn API		U2F API		WebAuthn API			
Chrome/Windows		Edge/Windows		Firefox/Windows		Safari/iOS											
U2F		CTAP2		U2F		CTAP2		U2F		CTAP2		U2F		CTAP2			
USB	NFC	BLE	USB	NFC	BLE	Hello	USB	NFC	BLE	USB	NFC	BLE	USB	NFC	BLE	Plat	
U2F API		WebAuthn API		U2F API		WebAuthn API		U2F API		WebAuthn API		U2F API		WebAuthn API			
Chrome/Android		Edge/Android		Firefox/Android		Safari/macOS											
U2F		CTAP2		U2F		CTAP2		U2F		CTAP2		U2F		CTAP2			
USB	NFC	BLE	USB	NFC	BLE	Plat	USB	NFC	BLE	USB	NFC	BLE	Plat	USB	NFC	BLE	Plat
U2F API		WebAuthn API		U2F API		WebAuthn API		U2F API		WebAuthn API		U2F API		WebAuthn API			
Chrome/macOS		Edge/macOS		Firefox/macOS													
U2F		CTAP2		U2F		CTAP2		U2F		CTAP2		U2F		CTAP2			
USB	NFC	BLE	USB	NFC	BLE	Plat	USB	NFC	BLE	USB	NFC	BLE	Plat	USB	NFC	BLE	Plat

Legend:  
Implemented / Stable (Green)  
In Development (Yellow)  
Not Supported / No ETA (Red)


# Nastavení PIN – Chrome nebo Windows Hello



## Možnosti přihlášení


### Spravovat způsob přihlášení k zařízení

Pokud chcete přidat, změnit nebo odebrat možnost přihlášení, vyberte ji.

 **Obličej ve Windows Hello**  
Tato možnost je nyní nedostupná – kliknutím získáte další informace.

 **Otisk prstu ve Windows Hello**  
Přihlásit se pomocí snímače otisku prstu (doporučeno)

 **PIN kód pro Windows Hello**  
Přihlásit se pomocí PIN kódu (doporučeno)

 **Klíč zabezpečení**  
Přihlásit se pomocí fyzického klíče zabezpečení  
Umožňuje spravovat fyzický klíč zabezpečení, který vás může přihlašovat k aplikacím.

[Další informace](#)

**Spravovat**

 **Heslo**  
Přihlásit se pomocí hesla účtu



# Základní scénář – nejprve připojit a pak aktivovat

Profil **Nastavení** Historie Osobní vizitka

[Nastavení](#) > Přístup ke službám veřejné správy

## VÝBĚR ÚROVNĚ ZÁRUKY

Úroveň záruky udává, jak moc může poskytovatel služby důvěřovat způsobu prokázání totožnosti.

<h3>ZNAČNÁ</h3> <p>Účet ověřený na značnou úroveň záruky umožňuje přístup k naprosté většině elektronických služeb veřejné správy včetně Portálu občana, datových schránek, katastru nemovitostí, ePortálu ČSSZ a dalších.</p> <p>Potřebujete fyzický či systémový klíč s FIDO certifikací minimálně na úrovni L1 nebo mobilní aplikaci MojeID Klíč.</p>	<h3>VYSOKÁ</h3> <p>Účet ověřený na vysokou úroveň záruky umožňuje přístup ke všem elektronickým službám veřejné správy, včetně těch vyžadujících nejsilnější zabezpečení (např. založení a administrace majetkového účtu pro správu státních dluhopisů).</p> <p>Vysokou úroveň záruky je možné získat pouze při použití počítače s prohlížečem <b>Chrome</b> a vybraných <b>fyzických bezpečnostních klíčů s FIDO certifikací minimálně na úrovni L2</b> (např. GoTrust Idem Key). V prohlížeči Chrome je pak nutné provádět i přihlašování ke službám vyžadujícím úroveň záruky „vysoká“.</p> <p>Váš prohlížeč: <b>Chrome</b> Verze: 95.0.4638</p>
--	---

[Pokračovat](#) [Pokračovat](#)

# Uživatelé s IdemKey neověření na CzechPointu

- V nastavení zvolí tlačítko odpovídající přidání dalšího přístupu
- Na rozcestníku zvolí úroveň záruky Vysoká
- Podle pokynů si nastaví PIN
- Nastavení PINu se ověří přihlášením s vynuceným zadáním PINu
- Ověří se totožnost buď přes CzechPoint nebo jinými prostředky na úrovni záruky Vysoká (eObčanka nebo karta I.CA)
- Úroveň záruky Značná uživateli zůstává

# Uživatelé s IdemKey ověření na CzechPointu

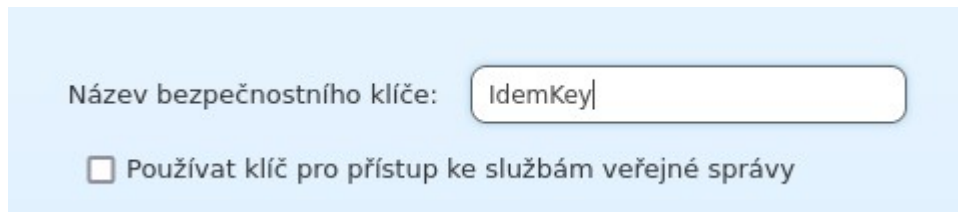
- U uživatelů, kteří mají IdemKey a byli na CzechPointu není možné jednoduše dovolit přidat PIN – bezpečnostní riziko
  - Přesto nechceme nutit tyto uživatel znovu jít na CzechPoint
- Dohodli jsme s MV, že tento scénář bude možný s dodatečným ověřením po zaslání jednorázového ověřovacího kódu na adresu trvalého bydliště.
  - Po spuštění podpory pro úroveň záruky Vysoká jednorázově rozešleme tyto dopisy – uživatel si nastaví PIN a na dedikované stránce potvrdí jednorázový kód.

# Uživatelé bez připojeného IdemKey

- Standardní připojení klíče k účtu a pokračování jako v případě „neověření na CzechPointu“
- Uživatel dostane obě úrovně záruky najednou

# Stánek s CheckPointem na konferenci

- Možnost připravit se dopředu a pak jen počkat na dopis
- Pokud máte již jiný prostředek aktivovaný nezapomeňte při připojování IdemKey do profilu odškrtnout volby která automaticky registruje klíč s ověřením jiného klíče



Název bezpečnostního klíče:

Používat klíč pro přístup ke službám veřejné správy

- V „Nastavení -> Přístup ke službám veřejné správy“ zvolte Získat přístup pro klíč a následně ověření na CzechPointu

# Problém napojení na NIA

- MojeID jako dvě položky v nabídce (dva IdP)
  - „Přihlášení na úroveň Značná“
  - „Přihlášení na úroveň Vysoká“
- Různé možnosti rozlišení IdP (~~podle LoA, podle IssuerID, podle cílového URL~~)
- Nutnost podepisovat odpovědi různými certifikáty
- Nutnost implementovat různé identifikátory uživatele pro oba IdP

# Stav implementace a plán nasazení

- Hlavní část hotová v průběhu září
- „Zásek“ na implementaci připojení na NIA
- Předpokládáme nasazení do produkce do konce listopadu

# Další využití úrovně záruky Vysoká

- Ověření na úrovni AML podle zákona o AML (§ 8a)
  - <https://www.zakonyprolidi.cz/cs/2008-253#p8a>
- Legalizace podpisu podle Zákona o právu na digitální služby (§ 6 1b) (od července 2022)
  - <https://www.zakonyprolidi.cz/cs/2020-12?#p6>
- Zahraniční služby přes eIDAS po notifikaci
  - Bohužel zatím neexistuje seznam služeb ostatních států



# Uznávání mojeID v EU podle nařízení eIDAS

- Žádost podává členský stát
- Minimálně 6 měsíců před vlastní notifikací je třeba předat ostatním členským státům popis jak systém vyhovuje požadavkům eIDAS
- Následuje „peer review“ proces v rámci eIDAS Cooperation Network zakončený vydáním závěrečného vyjádření („opinion“).
- Poté může členský stát oficiálně notifikovat systém

# Notifikované země

- Aktuální seznam (14) - DE, PT, IT, EE, ES, HR, LU, BE, CZ, NL, LV, SK, DK, LT
- Právě dokončené „peer review“ – SE, FR, MT
- Nastartované „peer review“ – NO, AT
- Přehled:

Czech Republic (Mobile eGovernment Key, mojeID)	Czech Republic	National identification scheme of the Czech Republic	Mobile eGovernment Key (MEG), mojeID	Low, Substantial, High	PRE-NOTIFIED	📅 27 Sep 2021
Norway	Norway	eID-gateway "ID-porten"	Buypass ID, BankID		PRE-NOTIFIED	📅 27 Sep 2021
Austria	Austria	ID Austria		High	PRE-NOTIFIED	📅 27 Sep 2021

# Peer review proces

- Zástupci členů eIDAS Cooperation Network nominují zástupce do tří skupin podle oblastí (*Enrolment, Electronic identification means management and authentication and interoperability, Management and organisation*)
- Probíhají tři kola dotazování (2 týdny pro posuzovatele na formulování otázek, 2 týdny pro posuzované na odpověď)
- V našem případě jsme obdrželi v prvním kole 84 otázek.
- Předpokládaný konec procesu je v únoru 2022

# Děkuji za pozornost

Jaromír Talíř • [jaromir.talir@nic.cz](mailto:jaromir.talir@nic.cz) • <https://www.mojeid.cz>

