mojeID update

Jaromír Talíř • jaromir.talir@nic.cz • 10. 11. 2021

Obsah

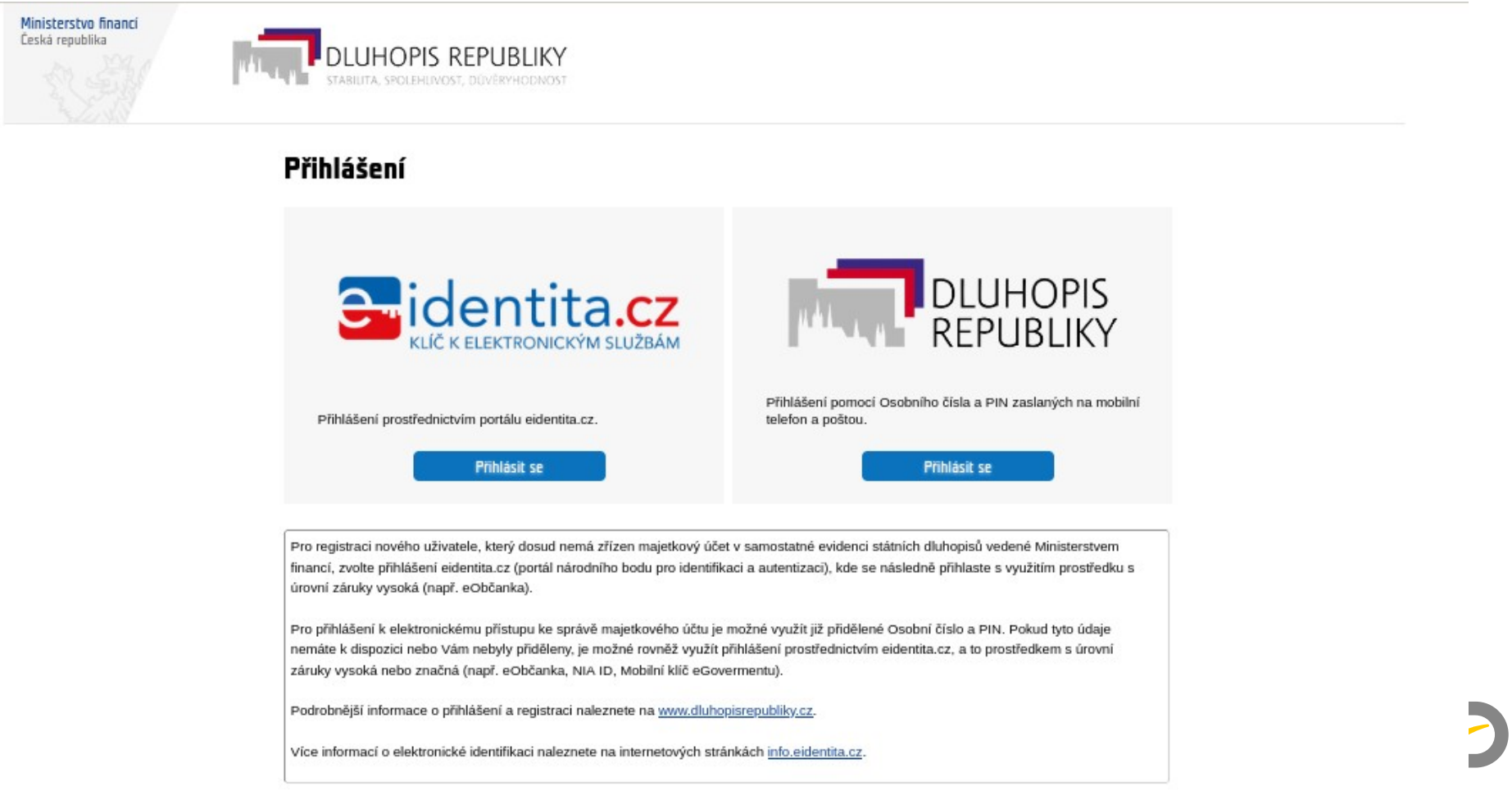
- Implementace úrovně záruky Vysoká
- Proces oznámení (“notifikace”) mojeID do EU

Akreditace na úroven 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

mojeID

Dluhopis republiky - https://pssd.sporicidluhopisycr.cz/pssd-war/

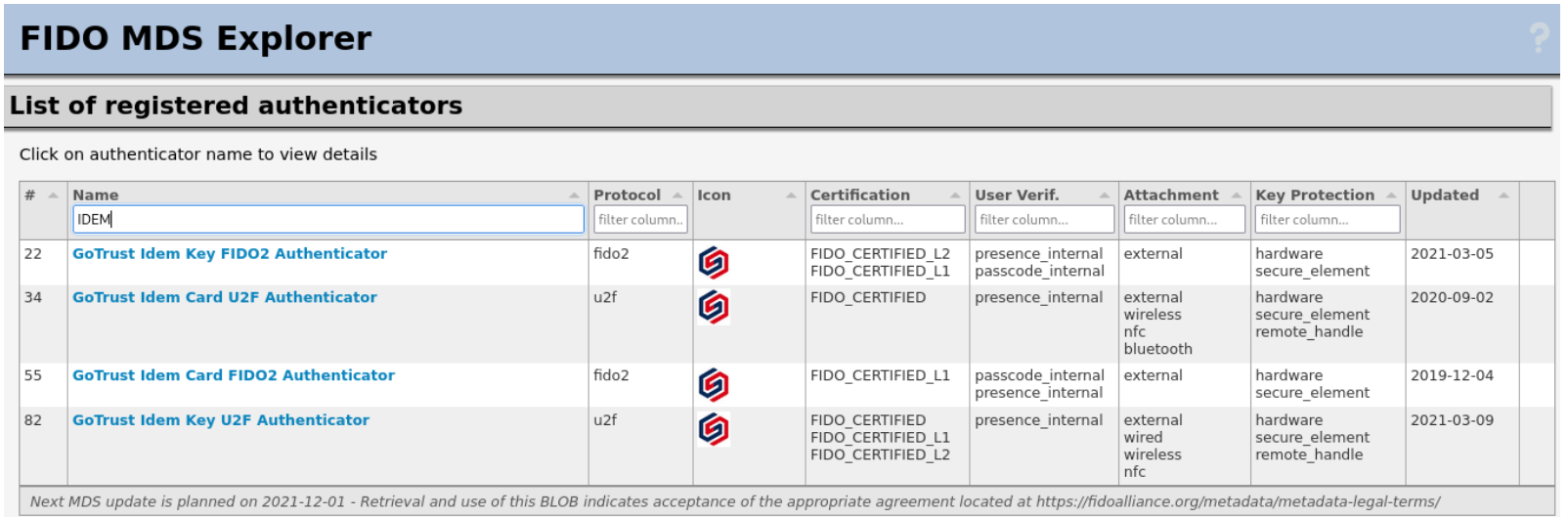


L2 certifikovaný klíč - GoTrust IdemKey

- Stále jediný klíč splňující parametry
  - L2 ceritifikace
  - 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

List of registered authenticators

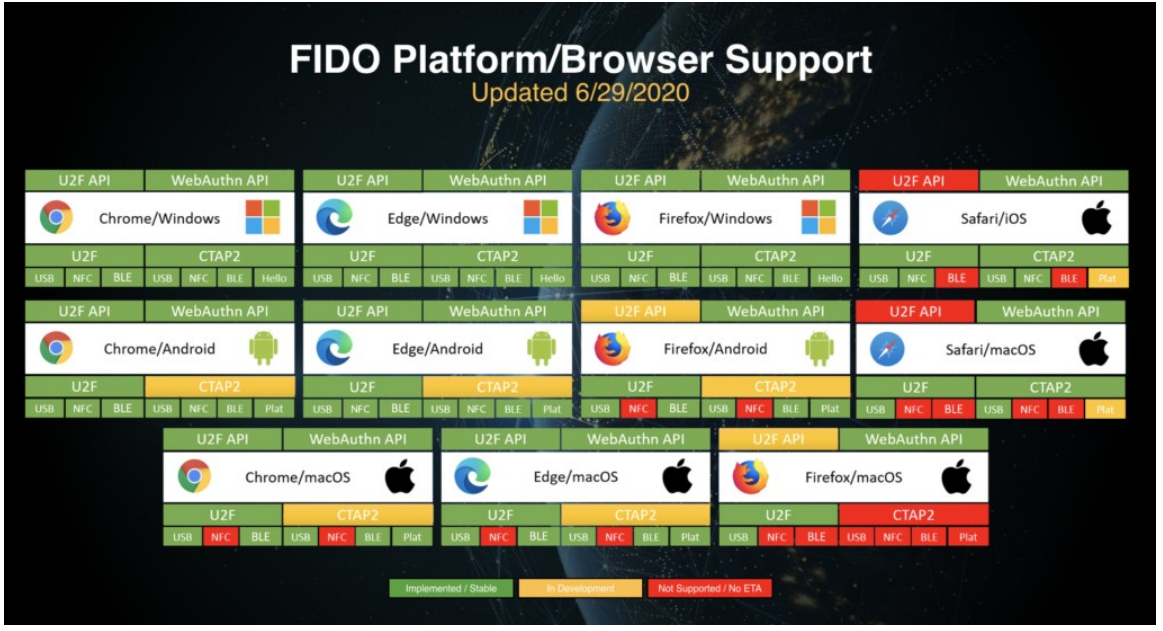
Click on authenticator name to view details

#	Name	Protocol	Icon	Certification	User Verif.	Attachment	Key Protection	Updated
	IDEM	filter column..		filter column...	filter column...	filter column...	filter column...	
22	**GoTrust Idem Key FIDO2 Authenticator**	fido2		FIDO_CERTIFIED_L2 FIDO_CERTIFIED_L1	presence_internal passcode_internal	external	hardware secure_element	2021-03-05
34	**GoTrust Idem Card U2F Authenticator**	u2f		FIDO_CERTIFIED	presence_internal	external wireless nfc bluetooth	hardware secure_element remote_handle	2020-09-02
55	**GoTrust Idem Card FIDO2 Authenticator**	fido2		FIDO_CERTIFIED_L1	passcode_internal presence_internal	external	hardware secure_element	2019-12-04
82	**GoTrust Idem Key U2F Authenticator**	u2f		FIDO_CERTIFIED FIDO_CERTIFIED_L1 FIDO_CERTIFIED_L2	presence_internal	external wired wireless nfc	hardware secure_element remote_handle	2021-03-09

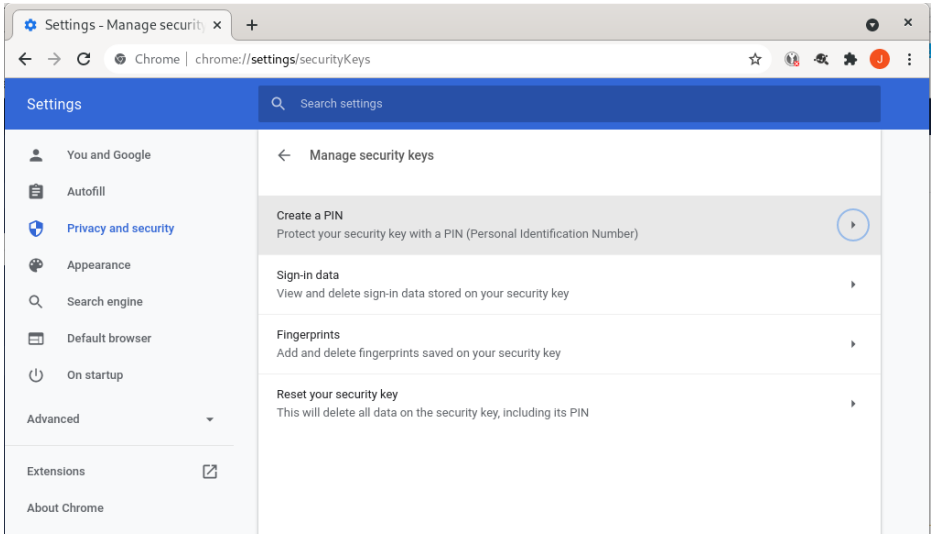
Next MDS update is planned on 2021-12-01 - Retrieval and use of this BLOB indicates acceptance of the appropriate agreement located at https://fidoalliance.org/metadata/metadata-legal-terms/

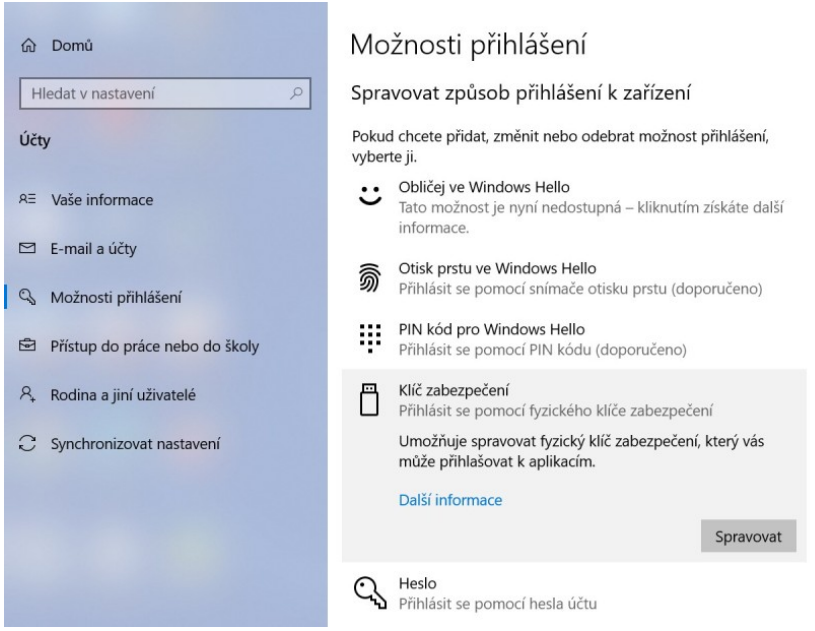
Vynucení PIN – podpora CTAP2 v prohlížeči

- Nebude možné použít Firefox na Linuxu a MacOS



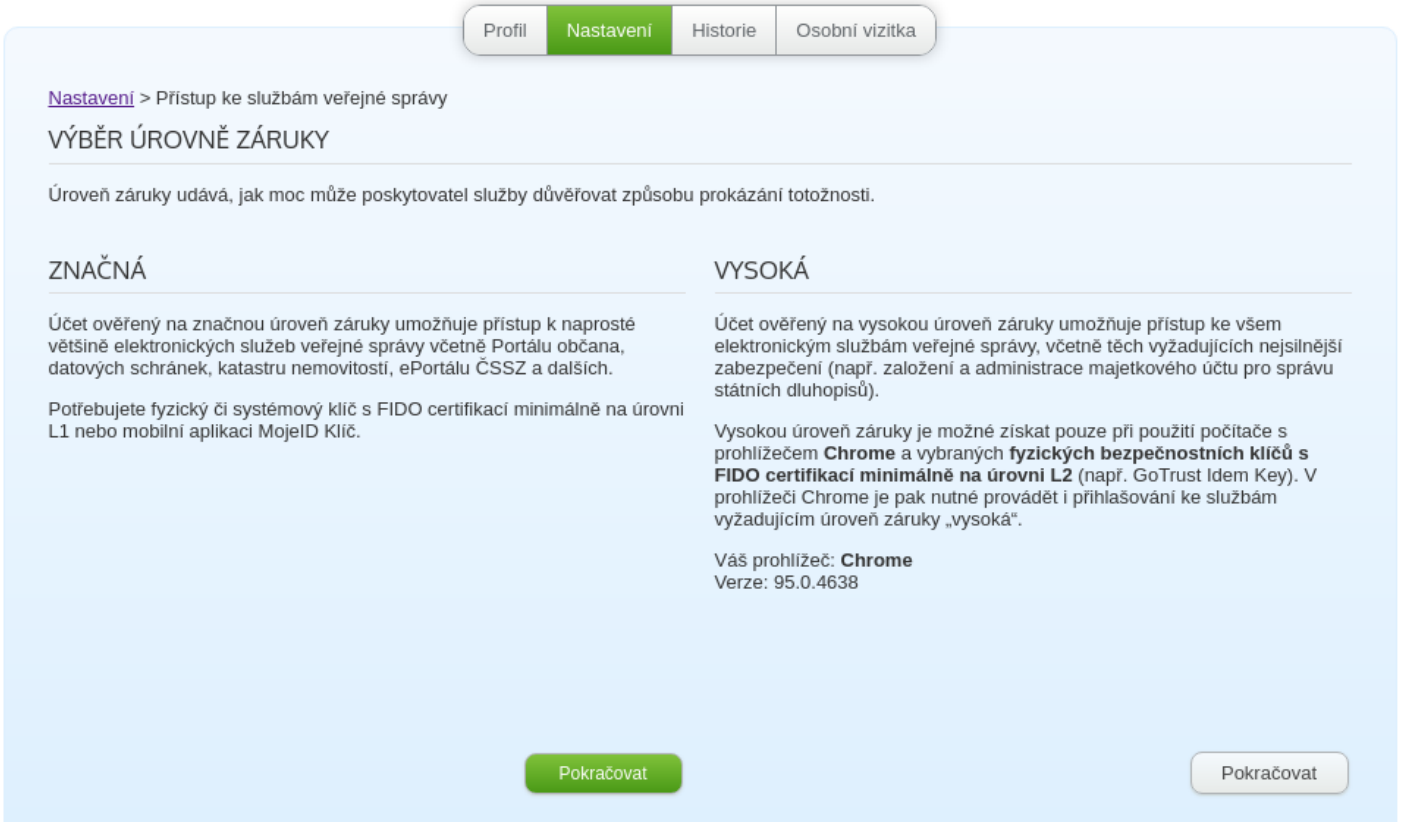
Nastavení PIN – Chrome nebo Windows Hello





mojeID

Základní scénář – nejprve připojit a pak aktivovat



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

mojeID

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.

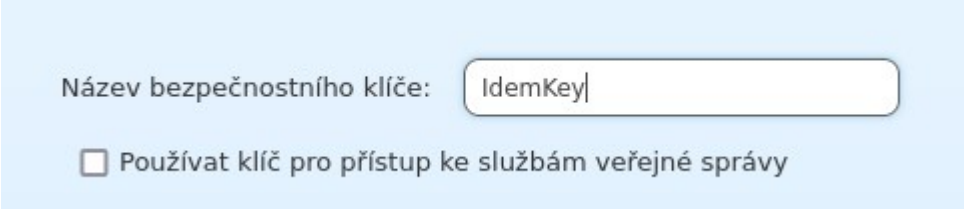
mojeID

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



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

mojeID

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

mojeID

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

mojeID

Děkuji za pozornost

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