

Peněženka Evropské digitální identity *v akci*

Jaromír Talíř • 04.10.2025

cz.nic | SPRÁVCE
DOMÉNY CZ

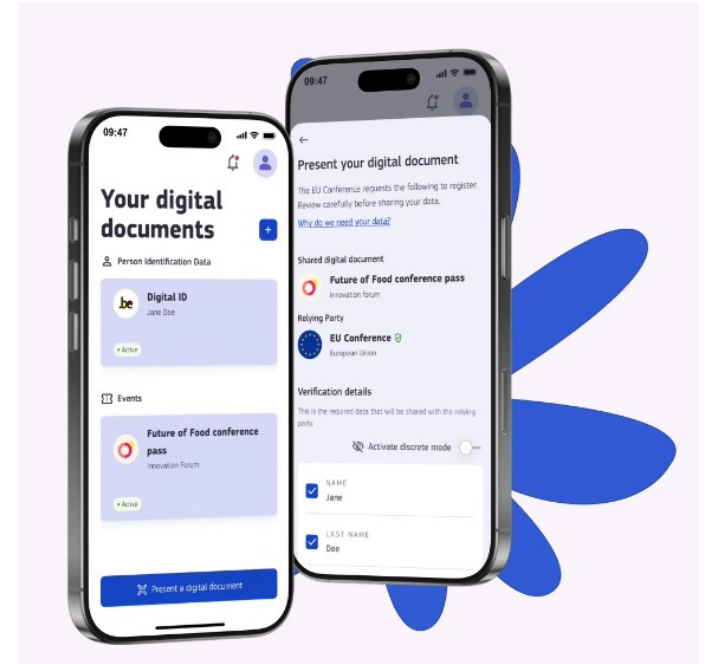
Obsah

- Aktuální stav legislativně technického vývoje
- Některé výzvy a jejich řešení
- Jak jsou na tom členské státy a ČR
- Dostupné peněženky
- Zapojení CZ.NIC do konsorcia EWC v rámci Large Scale Pilots
- Demo

Legislativa a standardy

Digitální peněženka

- Nový způsob digitální identity v Evropě
- Decentralizovaný přístup místo centralizovaného – pod kontrolou uživatele
- Možnost ukládat a selektivně prezentovat atributy identity
- Možnost digitálního podpisování dokumentů
- Návrh zveřejněn v roce 2021
- Finální verze vyšla v platnost 20. 5. 2024
- Více detailů na stránkách Evropské komise



Prováděcí nařízení

- Vznikají postupně v dávkách. První dávka vstoupila v platnost 24.12.2024
 - Povinnost pro členské státy zprovoznit peněženku do **24.12.2026**
 - Aktuálně přijato – 20
 - Ukončené veřejné připomínkové řízení – 5
 - V připomínkovém řízení do 2. 10. – 5
 - Mnoho jich je ještě v přípravě
- I ve schválených nařízeních jsou chybějící klíčové informace (protokoly, formáty)
 - Komise plánuje některá již schválení nařízení v blízkém období otevřít a upravit

Standardy

- Formáty:
 - ~~AnonCreds~~, ~~W3C VC~~, ISO MSO MDOC, IETF SD-JWT VC
 - SD-JWT-based Verifiable Credentials (SD-JWT VC) – Draft 11 - 15 září 2025
- Protokoly
 - ~~ISO 23220-3~~, ~~DIDComm~~, OpenID4VC
 - OpenID for Verifiable Presentations 1.0 – 9. července 2025
 - OpenID for Verifiable Credential Issuance 1.0 – 16. září 2025
- Zajištění důvěry
 - ~~HyperLedger Indy~~, ~~EBSI~~, ~~TRAIN~~, EU Trusted Lists

Architecture and Reference Framework

- Jednotící dokument pro technické řešení ekosystému
 - Přibližně 400 stránkové PDF
- Vývoj probíhá na Githubu
 - již 21 vydání, aktuálně verze 2.5.0 z 15. září
- Desítky diskuzních oblastí, kde je možné jednotlivé vlastnosti veřejně komentovat
- Finálně jednotlivé verze schvaluje komise zástupců členských států



Některé výzvy

Nepropojitelnost

- V nařízení je striktní požadavek na „Unlinkability“
 - Při používání peněženky by žádná organizace neměla mít možnost spojit si informace o aktivitě uživatele
- Verifier-verifier unlinkability
 - I když se dvě služby ve kterých uživatel použil peněženku domluví a vymění si data, nikdy by neměly mít možnost zjistit že jde o stejného uživatele
- Issuer-verifier unlinkability
 - I pokud se vydavatel atributu domluví se službou, a vymění si data o použití peněženky, neměla by existovat možnost zjistit, že jde o stejného uživatele
- Bohužel se naráží na technická omezení
 - Aktuálně se pracuje s řešením jednorázových potvrzení, které se nebudou používat opakovaně
 - V budoucnu by se mělo vyřešit pomocí mechanismů postavených na Zero Knowledge Proofs

Pseudonymy a autentizace

- Mechanismus autentizace musí zajistit, aby peněženka předala službě při každém přístupu stejný identifikátor
- Proběhl velký boj o to zda-li bude v datové sadě persistentní unikátní identifikátor
 - V základu nic takového není – preferováno zastánci soukromí
 - V rozšířené sadě je **personal_administrative_number** – záleží na členském státu
- Nařízení požaduje umožnit v peněžence definovat pseudonym pro každou službu a toto předávat
 - Možnosti řešení: FIDO/WebAuthn, SIOPv2, externí služba vydávající pseudonym

QR kód a DC API

- Existují v zásadě dva scénáře použití peněženky
- Same-device
 - Webová aplikace běží na telefonu na kterém je peněženka
 - Pro přechod do peněženky se používají „custom scheme“, např. openid4vp://
- Cross-device
 - Webová aplikace běží v počítači a peněženka na telefonu
 - Pro přechod do peněženky se používají ne příliš bezpečné QR kódy
- Řešením by mohlo být Digital Credential API
 - Představil Google a nyní se standardizuje v rámci W3C
 - Jedná se o API v prohlížeči (podobně jako WebAuthn), které by mělo zajistit vyšší bezpečnost
 - Zatím je jen v Chrome a vzbuzuje otázky ohledně další závislosti na prohlížeči

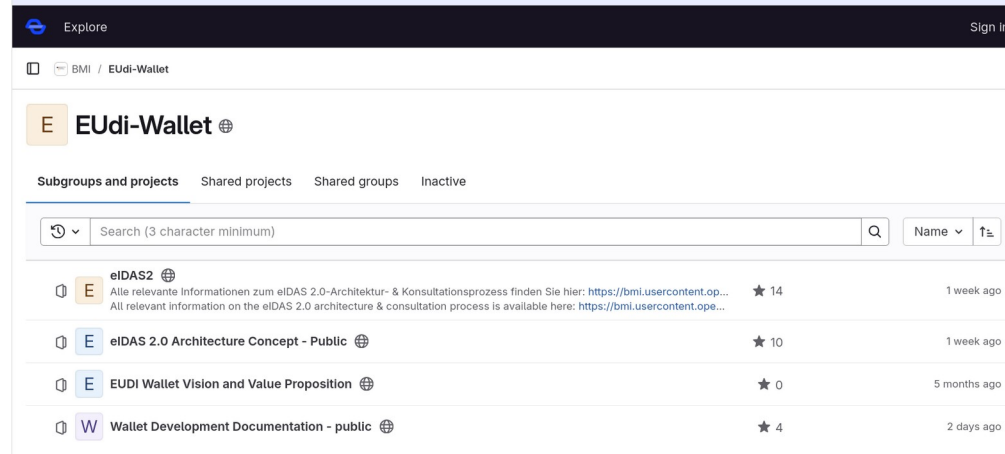
Úroveň záruky Vysoká

- Nejvyšší úroveň záruky vyžaduje certifikované HW úložiště na privátní klíče
 - Přímě na mobilním telefonu je to možné jen u několika high-end výrobků
- Několik zemí již oznámilo že vyvíjí hybridní systém s centrálním HSM
 - Klíč v HSM chráněný PINem
 - Každá transakce vyžaduje zadání PIN a vygenerování podpisu v HSM
 - Není možné použití offline
- Inicializace peněženky z existujících digitálních identit
 - Pokud máte notifikovaný prostředek na úrovni záruky vysoká (např. MojeID) stačí ho použít
 - V opačném případě bude nutné dodatečné ověření
 - Možná bude nutná osobní kontrola dokladů (vzdáleně nebo fyzicky)

Jak jsou na tom členské státy

Situace v okolních zemích

- Z řady zemí zaznívají obavy, že se to nedá stihnout
- Některé země má již aplikace tohoto typu z dřívějšíka a provedou jejich upgrade - Polsko
- Některé země se aktivně účastnili pilotů – Finsko, Německo
 - <https://gitlab.opencode.de/bmi/eudi-wallet/>



Situace v ČR

- Vznik pracovní skupiny při RVIS – 10/2023
- Tržní konzultace - 01/2025
- Rozhodnutí vlády o tom, že EUDIW má na starosti DIA a že klientská část se bude řešit formou koncese - 03/2025
- Výběrové řízení na koncesionáře formou soutěžního dialogu
 - Zahájeno v březnu 2025
 - Podle harmonogramu měl být cca 4 měsíční soutěžní dialog zahájen v květnu s následným podáním nabídek a smlouva s výhercem podepsána v prosinci.
 - Před pár dny byl teprve dokončen výběr účastníků soutěžního dialogu
- Paralelně běží příprava legislativy a státní části systému
- DIA veřejně deklarovala, že umožní existenci alternativních poskytovatelů

Použitelné peněženky

Referenční (NiScy) peněženka

- Konsorcium Netcompany Intrasoft a Scytales
- Financováno Evropskou komisí
- Open source
- Aktuálně není kompatibilní – nová verze v řádu dní
- <https://github.com/eu-digital-identity-wallet/eudi-app-android-wallet-ui/releases>
- <https://github.com/eu-digital-identity-wallet/eudi-app-ios-wallet-ui>



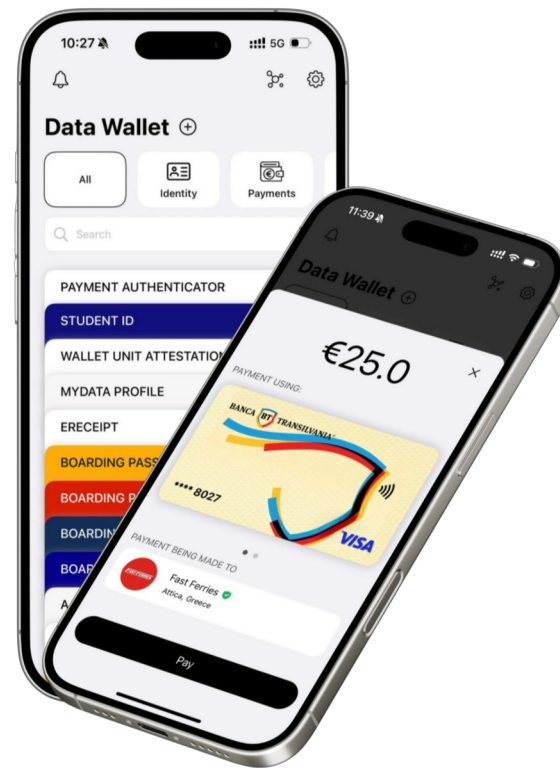
Lissi Wallet

- Lissi - <https://www.lissi.id/>
- Soukromá společnost z Německa
- Closed source
- Plně kompatibilní
- <https://play.google.com/store/apps/details?id=io.lissi.mobile.android.beta>



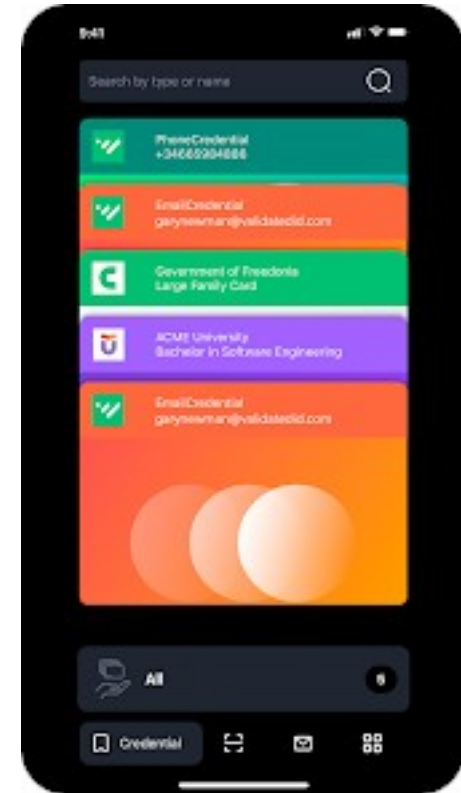
iGrant DataWallet

- iGrant.io - <https://www.igrant.io/>
- Soukromá společnost ze Švédska
- Closed source
- Plně kompatibilní
- <https://play.google.com/store/apps/details?id=io.igrant.mobileagent>



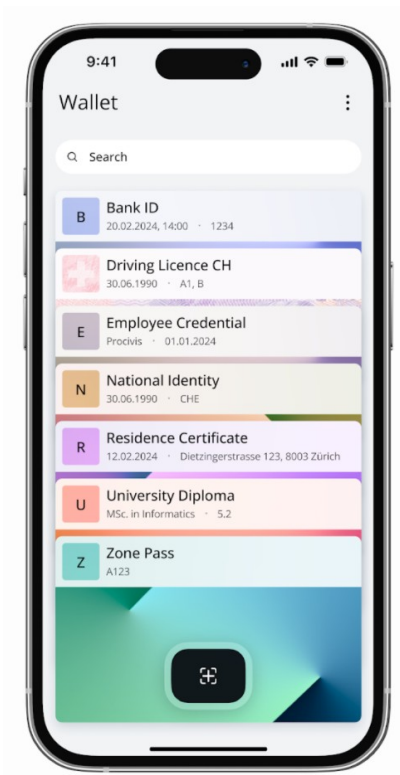
VID Wallet

- ValidatedID - <https://www.validatedid.com/>
- Soukromá společnost ze Španělska
- Closed source
- Aktuálně nekompatibilní – oprava v řádu týdnů
- <https://play.google.com/store/apps/details?id=com.vididentity.wallet.lsp>



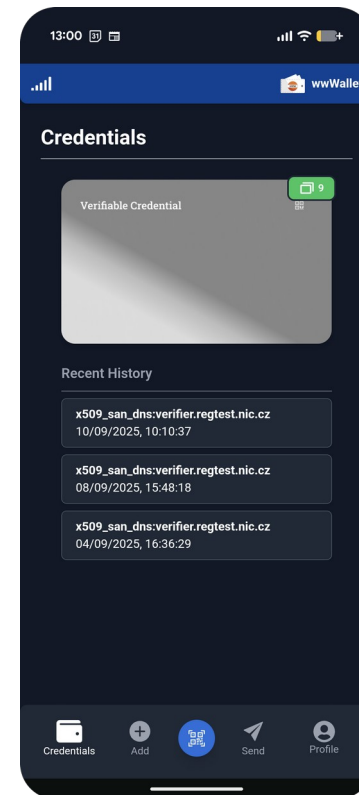
Procivis One Wallet

- Procivis - <https://www.procivis.ch/>
- Soukromá společnost ze Švýcarska
- Open source - <https://github.com/procivis/one-wallet/>
- Aktuálně nekompatibilní – oprava snad již příští týden
- <https://play.google.com/store/apps/details?id=ch.procivis.one.wallet.trial>



WWallet

- Yubico, SUNet, GRNet
- Švédsko a Řesko
- Open source - <https://github.com/wwWallet>
- Aktuálně nekompatibilní – oprava zatím neoznámena
- <https://demo.wwwallet.org>



Large Scale Pilots



Large Scale Pilots - konzorcium EWC

- Odstartovalo v dubnu 2023 a skončilo v červenci 2025
- Od pilotů k reálným transakcím
 - Reálný nákup vstupenky na řecký trajekt zaplacený s pomocí autorizace platby rumunské banky
 - Reálný hotelový check-in
- Scénáře se zapojením CZ.NIC
 - Vystavení PID s pomocí MojID
 - Ověření vlastnictví domény s využitím peněženky
 - Uložení pověření od vlastnictví domény a demonstrace jeho využití

Demo

Závěr

- Kdo chce, nemusí čekat. Již nyní je možné začít zkoušet různé scénáře
- První reálné peněženky se mohou začít objevovat v půlce příštího roku
- Priority pro DIA by měly být implementace státní části systému:
 - Systém pro registraci spoléhajících stran, aby až se objeví první země s peněženkou bylo možné ji hned začít používat
 - Systém pro vydávání PID a certifikační schéma aby vydavatelé peněženek mohli dobrovolně vstoupit na náš trh, klidně ještě dříve než bude hotová „oficiální“ peněženka

Děkuji vám za pozornost!

jaromir.talir@nic.cz