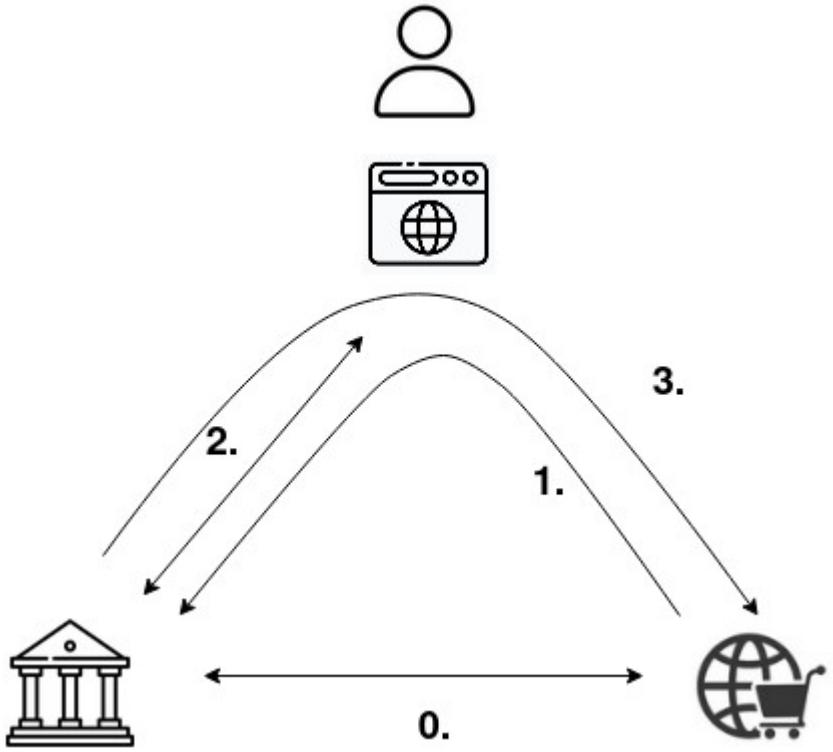
Peněženka Evropské digitální identity

7.10. 2023

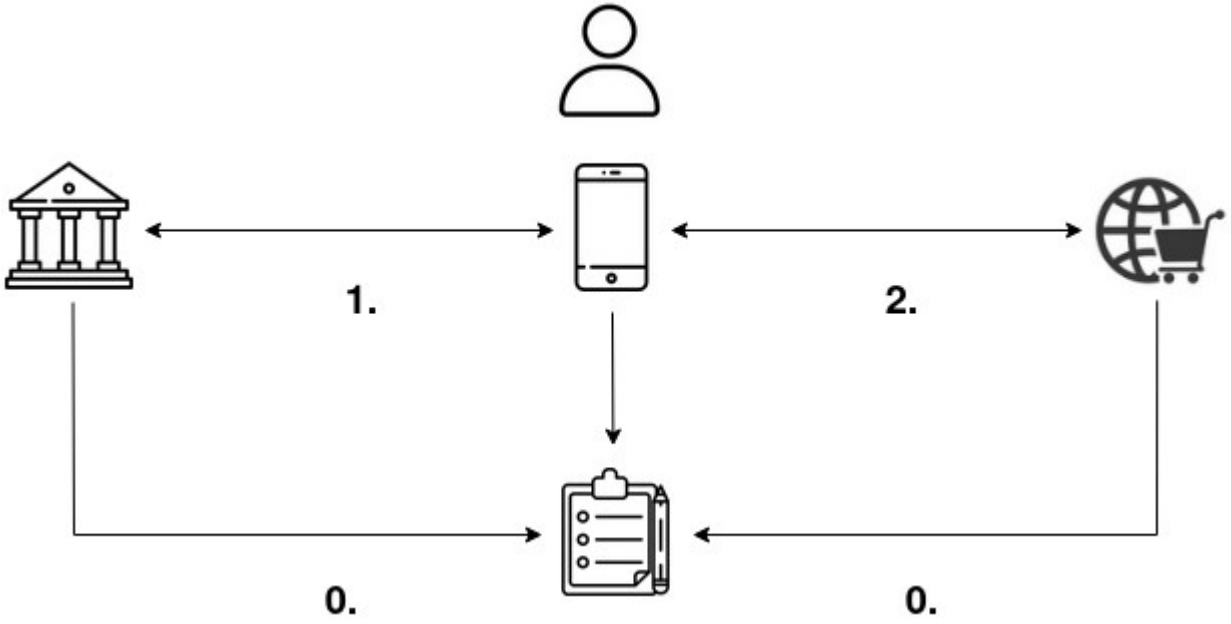
CZ.NIC | SPRÁVCE DOMÉNY CZ

Obsah

Federovaná identita



Decentralizovaná (self-sovereign) identita



Rozdíly

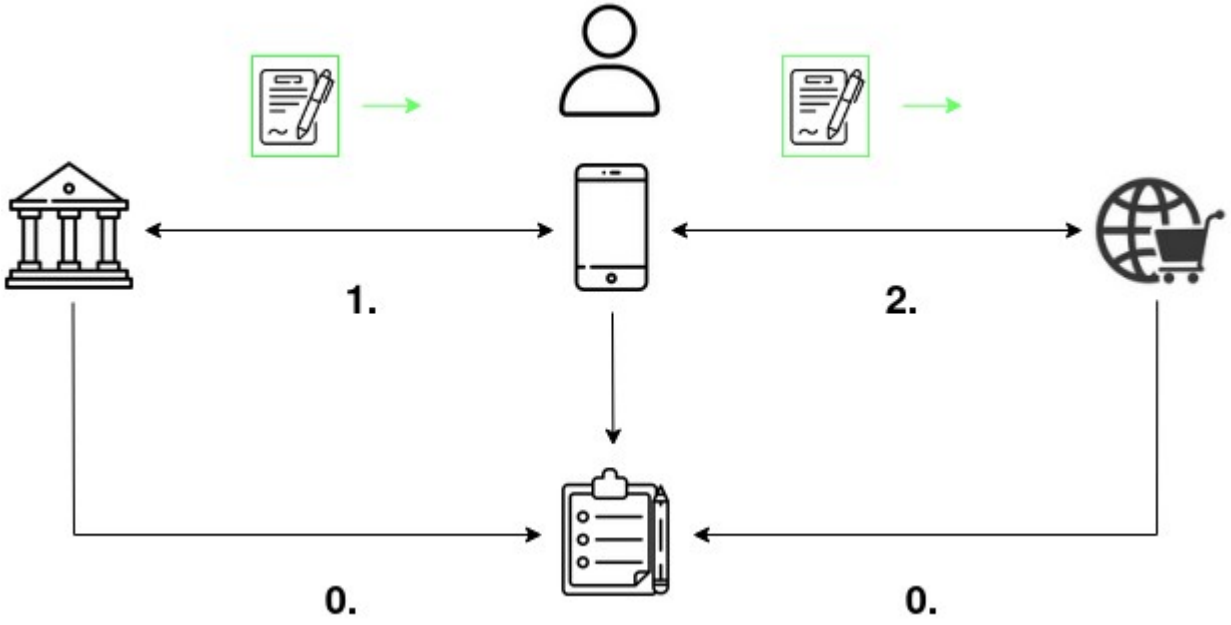
- *Výhody*
  - *Více soukromí pro uživatele - vydavatel pověření nemá možnost zjistit kdy a kde bylo pověření použito*
  - *Možnost offline použití*
  - *Univerzálnost a jednoduchost použití pro uživatele*

- *Nevýhody*
  - *Nutnost řešit revokace*

Technické parametry

- *Vybrané technické parametry*
  - *Parametry související s formátem pověření*
    - *V jakém formátu si budou účastníci vyměňovat data*
  - *Protokoly pro výměnu pověření*
    - *Jak spolu budou účastníci komunikovat*
  - *Správa důvěry*
    - *Jak si nastaví důvěru mezi účastníky*
- *Srovnávací projekt v rámci Open Wallet Foundation*
  - *https://openwallet-foundation.github.io/credential-format-comparison-sig/*

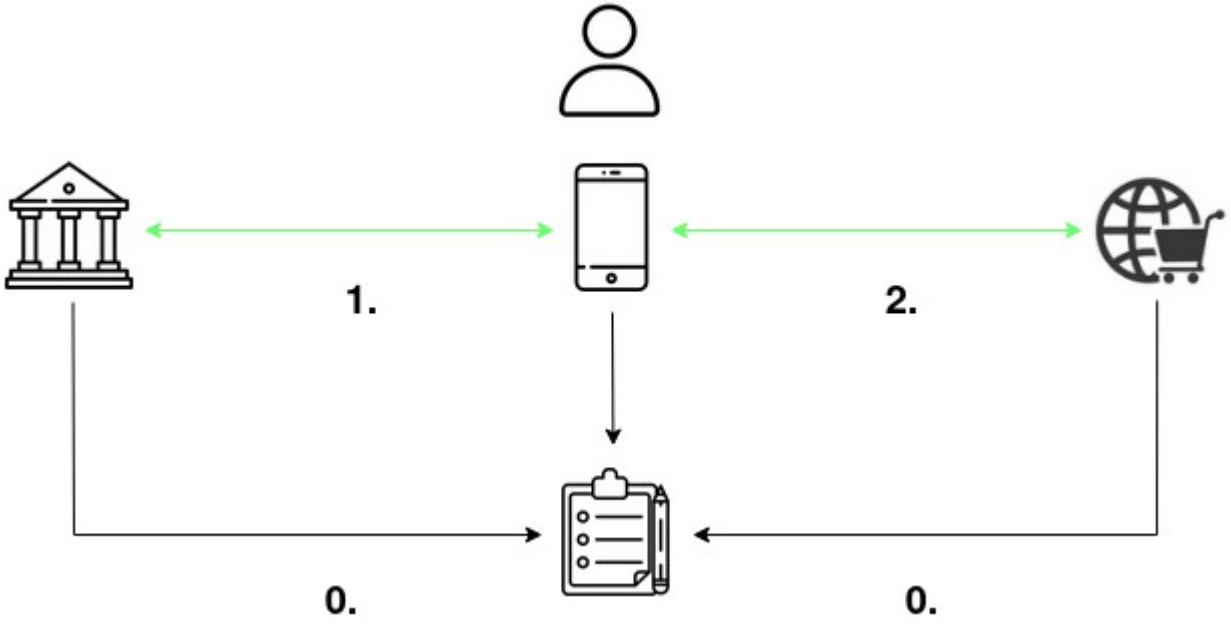
Formáty pro prověření



Formáty pro prověření

- *Klíčové vlastnosti*
  - *Omezené předávání (selective disclosure), nespojitelnost (unlinkability), rozsahy a predikáty, podpora v HW, podpora pro změnu kryptografie (PQ)*
- *Některé významné formáty*
  - *AnonCreds – jeden z prvních formátů z dílny HyperLedger Foundation*
  - *W3C VC – významný standard publikovaný W3C svázaný s použitím JSON-LD*
  - *mDOC – ISO 18015-5 (MDL) – mobilní řidičský průkaz, populární v USA, podpora Apple*
  - *SD-JWT VC – nejmladší standard z dílny IETF*

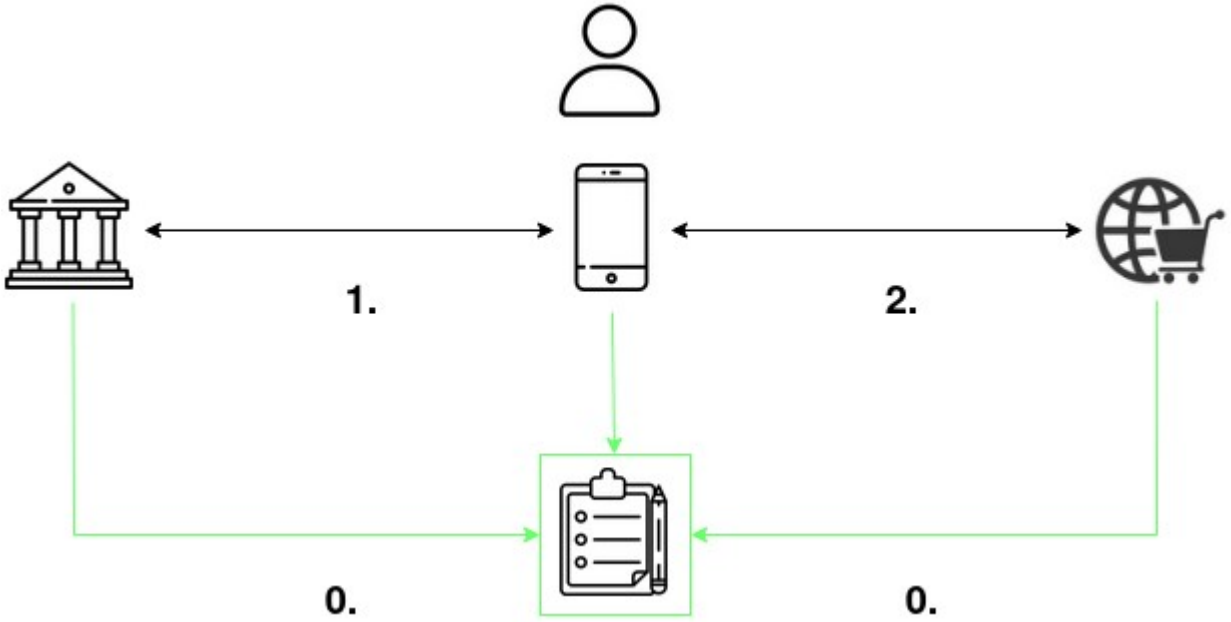
Protokoly



Protokoly

- *DIDComm – Aktuálně nejčastěji používaný ve světě blockchainu*
- *ISO 23220-3 – Protokol převážně vázaný na mDOC*
- *OpenID4VC – Sada protokolů z dílny OpenID Foundation*
  - *OID4VCI – API pro vystavení potvrzení do peněženky*
  - *OID4VP + SIOPv2 – Protokoly pro prezentaci potvrzení z peněženky*

Správa důvěry

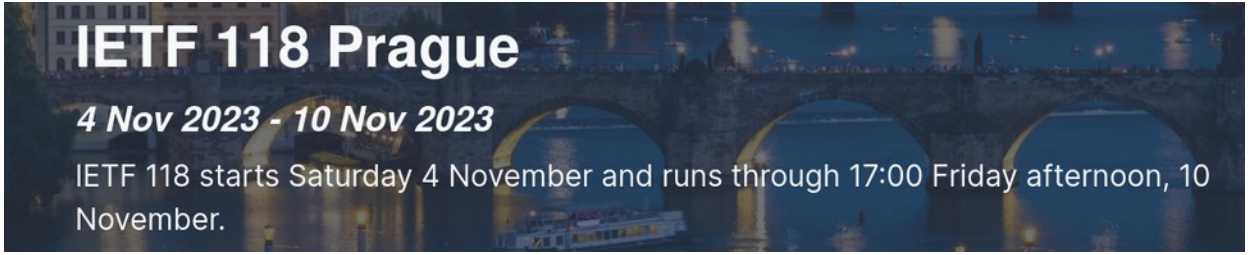


Správa důvěry

- *HyperLedger Indy – software použitý v mnoha instancích decentralizované identity založené na blockchainu*
- *EBSI – European Blockchain Services Infrastructure – celoveropská síť uzlů vybudovaná EK*
  - *Dva uzly v ČR, jeden provozuje CZ.NIC*
- *EU Trusted Lists – Existující řešení použité zejména pro CA*
- *TRAIN – Využití DNS pro vyhledání Trusted Lists*

IETF 118 v Praze

- *Mnoho standardů se právě teď diskutuje v rámci OAuthWG v IETF*
  - *https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/*
  - *https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/*
  - *https://datatracker.ietf.org/doc/draft-ietf-oauth-attestation-based-client-auth/*
  - *https://datatracker.ietf.org/doc/draft-looker-oauth-jwt-cwt-status-list/*
- *Buďte u toho: https://www.ietf.org/how/meetings/118/*



EUDIW – EUropean Digital Identity Wallet

- *Vize digitální peněženky, která umožní ukádat a prokazovat totožnost, oprávnění, kvalifikace, zdravotní potvrzení ale i digitálně podepisovat dokumenty*
- *Vývoj běží v několika paralelních procesech*
  - *Legislativa*
    - *Schválení textu nové verze nařízení eIDAS*
  - *ToolBox*
    - *Technické parametry řešení*
  - *Referenční implementace*
    - *Vzorová ukázka použitelná pro ostatní*
  - *Large Scale Pilots*
    - *Pilotování technologií na vybraných případech užití společnostmi soukromého i veřejného sektoru*

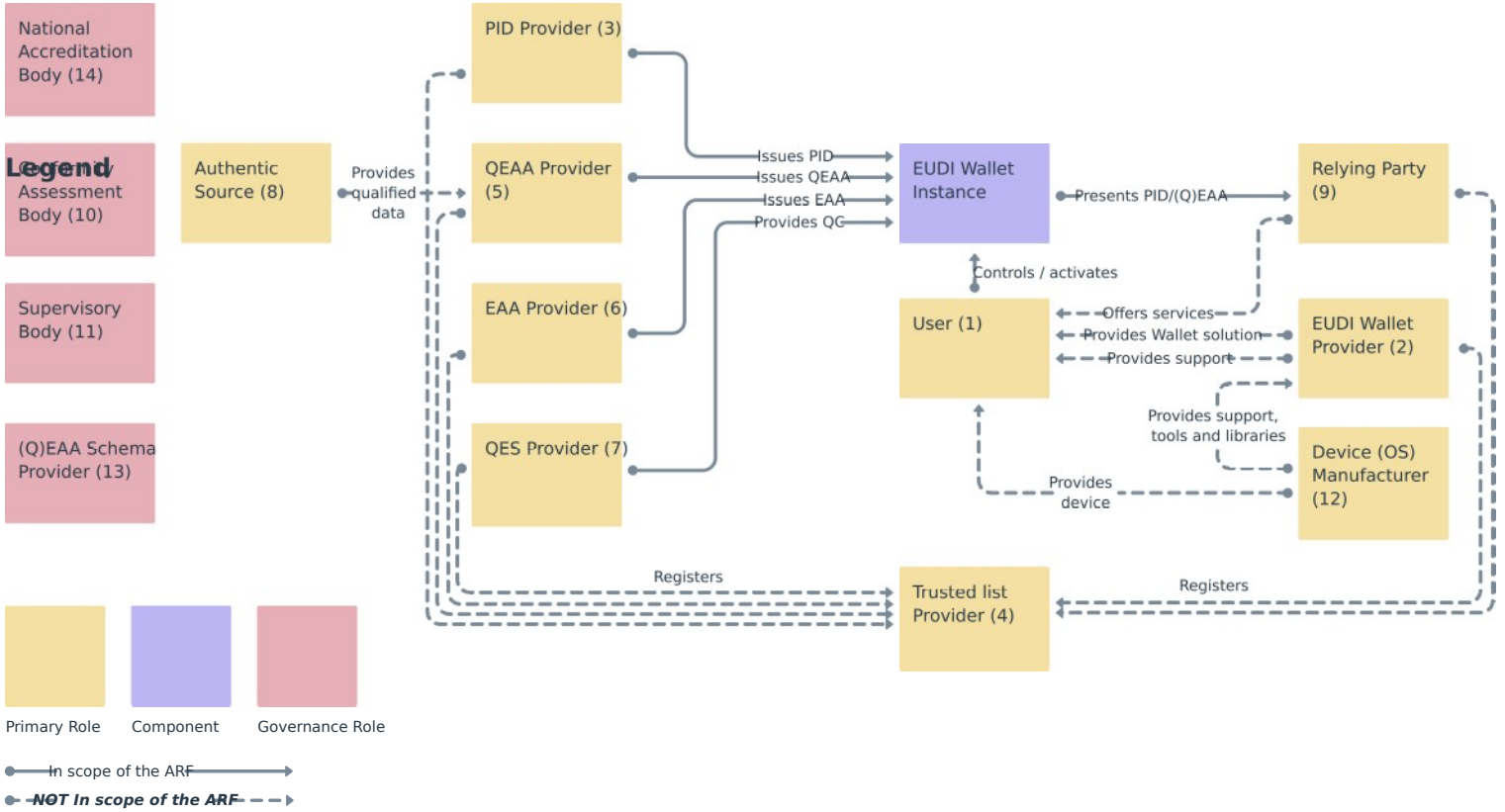
Legislativa

- *2021 návrh Evropské komise, 2022 návrh Evropské rady, 2023 návrh Evropského parlamentu – běží trialog mezi těmito institucemi*
- *V červnu na konci švédského předsednictví v radě publikována „provizorní dohada na sporných bodech“, která by se teď měla promítnout do legislativního textu*
- *Ideální scénář počítá s plnou dostupností v EU v roce 2026*
  - *Letos bude legislativa schválena, pak bude půl roku na vydání prováděcích nařízení a pak budou mít členské státy 2 roky na implementaci*

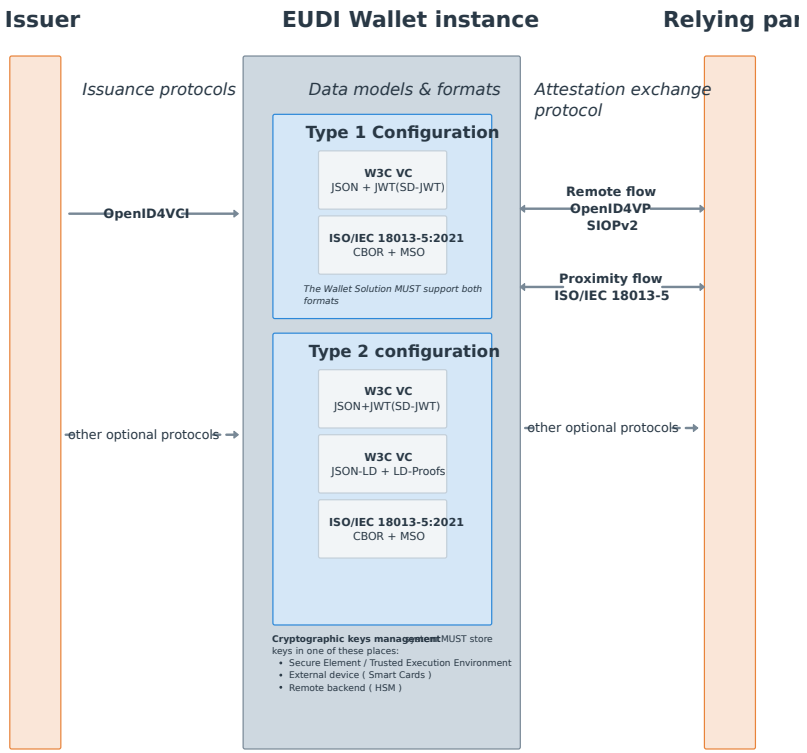
Toolbox

- *Vytváří ho eIDAS expert group – zástupci členských zemí*
- *Aktuální hlavní produkt je Architecture and Reference Framework (ARF)*
  - *K dispozici na GitHubu - https://github.com/eu-digital-identity-wallet*
- *Skupina se snaží pracovat agilně pomocí definice Epics, které postupně zpracovává*
  - *Verze 1.0 - únor 2023*
  - *Verze 1.1 - duben 2023 (Epic 1, 2)*
  - *Verze 1.2 - schválená v červnu, zatím nepublikovaná (Epic 3,4,5)*

ARF - architektura



ARF – formáty a protokoly



Referenční implementace

- *Vyvíjí konzorcium Netcompany-Intrasoft a Scytales (NiSCy)*
- *Sada open source knihoven, komponent a aplikace pro Android i iOS*
- *K prvnímu vydání verze 0.1 plánovanému na červen a odloženému na září stále nedošlo*
- *V plánu je vytvoření vývojářské komunity na Githubu a webinář spolu s publikací prvního vydání*
- *Jako správce národního eIDAS uzlu spolupracujeme s konzorciem na testování možnosti inicializace EUDIW pomocí této komponenty*

Digitální peněženka

- *Umožní uložit identitu jak fyzické tak právnické osoby*
- *Různé formy (mobilní nebo desktopová aplikace, cloudová služba)*
- *Bude vyžadována certifikace/atestace peněženky*
- *Open Wallet Foundation*
  - *Open source jádro pro digitální peněženky (jako je Blink pro prohlížeče)*
- *Peněženek bude určitě více druhů - každý stát se bude rozhodovat, jaké peněženky bude pro své občany uznávat*

Large Scale Pilots

- *Komise inciovala vznik konzorcií, které s 50% financováním mají pilotovat ekosystém kolem EUDIW*
  - *NOBID - >20 org.*
  - *POTENTIAL - >130 org., Autocont*
  - *DC4EU – >75 org., Kancelář zdravotního pojištění*
  - *EWC – >65 org., CZ.NIC, GenDigital, DIA*
- *Konzorcia začla oficiálně pracovat v dubnu*
  - *Primárně mají využívat referenční implementaci, která ale není k dispozici*

CZ.NIC v EWC

- *Nová směrnice NIS2 a její implementace v připravovaném ZKB vyžadují aby doménové registry více ověřovali držitele domén.*
- *V rámci pilotu budeme experimentovat s využitím EUDIW pro taková ověření*
  - *Nový portál pro výzvy k ověření totožnosti*
  - *Integrace do aplikace Doménový prohlížeč*
  - *Zapojení registrátorů*
- *Zároveň chceme prozkoumat možnost vystavení pověření o vlastnictví domény do EUDIW a jeho využití např. pro vydání TLS certifikátu*

MojeID v EWC

- *Jako poskytovatel identity chceme pilotovat jednouchou cestu jak z MojeID inicializovat EUDIW*
- *Zároveň budeme zkoumaž možnoti kombinace osobní aplikace a cloudové služby, např. pro synchronizaci pověření mezi více instancemi nebo po výměně telefonu*
- *Nabízí se i možnost implementace plně cloudové peněženky zejména užitečné pro digitální identitu právnické osoby.*

Závěr

- *„Don’t hold your breath“*
- *Stávající systém federované identity ještě zdaleka nekončí*
  - *Revize eIDAS staví EUDIW paralelně s federovaným světem a dokud v poslední zemi EU bude mít nějaký obyvatel centrální identitu, máme povinnost umožnit její použití v našich veřejných službách*
- *Českou cestu pomůže definovat nová pracovní skupina RVIS*
- *Mezitím nás jako předskokan čeká aplikace eDoklady pro offline digitální prokázání totožnosti*

Děkuji vám za pozornost!

7.10. 2023

CZ.NIC | SPRÁVCE DOMÉNY CZ