eDoklady: Technické standardy a protokoly a jejich užití v uživatelských scénářích

Následující dokument popisuje a zdůvodňuje dva povolené scénáře prokazování totožnosti či jiné právní skutečnosti pomocí mobilní aplikace, a to pouze při osobním kontaktu: **tyto scénáře jsou si postaveny na roveň a je na uvážení příslušného ověřujícího subjektu (orgánu veřejné moci, právnické osoby, fyzické osoby, …), který ve výsledku zvolí.**

Oba scénáře v maximální míře reflektují aktuální dění kolem Evropské peněženky digitální identity a snaží se zároveň reflektovat aktuální vybavenost ověřujících subjektů i jejich finanční možnosti.

Uživatel (fyzická osoba) je v obou scénářích vybaven mobilním zařízením s nainstalovanou aplikací (pracovně nazývanou *eDoklady*). Ověřující subjekt je v prvním scénáři vybaven mobilním zařízením s nainstalovanou čtecí aplikací, ve druhém scénáři pak počítačem (PC nebo notebookem) s připojením k síti. **Zdůrazňujeme, že mobilní elektronické průkazy jsou určeny pouze k prokázání při osobním kontaktu, jak stanoví i zákon, a nikoli pro elektronickou identifikaci.**

Obsah

1 Použité standardy a protokoly

Oba povolené scénáře se opírají o dokument *„Architecture and Reference Framework“*[1], na kterém bude založena referenční implementace Evropské peněženky digitální identity (tzv. EUDIW), která se bude pilotovat v rámci tzv. *large scale projektů*[2]. Ve zmíněném *Architecture and Reference Framework* se aktuálně počítá se standardem mDL dle ISO/IEC 18013-5 pro proximity flow, tj. kdy se uživatel nachází fyzicky blízko spoléhající se straně. Naopak remote flow, které spoléhá na vzdálený přenos údajů, je v dokumentu podporováno protokolem OpenID4VP. Zkušenosti získané v rámci *Architecture and Reference Framework* a pilotování referenční implementace následně poslouží při tvorbě implementačních aktů, které budou následně závazně specifikovat konkrétní požadavky na evropské peněženky digitální identity a celý ekosystém v souladu s připravovanou revizí nařízení eIDAS.

V návaznosti na výše uvedené tedy platí, že:

- scénář off-line (kombinace QR kódu pro inicializaci spojení a Bluetooth pro přenos údajů) se opírá o tzv. *proximity flow* založený na standardu mDL (ISO/IEC 18013-5),
- scénář on-line se opírá o tzv. *remote flow* založený na protokolu OpenID4VP.

***Architecture and Reference Framework* v aktuální verzi stanoví, že aplikace musí implementovat oba způsoby (scénáře), tedy *proximity flow* (ISO 18013-5) i *remote flow* (OpenID4VP), což uvedené splňuje.** Nicméně nadále ale platí, že aplikace *eDoklady* bude sloužit pouze pro prokazování při osobním kontaktu.

Více o použitých protokolech a standardech:

- protokol pro vystavení dat: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
- ISO norma pro výměnu dat mezi eDoklady a mobilní čtecí aplikací: https://www.iso.org/standard/69084.html
- protokol pro výměnu dat mezi eDoklady a webovou čtecí aplikací: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

Co se týče scénáře off-line, standard ISO/IEC 18013-5 definuje metody spojení a přenosu dat následovně:

Navázání spojení (device engagement):

- QR kód
- NFC (nebude implementováno)

Přenos dat (data retrieval):

- Bluetooth
- NFC (nebude implementováno)
- Wifi Aware (dle ARF volitelné, nebude implementováno)

Co se týče NFC, tato varianta je problematická z důvodu špatných vlastností pro přenos dat (pomalost přenosu, náchylnost na přerušení z důvodu vzdálení zařízení od čtečky v průběhu procesu)

[1] https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/releases, ARF dokument se průběžně bude aktualizovat.

[2] https://digital-strategy.ec.europa.eu/en/news/eu-digital-identity-4-projects-launched-test-eudi-wallet

a systémových omezení ze strany iOS (Apple). Standard na problematické vlastnosti upozorňuje (NOTE1, NOTE2). Z tohoto důvodu byla zvolena pro implementaci varianta kombinace QR kódu a Bluetooth.

NOTE 1 If QR is used for device engagement and the mDL reader chooses to use NFC for data transfer, then there is no mechanism available for the mDL reader to indicate the choice for NFC data transfer to the mDL. It is possible that the mDL holder is not aware that the mDL needs to interface with the mDL reader using NFC. On the contrary, if NFC is used for device engagement, this problem does not exist.

NOTE 2 Due to the limited data transfer rate for NFC, if a large amount of data is required for a transaction, it is possible that it is neither practical nor reasonable to have an mDL holder hold the device within the RF range of the mDL reader for the duration of the transaction. Furthermore, due to the loss of signal when a device leaves the RF field, any mDL holder interactions with the mDL causing the mDL to leave the RF field require a new transaction to be initiated. This can be avoided by having all mDL holder interactions with the mDL done while the mDL stays in the field or if mDL does not require any mDL holder interactions while it is in the RF field.

2 Scénář prokázání mobil-to-mobil (off-line)

Základní vlastnosti:

- Obě strany, tedy uživatel (fyzická osoba) i ověřující subjekt, jsou vybaveny mobilními zařízeními (telefon, tablet).
- **Nutně nevyžaduje při prokázání připojení k internetu ani jedné strany.**

2.1 Ukázka

1. Ověřující subjekt (úředník, policista, …) vyzve uživatele (fyzickou osobu) k prokázání totožnosti nebo jiné skutečnosti.
2. Uživatel otevře mobilní aplikaci *eDoklady* a zobrazí QR kód obsahující informace pro ustavení přenosu dat.
3. Ověřující subjekt načte QR kód pomocí čtecí aplikace na svém mobilním zařízení.
4. Obě aplikace ustaví vzájemnou šifrovanou komunikaci přes Bluetooth. Následná komunikace probíhá již pouze tímto kanálem.
5. Čtecí aplikace pošle základní informace o subjektu ověřovatele a výčet požadovaných údajů.
6. Aplikace *eDoklady* zobrazí uživateli obdrženou žádost o souhlas s předáním požadovaných údajů.
7. Uživatel potvrdí, příp. žádost zamítne (v případě zamítnutí žádné údaje z průkazu ověřujícímu subjektu odeslány nejsou).
8. V případě potvrzení aplikace *eDoklady* odešle požadované údaje.
9. Čtecí aplikace zobrazí stav průkazu a předané údaje ověřujícímu subjektu, zatímco aplikace *eDoklady* zobrazí uživateli informaci o úspěšném přenosu.

2.2 Požadavky na vybavenost subjektů

Požadavky na ověřovatele: mobilní zařízení (telefon nebo tablet, který podporuje čtení QR kódů a Bluetooth verze 4.0 či vyšší)

Ověřující subjekty budou vybaveny mobilními zařízeními, které budou podporovat požadované metody komunikace (zařízení musí umožnit obě metody, tedy čtení QR kódu a zároveň Bluetooth). Na zařízení bude instalována čtecí aplikace (ke stažení zdarma ze storů Google Play a App Store).

Zařízení musí využívat jednu z posledních tří verzí operačního systému Android (tedy podporovanými verzemi jsou aktuálně verze 11, 12 a 13, což je omezení stanovené vydavatelem Android, tedy společností Google, pro nové mobilní aplikace) nebo poslední verzi iOS. Zároveň musí zařízení podporovat Bluetooth verze 4.0 či vyšší, a to z důvodu integrace tzv. Bluetooth Low Energy (BLE).

Ve čtecí aplikaci se zobrazí předané údaje průkazu. Ověřující subjekt manuálně opíše vybrané údaje do formuláře svého informačního systému (typicky se jedná o opsání čísla občanského průkazu) nebo provede export dat průkazu z aplikace (zvažován mDL formát či typicky PDF).

Výhodou je, že pořízená mobilní zařízení budou připravena i pro kanál NFC, pokud bude v budoucnu vyžadován (např. v rámci Evropské peněženky digitální identity).

3 Scénář prokázání mobil-to-desktop (on-line)

Základní vlastnosti:

- Pouze uživatel (fyzická osoba) je vybaven mobilním zařízením (telefon, tablet). Ověřujícímu subjektu postačí počítač (PC, notebook nebo jiné zařízení s nainstalovaným webovým prohlížečem).
- **Vyžaduje připojení k internetu uživatele. V případě ověřujícího subjektu vyžaduje připojení k internetu** (LAN, mobilní data, veřejná wifi, hotspot, …) **nebo připojení do Centrálního místa služeb.**
- **Vhodný především pro přepážková (stabilní) pracoviště.**

3.1 Ukázka

Následující scénář je z pohledu technického popisu zjednodušený:

1. Ověřující subjekt (úředník, policista, …) vyzve uživatele (fyzickou osobu) k prokázání totožnosti nebo jiné skutečnosti. V této souvislosti upozorní uživatele na QR kód, který je viditelně umístěný např. na přepážce.
2. Uživatel otevře mobilní aplikaci *eDoklady* a zvolí akci pro předání průkazu on-line.
3. Aplikace *eDoklady* spustí fotoaparát pro nascanování QR kódu.
4. Uživatel nascanuje QR kód na přepážce.
5. Aplikace *eDoklady* naváže na pozadí on-line spojení se čtecí aplikací (konkrétně se serverem).
6. Server pošle základní informace o ověřujícím subjektu a výčet požadovaných údajů.
7. Aplikace *eDoklady* zobrazí uživateli žádost o souhlas s předáním požadovaných údajů.
8. Uživatel potvrdí, příp. žádost zamítne (v případě zamítnutí žádné údaje z průkazu ověřujícímu subjektu odeslány nejsou).
9. Aplikace *eDoklady* odešle požadované údaje. Obdržené údaje se předají do webové aplikace čtečky dokladů.
10. Ověřujícímu subjektu se ve čtecí aplikaci zobrazí stav průkazu a předané údaje.

3.2 Požadavky na vybavenost subjektů

Požadavky na ověřovatele: počítač (PC nebo notebook) připojený přímo k internetu nebo do Centrálního místa služeb

Ověřující subjekty musí disponovat počítačem (PC nebo notebookem) připojeným přímo k internetu nebo do Centrálního místa služeb. Na počítač se neinstaluje žádná aplikace, musí na něm být však nainstalován webový prohlížeč (Edge, Firefox, Chrome, Safari, …), protože čtecí aplikace bude k dispozici v podobě webové aplikace, kterou si ověřující subjekt (např. úředník) otevře právě v prohlížeči.

Tato webová čtecí aplikace bude sloužit dvěma hlavním cílům:

- správě fyzických míst (přepážek) a generování QR kódů (QR kód si následně ověřovatel může vytisknout a umístit viditelně a bezpečně na přepážku nebo obecně místo, kde přichází do styku s uživateli, anebo kód zobrazí uživateli na monitoru nebo displeji),
- zobrazení ověřovaných dokladů.

Ověřující subjekt bude moci provést export dat z webové aplikace (typicky PDF a strojově čitelný formát). Aktuálně se počítá také s možností napojení informačních systémů ověřujících subjektů na server webové čtecí aplikace, avšak až v průběhu prvního pololetí 2024.