Zadání eDokladovka23

Cílem projektu **eDokladovka23** je vytvoření služby, která občanům umožní důvěryhodně prezentovat druhé osobě údaje o jejich dokladech vydaných veřejnou správou.

Primárním uživatelským rozhraním občana bude aplikace pro mobilní zařízení, která nabídne občanovi možnost uložení, aktualizace a důvěryhodné prezentace údajů o dokladech vydaných Českou republikou.

V první fázi bude řešen Občanský průkaz s důrazem na otevřenost řešení pro vkládání dalších dokladů.

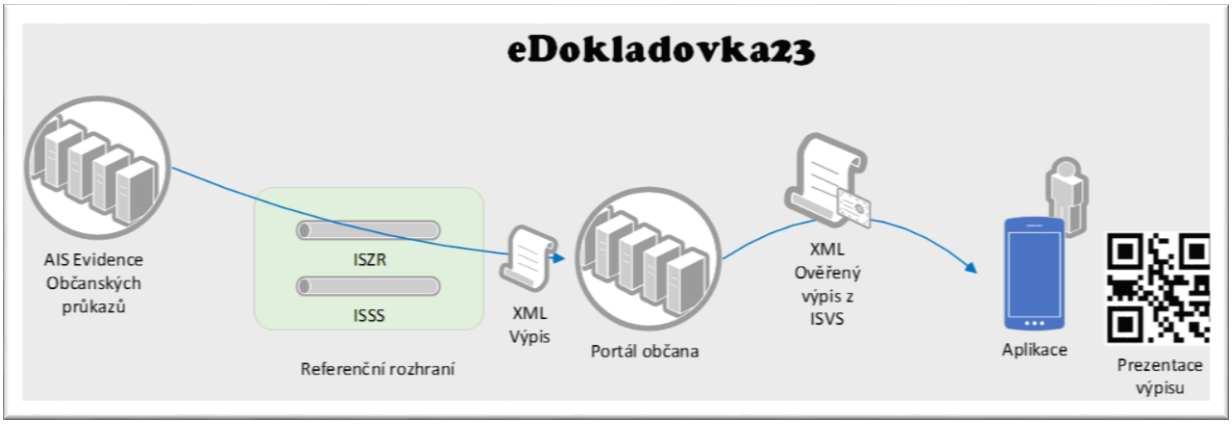
Zásadní požadavky na funkcionalitu řešení, která bude nabídnuta občanovi:

- Důvěryhodná prezentace uloženého dokladu **při osobním kontaktu**
- Možnost prokázání totožnosti na základě uloženého občanského průkazu
- Možnost prokázání limitního věku (starší než …) bez předání jiných údajů
- Ochrana použití – o předání údajů z dokladu ví pouze držitel Dokladovky a příjemce
- Otevřenost řešení umožňující rozšíření o další funkcionality a protokoly předávání dokladů

Uložený doklad bude realizován jako *ověřený výpis z informačního systému veřejné správy.* Tento výpis potvrzuje skutečnost, že tento doklad existuje a údaje na něm uvedené. Tento výpis dále nazýváme „datový balík“. Tento balík je opatřen náležitostmi jako ověřený výpis z ISVS.

Architektura řešení

Zásadním požadavkem řešení je, aby údaje o občanském průkazu pocházely z Agendového informačního systému evidence Občanských průkazů (AIS EOP). Tyto údaje jsou z pověření držitele eDokladovky23 (občana) získány dedikovanou uživatelskou částí Portálu občana a je z nich vytvořen datový obsah přenášený do občanem určené eDokladovky23.



Řešení tedy musí obsahovat následující komponenty:

- BackEnd
    - Informační systémy veřejné správy – evidence dokladů. Tyto evidence musí poskytovat výpis z ISVS prostřednictvím referenčního rozhraní
    - eDokladovka23 server – Dedikovaná část Portálu občana shromažďující požadavky určená pro obsluhu mobilní aplikace
- FrontEnd
    - Mobilní aplikace pro ukládání a prezentaci údajů z občanského průkazu
    - Mobilní aplikace pro čtení prezentovaných údajů

Doklad

Na základě údajů získaných z AIS EOP je v Portálu občana vytvořen datový obsah přenášený do Mobilní aplikace občana. Každá část datového obsahu je opatřena prvky vytvářejícími důvěru (elektronická pečeť a časové razítko):

- **Základní datový balík** obsahující kompletní informace uvedené na občanském průkazu kromě fotografie a podpisu
- **Redukované balíky** obsahující vybranou podmnožinu informací uvedených na dokladu – výčet bude řešen v průběhu projektu
- **Stavové informace** o občanském průkazu (např. nahlášena ztráta)
- **Fotografie držitele** občanského průkazu
- **Šablona prezentace dokladu** – určuje grafickou prezentaci občanského průkazu v mobilní aplikaci

Životní cyklus aplikace eDokladovka23

Personalizace eDokladovky

Jedná se o aplikaci, kterou uživatel získá z Google či Apple store. Následně provede připojení konkrétní instance aplikace ke své identitě prostřednictvím serverové části po prokázání totožnosti prostřednictvím Národního bodu.

Výsledkem je k personalizace instance aplikace na konkrétním zařízení. Od této chvíle může být využita pro ukládání a prezentaci dokladů.

Občan může mít v principu neomezené množství personalizovaných instancí aplikace na různých mobilních telefonech.

Naplnění eDokladovky údaji

Aplikace využívá „nevizuální přihlašování“ v Národním bodu a pro spuštění vyžaduje bezpečnostní zajištění na úrovni PIN/Otisk prstu/Face ID. Aplikace ukládá citlivé informace (klíče personalizace a podobně) minimálně na úrovni Android keystore či Apple secure enclave.

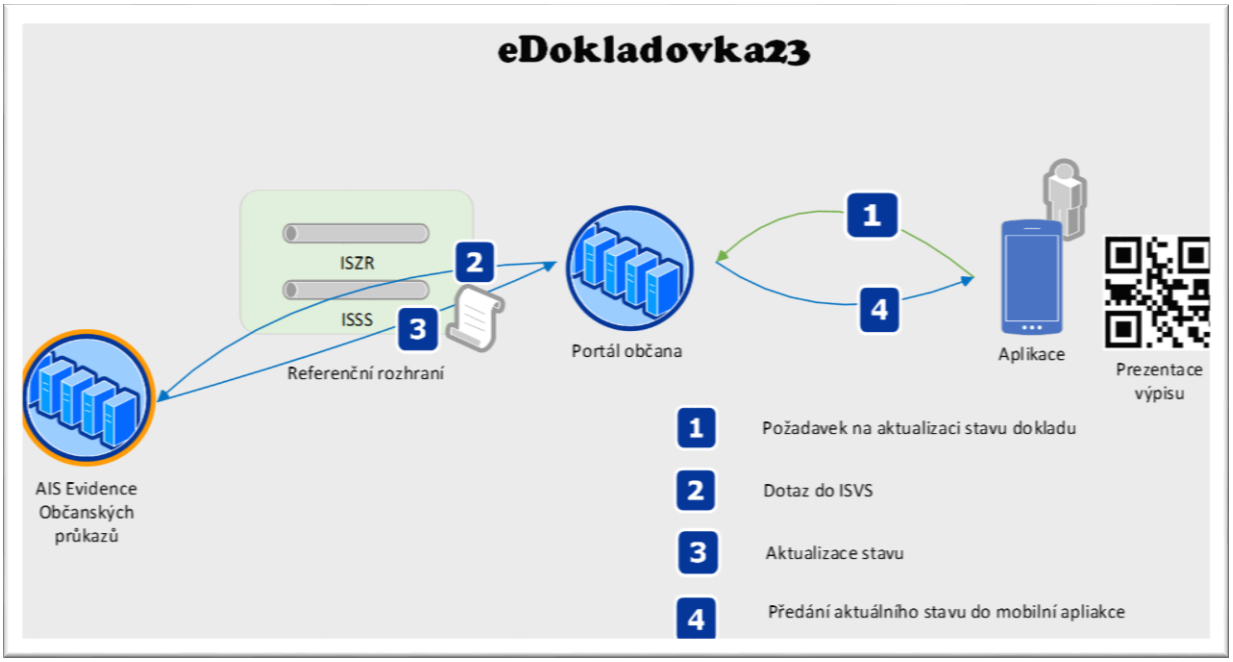
Držitel personalizované aplikace následně vyžádá naplnění aplikace údaji, tedy přenesení výše uvedených údajů o občanském průkazu do aplikace. Serverová část na Portálu občana na základě tohoto požadavku získá údaje o občanském průkazu z AIS EO, připraví odpovídající datový obsah, opatří prvky vytvářejícími důvěru a přenese ho do aplikace.

Serverová část dále provede interní registraci vazby Občan/Instance Aplikace/Doklad. Na základě této registrace pak provádí pravidelný update stavových údajů o občanském průkazu (odběr vyrozumění o změně údajů z AIS EOP a získání údajů o aktuální stavu dokladu).

Údržba údajů o občanském průkazu

Údaje vedené na občanském průkazu nemohou být z principu měněny, při změně údajů je vytvářen nový doklad. V přechodovém stavu může existovat doklad v různých stavech

- Platný avšak s některým údajem nesprávným – např. změna bydliště, změna jména
- Neplatný a nedůvěryhodný – např. nahlášena ztráta či odcizení



Datový obsah o údajích na Občanském průkazu je v Uživatelské části Portálu občana uložen v krytované podobě tak, aby nemohl být přečten správcem aplikace.

Údaje o stavu dokladu mohou být vedeny v otevřené formě.

Nelze přenášet údaje o dokladech mezi dvěma aplikacemi. Přenos je možný pouze ze serveru. Pro získání dokladů na jiné zařízení (výměna telefonu) je nutné nové zařízení registrovat v serverové části a opět do něj umístit všechny požadované doklady.

Součástí uživatelské části Portálu občana musí být základní údržba eDokladovky, která občanovi po přihlášení prostřednictvím národního bodu zobrazí jím registrované instance aplikace eDokladovka23, stav předání údajů o občanském průkazu do těchto instancí a umožní mu provést výmaz registrované instance (ztráta mobilního telefonu)

Prezentace občanského průkazu v mobilní aplikaci

Při každém požadavku na prezentaci údajů kdy od poslední prezentace oběhlo více jak 60 minut se aplikace pokusí kontaktovat BackEnd a získat aktuální stav údajů o dokladu. Tedy nikoli obsah dokladu, ale zda doklad nebyl například nahlášen jako ztracený.

Dále umožní prezentaci údajů:

- **Základní** – náhled údajů na dokladu včetně uvedení stavových informací ve vizuální formě
    - Zobrazena fotografie držitele, Jméno, Příjmení a číslo občanského průkazu, čas a datum poslední aktualizace údajů o dokladu
    - Zobrazen 2D kód čísla občanského průkazu ve shodném tvaru jak je uváděn na fyzickém občanském průkazu
    - Podbarvením náhledu je příjemce informován o tom, zda byla úspěšná aktualizace údajů
    - Zobrazení QR kódu obsahující požadovaný komunikační klíč (viz následující kapitola)

- **Datová** – po přesunutí obrazovky, aby bylo viditelné pro příjemce, že je součástí aplikace a nejde o statickou náhradu - podvrh. Prezentace datové části musí umožnit volbu
    - **Doklad** - QR kód obsahující základní datový balík dokladu opatřený pečetí a časovým razítkem vzniku
    - **Výběrové informace** – QR kód obsahující redukovaný datový balík opět opatřený pečetí a časovým razítkem vzniku
    - **QR kód obsahující odvozené údaje** o věku (starší než …) na základě údaje o datu narození a aktuálního data – současně je prezentován „semafor“ s věkovými limity tedy příjemce vidí, zda je držitel starší 18ti, 21ti, 55ti let

Proces prezentace údajů z eDokladovky

Každá prezentace údajů z eDokladovky musí probíhat následujícími etapami:

- **Navázání komunikace** – příjemce prezentuje svoji identitu, předává požadavek na doklad/rozsah údajů, předává klíč pro komunikaci. Rozsah údajů není libovolný, ale je dán dokumentovanými datovými obsahy viz výše
- **Schválení komunikace** – držitel eDokladovky schvaluje předání dokladu/údajů na základě vizualizace požadavku
- **Předání údajů** – technické předání údajů, které je zabezpečeno předaným komunikačním klíčem
- **Ověření předaných údajů** – příjemce ověřuje důvěryhodnost předaných údajů na základě ověření autenticity údajů a ověření, že byl použit požadovaný klíč pro komunikaci

Výše uvedený proces může být prezentován například následovně (detailní návrh musí být součástí nabídky na implementaci):

- Poskytovatel služeb prezentuje QR kód obsahující deklaraci jeho identifikace, požadovaný doklad a komunikační klíč. Tato prezentace může být elektronická s výhodou proměnného komunikačního klíče či statická (samolepka)
- Občan svojí aplikací přečte QR kód a jeho aplikace mu sdělí kdo požaduje jaký doklad či údaje. Pokud občan schválí požadavek, jsou generovány výše uvedené QR kódy obsahující požadovanou odpověď na komunikační klíč (detaily musí být popsány v nabídce pro implementaci)

Výše uvedeným postupem je zajištěno, že příjemci informací nemůže být prezentován výstup vizuálně napodobující aplikaci eDokladovka, neboť prezentovaný QR kód je dynamicky generován na základě předaného komunikačního klíče.

Současně aplikace eDokladovka prezentuje fotografii oprávněného držitele poskytnuté jako součást dat o dokladu, která je doplněna odpovědí na aktuální předaný komunikační klíč. Způsob integrace fotografie a QR kódu může být na principu HalfTone QR code či jiných technologií. Příjemce však musí mít možnost porovnání prezentované fotografie s podobou držitele.

Nouzová prezentace občanského průkazu

V případě, že aplikace pro prezentaci není funkční, může občan po přihlášení do uživatelské části Portálu občana prostřednictvím národního bodu prezentovat údaje o občanském průkazu prostřednictvím WWW aplikace. Při této formě není používán komunikační klíč a proto příjemce musí být zvláště obezřetný při ověření, zda mu nejsou předkládány podvržené údaje.

Aplikace pro čtení

Volně dostupná aplikace, která umožní čtení a verifikaci údajů pomocí všech výše uvedených OR kódů s ověřením autenticity prezentující aplikace. Současně bude obsahovat popsané

rozhraní , které umožní napojení na jiné programové vybavení pro případné další zpracování prezentovaných údajů.

Příjemce informací z aplikace si musí být vědom toho, že zpracovává osobní údaje a je jeho zodpovědností dodržovat zákonné požadavky

Scénáře použití

Předložení dokladu úřední osobě

Úřední osoba (např. policista) vyžaduje předložení dokladu. Občan prezentuje doklad na obrazovce mobilního zařízení. Policista

- Buď je připojen ke svým systémům online, pak z vizualizované formy načte čárový kód čísla dokladu, provede vlastní dotaz do Registru obyvatel a Evidence občanských průkazů. Získá údaje o osobě včetně kvalitní fotografie a ověří totožnost
- Nebo je offline, pak požádá o předání plného datového bloku. Občan přesune obrazovku na plný datový blok a policista svým zařízením čte QR kód.

Předkládaný datový blok je opatřen prvky vytvářejícími důvěru (pečeť a časové razítko) a může být tedy úřední osobou akceptován.

Současně aplikace provádí dotaz na aktuální hodnotu stavových informací a předává je:

- Buď je offline a nemůže aktualizovat stav dokladu – Aplikace výrazně upozorňuje na tuto situaci a zobrazuje údaj, kdy byl stav dokladu naposled aktualizován
- Je online – zobrazuje aktuální stav dokladu

Předložení dokladu neúřední osobě

Druhá osoba vyžaduje předložení dokladu například při ubytování. Při ubytování má provozovatel povinnost vést ubytovací knihu v rozsahu údajů Typ a číslo dokladu, Jméno, Příjmení, Datum narození, Trvalé bydliště.

Občan prezentuje doklad na obrazovce mobilního zařízení. Příjemce

- Buď mu postačují údaje uvedené na obrazovce
- Nebo je požádá o předání redukovaného datového bloku. Je na rozhodnutí občana, zda datový blok poskytne. Příjemce pak svým zařízením čte QR kód.

Předkládaný datový blok je opatřen prvky vytvářejícími důvěru (pečeť a časové razítko) a může být tedy akceptován.

Současně aplikace provádí dotaz na aktuální hodnotu stavových informací a předává:

- Buď je offline a nemůže aktualizovat stav dokladu – Aplikace výrazně upozorňuje na tuto situaci a zobrazuje údaj, kdy byl stav dokladu naposled aktualizován

- Je online – zobrazuje aktuální stav dokladu

Je tedy omezeno předávání fyzického občanského průkazu byť jen na krátkou dobu a navíc údaje jsou přenášeny elektronicky, čímž je zabráněno chybám.

Současně je opět automaticky zobrazen stav občanského průkazu a ubytovatel pozná případ, kdy je mu předkládán občanský průkaz neplatný či jinak rizikový.

Poskytnutí služby závisí na věku

Je prezentována pouze fotografie a QR kód obsahující věkové limity. Z něj se příjemce dozví například, že osoba je starší 21 let, ale mladší 55. Je tedy minimalizováno předávání osobních údajů.

Naopak starší osoba může tímto prezentovat například nárok na slevu v dopravě bez nutnosti poskytnout osobní údaj jako je datum narození.

Další rozvoj

Celé řešení jak na serverové straně tak na straně aplikace musí umožnit rozvoj řešení

- Prezentace dalších dokladů bez změny způsobu předávání. Tedy například řidičského průkazu, zbrojního pasu atd. Postup pro doplnění dalšího dokladu musí být popsán a vyžadovat pouze parametrizaci řešení
- Doplnění dalších protokolů – předpokládáme požadavek na doplnění protokolů mDL (ISO/IEC 18013-5) a Verifiable Credentials Data Model https://www.w3.org/TR/vc-data-model/ . Při doplnění těchto protokolů může být mobilní aplikace i serverová část programově aktualizována
- Doplnění Personal Identification Data – Dle návrhu eIDAS 2.0 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281 . V této části není ještě ujasněno technické rozhraní