

# INTEGRAČNÍ MANUÁL NA WEBOVÉ APLIKACE EDOKLADY

Verze	Datum	Popis změn
1.0	3. 5. 2024	První verze.
1.1	19. 6. 2024	Doplněny požadavky na certifikáty pro komunikaci s API, upřesnění variant Browser flow a Server flow (včetně příloh webová-čtečka-api.yml a integrační-api.yml). Doplněna kap. 2.3 – EDU prostředí.
1.2	2. 10. 2024	Doplněn identifikátor občanského průkazu do kap. 1.3, přidána kap. 2.3.1 s informacemi o testovacích datech.
1.3	2. 12. 2024	Přidány atributy s jednotlivými údaji trvalého bydliště. Doplněn CBOR popis občanského průkazu. Aktualizován popis simulací na EDU prostředí.

# OBSAH

<b>1. Schéma digitálních stejnopisů .....</b>	<b>3</b>
1.1. Popis typů hodnot .....	3
1.2. Podporované digitální stejnopisy .....	4
1.3. Občanský průkaz .....	4
1.4. CBOR struktura .....	5
<b>2. Konfigurace integračního API .....</b>	<b>7</b>
2.1. Povolení integrací .....	7
2.2. Autentizační certifikáty .....	7
2.3. EDU prostředí .....	7
2.3.1 Testovací data .....	7
<b>3. Integrace s Webovou ověřovací aplikací .....</b>	<b>8</b>
3.1. Varianta 1. – Export do schránky .....	8
3.2. Varianta 2. – Integrační API Browser flow .....	9
3.2.1. Popis procesu ověření .....	10
3.3. Varianta 3. – Integrační API Server flow .....	12
3.3.1 Virtuální přepážka .....	12
3.3.2. Popis procesu ověření .....	12
<b>4. Správa lokálních účtů .....</b>	<b>15</b>
4.1. Organizační role .....	15
4.2. Popis dostupných operací .....	15
<b>5. Správa skupin .....</b>	<b>15</b>
5.1. Popis dostupných operací .....	15

# 1. Schéma digitálních stejnopisů

Tato kapitola obsahuje popis schémat podporovaných digitálních stejnopisů.

## 1.1. Popis typů hodnot

Jednotlivé atributy mají různé datové typy. Tyto typy jsou zachyceny a popsány v tabulce - *Datové typy hodnot atributů*.

Tabulka 0-1 - Datové typy hodnot atributů

Typ hodnoty	Popis
PHOTO	Base64 kódovaná fotografie držitele dokladu.
STRING	Textový řetězec.
DATE	Datum ve formátu ISO 8601 (ukázka: 2018-04-23).
BOOLEAN	Tvrzení pravda/nepravda. Možné hodnoty: <ul style="list-style-type: none"><li>▪ true</li><li>▪ false</li></ul>
SEX	Pohlaví, možné hodnoty: <ul style="list-style-type: none"><li>▪ MALE</li><li>▪ FEMALE</li></ul>
CHANGE_OF_DATA	Změna dokladu, možné hodnoty: <ul style="list-style-type: none"><li>▪ NO_CHANGE – Není evidována změna OP.</li><li>▪ YES_RESIDENT_ADDRESS – Evidována změna trvalého bydliště.</li><li>▪ YES_OTHER_DATA – Evidována změna jiných údajů <b>uvedených</b> na občanském průkaze (jméno, příjmení, datum narození, pohlaví, rodinný stav).</li><li>▪ YES_RESIDENT_ADDRESS_AND_OTHER_DATA – Evidována změna trvalého bydliště a jiných údajů <b>uvedených</b> na občanském průkaze (jméno, příjmení, datum narození, pohlaví, rodinný stav).</li></ul>
IMAGE	Base64 kódovaný obrázek

## 1.2. Podporované digitální stejnopisy

Momentálně je podporován pouze občanský průkaz, časem je ale možné, že přibudou další digitální stejnopisy podporovaných průkazů.

## 1.3. Občanský průkaz

Občanský průkaz má technický identifikátor "org.iso.18013.5.1.CZ.mID". Tento identifikátor se následně používá při komunikaci s API, například při zavolání žádosti o provedení ověření.

Níže je tabulka popisující dostupné atributy z digitálního stejnopisu reprezentující občanský průkaz.

Tabulka 0-2 Schéma atributů občanského průkazu

Název	Popis	Datový typ	Povinné <sup>1</sup>
portrait	Fotografie držitele	PHOTO	ANO
family_name	Příjmení	STRING	ANO
given_name	Jméno	STRING	ANO
resident_address	Trvalý pobyt	STRING	ANO
resident_district	Trvalý pobyt - Okres (pokud má držitel průkazu nahlášenu adresu trvalého pobytu na úřadě, součástí tohoto atributu je informace, že se jedná o adresu úřadu, např. „PRAHA 4 - ADRESA ÚŘADU“.	STRING	ANO
resident_city	Trvalý pobyt - Obec	STRING	ANO
resident_part_of_city	Trvalý pobyt - Část obce	STRING	ANO
resident_street	Trvalý pobyt - Ulice	STRING	ANO
resident_house_number	Trvalý pobyt - Orientační číslo	STRING	ANO
resident_house_number_sign	Trvalý pobyt - Znak orientačního čísla	STRING	ANO
resident_city_house_number	Trvalý pobyt - Popisné číslo	STRING	ANO
resident_house_number_type	Trvalý pobyt - Druh čísla domu (obsahuje buďto znak 'P' pokud atribut 'Popisné číslo' značí číslo popisné nebo 'E' pokud značí číslo evidenční)	STRING	ANO
personal_number	Rodné číslo	STRING	ANO

---

<sup>1</sup> Údaj ve sloupci „Povinné“ reflektuje informaci, zda daný údaj musí být povinně uveden v rámci konkrétního průkazu, ze kterého byl vytvořen jeho digitální stejnopis. Některé údaje mohou být v rámci průkazu uvedeny volitelně. Pokud jde ale o rozpad adresy trvalého pobytu na jednotlivé údaje, tak ne všechny tyto údaje musí být uvedeny na průkaze. Pokud některý z těchto údajů není na průkaze uveden, tak se přes API vrací prázdný řetězec. Stejně tak v získané CBOR struktuře, pokud některý z těchto údajů trvalé adresy není na průkaze uveden, tak v CBOR struktuře bude uveden prázdný řetězec.

birth_date	Datum narození	DATE	ANO
birth_place	Místo narození	STRING	ANO
nationality	Národnost	STRING	ANO
sex	Pohlaví	SEX	ANO
signature_usual_mark	Podpis	IMAGE	ANO
document_number	Číslo OP	STRING	ANO
issue_date	Datum vydání	DATE	ANO
expiry_date	Platnost do	DATE	ANO
issuing_authority	Vydal	STRING	ANO
change_of_data	Příznak s evidencí změnou údajů OP	CHANGE_OF_DATA	ANO
official_records	Úřední záznamy	STRING	NE
marital_status	Rodinný stav	STRING	NE
title	Titul	STRING	NE
age_over_15	Starší než 15 let	BOOLEAN	ANO
age_over_18	Starší než 18 let	BOOLEAN	ANO
age_over_21	Starší než 21 let	BOOLEAN	ANO
age_over_60	Starší než 60 let	BOOLEAN	ANO
age_over_65	Starší než 65 let	BOOLEAN	ANO

## 1.4. CBOR struktura

Z Webové ověřovací aplikace je možné získat CBOR strukturu předaných údajů. Buď přes integrační API, pokud se pošle atribut *includeMDoc*, nebo také pomocí exportu v grafickém rozhraní Webové ověřovací aplikace.

Tato struktura odpovídá typu *mDoc*, který je definován ve standardu ISO-18013-5.

Atributy občanského průkazu jsou v této struktuře dostupné pod jmenným prostorem "org.iso.18013.5.1.CZ". Názvy jednotlivých atributů odpovídají údajům v tabulce 0-2.

*Tabulka 0-3 Schéma CBOR struktury*

Název	CBOR typ	Poznámka
portrait	bstr	PNG obrázek
family_name	tstr	
given_name	tstr	
resident_address	tstr	
resident_district	tstr	
resident_city	tstr	
resident_part_of_city	tstr	
resident_street	tstr	
resident_house_number	tstr	
resident_house_number_sign	tstr	

resident_city_house_number	tstr	
resident_house_number_type	tstr	
personal_number	tstr	
birth_date	full-date	
birth_place	tstr	
nationality	tstr	
sex	uint	1 - Muž 2 - Žena Vychází z ISO/IEC 5218
signature_usual_mark	bstr	PNG obrázek
document_number	tstr	
issue_date	full-date	
expiry_date	full-date	
issuing_authority	tstr	
change_of_data	uint	0 – Není evidována změna OP. 1 – Evidována změna trvalého bydliště. 2 – Evidována změna jiných údajů <b>uvedených</b> na občanském průkaze (jméno, příjmení, datum narození, pohlaví, rodinný stav). 3 – Evidována změna trvalého bydliště a jiných údajů <b>uvedených</b> na občanském průkaze (jméno, příjmení, datum narození, pohlaví, rodinný stav).
official_records	tstr	
marital_status	tstr	
title	tstr	
age_over_15	bool	
age_over_18	bool	
age_over_21	bool	
age_over_60	bool	
age_over_65	bool	

## 2. Konfigurace integračního API

Konfigurace integračního API je dostupná ve Správě ověřovatelů.

### 2.1. Povolení integrací

Ve Správě ověřovatelů jsou vypsány dostupné integrace, které je možné povolit. Momentálně je možné povolit následující integrace:

- Rozhraní pro práci s Webovou ověřovací aplikací. Tato integrace v sobě zahrnuje:
  - Integrace s Webovou ověřovací aplikací
- Rozhraní pro napojení na Interní IdP ve Správě ověřovatelů. Tato integrace v sobě zahrnuje:
  - Správa lokálních účtů
  - Správa skupin

### 2.2. Autentizační certifikáty

Pro napojení na Integrační rozhraní je potřeba nastavit platné X509 klientské SSL certifikáty, které budou použity pro autentizaci.

Pro účely komunikace s API bude nutné využívat komerční serverové certifikáty vydané následujícími kvalifikovanými poskytovateli služeb vytvářejících důvěru v ČR:

- První certifikační autorita, a. s.
- Česká pošta, s. p.
- elidentity a. s.
- Správa základních registrů (vydávání nových certifikátů bylo ukončeno, nicméně existující komerční serverové certifikáty je případně možné použít)
- Správa státních služeb vytvářejících důvěru

Technické požadavky na certifikát – použitelnost pro protokol TLS 1.2 a vyšší.

### 2.3. EDU prostředí

Pro účely otestování integrace je k dispozici veřejně dostupné EDU prostředí:

- Webová ověřovací aplikace: <https://ctecka-edu.edoklady.gov.cz>
- Správa ověřovatelů: <https://sprava-edu.edoklady.gov.cz>
- Integrační rozhraní pro API: <https://capi-edu.edoklady.gov.cz/>

Pro účely komunikace s API v rámci EDU prostředí je možné využívat stejné typy komerčních serverových certifikátů jako pro produkční prostředí dle kap. 2.2 a navíc je pro EDU prostředí možné využívat testovací komerční serverové certifikáty od První certifikační autority, a.s. a České pošty, s.p. (provozovatel certifikační autority PostSignum).

#### 2.3.1 Testovací data

Na EDU prostředí je k dispozici výběr několika testovacích datových sad občanských průkazů. Tyto sady se liší v tom, jaké všechny atributy obsahují. Jsou zde přítomny testovací sady, které obsahují

pouze povinné atributy. Také je zde dostupná testovací sada, která obsahuje maximální možnou množinu hodnot atributů občanského průkazu.

Kromě simulované sady občanských průkazů je na EDU prostředí také možnost vybrat druh simulovaného scénáře průběhu procesu ověření. Tímto lze otestovat nestandardní situace, které mohou při ověření nastat. Tyto scénáře jsou popsány níže.

#### PLATNÝ DOKLAD

V tomto scénáři se simuluje situace, kdy držitel poskytne digitální stejnopis platného občanského průkazu podle zvolené testovací sady. Pokud ovšem ověřovatel provede vyžádání atributu, **který vybraný testovací občanský průkaz nemá**, tak dojde k výsledku ověření MISSING\_DATA. To může nastat v reálné situaci třeba tím způsobem, že si ověřovatel řekne o atribut „titul“, který je ovšem nepovinný, a držitel ho nemusí mít na občanském průkaze.

#### NEDŮVĚRYHODNÝ DOKLAD

Tento scénář simuluje situaci, kdy držitel se prokáže digitálním stejnopisem občanského průkazu, který je opečetěn pomocí nedůvěryhodného certifikátu. V této situaci by neměl ověřovatel takovýto stejnopis akceptovat, protože se může jednat o podvrh.

#### TIMEOUT

Simulace scénáře, kdy nedojde ke včasnému dokončení transakce.

#### NEZNÁMÁ CHYBA

Simulace scénáře, kdy dojde na straně Webové ověřovací aplikace k neočekávané chybě při zpracování údajů z digitálního stejnopisu občanského průkazu.

#### EXPIROVANÝ DIGITÁLNÍ STEJNOPIS DOKLADU

Simulace scénáře, kdy se držitel prokáže digitálním stejnopisem občanského průkazu, který již ale není platný. Digitální stejnopisy průkazů mají platnost 48 hodin po vystavení do mobilní aplikace eDoklady.

#### DRŽITEL ÚDAJŮ ODMÍTL PŘEDÁNÍ ÚDAJŮ

Simulace scénáře, kdy držitel dokladů odmítl jejich předání.

## 3. Integrace s Webovou ověřovací aplikací

Webová ověřovací aplikace poskytuje několik způsobů integrace. Každá integrace může být vhodná pro odlišné typy organizací.

### 3.1. Varianta 1. – Export do schránky

Tato varianta umožňuje ověřovateli po zobrazení obdržených údajů ve Webové ověřovací aplikaci provést jejich export do schránky. Lze exportovat pouze ty údaje, ke kterým byl vyžádán souhlas s jejich dalším zpracováním.

Funkcionalita exportu údajů do schránky byla nasazena do produkce dne 2. května 2024.

Data jsou exportována v JSON formátu a mají následující strukturu:



Tabulka 0-4 Schéma JSON formátu

Cesta v JSON	Popis	Ukázka hodnoty
presentationResult	Výsledek ověření předaných údajů. Možné hodnoty jsou: <ul style="list-style-type: none"> <li>SUCCESS – předané údaje jsou validní</li> <li>UNTRUSTED – předané údaje nejsou důvěryhodné</li> <li>EXPIRED – vypršela časová platnost předaných údajů</li> </ul>	SUCCESS
exportedAt <sup>2</sup>	Datum a čas vytvoření daného exportu. Formát je dle normy ISO 8601.	2024-11-22T10:00:00Z
presentedDocuments	Pole obdržených digitálních stejnopisů. V současné implementaci zde bude zatím pouze jeden (občanský průkaz).	
presentedDocuments.name	Identifikátor typu digitálního stejnopisu.	org.iso.18013.5.1.CZ.mID
presentedDocuments.validTo	Časové razítko s dobou platnosti obdrženého mDoc digitálního stejnopisu.	1713965019
presentedDocuments.validFrom	Časové razítko začátku doby platnosti obdrženého mDoc digitálního stejnopisu.	1713792219
presentedDocuments.credentials	Pole obdržených atributů.	
presentedDocuments.credentials.name	Identifikátor atributu.	portrait
presentedDocuments.credentials.attributeDataType	Typ hodnoty, viz Tabulka 0-1 - Datové typy hodnot atributů	STRING
presentedDocuments.credentials.value	Hodnota atributu.	Jan
presentedDocuments.mDoc	Digitální stejnopis v mDoc CBOR formátu. Obsahuje mDoc dle standardu ISO-18013-5.	

Ukázkový JSON soubor je obsažen v příloze export-ukázka.json.

### 3.2. Varianta 2. – Integrovaní API Browser flow

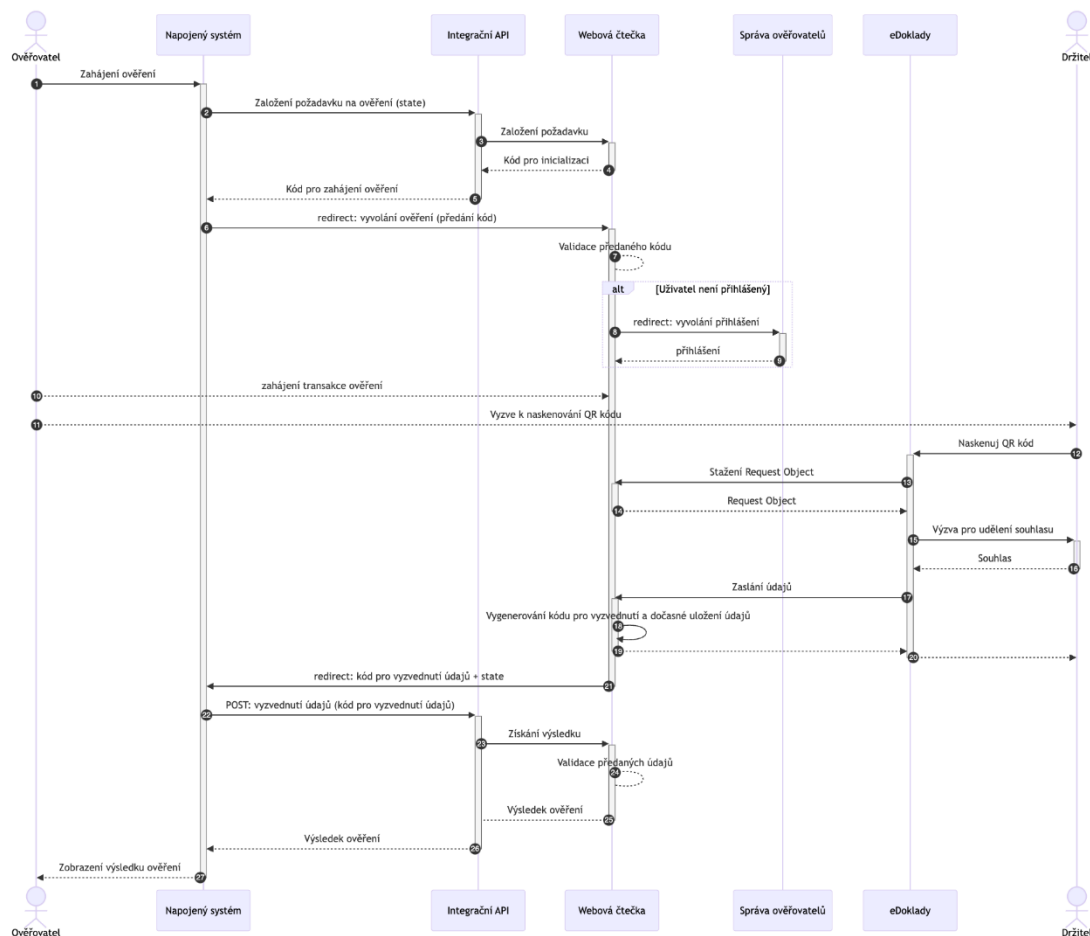
Tato varianta popisuje způsob integrace s Webovou ověřovací aplikací, která používá její grafické webové rozhraní a Integrovaní API. Webové rozhraní je použito pro výběr sady údajů pro ověření. Integrovaní API je použito pro vyzvednutí získaných údajů.

<sup>2</sup> Aktuálně na produkci nasazeno není, předpokládáme nasazení v následujícím release.

### 3.2.1. Popis procesu ověření

Integrační API je popsáno v přílohách **webová-čtečka-api.yml** a **integrační-api.yml**.

Níže je zobrazen sekvenční diagram znázorňující proces ověření pomocí Browser flow.



Obrázek 1 Sekvenční diagram Browser flow

Jednotlivé kroky jsou popsány níže:

1. Ověřovatel v napojeném systému zahájí proces ověření údajů
2. Napojený systém založí přes Integrační API požadavek na provedení ověření. Napojený systém v tomto volání specifikuje návratovou URI adresu a volitelně **state** parametr, který je případně vrácen zpět při přesměrování do napojeného systému. Tento parametr může napojený systém použít pro identifikaci odpovědi z Webové čtečky. Endpoint je detailně popsán v příloze **integrační-api.yml**, operace **requestBrowserPresentation**.
3. Webová čtečka založí požadavek na ověření údajů a vrátí **code** parametr, který je potřeba následně použít při přesměrování prohlížeče na Webovou čtečku.
4. Vrácení **code** parametru.
5. Vrácení **code** parametru do napojeného systému.
6. Napojený systém provede přesměrování webového prohlížeče na danou adresu webové čtečky. V rámci tohoto přesměrování systém musí předat **code** parametr z předchozího volání.

- a) Endpoint je detailně popsán v příloze **webová-čtečka-api.yml**, operace **requestBrowserFlowPresentation**
  - b) Seznam údajů, o které je možné požádat, je specifikován v kapitole Podporované digitální stejnopisy
7. Validace obdrženého **code** parametru.
  8. Pokud ověřovatel není přihlášený, webová čtečka zahájí proces přihlášení.
  9. Ověřovatel se „vrací“ přihlášený do webové čtečky.
  10. Ověřovatel vybere přepážku, sadu pro ověření a zahájí proces ověření.
  11. Ověřovatel vyzve držitele eDokladů k naskenování QR kódu přepážky, ke které je daný ověřovatel přihlášen.
  12. Držitel eDokladů naskenuje QR kód.
  13. Aplikace eDoklady stáhne Request Object, ve kterém je seznam požadovaných údajů pro předání.
  14. Zaslání Request Object.
  15. Aplikace eDoklady si vyžádá souhlas s předáním údajů.
  16. Držitel eDokladů udělí souhlas.
  17. Zaslání údajů do Webové čtečky.
  18. Dojde k dočasnému uložení předaných údajů a vygenerování kódu (**code**), který je potřebný pro jejich následné vyzvednutí přes Integrační API. K vyzvednutí údajů musí dojít do 10 minut od té doby, co byly přijaty na Webové čtečce.
  19. Konec komunikace z pohledu aplikace eDoklady.
  20. Zobrazení informace o předání údajů držiteli eDokladů.
  21. Přesměrování prohlížeče na požadovanou URI. Při tomto přesměrování dojde k předání parametrů **code** a **state**.
  22. Napojený systém pomocí předaného **code** parametru a svého SSL autentizačního certifikátu provede vyzvednutí obdržených údajů. Volání daného endpointu je detailně popsáno v příloze **integrační-api.yml**, operace **getBrowserFlowTransactionResult**.
  23. Získání výsledku z Webové čtečky.
  24. Kontrola obdržených údajů. Údaje jsou rozparsovány a validovány
  25. Vrácení výsledku ověření údajů.
  26. Předání údajů. Integrační API vrací výsledek validace obdržených údajů a samotné obdržené údaje. Struktura vrácených údajů je popsána v příloze **integrační-api.yml**, operace **getBrowserFlowTransactionResult**.
  27. Napojený systém zobrazí obdržené údaje.

V případě, kdy ověřující subjekt potřebuje export obdržených údajů do PDF souboru, tento export si může ověřující subjekt vytvořit na vlastní straně s využitím obdržených údajů pomocí vlastních procesů.

### 3.3. Varianta 3. – Integrovaný API Server flow

Tato varianta je založená pouze na serverové komunikaci s integrovaným API Webové čtečky. Tato varianta počítá s tím, že si napojený systém bude přes API Webové čtečky spravovat QR kódy a sám bude řešit jejich zobrazení. Zobrazení QR kódu může být řešeno například vtištěním na papír nebo zobrazením na monitoru.

#### 3.3.1. Virtuální přepážka

QR kódy budou vázány na tzv. Virtuální přepážky. Na virtuální přepážky budou také vázány jednotlivé procesy ověření.

Je na napojeném systému, jak bude s virtuálními přepážkami pracovat. Jeden způsob využití je například založení virtuální přepážky pro každou fyzickou přepážku. Další způsob je vytvoření virtuální přepážky pro každého uživatele napojeného systému.

Po založení virtuální přepážky se automaticky vygenerují data pro QR kód (na straně Webové čtečky). Tyto data mají stanovenou dobu platnosti. Po této době je nutné pro danou přepážku vygenerovat nový QR kód.

API pro správu přepážek je popsáno v příloze **integrovaný-api.yml**. Jednotlivé endpointy jsou označeny tagem `virtualServiceCounters`.

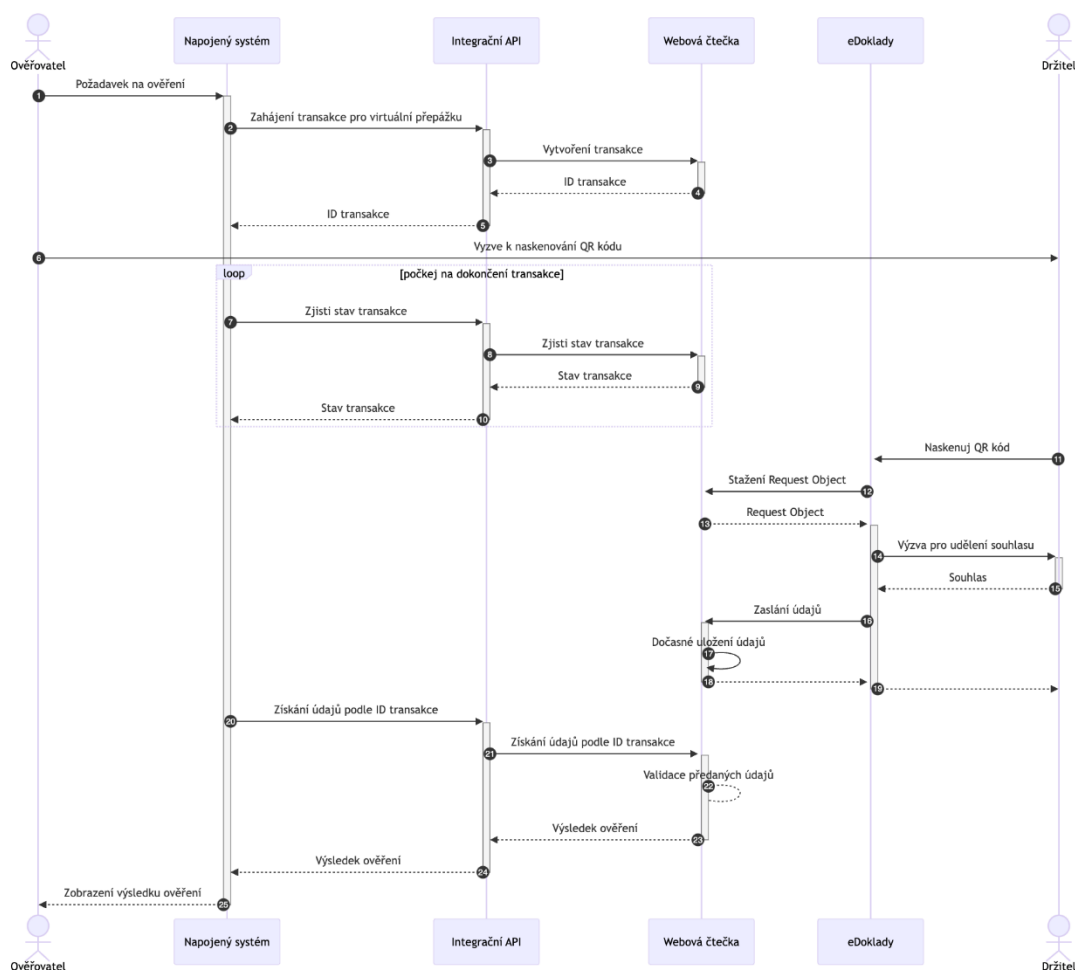
Dostupné operace pro virtuální přepážky:

- Vytvoření
- Editace
- Smazání
- Vygenerování dat pro nový QR kód.

#### 3.3.2. Popis procesu ověření

Integrovaný API je popsáno v příloze **integrovaný-api.yml**.

Proces ověření je znázorněn na sekvenčním diagramu níže.



Obrázek 2 Sekvenční diagram Server flow

Jednotlivé kroky jsou popsány níže:

1. Ověřovatel v napojeném systému zahájí proces ověření údajů
2. Napojený systém zavolá Integrovaná API pro zahájení nového procesu ověření – **transakce**. Při tomto volání napojený systém specifikuje virtuální přepážku, pro kterou chce zahájit proces ověření. Také při tomto volání specifikuje množinu údajů, které chce získat od držitele eDokladů. Endpoint je detailně popsán v příloze **integrovaná-api.yml**, operace **requestServerFlowPresentation**
3. Webová čtečka zahájí novou **transakci** pro danou sadu údajů a danou přepážku.
4. Vrácení **ID transakce** do Integrovaného API.
5. Vrácení **ID transakce**, která byla založena ve webové čtečce do napojeného systému.
6. Ověřovatel vyzve držitele k naskenování QR kódu, který náleží **virtuální přepážce**, pro kterou byla zahájena daná **transakce**.
7. Systém volá Integrovaná API, aby zjistil stav dané transakce. Endpoint je detailně popsán v příloze **integrovaná-api.yml**, operace **getServerFlowTransaction**. Tento endpoint by měl být volán pro každou transakci s prodlevou alespoň 2 sekund, aby nedocházelo ke zbytečnému zatížení systému Webové čtečky.
8. Zjištění stavu transakce ve Webové čtečce.
9. Vrácení stavu transakce.

10. Vrácení stavu transakce.
11. Držitel eDokladů naskenuje QR kód.
12. Aplikace eDoklady stáhne Request Object, ve kterém je seznam požadovaných údajů pro předání.
13. Zaslání Request Object.
14. Aplikace eDoklady si vyžádá souhlas s předáním údajů.
15. Držitel eDokladů udělí souhlas.
16. Zaslání údajů do Webové čtečky.
17. Dočasné uložení obdržených údajů. K vyzvednutí údajů musí dojít do 10 minut od té doby, co byly přijaty na Webové čtečce.
18. Konec komunikace z pohledu aplikace eDoklady.
19. Zobrazení informace o předání údajů držiteli eDokladů.
20. Napojený systém pomocí **ID transakce** a svého SSL autentizačního certifikátu provede vyzvednutí obdržených údajů. Endpoint je detailně popsán v příloze **integrační-api.yml**, operace **getServerFlowTransactionResult**
21. Získání výsledku z Webové čtečky.
22. Kontrola obdržených údajů. Údaje jsou rozparsovány a validovány
23. Vrácení výsledku ověření údajů.
24. Předání údajů. Webová čtečka vrací výsledek validace obdržených údajů a samotné obdržené údaje. Struktura vrácených údajů je popsána v příloze **integrační-api.yml**, operace **getServerFlowTransactionResult**.
25. Napojený systém zobrazí obdržené údaje.

V případě, kdy ověřující subjekt potřebuje export obdržených údajů do PDF souboru, tento export si může ověřující subjekt vytvořit na vlastní straně s využitím obdržených údajů pomocí vlastních procesů.

## 4. Správa lokálních účtů

V rámci Správy ověřovatelů je možné přes integrační API spravovat lokální účty (tj. účty, při kterých není využívána autentizace prostřednictvím ISDS nebo JIP/KAAS, ale autentizace prostřednictvím modulu interního IdP v rámci Správy ověřovatelů). Lokální účty jsou navázány vždy na konkrétní ověřující subjekt uvedený v rámci Správy ověřovatelů. Tyto účty mohou být použity pro tyto účely:

- Přihlášení do Webové čtečky
- Přihlášení do Správy ověřovatelů (pokud má účet roli Správce organizace)
- Registraci ověřovacího profilu v mobilní aplikaci eDoklady

Úprava grafického rozhraní webových aplikací eDokladů je aktuálně předmětem vývoje.

### 4.1. Organizační role

Každý lokální účet má specifikovanou organizační roli v rámci organizace. Dostupné organizační role jsou:

- VERIFIER – Ověřovatel. Tento účet lze použít na přihlášení do Webové ověřovací aplikace a pro zaregistrování ověřovacího profilu v aplikaci eDoklady.
- ADMIN – Správce organizace. Tento účet má stejné pravomoci jako ověřovatel. Navíc je s tímto účtem možné se přihlásit do Správy ověřovatelů.

### 4.2. Popis dostupných operací

Jednotlivé operace jsou detailně popsány v příloze *integrační-api.yml*.

## 5. Správa skupin

V rámci webových aplikací eDokladů je možné zakládat skupiny. Do těchto skupin je možné přiřadit uživatele ze Správy ověřovatelů. Při přiřazení uživatele do skupiny je také specifikována role, kterou uživatel má mít v rámci této skupiny. Dostupné role v rámci skupiny jsou:

- MEMBER – Člen skupiny. Tento uživatel může používat přepážky skupiny a její ověřovací sady.
- ADMIN – Správce skupiny. Tento uživatel má stejné pravomoci jako člen skupiny. Navíc může přidávat a odebírat členy, spravovat přepážky a ověřovací sady.

V rámci skupin je možné spravovat přepážky pro ověření pro Webovou ověřovací aplikaci. Přepážky jsou potom dostupné pouze uživatelům, kteří jsou do dané skupiny přiřazeni.

Ke skupinám jdou přiřadit ověřovací sady. V rámci organizací budou spravovány skupinové ověřovací sady. Tyto sady poté budou moci správci organizace a správci skupin přiřadit jednotlivým skupinám.

### 5.1. Popis dostupných operací

V rámci skupin je možné zakládat přepážky z Webové ověřovací aplikace. Dostupné operace jsou detailně popsány v příloze *integrační-api.yml*.