DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

INTEGRAČNÍ MANUÁL NA WEBOVÉ APLIKACE EDOKLADY_[1]

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] Dokument v některých kapitolách popisuje budoucí stav, jak bude implementováno, nicméně pro účely lepšího porozumění je dokument psán v přítomném čase.

OBSAH

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: ▪ true ▪ false
SEX	Pohlaví, možné hodnoty: ▪ MALE ▪ FEMALE
CHANGE_OF_DATA	Změna dokladu, možné hodnoty: ▪ NO_CHANGE – Není evidována změna OP. ▪ YES_RESIDENT_ADDRESS – Evidována změna trvalého bydliště. ▪ YES_OTHER_DATA – Evidována změna jiných údajů. ▪ YES_RESIDENT_ADDRESS_AND_OTHER_DATA – Evidována změna trvalého bydliště a jiných údajů.
IMAGE	Base64 kódovaný obrázek

1.2. Podporované digitální stejnopisy

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

1.2.1. Občanský průkaz

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

Tabulka 0-2 Schéma atributů občanského průkazu

Název	Popis	Datový typ	Povinné[2]
portrait	Fotografie držitele	PHOTO	ANO
family_name	Příjmení	STRING	ANO
given_name	Jméno	STRING	ANO
resident_address	Trvalý pobyt	STRING	ANO
personal_number	Rodné číslo	STRING	ANO
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

[2] 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.

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.
- eIdentity a. s.
- Správa základních registrů (vydávání nových certifikátů bylo ukončeno, nicméně existující komerční serverové certifikáty je případné 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).

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:

Cesta v JSON	Popis	Ukázka hodnoty
presentationResult	Výsledek ověření předaných údajů. Možné hodnoty jsou: ▪ SUCCESS – předané údaje jsou validní ▪ UNTRUSTED – předané údaje nejsou důvěryhodné ▪ EXPIRED – vypršela časová platnost předaných údajů	SUCCESS
exportedAt[3]	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 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] Aktuálně na produkci nasazeno není, předpokládáme nasazení v následujícím release.

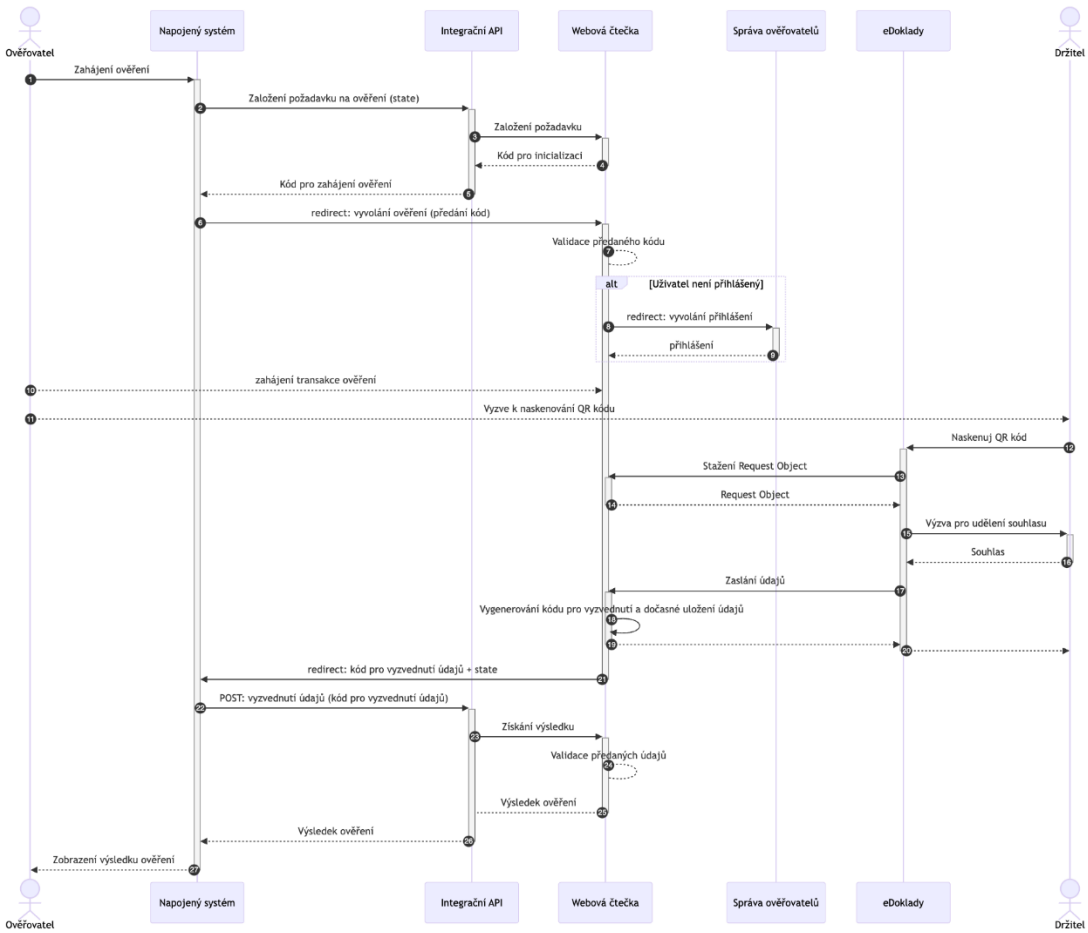
3.2. Varianta 2. – Integrační API Browser flow

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

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 přesměrovaní 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. – Integrační API Server flow

Tato varianta je založená pouze na serverové komunikaci s integračním 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 vytištěním 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 nepojeném 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 platnost. Po této době je nutné pro danou přepážky vygenerovat nový QR kód.

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

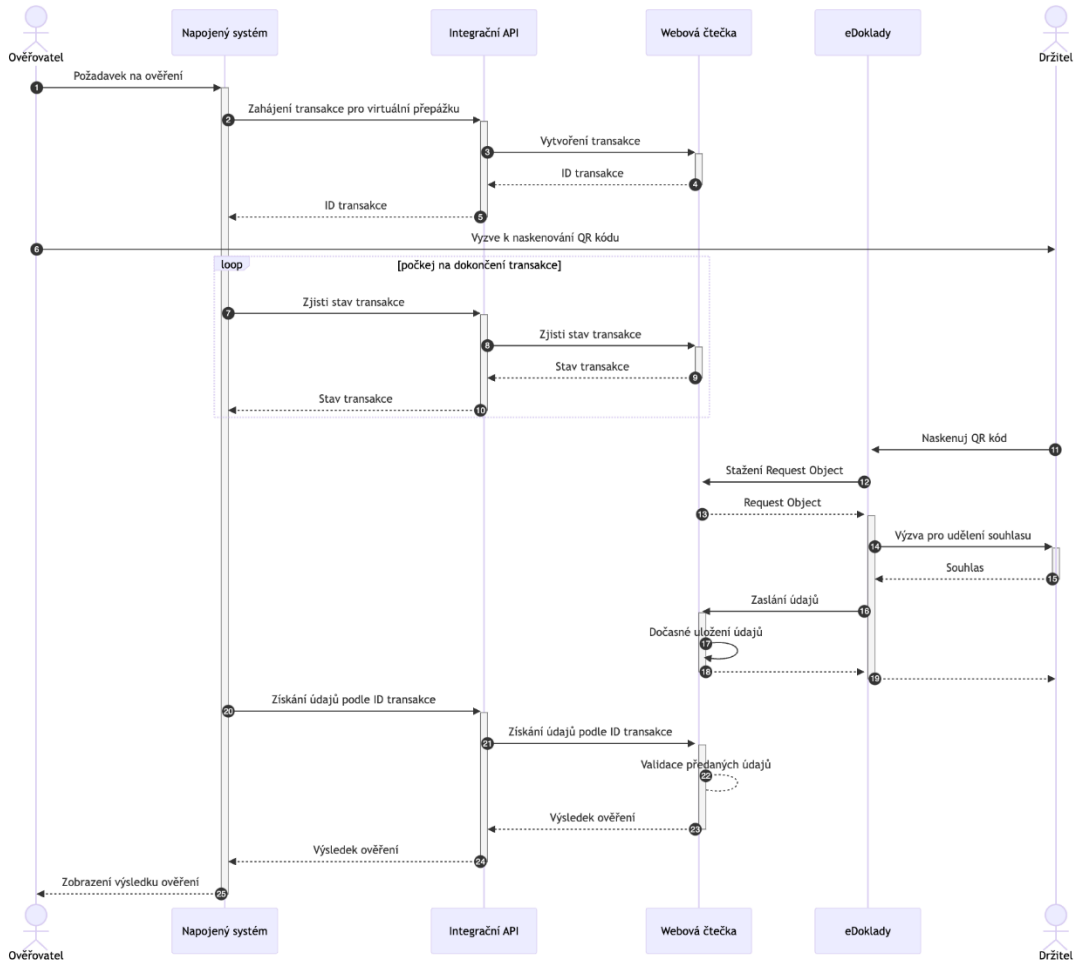
Dostupné operace pro virtuální přepážky:

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

3.3.2. Popis procesu ověření

Integrační API je popsáno v příloze ***integrační-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 Integrační 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 ***integrační-api.yml***, operace ***requestServerFlowPresentation***
3. Webová čtečka zahájí novou ***transakci*** pro danou sadu údajů a danou přepážku.
4. Vrácení *ID* ***transakce*** *do Integračního 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 Integrační API, aby zjistil stav dané transakce. Endpoint je detailně popsán v příloze ***integrační-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.

Úprava grafického rozhraní webových aplikací eDokladů je aktuálně předmětem vývoje.

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***.