Operačný program
Efektívna verejná správa

Európska únia
Európsky sociálny fond

Výstup č. 3

Overenie riešenia služby Moje dáta

Zmluva o dielo č. 334/2018 Návrh štandardov pre službu Moje dáta a manažment osobných údajov

Projekt:

Zlepšenie využívania údajov vo verejnej správe

ITMS kód projektu:

314011S979

Tento projekt je podporený z Európskeho sociálneho fondu

Obsah

1 Manažérske zhrnutie 4
2 Úvod 6
2.1 Zadanie 6
2.2 Definícia úspechu 7
2.3 Príbeh zavádzania 7
3 Prípad použitia 9
3.1 Koncept riešenia 9
3.2 Používatelia riešenia 9
3.3 Zainteresované strany 10
3.4 Model scenárov použitia 10
3.4.1 Stiahnutie aplikácie 11
3.4.2 Zobrazenie potvrdenia 11
3.4.3 Zdieľanie údajov 11
3.4.4 Manažment súhlasov - Implementované po 1.9.2019 12
3.4.5 Logovanie prístupov 13
3.4.6 Reklamácia správnosti údajov - nebude súčasť pilotu 13
3.5 Požiadavky na riešenie 13
4 Architektúra riešenia 14
4.1 Výber alternatív 14
4.2 Aplikačná architektúra 15
4.2.1 API Moje dáta - Komerčný portál 16
4.2.2 Rozhranie Moje dáta - Mobilné ID 17
4.2.3 API Moje dáta - CSRÚ 17
4.3 Aplikačné komponenty 18
4.4 Dátová architektúra 19
4.4.1 Osobný účet osoby 19
4.4.2 Potvrdenie o návšteve školy 19
4.4.3 Záznam súhlasu 22
4.4.4 Záznam stavu súhlasu 23
4.4.5 Autorizačný token 23
4.4.6 Notifikácia 24
5 Implementácia 25
5.1 Aktivity a úlohy 25
5.1.1 Vytvorenie konceptu identity a autentifikácie pre prístup k dátam o návšteve školy, návrh zoznamu oprávnených používateľov a konzumentov dát (aj v rámci CSRÚ) 25
5.1.2 Výber vhodného PIMS (Personal Information Management System) a zabezpečenie licencií pre občanov SR 26
5.1.3 Implementácia API rozhrania pre získania potvrdenia o návšteve školy v rámci Centrálnej integračnej platformy 26
5.1.4 Návrh a nastavenie systému synchronizácie dát a off-line režim 26
5.1.5 Návrh a vývoj procesu autentifikácie aplikácie (cez eID respektíve koncept mobile ID) 26
5.1.6 Nastavenie pilotného PIMS pre prácu s potvrdeniami o návšteve školy 26
5.1.7 Implementácia vizualizácie potvrdenia o návšteve školy 26

5.1.8 Návrh a vývoj konektoru medzi digi.me a Talend 26
5.1.9 Overenie návrhu konceptu riešenia na skupine budúcich používateľov 27
5.1.10 Testovanie riešenia v praxi 27
5.1.11 Nasadenie riešenia do produktívnej prevádzky a vyhodnotenie pilotnej prevádzky 27
5.2 Prehľad dostupnosti funkcionalít 27
5.3 Otvorené otázky 28
6 Aplikačné programové vybavenie 29
6.1 Riešenie prepojenia medzi komerčným portálom a aplikáciou Moje dáta 29
6.2 Mock služby 29
6.3 Ukážka integrácie s digi.mi 33

1 Manažérske zhrnutie

Experimentálny prístup

V rámci prípravy pre zavedenie služby Moje dáta sme doteraz navrhli:

- Koncept manažmentu osobných údajov vo verejnej správe, ktorý určuje základný rámec pre zavedenie služby Moje dáta, ako i príručku pre jej implementáciu,
- Štandard Open API pre Moje dáta.

Aby bolo možné navrhnuté riešenie čo najlepšie overiť v praxi, rozhranie pre službu Moje dáta bude implementované a overené na základe jednoduchého testu v rámci testovacieho prostredia centrálnej integračnom platformy. Cieľom tohto dokumentu je zadanie pre implementáciu navrhnutého štandardu API pre Moje dáta a overenie jeho vhodnosti pre vybrané reálne objekty evidencie (dostupné cez platformu integrácie údajov). Dokument tak navrhuje pilotné riešenie služby Moje dáta. Táto služba bude otestovaná na potvrdení o štúdiu pre stredoškolských študentov starších ako 16 rokov a vysokoškolských študentov. Študenti získajú prístup k potvrdeniu o návšteve školy a budú môcť zdieľať svoje potvrdenie o štúdiu tretím stranám, ktoré na neho nemajú automatický zákonný nárok, ale využívajú ho v poskytovaní svojich služieb. Overia sa tak aj nové technológie, ktoré sú so službou Moje dáta spojené, ako je mobilný e-Government, Open API pre tretie strany, bezpečný manažment osobných údajov a koncept adresných služieb. Riešenie tak pomôže implementovať GDPR a Zákon o ochrane osobných údajov v praxi, najmä § 15Podmienky poskytnutia súhlasu v súvislosti so službami informačnej spoločnosti, kde prevádzkovateľ v súvislosti s ponukou služieb informačnej spoločnosti spracúva osobné údaje na základe súhlasu dotknutej osoby zákonne, ak dotknutá osoba dovŕšila 16 rokov veku. Ak má dotknutá osoba menej ako 16 rokov, takéto spracúvanie osobných údajov je zákonné iba za podmienky a v rozsahu, v akom takýto súhlas poskytol alebo schválil jej zákonný zástupca.

Rozsah pilotného overenia: "Minimum Viable Product"

V prvej časti dokumentu je uvedená motivácia zavedenia riešenia, predstavené, čo by malo riešenie spĺňať a hlavne, kedy bude projekt vyhodnotený ako úspešný.

Ďalej je rozpracovaný spôsob použitia aplikácie. Je načrtnutý základný koncept riešenia, sú zanalyzovaní používatelia riešenia a tiež zainteresované strany. V modeli scenárov použitia sú vysvetlené prípady použitia, na ktorých bude riešenie overené. Tieto zahŕňajú:

- Stiahnutie aplikácie a personalizácia aplikácie
- Zabezpečenie prístupu k údajom a zobrazenie potvrdenia
- Zdieľanie údajov
  - Funkcionalita implementovaná do 1.9.2019
    - Zdieľanie emailom
    - Zobrazenie údajov cez PIN kód
  - Funkcionalita implementovaná po 1.9.2019
    - Zobrazenie údajov cez QR kód
    - Na základe dlhodobého súhlasu
- Manažment súhlasov
- Log prístupov k dátam

Po scenároch použitia sú uvedené požiadavky, ktoré musí riešenie spĺňať.

Architektúra pilotného overenia: použitie najmodernejších dostupných technológií v komunite MyData

Architektúra riešenia je navrhnutá v samostatnej kapitole. Je tu predstavený návrh alternatív, z ktorých je možné vybrať pri budúcom riešení. Jedna zahŕňa vývoj vlastného riešenia, druhá predstavuje využitie funkčného riešenia Digi.me. Digi.me predstavuje momentálneho lídra v riešeniach postavených na MyData. Ďalej je v kapitole spracovaná aplikačná a dátová architektúra.

Koncept riešenia tiež obsahuje návrh krokov, ktoré je potrebné realizovať pre úspešnú implementáciu od prvotných návrhov dátových prepojení po nasadenie riešenia do pilotnej prevádzky a jej vyhodnotenie. Každá aktivita má uvedenú organizáciu, ktorá je zodpovedná za jej realizáciu.

2 Úvod

Jednou z vízií Slovenska, kam sa posunúť ďalej v eGovernmente a digitálnych službách, je práca s dátami a využívanie možnosti, ktoré nám dáta ponúkajú. Zavedenie Manažmentu osobných údajov a služba Moje dáta, sú aktivity realizované s cieľom podpory tohto posunu. Vďaka nim budú mať ľudia prístup k svojim údajom a budú ich môcť spravovať. Možnosti, ktoré im služba poskytne zahŕňajú prezeranie údajov, videnie, kto k ich údajom pristupoval, možnosť reklamácie a tiež zdieľania údajov. Občanom to prinesie väčšiu kontrolu nad ich dátami a tiež zjednodušenie života vďaka možnosti zdieľania údajov s ďalšími subjektami.

V rámci realizácie aktivity bol spracovaný koncept, ako by služba Moje dáta mala fungovať a na jeho základe navrhnuté štandardy, aby služba mohla byť využívaná v praxi. Ďalším krokom je otestovanie navrhnutého riešenia. Ako vhodná služba na tento účel sa vybralo potvrdenie o návšteve školy. Navrhovaný pilot vyvinie riešenie, ktoré umožní študentom jednoducho a v bezpapierovej podobe zdieľať svoje potvrdenie o štúdiu s tretími organizáciami, ktoré nie sú štátnymi orgánmi, alebo sú štátnymi orgánmi, ale nemajú zákonný nárok na získavanie týchto dokumentov bez súhlasu študenta. Získavanie potvrdení o štúdiu pre štátne orgány, ktoré majú na tieto dokumenty zákonný nárok, je riešené v rámci iného projektu.

2.1 Zadanie

Podrobnejšie zadanie projektu je v nasledujúcej tabuľke.

Tabuľka 1: Zadanie projektu

Požiadavka	Zadanie
Vytvorenie „Proof of Concept" pre službu Moje dáta.	Služba Moje dáta bude overená na prípade **Potvrdenia o návšteve školy** Študent bude môcť vidieť tretie strany, ktoré pristupovali k jeho potvrdeniu o štúdiu cez služby Moje dáta Overí sa tiež záujem tretích strán využiť rozhranie Moje dáta pre ponuku adresných služieb.
Aby bolo možné navrhnuté riešenie čo najlepšie overiť v praxi, rozhranie bude implementované a overené na základe jednoduchého testu v rámci testovacieho prostredia centrálnej integračnej platformy.	Riešenie bude overené v praxi a reálne nasadené do produkcie v rámci aktivít druhého balíčka boja proti byrokracii (ktorého je potvrdenie o návšteve školy súčasťou). Riešenie tak musí umožniť zapojeným študentom deklarovať, že navštevujú školu, a inštitúciám overiť takúto deklaráciu (cez takzvaný komerčný portál a API).
Cieľom je implementácia navrhnutého štandardu API pre Moje dáta a overenie jeho vhodnosti pre vybrané reálne objekty evidencie (dostupné cez platformu integrácie údajov).	Riešenie bude postavené v rámci Centrálnej integračnej platformy. Objekt evidencie: Potvrdenie o návšteve školy
Výstup: Aplikačné programové vybavenie v otvorenom formáte (rozhranie služby Moje dáta)	Aplikačné programové vybavenie bude dostupné cez platformu github.

2.2 Definícia úspechu

Splnenie nasledovných cieľov bude znamenať úspešnú realizáciu projektu:

Riešenie bude funkčné

- Študent bude môcť zdieľať svoje potvrdenie o štúdiu s tretími stranami
- Tretie strany budú schopné získať potvrdenie o štúdiu
- Riešenie bude obsahovať informácie o všetkých študentoch stredných škôl na území SR od veku 16 rokov a študentoch vysokých škôl na území SR
- Riešenie bude otestované na reálnych dátach z RIS **1.9.2019**
- Riešenie bude možné používať používateľmi v testovacej prevádzke **od 1.9.2019**
- Riešenie bude nasadené do produktívnej prevádzky od 1.11.2019

Riešenie bude využívané

Tabuľka 2: Merateľné ukazovatele

Merateľný ukazovateľ	Hodnota k 1.1.2020 Stredné školy	Hodnota k 1.1.2020 Vysoké školy
Počet úspešne stiahnutých aplikácií pre Android a iOS	> 5,000	> 15,000
Počet realizovaných overení cez službu Moje dáta	> 20,000	> 80,000

Po spustení riešenia (1.9.2019) budú merateľné ukazovatele transparentne zverejňované.

2.3 Príbeh zavádzania

Zdieľanie potvrdenia o štúdiu tretím stranám bude realizované spoločne s projektom zdieľania potvrdenia o štúdiu medzi štátnymi orgánmi, ktoré majú na túto informáciu zákonný nárok. Projekt zdieľania medzi štátnymi orgánmi bude pracovať s potvrdeniami o štúdiu na základných, stredných a vysokých školách. Bude v rámci neho nastavená infraštruktúra na získavanie týchto informácií z Rezortného informačného systému Ministerstva školstva.

Zabezpečenie zdieľania potvrdení tretím stranám opisovaný v tomto zadaní využije spoločnú infraštruktúru na získavanie vstupných dát cez Centrálnu integračnú platformu. V rámci pilotného projektu bude vybudované rozhranie a infraštruktúra na zdieľanie s tretími stranami. Pilotné riešenie bude určené pre študentov starších ako 16 rokov, pretože títo môžu realizovať právne úkony a zdieľanie dát tretej strane takúto oprávnenosť vyžaduje. Žiaci do 16 rokov zároveň spadajú do povinnej školskej dochádzky a potvrdenie o návšteve školy nie je potrebné. Pilot ale navrhne podobu tohto rozhrania. Pilot bude spustený k 1.9.2019, tak aby ho študenti mohli začať využívať od nového školského roku.

Benefity riešenia

- Zvýšenie užívateľského komfortu a kontroly nad spracovaním dát pre študentov a rodičov z RIS, možnosť aktívne pracovať s týmito údajmi a používať ich v konaniach (napríklad pri cezhraničných životných situáciách)
- Zníženie rizík pri nasadzovaní riešení znižovania byrokracie do praxe (vďaka zapojeniu občanov)
- Zníženie rizík problémov pri spracovaní osobných údajov, nesúladu s GDPR a podobne

- Ušetrenie času pri spracovaní potvrdení o návšteve školy pre konzumentov, možnosť automatizácie procesov
- Overenie konceptu mobilnej identity

3 Prípad použitia

3.1 Koncept riešenia

Riešenie sprístupnenia potvrdenia o návšteve školy cez službu Moje dáta bude realizované prostredníctvom mobilnej aplikácie. Študent bude môcť v tejto aplikácii realizovať všetky navrhované funkcionality, ako prezeranie potvrdenia, jeho zdieľanie a sledovanie, kto k potvrdeniu vo verejnej správe pristupoval a prečo. Údaje do aplikácie budú zabezpečené súčasne realizovaným projektom pre zdieľanie potvrdení o návšteve školy v rámci inštitúcii verejnej správy. Ide o súčasť programu Manažment údajov, ktorého zámerom je zavedenie princípu „jeden-krát a dosť“ úpravou legislatívy a technickými prostriedkami (dátová integrácia s Centrálnou integračnou platformou). Týmto spôsobom bude na Centrálnu integračnú platformu pripojený aj Rezortný informačný systém Ministerstva školstva SR (RIS), ktorý eviduje informácie o štúdiu na školách v rámci SR a získava ich z jednotlivých školských informačných systémov. Používateľ z verejnej správy získa prístup k potvrdeniu o návšteve školy cez portál over.si alebo si ho zobrazí priamo vo svojom informačnom systéme (ak bola realizovaná dátová integrácia). Tieto prístupy k potvrdeniu o návšteve školy budú evidované v rámci logu a dostupné cez službu Moje dáta.

Služba Moje dáta umožní systematický manažment osobných údajov, ktoré sú evidované v informačných systémoch verejnej správy. Znamená to, že používateľ bude môcť získať aktuálnu verziu dát, ktoré sú o ňom evidované, zdieľať údaje a udeľovať súhlas tretím stranám pre prístup k údajom (tretie strany, ktoré nemajú prístup k údajom zo zákona).

Študent sa bude musieť do aplikácie Moje dáta prihlásiť, aby bolo zabezpečené, že aktivity s dátami vykonáva oprávnená osoba. Zdieľanie potvrdenia o štúdiu bude prebiehať prostredníctvom zaslania emailu alebo prostredníctvom dočasného súhlasu (vygenerovaného PIN kódu). Používateľ mimo verejnej správy (napríklad zamestnanec banky, čo udeľuje zvýhodnené produkty pre študentov; zamestnanec dopravného podniku) bude môcť pristupovať k potvrdeniu o návšteve školy cez takzvaný Komerčný portál (KP).

Jedná sa o webové rozhranie, ktoré zobrazí potvrdenie o štúdiu po vložení PIN kódu spojeného s dočasným súhlasom, ktorý udelí študent pracovníkovi prostredníctvom aplikácie priamo na mieste počas spoločnej interakcie. Tretí spôsob zdieľania bude prebiehať na základe súhlasu udeleného študentom na pozadí cez API. V rámci pilotného overenia bude vypracovaný návrh riešenia tohto tretieho spôsobu zdieľania.

3.2 Používatelia riešenia

Návrh zoznamu oprávnených používateľov a konzumentov dát:

- Študent strednej a vysokej školy od 16 rokov - bude využívať funkcionalitu riešenia určenú pre študenta. Pre využívanie riešenia bude študent bude musieť byť autentifikovaný.
- Tretie strany - Budú získavať prostredníctvom riešenia potrebné potvrdenia o štúdiu. Môže sa jednať o dopravcov, banky alebo iné spoločnosti, zohľadňujúce štatút študenta v svojich službách. Tretie strany nemusia byť v pilotnom riešení autentifikované.

Súčasťou riešenia bude vytvorenie konceptu identity, autentifikácie a autorizácie.

3.3 Zainteresované strany

Tabuľka 3: Zoznam zainteresovaných strán

Kategória	Zainteresovaná strana	Postavenie podľa GDPR
Poskytovateľ dát	stredné školy a vysoké školy budú vydávať potvrdenia o štúdiu pre svojich študentov dáta zo všetkých škôl sú konsolidované v Rezortnom informačnom systéme	Prevádzkovateľ
Konzument dát	tretie strany, ktoré potrebujú získať potvrdenie o štúdiu	Prevádzkovateľ
Správca dát	Ministerstvo školstva, vedy, výskumu a športu SR (MŠ SR) Rezortný informačný systém	Prevádzkovateľ
Operátor	Úrad podpredsedu vlády SR pre investície a informatizáciu (ÚPVII) prevádzkovateľ riešenia Centrálnej integračnej platformy (starší názov je CSRÚ – Centrálna správa referenčných údajov) prevádzkovateľ pilotného riešenia pre Manažment osobných údajov (MOÚ), ktoré zabezpečuje autentifikáciu, autorizáciu a funkčnosť riešenia, ako napríklad možnosť zasielania potvrdení riešenia o štúdiu emailom. V pilotnom riešení bude túto úlohu plniť služba Digi.me	Sprostredkovateľ

3.4 Model scenárov použitia

Návrh scenárov použitia potvrdenia o návšteve školy v praxi, vrátane sekvenčných diagramov pre prístup k dátam a spracovanie dát.

Scenáre použitia pre študenta sú uvedené v nasledujúcej tabuľke.

Tabuľka 4: Podporované scenáre použitia v pilotnom riešení

ID	Scénar použitia	Dôležitosť
Realizované do 1.9.2019		
1.	Stiahnutie aplikácie (a personalizácia)	Kľúčová súčasť PoC
2.	Zobrazenie údajov	Kľúčová súčasť PoC
3.	Zdieľanie údajov emailom	Kľúčová súčasť PoC
4.	Zdieľanie údajov na základe jednorazového súhlasu (cez PIN kód)	Kľúčová súčasť PoC
Implementované po 1.9.2019		
5.	Logovanie prístupov	Kľúčová súčasť PoC

ID	Scénar použitia	Dôležitosť
6.	Zdieľanie údajov cez QR kód	Doplnková funkcionalita
7.	Automatické zdieľanie údajov na základe dlhodobého súhlasu	Doplnková funkcionalita
8.	Manažment súhlasov	Doplnková funkcionalita
9.	Reklamácia správnosti údajov	Nie je súčasť PoC

Scenáre použitia pre používateľa dát (tretiu stranu):

- Spracovanie potvrdenia o návšteve školy (email)
- Spracovanie potvrdenia o návšteve školy cez komerčný portál
- Overenie platnosti potvrdenia o návštevy školy
- Evidencia potvrdenia o návšteve školy

3.4.1 Stiahnutie aplikácie

Študent má záujem zdieľať svoje potvrdenie o štúdiu. Keďže navrhované pilotné riešenie je postavené na aplikácii, študent si ju musí stiahnuť a nainštalovať. Aplikácia preto bude dostupná na Google Play pre mobilnú platformu Android. Na prihlásenie do aplikácie bude potrebné, aby zadal svoje identifikačné údaje a autentifikačné údaje. Vhodný spôsob mobilnej identifikácie a autentifikácie bude predmetom overenia riešenia. Ak je používateľ aplikácie študentom, do jeho osobného šifrovaného úložiska sa mu stiahne aktuálna verzia potvrdenia o návšteve školy, s ktorou môže ďalej pracovať.

3.4.2 Zobrazenie potvrdenia

Študent si môže v aplikácii zobraziť pre neho aktuálne platné potvrdenie o návšteve školy.

3.4.3 Zdieľanie údajov

Možnosť bezpečne zdieľať údaje je kľúčová funkcionalita Mojich dát. Študent má viacero možností ako zdieľať svoje potvrdenie o návšteve školy:

- Prvou je zaslať potvrdenie na emailovú adresu (alebo zdieľať cez aplikácie dostupné na mobilnom telefóne, ako sú napríklad whatsapp, messenger, threema).
- Druhou je možnosť priamo počas interakcie, počas ktorej je vyžadované potvrdenie o návšteve školy, povoliť v aplikácii prístup k potvrdeniu. Súhlas bude spojený s PIN kódom, na základe ktorého si môže tretia strana zobraziť a uložiť požadované potvrdenie.
- Tretia možnosť, ktorá bude realizovaná až v ďalšej fáze, umožní študentovi dať službe tretej strany súhlas s prístupom k jeho potvrdeniu o štúdiu. Zistenie informácií bude potom prebiehať prostredníctvom API bez interakcie študenta.

Všetky navrhované formy zdieľania údajov je nutné pred začatím implementácie otestovať na vzorke budúcich používateľov (študenti, služby tretích strán), aby sa potvrdilo, že navrhovaná forma spĺňa očakávania a bude používaná v praxi.

3.4.3.1 Zdieľanie údajov emailom

Študent môže potvrdenie, ktoré si zobrazí na obrazovke zdieľať emailom, alebo inou dostupnou komunikačnou platformou (napríklad whatsapp, messenger, threema, signal). Potvrdenie bude zaslané v pdf formáte a bude obsahovať zaručený podpis vydávajúcej organizácie (poskytovateľ dát - RIS).

3.4.3.2 Zdieľanie údajov na základe jednorazového súhlasu (cez PIN kód)

Študent môže túto funkcionalitu využívať v situácii, keď potrebuje v daný moment preukázať, že je skutočne študentom a je k potvrdeniu tohto faktu od neho vyžadované potvrdenie o štúdiu. Aplikácia mu umožní vygenerovať PIN kód, na základe ktorého si môže druhá strana (konzument údajov) pozrieť jeho potvrdenie o štúdiu cez Komerčný portál. To bude prebiehať tak, že konzument údajov zadá získaný PIN kód do špeciálnej stránky Komerčného portálu, kde sa mu následne zobrazí potvrdenie o návšteve školy. Z tohto rozhrania bude mať možnosť si ho stiahnuť a ďalej s potvrdením pracovať. Platnosť PIN kódu bude časovo obmedzená (súčasný odhad je 1 hodina).

Jedná sa o riešenie určené špeciálne pre pilotné overenie, keďže neumožňuje zistiť, kto a kedy k danej informácii pristúpil.

3.4.3.3 Zdieľanie údajov cez QR kód - Implementované po 1.9.2019

Informácie, ktoré sú obsiahnuté v potvrdení o návšteve školy, bude možné vložiť do QR kódu, ktorý bude možné čítať a interpretovať. Aplikácia umožní jednoduchým spôsobom tento QR kód vygenerovať.

3.4.3.4 Automatické zdieľanie údajov na základe dlhodobého súhlasu - Implementované po 1.9.2019

Tretí spôsob zdieľania nebude súčasťou pilotného overenia, bude implementovaný v ďalšej fáze. Umožní študentovi vybrať organizácie a dať im súhlas k prístupu k svojmu potvrdeniu o štúdiu. Súhlas bude udeľovaný prostredníctvom rozhrania v aplikácii. Súhlas bude obsahovať viaceré parametre, ako napríklad účel prístupu k údajom alebo časovú platnosť. Bude možné poskytnúť konzumentom dát jednorazový ale aj časovo neobmedzený súhlas, ktorý im umožní, na základe notifikácií získavať informácie o zmenách, ktoré sa udejú. Tretia strana tak bude vedieť získať informáciu, že študent je v ďalšom ročníku, prípadne že ukončil štúdium. Získavanie informácii bude prebiehať prostredníctvom Open API. Riešenie musí byť jednoduché a jediná nutná interakcia študenta bude pri udeľovaní súhlasu. Na jeho základe bude poskytovateľovi a konzumentovi dát zaslaný token, ktorý umožní konzumentovi dát za splnení podmienok v súhlase pristúpiť k odsúhlasenému datasetu. Tretia strana tak získa potvrdenie o štúdiu.

Aby tretie strany (konzumenti dát) mohli využívať túto formu získavania informácií, budú sa musieť zaregistrovať v Centrálnom registri služieb (plánovaná súčasť Modulu MOÚ). Poskytnú tu informácie napríklad o svojich komunikačných rozhraniach.

V prípade, ak chce tretia strana pristupovať k údajom a nemá udelený súhlas, používateľ bude v aplikácií notifikovaný o požiadavke na prístup, ktorá môže byť povolená, alebo zamietnutá.

3.4.4 Manažment súhlasov - Implementované po 1.9.2019

Táto funkcionalita umožní používateľovi spravovať svoje udelené dlhodobé súhlasy. Umožní mu prezerať udelené súhlasy, vrátane detailných informácií, ako kedy alebo komu boli udelené a ako boli tieto súhlasy využívané. Bude tu môcť vytvárať a udeľovať nové súhlasy, meniť podmienky aktuálne platných alebo pozastavovať a rušiť ich platnosť.

3.4.5 Logovanie prístupov

Používateľ bude vidieť informácie, kto pristúpil k jeho údajom na základe zákonného nároku (platí pre prístup cez Centrálnu integračnú platformu) a na základe súhlasu. Pri zdieľaní emailom nebude možné zistiť, či a kým bolo toto potvrdenie zobrazené. Pri zobrazení PIN kódom bude vytvorený záznam o tejto udalosti.

3.4.6 Reklamácia správnosti údajov - nebude súčasť pilotu

V službe sa môžu objavovať dáta, ktoré nebudú súhlasiť so skutočnosťou. Je preto dôležité, aby mal používateľ možnosť reklamovať tieto dáta. Aplikácia umožní jednoduchým spôsobom zaslať informáciu, že zobrazené potvrdenie o štúdiu nesúhlasí so skutočnosťou. Operátor následne službe poskytujúcej potvrdenia poskytne reklamáciu, ktorá k nej zaujme stanovisko. Informácia o stave riešenia a jeho výsledku bude poskytovaná používateľovi.

Táto funkcionalita je nutná, aby sa v systéme odstraňovali chyby a zabezpečovala sa tým jeho dôveryhodnosť.

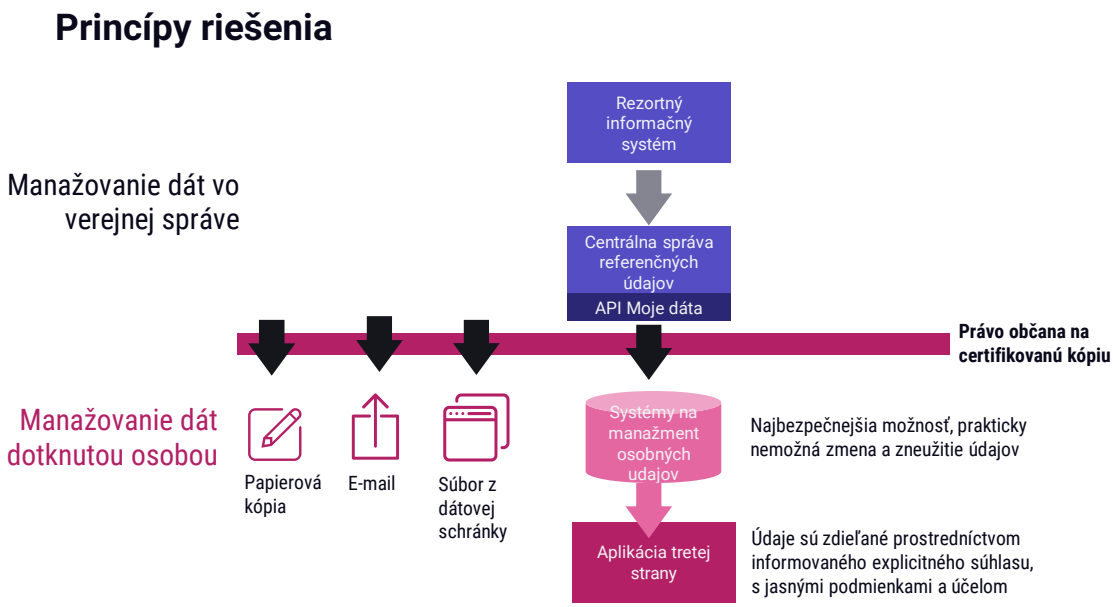
Funkcionalita reklamácie správnosti údajov nebude súčasťou pilotného overenia.

3.5 Požiadavky na riešenie

ID	Kategória	Požiadavka
1.	Mobilná aplikácia	Mobilná aplikácia Moje dáta je dostupná pre platformy: Android
2.		Mobilná aplikácia Moje dáta umožňuje dôveryhodnú personalizáciu (cez vybrané spôsoby autentifikácie)
3.	Použitie potvrdenia o návšteve školy	Potvrdenie o návšteve školy je možné zobraziť a bezpečne uložiť v mobilnej aplikácií
4.		Potvrdenie o návšteve školy bude možné zdieľať cez email (vo formáte podpísaného PDF)
5.		Pre prístup k potvrdeniu cez komerčný portál bude generovaný dočasný súhlas spojený s PIN kódom: riešenie musí zabezpečiť overenie PIN a zaslanie súhlasu pre tretiu stranu
6.		Pre KP bude navrhnuté špeciálne API, ktoré umožní zdieľať potvrdenie o návšteve školy na základe súhlasu
7.		Návrh funkčného spôsobu ako potvrdenie o návšteve školy zobraziť ako QR kód
8.	API	Potvrdenie o návšteve školy bude dostupné prostredníctvom API na základe manažmentu súhlasov
	Log	V rámci mobilnej aplikácie používateľ uvidí, kto pristupoval k jeho údajom (v rámci Centrálnej integračnej platformy)

4 Architektúra riešenia

Obrázok 1: Architektonické princípy riešenia



4.1 Výber alternatív

Alternatíva 1: Vývoj nového riešenia

Vývoj nového riešenia postaveného na princípoch Moje dáta môže implementovať API zo štandardu MyData.org. Znamená to, že sa vytvorí pilotná aplikácia (prototyp), ktorý dokáže pokryť definované prípady použitia.

Alternatíva 2: Integrácia s fungujúcim systémom na manažment osobných údajov (PIMS)

Použitie digi.me

Digi.me je existujúce softwarové riešenie pracujúce na princípoch Moje dáta. V rámci pilotnej prevádzky Moje dáta bude jeho úloha poskytovanie funkcionality služby Moje dáta, ako správa osobných účtov, súhlasy, notifikácie a prenos potvrdení o štúdiu z platformy Talend do Komerčného portálu.

Digi.me obsahuje kľúčové komponenty potrebné na spustenie pilota. Bude potrebné vytvoriť požadované prepojenia a prispôsobiť súčasnú funkcionalitu služby.

Digi.me je implementované spôsobom, aby umožnilo realizáciu práv vyplývajúcich GDPR a riešenie je budované spôsobom, aby dokázalo realizovať inovácie v oblasti osobných údajov a ich ochrany.

Digi.me ako software je v súčasnosti plne funkčné a zahŕňa:

- Prepojenie na:
  - Zdravotnícke údaje, funkčné v USA, VB, na Islande a ďalšie sú vo vývoji
  - Sociálne siete
  - Finančné služby
  - Nositeľné technológie (wearables)
  - Mediálne služby

- Bezpečné individuálne úložisko dát na jednej zo služieb ako napríklad MS One Drive, Dropbox, Google drive a iné. Používateľ si vyberá, ktorú službu chce použiť. Osobné dáta sú na vybranom úložisku šifrované. Ich obsah nemožno editovať, len ho vidieť po zadaní master hesla do mobilnej aplikácie digi.me. Digi.me nikdy nevidí, nepoužíva a nedrží používateľské dáta. Len ich šifrovane sprostredkováva oprávneným tretím stranám.
- Aplikáciu pre iOS a Android
- Funkčný proces práce so súhlasmi, ktorý umožňuje zdieľanie údajov s tretími stranami
- Vysokú úroveň bezpečnosti:
  - Digi.me bolo bezpečnostne preverené na úroveň práce so zdravotníckymi údajmi.
  - Preverené a schválené verejnými inštitúciami na ochranu dát
  - Podstúpila analýzu, ktorá preukázala schopnosť sledovateľnosti údajov
  - Plne kompatibilné s GDPR

Tabuľka 5: Výber alternatív

ID	Kritérium	Alt 1	Alt 2
1.	Dostupná funkcionalita		X
2.	Náklady		X
3.	Nezávislosť	X	
4.	Bezpečnosť		X
5.	Stabilita		X

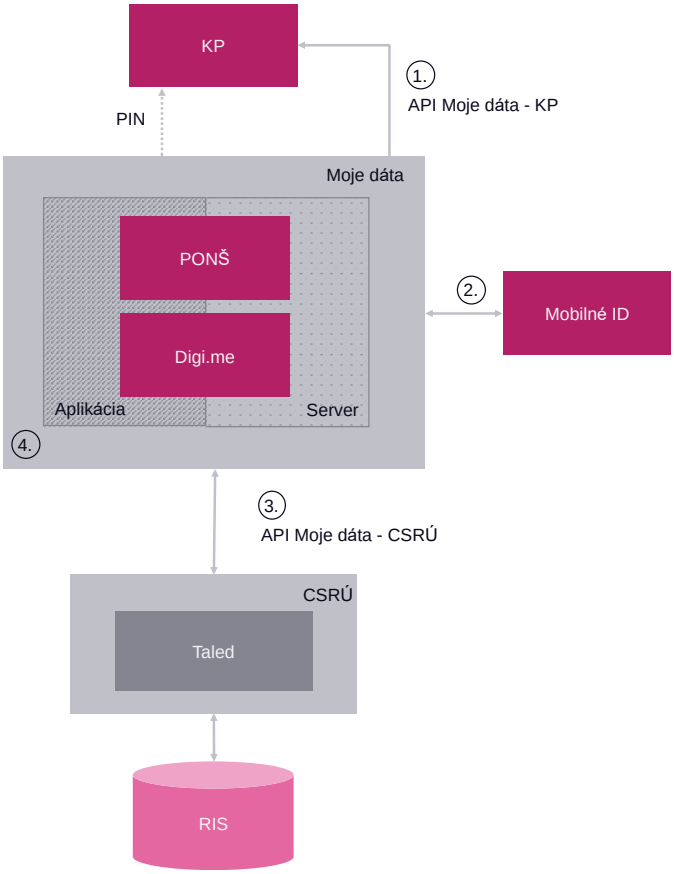
Na základe posúdenia kľúčových parametrov sa ako najlepšia možnosť, ktorou postupovať, ukázala alternatíva 2 - využiť koncept digi.me.

4.2 Aplikačná architektúra

Tabuľka 6: Kľúčové komponenty pilotného riešenia

ID	Komponent
1.	API Moje dáta – Komerčný portál
2.	API pre mobilnú autentifikáciu
3.	API Moje dáta – CSRÚ (konektor na Centrálnu správu referenčných údajov)
4.	Aplikácia Moje dáta

Obrázok 2: Aplikačná architektúra



4.2.1 API Moje dáta - Komerčný portál

Používatelia:

- Aplikácia Moje dáta (AMyD) v roli Klientska aplikácia
- Server Moje dáta (SMyD) v roli Operátor
- Komerčný portál (KP) v roli Konzumenta dát

Scénar použitia:

1. Vygenerovanie súhlasu:
   - Používateľ študent v AMyD vygeneruje dočasný súhlas na zdieľanie údajov, ktorý je spojený s jedinečným {pin}. Na prístup k svojmu osobnému účtu prostredníctvom AMyD využije používateľ Externé API pre osobný účet. Súhlas bude Operátorovi zasielaný prostredníctvom API UI Operátora.
2. Získanie súhlasu na strane KP:
   - Používateľ KP vloží {pin} a volá API SMyD pre konzumetov dát **/consent/{pin},** ID Inštancie KP, ID Užívateľa (nepovinné), ID Organizácie (nepovinné), Účel
   - API mu vráti dátový objekt súhlasu s ID AMyD, vrátane ID AMyD.
   - KP si uloží súhlas pre potreby volania ďalšej služby
3. Dátový prenos:

- KP volá API SMyD **/confirmation_of_school_attendance/{consent},** pričom ako vstupné parametre vyplní: ID Inštancie KP, ID AMyD, ID Užívateľa ? (nepovinné), ID Organizácie ? (nepovinné), Typ požadovaného výstupu
- Ak je súhlas v poriadku, API vráti na základe typu požadovaného výstupu:
  - pdf,
  - podpísaný pdf kontajner,
  - link na dočasne platnú vizualizáciu pdf,
  - xml (dátová štruktúra potvrdenia).
- SMyD zaznamená informáciu o prístupe, generovanú automaticky, a o úspešnom alebo neúspešnom dátovom prenose na základe súhlasu do transparentného logu AMyD
- Ak je dátový prenos úspešný a KP dokázal dátový objekt spracovať, KP volá API pre notifikácie **/notifications**, ktorým oznamuje SMyD, že údaje boli úspešné spracované v danom čase a daným spôsobom.
- Táto notifikácia sa následne zapíše do transparentného logu AMyD.

4.2.2 Rozhranie Moje dáta - Mobilné ID

Riešenie mobilnej autentifikácie bude otestované pre služby dostupné k 15.7.2019. Uvažuje sa s overením nasledujúcich služieb:

- Služba DCOM (spoločnosť PoSAM)

Počíta sa s overením riešení mobilnej identity, ktoré budú prístupné na použitie k 15.7.2019.

Rozhranie mobilnej autentifikácie musí podporovať funkciu LOGIN s využitím IAM ÚPVS alebo alternatívny dôveryhodný spôsob.

Pre samotné zavedenie rozhrania do praxe bude realizovaný experiment v spolupráci s BRISK.

4.2.3 API Moje dáta - CSRÚ

Rozhranie popisujúce komunikáciu medzi aplikáciou Moje dáta (časť digi.me) a Centrálnou integračnou platformou bude finálne potvrdené na základe diskusie s digi.me.

Použije sa návrh RESTFul API podľa štandardu OpenAPI 2.0.

Používatelia:

- Aplikácia Moje dáta (AMyD) v roli Klientska aplikácia
- Server Moje dáta (SMyD) v roli Operátor
- Server CSRÚ v roli Poskytovateľ dát

Scenáre použitia:

Rozhranie pokrýva nasledujúce scenáre:

- Sprístupnenie údajov
- Aktualizácia údajov
- Notifikácia o zmene údajov
- Sprístupnenie logu

Sprístupnenie údajov

1. AMyD je spárovaná s identitou

  - V rámci AMyD je uložené špeciálne ID osoby (PČO) a autentifikačný token
2. AMyD cez SMyD volá službu CSRÚ/confirmation_of_school_attendance/{ID osoby}
  - ID osoby a autentifikačné údaje sú odoslané na server CSRÚ
  - Spojenie je potvrdené
  - CSRÚ vyhľadá príslušné súbory (pdf, podpísaný kontajner) a zašle ich ako odpoveď
  - Prevod potvrdenia je zaznamenaný

Aktualizácia údajov

1. AMyD je spustená a cez SMyD volá službu CSRÚ /confirmation_of_school_attendance/modification/{ID osoby}:
  - súčasťou volania je tiež id posledného potvrdenia o návšteve školy a dátum poslednej aktualizácie
  - CSRÚ zistí, či došlo k zmene a vráti túto informáciu
2. Ak došlo k zmene SMyD sa volá službu /confirmation_of_school_attendance/{ID osoby} pre potreby získania nového dokumentu a ten je následne zaslaný do AMyD

Sprístupnenie logu

Štruktúra logu:

- RČ alebo PČO ak je na vstupe
- Orgán verejnej moci
- Prístup k mojim dátam (Objekt evidencie)
- Dátum vytvorenia/Dátum nahliadnutia
- Účel nahliadnutia

Scénar:

1. AMyD je spárovaná s identitou
  - V rámci AMyD je uložené špeciálne ID osoby (PČO) a autentifikačný token
2. AMyD cez SMyD volá službu CSRÚ /log/{ID osoby}
  - ID osoby a autentifikačné údaje sú odoslané na server CSRÚ
  - Spojenie je potvrdené
  - Súčasťou volania je i dátum, od kedy sú údaje požadované
  - CSRÚ vygenerujé tabuľku prístupov k údajom (na základe interného logu)
  - CSRÚ vráti tabuľku

Notifikácia o zmene údajov

1. CSRÚ oznamuje, že došlo k zmene údajov pre dané ID osoby a objekt evidencie
2. AMyD žiada nový objekt evidencie

4.3 Aplikačné komponenty

Tabuľka 7: Prehľad aplikačných komponentov

ID	Aplikačný komponent	Popis
1	Moje dáta - Digi.me	Aplikácia a serverová časť PIMS, štandardné riešenie digi.me

ID	Aplikačný komponent	Popis
2	Moje dáta- PONŠ	Špeciálne vyvinutá aplikácia nad SDK digi.me, ktorá obsahuje špecifickú funkcionalitu potrebnú na riešenie
3	Komerčný portál	Webové portál, ktorý umožní používateľom mimo verejného sektora overovať potvrdenia o návšteve školy. Na úvod pôjde o anonymné riešenie, ktoré zobrazí pdf potvrdenia o návšteve školy na základe zadaného PIN.
4	CSRÚ	Centrálna integračná platforma postavená na technológií Talend. Zabezpečuje dátovú integráciu medzi informačnými systémami vo verejnej správe na princípe výmeny objektov evidencie. CSRÚ bude sprostredkovávať integráciu medzi RIS a praktickými aplikáciami.
5	RIS	Rezortný informačný systém - eviduje informácie o štúdiu pre školy v rámci SR a je zdrojovým systémom pre potvrdenia o návšteve školy
6	Mobilné ID	Riešenie, ktoré umožňuje dôveryhodnú identifikáciu a autentifikáciu študentov

4.4 Dátová architektúra

Použité dátové objekty:

- Osobný účet osoby
- Potvrdenie o návšteve školy
- Záznam súhlasu
- Záznam stavu súhlasu
- Autorizačný token
- Notifikácia

4.4.1 Osobný účet osoby

Informácie nachádzajúce sa v osobnom účte:

- Prihlasovacie údaje
- Základné osobné údaje
- Kontaktné údaje
- Kryptografické kľúče vlastníka účtu (minimálne verejné)
- Pripojené služby a súhlasy spolu s ich stavmi

4.4.2 Potvrdenie o návšteve školy

Dátový objekt obsahujúci potvrdenie o návšteve školy.

Vstup do systému

- Vo formáte pdf v kontajneri obsahujúcom zaručený podpis jednoznačne identifikujúci vydavateľa potvrdenia o štúdiu

Výstup zo systému

- pdf
- podpísaný pdf kontajner
- link na dočasne platnú vizualizáciu pdf

Pdf s potvrdením o štúdiu bude získavané zo systému RIS. Tento systém v poli Informácia poskytuje následné možné odpovede:

- Fyzická osoba je evidovaná ako študent resp. žiak. Podrobnosti sú uvedené viď nižšie v sekcii Štúdiá
- Fyzická osoba nie je evidovaná ako študent resp. žiak
- Fyzická osoba sa nenašla
- Našlo sa viacero fyzických osôb pre zadané vstupné údaje

Vzorové pdf je ukázané na obrázku. Obsahuje informácie o:

- Dátume a čase žiadosti
- Údaje o osobe
- Údaje o štúdiu a jeho stave
- Údaje o žiadateľovi

Obrázok 3: Vzorové pdf potvrdenia o štúdiu

Potvrdenie o návšteve školy

Dátum a čas žiadosti	05.05.2004 02:01:01		
Informácia	Fyzická osoba je evidovaná ako študent resp. žiak. Podrobnosti sú uvedené viď nižšie v sekcii Štúdiá.		

Údaje o osobe

Meno	Jana		
Priezvisko	Novákova		
Rodné priezvisko	Šiňáková		
Dátum narodenia	2009-07-08	**Rodné číslo**	095708/0157

1. Štúdium

EDUID Školy	910000155		
Názov školy	Moja skola Martinova		
Sídlo školy	Komenskeho 22/11/33, Bardejov		
Štúdium od	01.01.2018		
Školský rok	2018/2019	**Ročník**	prípravný
Forma štúdia	denná - poldenná		
Metóda štúdia	riadne štúdium		
Prerušenie od	06.01.2018	**Prerušenie do**	..
Dôvod prerušenia	Iný		
Dátum platnosti aktualizácie danej školy	03.09.2018		
Platnosť údajov k	31.10.2018		

2. Štúdium

EDUID Školy	910000193
Názov školy	Základná škola Tibora teraz Konzervatorium
Sídlo školy	Nová 1/1, Kechnec
Štúdium od	02.01.2018

4.4.3 Záznam súhlasu

Dátový objekt súhlasu obsahuje nasledujúce informácie:

Tabuľka 8: Technický popis záznamu súhlasu

Kľúč	Typ	Popis
Spoločná časť		
version	String	Verzia špecifikácie služby Moje dáta, podľa ktorej bol súhlas vytvorený
cr_id	String	ID záznamu súhlasu jednoznačne ho identifikujúce
surrogate_id	String	ID vlastníka osobného účtu
rs_description	Object	Popis dátovej zostavy
slr_id	String	ID záznamu pripojenia služby
service_description _version	String	Verzia popisu služby použitá pri udelení súhlasu
consent_proposal	Object	**Kľúč** / **Popis** url: URL adresa návrhu súhlasu (t.j. To, čo sa používateľovi zobrazilo) hash: SHA-256 hash návrhu súhlasu
iat	Integer	Čas vydania súhlasu
nbf	Integer	Čas pred ktorým súhlas nie je platný, VOLITEĽNÉ
exp	Integer	Čas po ktorom súhlas nie je platný, VOLITEĽNÉ
operator	String	ID Operátora, u ktorého bol súhlas vytvorený
subject_id	String	ID služby, ktorej bol súhlas vydaný
role	String	Poskytovateľ alebo konzument dát
Časť špecifická podľa role služby		
pop_key	JWK	[IBA POSKYTOVATEĽ DÁT]: Verejný kľúč užívateľa tokenu (konzumenta dát) ako JWK. Používa sa na overenie žiadosti o údaje. Štruktúra JWK MUSÍ obsahovať parameter „kid“.
token_issuer_key	JWK	[IBA POSKYTOVATEĽ DÁT]: Verejný kľúč vydavateľa tokenu (operátora). Používaný poskytovateľom dát na overenie tokenu autorizácie. Štruktúra JWK MUSÍ obsahovať parameter „kid“.
source_cr_id	String	[IBA KONZUMENT DÁT] Identifikuje dátovú zostavu (potvrdenie o štúdiu) u poskytovateľa dát
usage_rules[1..n]	Array of Objects	**Kľúč** / **Popis** purposeId: ID účelu

Kľúč	Typ	Popis
	datasets	Pole ID dátovej zostavy

4.4.4 Záznam stavu súhlasu

Dátový objekt súhlasu obsahuje nasledujúce informácie:

Tabuľka 9: Záznam stavu súhlasu

Kľúč	Typ	Popis
version	String	Verzia špecifikácie služby Moje dáta, podľa ktorej bol súhlas vytvorený
record_id	String	Unikátne ID záznamu stavu súhlasu
surrogate_id	String	ID vlastníka osobného účtu
cr_id	String	ID záznamu súhlasu
consent_status	String	Stav súhlasu: Aktívny / Pozastavený / Odvolaný
iat	Integer	Čas vytvorenia záznamu súhlasu
prev_record_id	String	Odkaz na ID predchádzajúceho záznamu stavu súhlasu

4.4.5 Autorizačný token

Prenos dát prebieha na základe overenia podpísaného JSON Web tokenu(JWT). Jeho štruktúra je nasledujúca:

Tabuľka 10 Štruktúra autorizačného tokenu

Kľúč	Typ	Popis
iss	String	Unikátne ID autorizačného serveru, ktorý vydal JWT
cnf	Object	Kľúč / Typ / Popis kid / String / ID verejného kľúča užívateľa tokenu (Konzument údajov). Používané na overenie dátovej požiadavky
aud	Array of Strings	Úplný zoznam vzorov URL adries, na ktoré sú povolené dátové požiadavky s daným tokenom.
exp	Integer	Čas exspirácie tokenu alebo čas po ktorom token NESMIE byť akceptovaný.
nbf	Integer	Čas pred ktorým token NESMIE byť akceptovaný.
iat	Integer	Čas vydania JWT.
jti	String	JWT ID(jti) - unikátny identifikátor JWT
cr_id	String	ID záznamu súhlasu viažuceho sa k tokenu

4.4.6 Notifikácia

Informácie obsiahnuté v dátovom objekte notifikácie:

Tabuľka 11 Štruktúra notifikácie

<table>
<tr><th>Kľúč</th><th>Typ</th><th>Popis</th></tr>
<tr><td>iat</td><td>string</td><td>Čas vytvorenia notifikácie</td></tr>
<tr><td>service_id</td><td>string</td><td>ID služby, ktorá vydala notifikáciu</td></tr>
<tr><td>sub</td><td>string</td><td>Id používateľa</td></tr>
<tr><td>messages[]</td><td>Array of objects</td><td>
<table>
<tr><td>subject</td><td>string</td><td>Predmet notifikácie</td></tr>
<tr><td>id</td><td>string</td><td>ID notifikácie</td></tr>
<tr><td>message</td><td>string</td><td>Text notifikácie</td></tr>
<tr><td>url</td><td>string</td><td>URL pre ďalšie informácie</td></tr>
</table>
</td></tr>
</table>

5 Implementácia

5.1 Aktivity a úlohy

V tomto dokumente sú realizované nasledujúce predpoklady implementácie:

- Návrh konceptu riešenia sprístupnenia potvrdenia o návšteve školy cez službu Moje dáta,
- Návrh scenárov použitia potvrdenia o návšteve školy v praxi, vrátane sekvenčných diagramov pre prístup k dátam a spracovanie dát,
- Návrh Open API rozhrania pre získanie potvrdenia o návšteve školy na základe štandardu mydata.org,
- Návrh dátového modelu a objektu evidencie potvrdenia o návšteve školy.

Tabuľka 12: Ďalšie potrebné aktivity a harmonogram

ID	Aktivita	Termín
1	Vytvorenie konceptu identity a autentifikácie pre prístup k dátam o návšteve školy, návrh zoznamu oprávnených používateľov a konzumentov dát (aj v rámci CSRÚ)	15.7.2019
2	Výber vhodného PIMS (Personal Information Management System) a zabezpečenie licencií pre občanov SR	15.7.2019
3	Implementácia API rozhrania pre získania potvrdenia o návšteve školy v rámci Centrálnej integračnej platformy	1.8.2019
4	Návrh a nastavenie systému synchronizácie dát a off-line režim	1.8.2019
5	Návrh a vývoj procesu autentifikácie aplikácie (cez eID respektíve koncept mobile ID)	1.8.2019
6	Nastavenie pilotného PIMS pre prácu s potvrdeniami o návšteve školy	31.8.2019
7	Implementácia vizualizácie potvrdenia o návšteve školy	31.8.2019
8	Návrh a vývoj konektoru medzi digi.me a Talend	31.8.2019
9	Overenie návrhu konceptu riešenia na skupine budúcich používateľov	1.10.2019
10	Testovanie riešenia v praxi	1.10.2019
11	Nasadenie riešenia do produktívnej prevádzky a vyhodnotenie pilotnej prevádzky	1.11.2019

Nasleduje špecifikácia požiadaviek na jednotlivé aktivity.

5.1.1 Vytvorenie konceptu identity a autentifikácie pre prístup k dátam o návšteve školy, návrh zoznamu oprávnených používateľov a konzumentov dát (aj v rámci CSRÚ)

- Potvrdenie o štúdiu môže spracovať osoba, ktorá má na to právo
- Vytvorený zoznam konzumentov dát
- Vytvorený centrálny register služieb a vytvorená možnosť registrácie konzumentov dát do neho

5.1.2 Výber vhodného PIMS (Personal Information Management System) a zabezpečenie licencií pre občanov SR

- Vybraný PIMS (môže byť aj viacero), spolupracujúci s implementovaným riešením
- Používatelia môžu prostredníctvom PIMS spravovať svoje dáta
- Aspoň jeden PIMS dostupný pre používateľov zdarma

5.1.3 Implementácia API rozhrania pre získania potvrdenia o návšteve školy v rámci Centrálnej integračnej platformy

- Nasadené funkčné API na Centrálnej integračnej platforme, schopné získavať potvrdenia o štúdiu z RIS
- Možnosti dátového prenosu dostatočné na zvládnutie náporu prenosu potvrdení o štúdiu v špičkách školského roku
- API v podobe, ktorá umožňuje s RIS komunikovať a bude RISom využívaná

5.1.4 Návrh a nastavenie systému synchronizácie dát a off-line režim

- Navrhnuté a funkčná synchronizácia dát a off-line režim
- Systém je schopný získavať potrebné dáta z RIS
- Riešenie zobrazuje dáta konečnému používateľovi
- Synchronizácia je dostatočne rýchla, aby bolo používanie komfortné

5.1.5 Návrh a vývoj procesu autentifikácie aplikácie (cez eID respektíve koncept mobile ID)

- Návrh autentifikácie
- Dostupný pre všetkých možných používateľov
- Implementovaná autentifikácia
- Možné overovať všetkých používateľov aplikácie

5.1.6 Nastavenie pilotného PIMS pre prácu s potvrdeniami o návšteve školy

- aspoň jeden PIMS dostupný zdarma nastavený do podoby, ktorá umožňuje používateľom spravovať svoje potvrdenie o štúdiu
- Nastavenie PIMS zohľadňuje očakávania používateľov zistené pri overovaní návrhu konceptu

5.1.7 Implementácia vizualizácie potvrdenia o návšteve školy

- Riešenie bude zobrazovať relevantné potvrdenie o návšteve školy podľa požiadavky používateľa

5.1.8 Návrh a vývoj konektoru medzi digi.me a Talend

- Technická špecifikácia ako podklad pre implementáciu
- Vyvinutý funkčný konektor
- Schopnosť získať konektorom potvrdenie o štúdiu o každom študentovi, ktorý by mohol byť používateľom služby Moje dáta

- Dostatočná rýchlosť získavania informácií pre pohodlné používanie

5.1.9 Overenie návrhu konceptu riešenia na skupine budúcich používateľov

- Uskutočnené viaceré focus group s budúcimi používateľmi - študentami a tretími stranami na zistenie očakávaní a preferencií pri využívaní
- Výstupy z overenia návrhu zohľadnené a zahrnuté v dizajne riešenia
- Potvrdené, že riešenie bude v navrhovanej podobe využívané budúcimi používateľmi

5.1.10 Testovanie riešenia v praxi

- Otestovanie celého riešenia v praxi
- Používateľ je schopný zdieľať svoje potvrdenie o štúdiu
- Tretia strana je schopná nazdieľané potvrdenie o štúdiu získať

5.1.11 Nasadenie riešenia do produktívnej prevádzky a vyhodnotenie pilotnej prevádzky

- Spustenie prevádzky, ktorá umožňuje každému z cieľových používateľov využívať riešenie
- Zadefinované kritéria úspešnosti projektu
- Vyhodnotenie pilotnej prevádzky a splnenia definovaných kritérií úspešnosti
- Zber podnetov na zlepšenie
- Vytvorenie plánu ďalších krokov

5.2 Prehľad dostupnosti funkcionalít

Dostupnosť jednotlivých funkcionalít riešenia k 1. 9.2019 a k 1.11.2019 je uvedená v Tabuľka 13.

Tabuľka 13: Prehľad dostupnosti funkcionalít v rámci pilotného riešenia pre jednotlivé míľniky

Riešenie	1.9.2019	1.11.2019
Dáta	Dáta zo školského roku 2018/19 • SŠ SR (RIS) • VŠ SR	Dáta zo školského roku 2019/20 • SŠ SR (RIS) • VŠ SR • **SŠ polícia a hasiči**
Formát	• PDF	• PDF • **XML**
Dostupnosť	• Komerčný portál (MŠVVaŠ)	• Komerčný portál (MŠVVaŠ) • Open API pre 3.strany • Integrácia mobilných aplikácií 3.strán

Riešenie	1.9.2019	1.11.2019
Zabezpečenie Komerčný portál – MyData	• SSL protokol[1]	• SSL protokol • PKI[2]
Mobilná identita	DEUS	DEUS
Platforma	Android	**Android**
Dostupnosť v „obchode“	Áno	Áno
Nové funkcie mobilnej aplikácie	• Stiahnutie aplikácie (a personalizácia) • Zobrazenie údajov • Zdieľanie potvrdenia o návšteve školy cez PIN • Zdieľanie potvrdenia o návšteve školy cez email	• Logovanie prístupov cez CSRÚ • „Preukaz“ študenta • Automatické zdieľanie na základe dlhodobého súhlasu • Zdieľanie údajov cez QR kód
Komerčný partneri	• N/A	• **Tatra banka** • Vybraný dopravca (TBC) • **ISIC (TBC)**
Užívatelia	• **Obmedzená testovacia skupina (do 100 študentov)**	• Všetci SŠ a VŠ študenti, ktorí si stiahnu aplikáciu
Komunikácia	• Tlačová správa • Pracovná skupina	• Nadlinková komunikácia v spolupráci s partnermi • Online kampaň

5.3 Otvorené otázky

ID	Otvorená otázka	Riešenie
1	Presná špecifikácia API medzi digi.me a Talend	
2	Nasadenie riešenia do vládneho cloudu	Využitie hybridného modelu vládneho cloudu
3	Výber spôsobu mobilnej autentifikácie pre personalizáciu aplikácie	Na základe rozhodnutia vedenia bola zvolená autentifikácia DEUS
4	Vytvorí sa špecifická nadstavba nad PIMS digi.me?	Áno, pre generovanie PIN

[1] SSL protokol: základný sieťový protokol, ktorý zabezpečuje šifrovanie medzi webovým klientom a webovým serverom

[2] PKI Infraštruktúra: systém asymetrických kľúčov, ktorý zabezpečí že šifrovaný bude samotný obsah webovej stránky

6 Aplikačné programové vybavenie

Aplikačné programové vybavenie bude dostupné v rámci platformy github.

6.1 Riešenie prepojenia medzi komerčným portálom a aplikáciou Moje dáta

Použije sa návrh RESTFul API podľa štandardu OpenAPI 2.0.

Externé API pre SMyD

Príkaz	Cesta	Popis
Auth		
GET	/consent/{pin}	Vráti objekt súhlasu na základe zadaného pin, vrátane identifikácie osobného účtu aplikácie Moje dáta (koho sa súhlas týka). Vstup: Vstup: pin (nepovinné), ID Inštancie KP, ID Užívateľa (nepovinné), ID Organizácie (nepovinné), Účel Výstup: consent
GET	/confirmation_of_school_attendance/{cr_id}	Na základe súhlasu a vstupných parametrov API vráti PDF potvrdenia o návšteve školy Vstup: ID AMyD, ID Inštancie KP ? (nepovinné), ID Užívateľa? (nepovinné), ID Organizácie ? (nepovinné), Typ požadovaného výstupu (nepovinné) Výstup: na základe typu požadovaného výstupu: – pdf, – podpísaný pdf kontajner, – link na dočasne platnú vizualizáciu pdf (v pilote nebude dostupné), – xml.
POST	/notifications/{surrogate_id}	Zaslanie notifikácií používateľovi o spracovaní potvrdenia o návšteve školy Vstup: surrogate_id: transakcia

6.2 Mock služby

GET /consent/{pin}

https://7c7qogbe86.execute-api.eu-central-1.amazonaws.com/dev/consent/1234

OK return:

{
"success": true,
"pin": "1234",
"consent": {
"version": "1.0.0",

"cr_id": "SDAF123456789",
"surrogate_id": "33SDA4",
"rs_description": {
"resource_set": {
"rs_id": "String",
"dataset": [
{
"dataset_id": "PONS_ID",
"distribution_id": "String",
"distribution_url": "https://7c7qogbe86.execute-api.eu-central-1.amazonaws.com/dev/confirmation-of-school-attendance"
}
]
}
},
"slr_id": "122314",
"service_description_version": "213",
"consent_proposal": {
"url": "",
"hash": ""
},
"iat": 1562868000,
"nbf": 1562871600,
"operator_id": "1",
"subject_id": "1.1.1.1",
"role": "",
"usage_rules": [
{
"purposeId": "String",
"datasets": [
"String"
]
}
]
}

}

NOT OK return:

{
"success": false,
"message": "Incorrect PIN"
}

GET /confirmation_of_school_attendance/{ cr_id}

https://7c7qogbe86.execute-api.eu-central-1.amazonaws.com/dev/confirmation-of-school-attendance/SDAF123456789

OK return:

{
"success": true,
"surrogate_id": "SDAF123456789",
"data":
"JVBERi0xLjYNJeLjz9MNCjEyIDAgb2JqDTw8L0xpbmVhcml6ZWQgMS9MIDUxMzg5L08gMTQvRSA0MjQ5Ny9OIDIvVCA1MTA4MC9IIFsgNDkwIDIwNl0+Pg1lbmRvYmoNICAgICAgICAgICAgICAgICAgDQozMSAwIG9iag08PC9EZWNvZGVQYXJtczw8L0NvbHVtbnMgNC9QcmVkaWN0b3IgMTI+Pi9GaWx0ZXIvRmxhdGVEZWNvZGUvSURbPDRCQUY3NkY4OTQwQjgzNTQwMzI0MjhCRTNDRDBEQkM2PjwyOTUzOTgwRUNGM0E1MzQ3QTAxNzE4MDM4R ... "
}

NOT OK return:

{
"success": false,
"message": "Incorect ID"
}

POST /notifications/{surrogate_id}

https://7c7qogbe86.execute-api.eu-central-1.amazonaws.com/dev/notifications/33SDA4/

OK return:

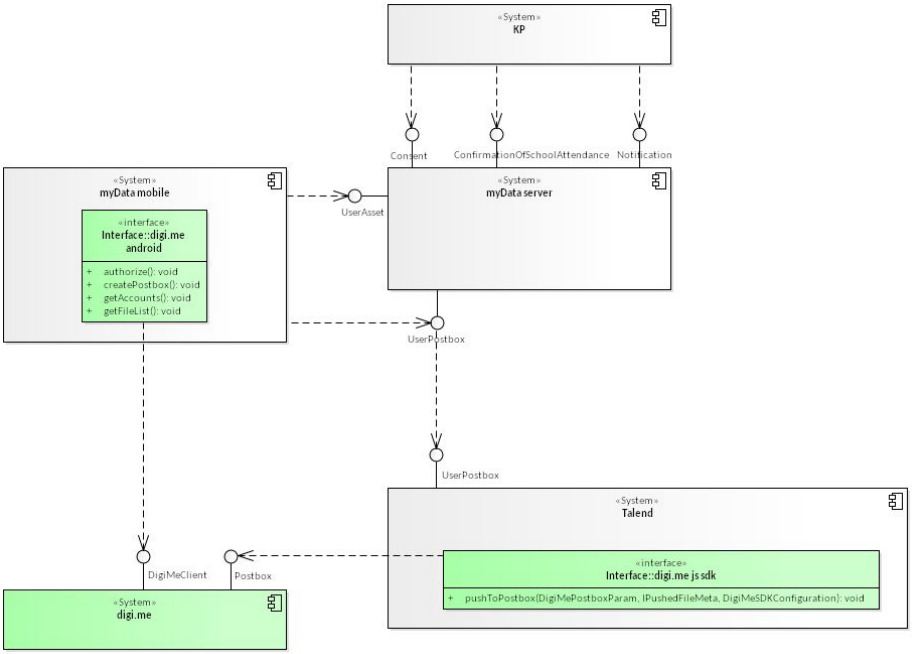
{
"success": true,
"surrogate_id": "33SDA4",

"message": "Successfully sent notification."
}

6.3 Ukážka integrácie s digi.mi

Component Diagram

This component diagram depicts components used within the solution.



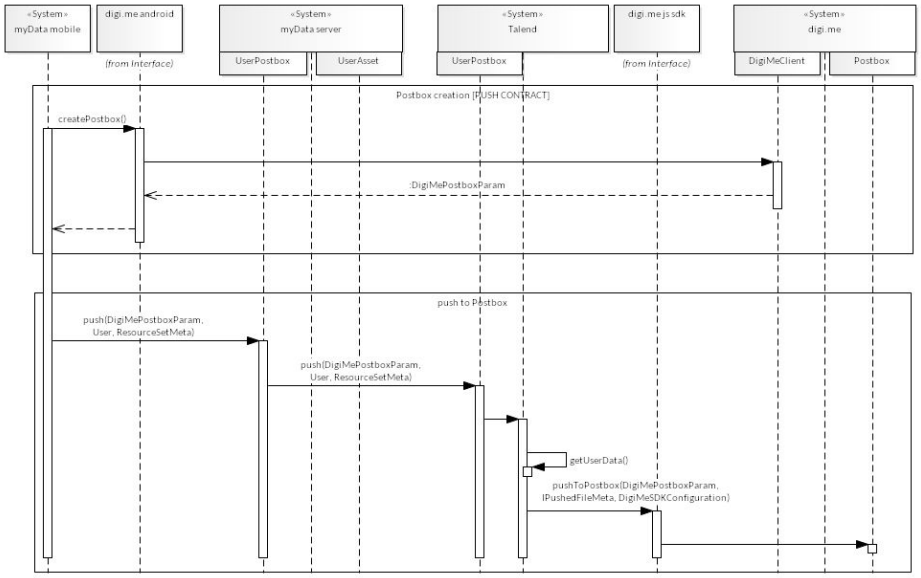
Component name	Component description
myData mobile	mobile application used by end users used to provide my account functionality
myData server	used as MyData proxy service according to the MyData architecture it will be providing MyData functionality to the services which are not MyData compliant.
digi.me	personal data storage and digital consent management
Talend	integration platform for Slovak Government services
KP	anonymous commercial portal

TODO: add mID system, used for user (Slovak citizen) authentication

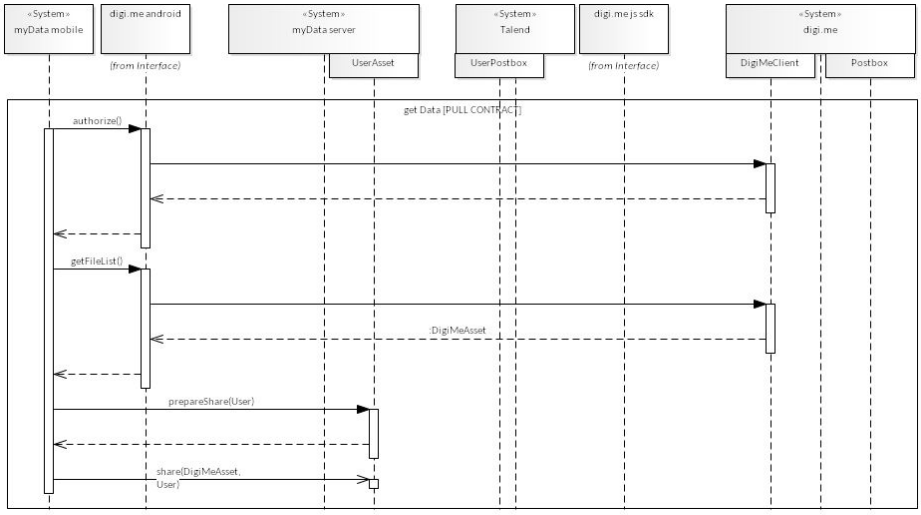
Sequence Diagram

Following diagrams show the communication flow between systems

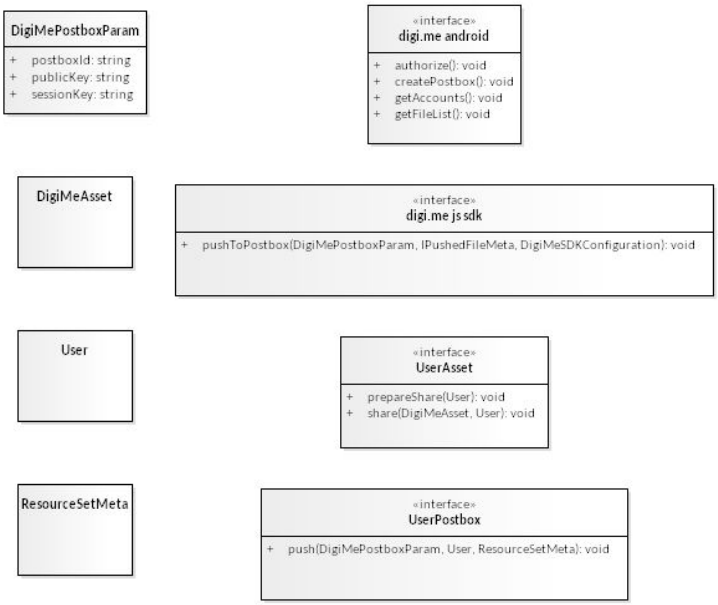
Pushing data to personal data storage



Sharing data from personal data storage



Object used within the solution



Consent Record description

Following table describes the consent record from the MyData architecture perspective.

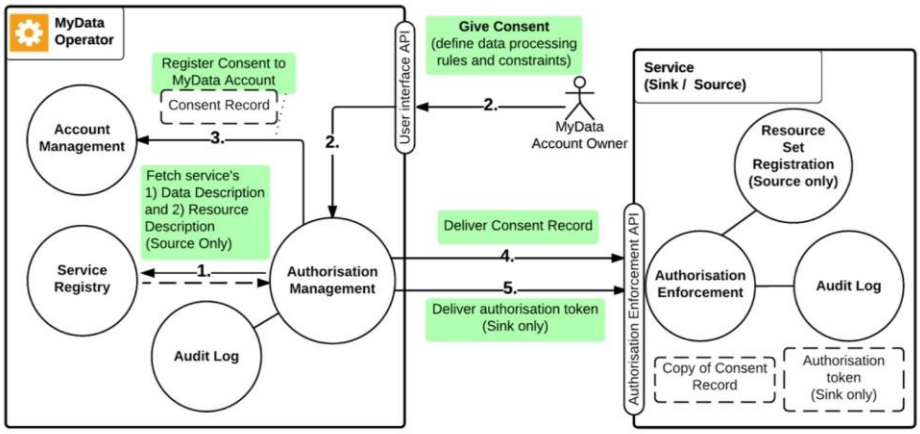
Key	Type	Description
version	String	Version number
cr_id	String	Unique ID of consent record
surrogate_id	String	Surrogate ID - owner of the account
rs_description	Object	Record set description
slr_id	String	Record ID for connected service
service_description _version	String	Version of the description used for consent
consent_proposal	Object	**Key** / **Description** url: URL address of the consent proposal (it means what was displayed to the user) hash: SHA-256 hash consent proposal
iat	Integer	Date and time of consent issue
nbf	Integer	Consent valid From
exp	Integer	Consent valid To
operator	String	Operator ID, who has issued the consent
subject_id	String	Service ID, to which the consent has been issued
usage_rules[1..n]	Array of Objects	**Key** / **Description** purposeId: Purpose ID datasets: Array of data set IDs

MyData authorisation concept and consent based approach

Authorisation is initiated by the Account Owner and it consists of five steps as shown in Figure:

1. Fetch service's Data Description and Resource Description (Source)
2. Information about the service is presented to Account Owner including what information the Sink would like to have and for what purpose. Account Owner then defines data processing rules and constraints, which must meet the Sink's minimum requirements for the Consent to be actionable.

3. Consent Record is stored in Account Owner's MyData Account
4. Consent Record is delivered to the Service.
5. Authorisation token is delivered to the Sink service.



Implementation details

Push to Postbox Implementation (digi.me)

```
const pushToPostbox = async (
    sessionKey: string,
    postboxId: string,
    publicKey: string,
    data: IFileMeta<IPushedFileMeta>,
    options: DigiMeSDKConfiguration,
): Promise<any> => {
    const key: string = getRandomHex(64);
    const rsa: NodeRSA = new NodeRSA(Buffer.from(publicKey, "utf8"),
"pkcs1-public");
    const encryptedKey: Buffer = rsa.encrypt(Buffer.from(key, "hex"));
    const ivString: string = getRandomHex(32);
    const iv: Buffer = Buffer.from(ivString, "hex");
    const encryptedData: Buffer = encryptData(
        iv,
        Buffer.from(key, "hex"),
        Buffer.from(data.fileData, "base64"),
    );
    const encryptedMeta: Buffer = encryptData(
        iv,
        Buffer.from(key, "hex"),
        Buffer.from(JSON.stringify(data.fileDescriptor), "utf8"),
    );
    const url: string =
`https://${options.host}/${options.version}/permission-access/postbox/${postboxI
d}`;
    const form: FormData = new FormData();
    form.append("file", encryptedData, data.fileName);

    const headers = {
        accept: "application/json",
        contentType: "multipart/form-data",
        sessionKey,
        metadata: encryptedMeta.toString("base64"),
        symmetricalKey: encryptedKey.toString("base64"),
        iv: ivString,
    };

    try {
        const response = await net.post(url, {
            headers,
            body: form,
        });
```

```
        return response.body;
    } catch (error) {

        if (!(error instanceof HTTPError)) {
            throw error;
        }

        const errorCode = get(error, "body.error.code");

        if (errorCode === "SDKInvalid") {
            throw new SDKInvalidError(get(error, "body.error.message"));
        }

        if (errorCode === "SDKVersionInvalid") {
            throw new SDKVersionInvalidError(get(error, "body.error.message"));
        }

        throw error;
    }
};
```

Complete source can be found:
https://github.com/digime/digime-js-sdk/blob/v0.3.0-postbox.6/src/postbox.ts

Sample Client implementation

```
app.get('/push', function(req, res) {
 const postboxId = req.query.postboxId;
 const buff = new Buffer(req.query.postboxPublicKey, 'base64');
 const postboxPublicKey = buff.toString('utf8');
 const postboxSessionKey = req.query.postboxSessionId;
 console.log(`Triggered push to postbox ${postboxId} ${postboxPublicKey}`);
 // First thing to do is to establish a session by using our Application ID and
Contract ID
 establishSession(APP.appId, APP.contractId).then(async (session) => {
     console.log(`Session key: ${postboxSessionKey}`);
     try {
     const pdfData = await readFileAsync('./samplePONS.pdf', 'base64');
     const pushedData = {
       fileData: pdfData,
       fileName: "samplePONS.pdf",
       fileDescriptor: {
           mimeType: "application/pdf",
           tags: ["samplePONS.pdf", "PONS test"],
           reference: ["samplePONS.pdf"],
           accounts: []
       }
     }
     console.log(JSON.stringify(pushedData));
```

```
    const result = await pushDataToPostbox(postboxSessionKey, postboxId,
postboxPublicKey, pushedData);
    console.log(`Successfully pushed data to postbox ${postboxId}`);
    res.json({
        success: true,
        message: `Successfully pushed data to postbox ${postboxId}`,
        pushCompleteURL: getPushCompleteURL(postboxSessionKey, postboxId),
        response: result
    });
    } catch (error) {
    console.log(error);
    res.status(500).json({
        success: false,
        message: error.message,
    });
    }
 });
});
```