projekt_1060_Pristup_k_projektu_detailny

PRÍSTUP K PROJEKTU

(Project approach)

Identifikovanie požiadaviek **na technickú časť riešenia**

Identifikácia projektu

Povinná osoba	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (MIRRI)
Názov projektu	Slovensko v Mobile
Zodpovedná osoba za projekt	Jozef Toman
Realizátor projektu	Slovensko IT, a.s.
Vlastník projektu	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (MIRRI)

Schvaľovanie dokumentu

Položka	**Meno a priezvisko**	**Organizácia**	**Pracovná pozícia**	**Dátum**	**Podpis** (alebo elektronický súhlas)
Vypracoval		Slovensko IT		25.02.2021	
Overil	Jozef Toman	MIRRI			

- **OBSAH**

2 ÚČEL DOKUMENTU

V súlade s Vyhláškou 85/2020 Z.z. o riadení projektov - *je dokument* ***Prístup k projektu*** *pre iniciačnú fázu určený na rozpracovanie detailných informácií prípravy projektu.*

Dokument Prístup k projektu v zmysle vyššie uvedenej vyhlášky má o.i popisovať riešenie projektu v oblastiach:

1. *Architektúry riešenia – aplikačná vrstva, technologická vrstva*
2. *Požiadaviek na dátový model, dátové konverzie a migrácie*
3. *Požiadavky UX dizajn (front-end a back-end vizual)*
4. *Požiadaviek na vládny cloud*
5. *Kapacitné požiadavky na HW, SW a licencie*
6. *Požiadaviek na bezpečnosť riešenia*
7. *Požiadavky na testovanie a akceptačné kritéria*
8. *Požiadavky na prevádzku, výkonnosť, dostupnosť a zálohovanie*
9. *Požiadavky na integrácie, rozhrania a spoločné komponenty*
10. *Požiadavky na dokumentáciu a školenia*

2.1 Konvencie používané v dokumentoch – označovanie požiadaviek

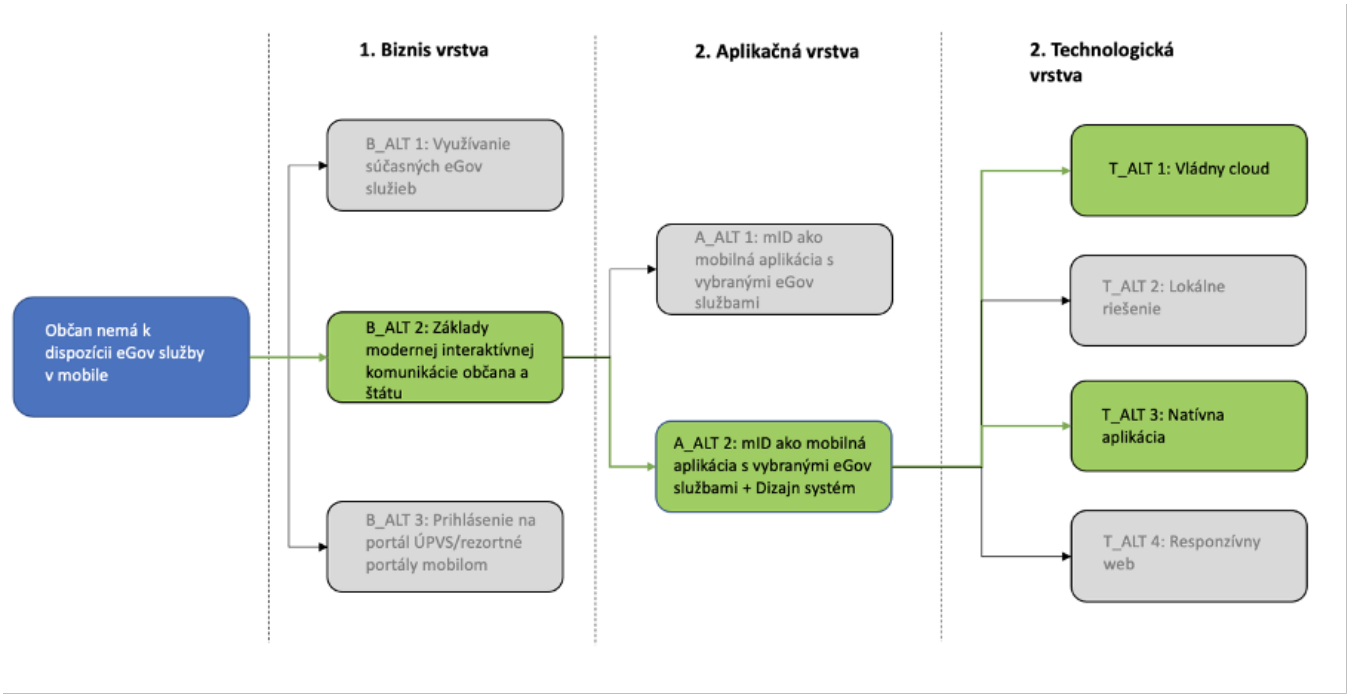
Používateľské príbehy (User Stories) majú nasledovnú konvenciu:

Us_mMm_R_xx_yy

- Us – užívateľská požiadavka (user stories)
- mMm – označenie modulu (mId – Mobilné ID; ePu – ePush; KSl – Kontextové služby; mSch – Mobilná schránka; mPo – Mobilné podanie; mDo – Mobilné doklady; SNa – Smart návody, DSy – Dizajn systém; Gen – General (všeobecné)
- R – označenie požiadavky
- xx – číslo epicu
- yy – číslo user story

3 OPIS NAVRHOVANÉHO RIEŠENIA

Nasledujúca schéma sumarizuje výber alternatív z pohľadu biznis, aplikačnej a technologickej vrstvy.



Na základe multikriteriálnej analýzy, kde boli definované viaceré alternatívy z pohľadu biznis, aplikačnej a technologickej vrstvy, sa ako vybraná alternatíva stanovilo riešenie vývoj natívnej mobilnej aplikácie spolu s vedľajším produktom Dizajn systému pre tieto aplikácie, umiestnené vo vládnom cloude.

Rozsah projektu môžeme rozdeliť na 2 ucelené časti:

1. **Hlavný produkt** – vytvorenie **natívnej mobilnej aplikácie SVM** vrátane registrácie osoby a autentifikácie osoby cez mID a
2. **Vedľajšie produkty** – vybudovanie **Dizajn systému pre natívne mobilné aplikácie**, ktorá obsahuje jednotný dizajn pre moduly eGOV pre mobilné aplikácie, opakovane použiteľné elementy publikované aj ako Open-source a návrhové vzory pre vytváranie aplikácií používajúcich eGOV služby. Vedľajším produktom je rovnako proces overenia a certifikácie aplikácií pre možnosť využívania eGOV služieb štátu.

1. Hlavný produkt - Natívna mobilná aplikácia Slovensko v mobile (Mobilná aplikácia SVM)

Hlavným produktom projektu bude natívna mobilná aplikácia, ktorá integruje a sprístupní existujúce eGOV služby cez mobilný prístupový kanál (natívne aplikácie) a zároveň vytvára nové mobilné služby. Vybrané služby SVM budú prístupné cez Open API 3+ pre integrované aplikáciu tretích strán, ktoré prejdú procesom overenia zhody (compliance) a ktoré chcú využívať eGOV služby v mobilnom zariadení občana alebo chcú využiť modul MeID v SVM ako autentifikačný prostriedok.
SVM bude obsahovať tieto funkčné časti:

- A. Registrácia mID - Jednotná registrácia fyzickej osoby a jej mobilných zariadení (celý životný cyklus registrácie, rôzne kanále registrácie: portál slovensko.sk a vytvorené API rozhranie pre budúce integrované subjekty, napr.: Slovenská pošta alebo iné komerčné a nekomerčné integrované subjekty a ich obslužné miesta
- B. Prístup k vybraným službám eGOV prostredníctvom Modulov, ktoré budú ďalej sprístupnené pre integrované aplikácie tretích strán (OVM, banky, poisťovne, iné komerčné subjekty).
    - **Mobile ID** (centrálny modul eGOV, pre-rekvizita pre ostatné moduly) - mobilný autentifikátor fyzickej osoby (rozhranie na Modul IAM a OAuth2), pre natívne mobilné aplikácie,
    - **Autentifikácia cez registrované mobilné zariadenie** pre webové aplikácie (prihlasenie.slovensko.sk aj iné integrované webové aplikácie),
    - **ePush** (centrálny modul eGOV, pre-rekvizita pre ostatné moduly) - pre podporu interakcie štátu s občanom /notifikačných služieb/ push notifikácie (rozhranie na Modul ÚPVS eNotify),
    - **Kontextové služby** – poskytnutie služieb na základe dát používateľa, vybrané scenára a procesy schválené v analytickej fáze a overené UX testami počas analýzy,
    - **Mobilná schránka** - elektronická komunikačná schránka (rozhranie na Modul ÚPVS eDesk),
    - **Mobilné podanie** – (1) podpisovanie dokumentov (podaní) alebo poskytnutie súhlasu na používanie dokladu vozidla – elektronický podpis ako náhrada vlastnoručného podpisu (úroveň 3 zabezpečenia, tzv. „podpis klikom“), (2) potvrdenie súhlasu/oboznámenia sa s podmienkami alebo informáciou (napr. Informovaný súhlas, nejedná sa o prístup k osobným údajom, tzv. consent management), (3) možnosť vytvorenia podania sprístupnené cez mobilné rozhranie,
    - **Mobilné platby** - modul mobilných platieb, napr. úhrada správnych/súdnych poplatkov (rozhranie na Modul ÚPVS MEP/PEP),
    - **Mobilné doklady** – modul načítania dokladov, ktoré vydávajú štátne inštitúcie (PoC doklady vozidla a doklad PN),
    - **Smart návody** – občan má k dispozícii jednoduchý a prehľadný návod, ako vybaviť službu. Predpokladá sa využitie pre také služby, ktoré nie sú E2E poskytované cez SVM mobilnou aplikáciou (napr. časť služby vyžaduje kroky procesu, ktoré nie je možné aplikáciou podporiť. V tom prípade aplikácia poskytne smart návod, ako proces/službu dokončiť a aké ďalšie kroky sú vyžadované).

2. Vedľajší produkt – Vybudovanie Dizajn systému pre natívne mobilné aplikácie

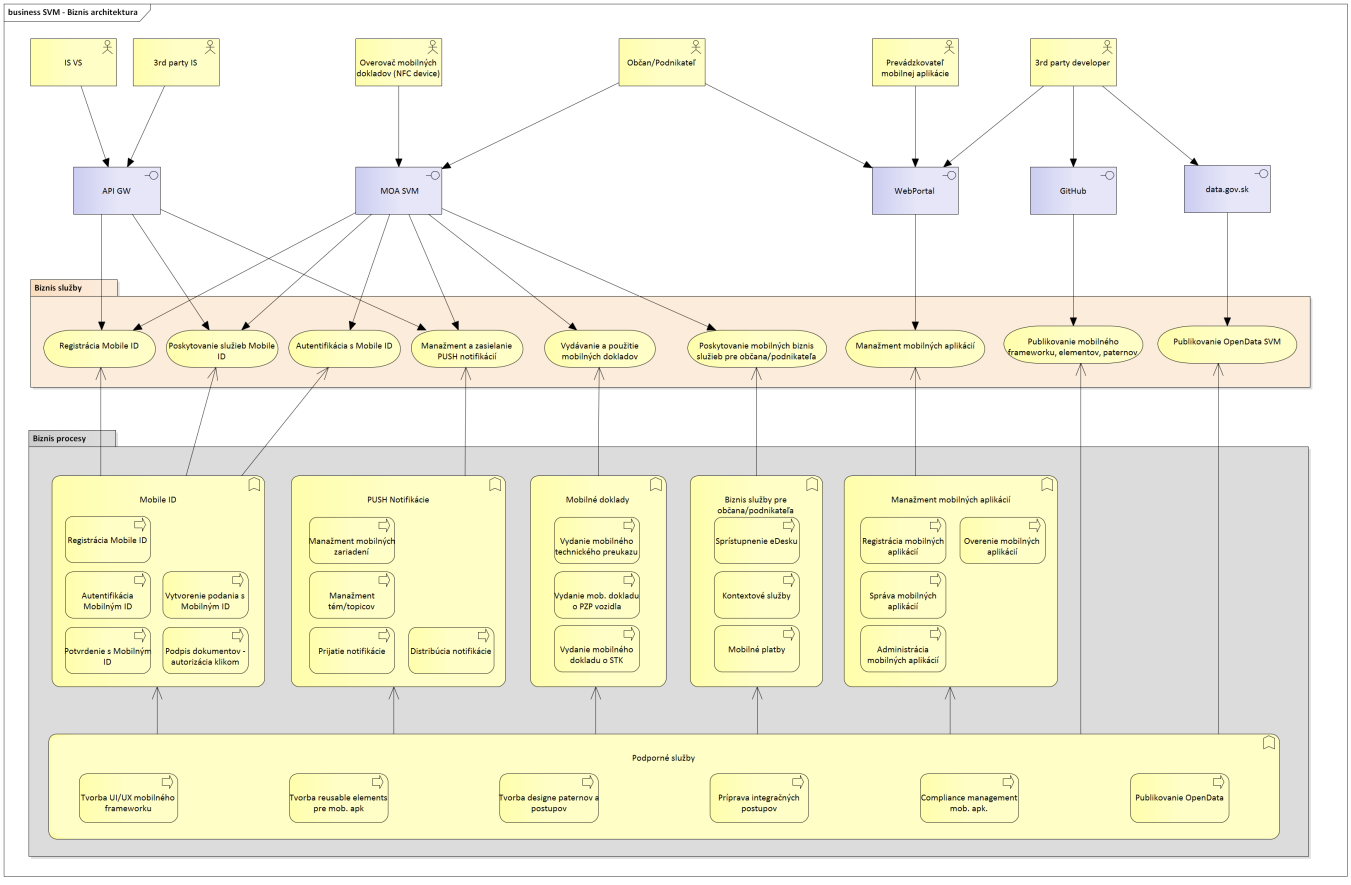
Cieľom projektu Slovensko do vrecka nie je len vytvorenie štátnej mobilnej aplikácie, ale poskytovať eGOV mobilné služby ako ucelený framework pre akékoľvek inštitúcie štátneho alebo verejného sektora. Základom je vybudovanie platformy, ďalej nazývanej aj ako Dizajn systém pre natívne mobilné aplikácie, ktorá poskytne jednotlivé funkcionality ako ucelené, opätovne použiteľné moduly, resp. knižnice pre iné aplikácie. Výhodou riešenia je možnosť využitia centrálnych mobilných eGOV služieb bez nutnosti vlastného vývoja. Komponenty aj časti kódu budú zdieľané ako open-source.
Akákoľvek inštitúcia môže napríklad využiť Modul mID, namiesto vytvorenia vlastného autorizačného a autentifikačného riešenia aplikácie. Banky alebo iné inštitúcie budujú vlastné autentifikačné a autorizačné moduly do svojich aplikácií, čo je časovo aj finančné náročné. Cieľom je publikovať a následne udržiavať komponenty a knižnice, ktoré budú vložené ako súčasť zdrojového kódu externej aplikácie. Benefitom riešenia je úspora času a nákladov spojených s programovaním vlastných služieb a rovnako aj možnosť využívať služby štátu ako integrálna súčasť podnikových procesov pri interakciách so zákazníkom/ občanom.

4 ARCHITEKTÚRA RIEŠENIA PROJEKTU

4.1 Biznis vrstva

4.1.1 Návrh biznis architektúry

Nasledujúci diagram znázorňuje návrh budúcej architektúry biznis služieb Slovensko v mobile. Primárnym cieľom je vytvorenie natívnej mobilnej aplikácie prostredníctvom ktorej bude môcť občan pristupovať k elektronickým službám eGOVermentu. V neposlednom rade je cieľom projektu vytvoriť, publikovať a rozvíjať jednotný prístup k budovaniu mobilného kanála eGOVermentu SR a to formou publikovania jednotného UI/UX frameworku, elementov, návrhových vzorov (patterns) a integračných postupov pre všetkých tvorcov a používateľov mobilných aplikácií sprístupňujúcich eGOV služby pre občana. Pre daný framework je dôležité jeho aktívne rozširovanie a udržiavanie podľa aktuálnych trendov pre mobilné aplikácie. Dizajn systém pre natívne mobilné aplikácie musí byť priebežne upravovaný/zlepšovaný, aby čo najviac reflektoval potreby koncového používateľa služieb.

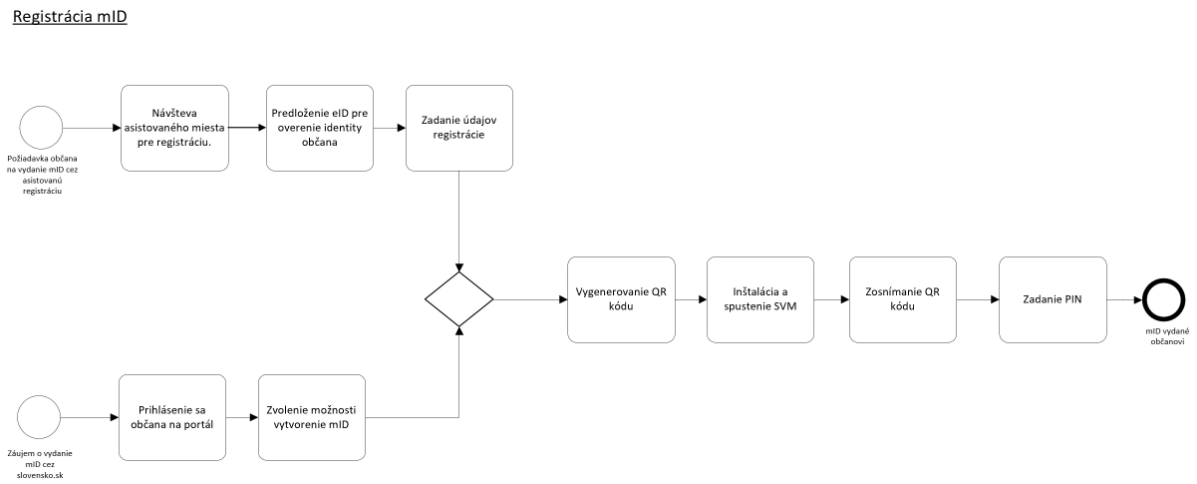


4.1.2 TO-BE procesy

Nižšie popísané budúce procesy boli navrhnuté tak, aby reflektovali benefity riešenia a rovnako vychádzajú z jednotlivých funkcionalít SVM.

Registrácia mID:

Nasledujúci diagram znázorňuje registráciu mID prostredníctvom portálu slovensko.sk alebo prostredníctvom asistovanej registrácie:



Jednotlivé kroky registrácie mID sú nasledovné:

1. Občan príde na miesto asistovanej registrácie alebo sa prihlási na slovensko.sk
2. A: v prípade asistovanej registrácie predkladá eID na overenie jeho identity a pracovník asistovanej registrácie zadáva so systému (integrovaného na SVM) údaje pre registráciu, B: v prípade registrácie cez portál zadáva možnosť vystavenia/registrácie mID priamo na portáli
3. SVM vygeneruje QR kód, ktorý slúži ako identifikátor pre spárovanie identity s mobilným zariadením
4. O bčan sťahuje a inčtaluje aplikáciu SVM
5. Občan načíta cez aplikáciu SVM QR kód a mobilné zariadenie je spárované s jeho identitou.
6. Následne občan zadá PIn na prihlásenie sa do aplikácie. Výsledkom registrácie je mID, resp vygenerovaný mobilný token uložený na zariadení občana

Prihlasovanie na portál

V súčasnosti nie je možné prihlásiť sa k eGOV službám iným spôsobom, ako cez čítačku a fyzický eID. Uvedené má za následok, že eGOV služby sú obmedzené na 1 kanál prístupu a nie je možné využiť mobilné platformy, ktoré sú v súčasnosti užívateľmi preferované. Proces prihlasovania je nielen obmedzený na platformu, ale rovnako vytvára priestor na optimalizáciu času spojeného so samotným prihlásením. Riešenie SVM poskytuje možnosť multikanálového prístupu k eGOV službám cez tzv. MobileID. Samotnému prihláseniu predchádza registrácia pre vytvorenie Mobile ID, prostredníctvom:

1. prihlásenia sa na portál slovensko.sk prostredníctvom eID a vygenerovanie MobileID
2. asistovanej registrácie na Integrovanom obslužnom mieste občana cez systém, ktorý je integrovaný na registráciu SVM.

Výsledkom registrácie je vygenerovaný mobilný token MobileID, nainštalovaná natívna mobilná aplikácia a registrované mobilné zariadenie pre prístup k eGOV službám.

Po registrácii Mobile ID je možné prihlásiť sa na portál slovensko.sk nasledovne:

1. Načítanie stránky slovensko.sk a kliknutie na možnosť „Prihlásiť prostredníctvom mID“
2. A: Portál slovensko.sk vygeneruje QR kód/zašle one time password do aplikácie (bude potvrdené v detailnej analýzy) alebo
3. B: Portál požiada používateľa o otvorenie aplikácie, aplikácia mu vygeneruje pass-code, ktorý zadá do portálu.
4. Používateľ sa prihlási do aplikácie SVM cez PIN/FaceID/TouchID a odfotí v aplikácii QR kód
5. Po odfotení je používateľ prihlásený na portáli slovensko.sk

Nasledujúci diagram zobrazuje proces AS-IS a TO-BE prihlásenia:

AS-IS

TO-BE

Prečítanie správy z eDesk

Jednou z funkcionalít portálu slovensko.sk je Schránka správ, tzv. Modul eDesk, ktorý zabezpečuje komunikáciu medzi občanom a OVM. Informácia o tom, že občan dostal správu do eDesk prichádza SMS alebo emailom. Následne používateľ musí prejsť na portál slovensko.sk, prihlásiť sa čítačkou a eID a načítať prijatú správu. V rámci riešenia SVM používateľ prijme push notifikáciu o prijatí správy v eDesk a pristupuje k správe priamo v aplikácii. V rámci tohto procesu je ušetrený čas používateľa, kedy odpadá potreba pracovať vo viacerým aplikáciách pre prečítanie správy (mail, slovensko.sk). Proces načítania správy cez aplikáciu SDV je nasledovný:

1. Prijatie PUSH notifikácie o prijatej správe
2. Používateľ sa prihlási do aplikácie SVM cez PIN/FaceID/TouchID
3. Načítanie správy v Schránke správ

Nasledujúce diagramy zobrazujú proces AS-IS a TO-BE načítania správy v eDesk:

AS-IS

TO-BE

Kontrola mobilného dokladu

V súčasnosti umožňuje viacero webových stránok kontrolu exspirácie STK, resp. dokladu EK a TK, ale overenie platnosti Technického preukazu nie je možné vykonať online. Benefity riešenia mobilných dokladov umožňujú nielen komfortné preukázanie sa cez mobilné zariadenie (predpoklad, že občan má mobilný telefón stále pri sebe), ale elektronizácia rovnako umožňuje poskytnúť doklad o vozidle inej osobe (napr. ak vozidlo využívajú viacerí členovia domácnosti alebo zamestnanci). Kontrola dokladu je podmienená verifikáciou zo strany policajta, napr. pri cestnej kontrole a podmienkou je rovnako aj využitie dynamických prvkov priamo v aplikácii pri doklade, aby sa zamedzilo situácii, kedy je doklad uložený ako PDF súbor alebo obrázok v telefóne.

Nasledujúci proces znázorňuje šetrenie času na strane občana pri kontrole exspirácie dokladu:

AS-IS

TO-BE

Proces verifikácie dokladu pri cestnej kontrole sa predpokladá nasledovne:

1. Používateľ sa prihlási do aplikácie SVM,
2. Používateľ vyberie vozidlo, pre ktoré chce načítať doklad,
3. Predloží doklad, ktorého je možné skontrolovať prostredníctvom 2 validačných prvkov:
    a. Vizualizácia mobilného dokladu – meniace sa prvky dokladu
    b. NFC technológia pre overenie mobilného dokladu
4. Policajt skontroluje doklad cez aplikáciu SVM

Proces nahratia dokladu (ktorého používateľ nie je vlastníkom):

1. Používateľ, ktorý už má nahratý doklad, sa prihlási do aplikácie SVM
2. Doklad je reprezentovaný kódom alebo jedinečným číslom
3. Druhý používateľ sa prihlási do aplikácie SVM a zadá požiadavku na nahratie dokladu
4. Druhý používateľ odfotí kód dokladu alebo zadá číslo dokladu
5. Vlastník vozidla potvrdí, že doklad bude nahraný v aplikácii druhého používateľa

6. Doklad sa zobrazí druhému používateľovi v zozname dokladov SVM

Vlastník vozidla môže manažovať svoje doklady, ktoré sú uložené v aplikácii SVM iného používateľa. Vlastník vozidla môže kedykoľvek zrušiť zdieľanie dokladu. Druhý používateľ je upozornený na akúkoľvek zmenu nad dokladom, ktorú vykonal vlastník dokladu.

Vytvorenie elektronického podania

Elektronické podanie prostredníctvom aplikácie SVM sa od štandardného podania cez portál ÚPVS alebo iné rezortné portály, odlišuje v spôsobe vytvárania podania. Kým pri klasickom elektronickom podaní je iniciátorom procesu samotný občan, pri mobilnom podaní je iniciátorom procesu OVM. V prípade, ak OVM požaduje vytvorenie podania, prihlásený používateľ SVM je notifikovaný cez aplikáciu.

V rámci mobilných zariadení existujú obmedzenia týkajúce sa samotnej mobilnej platformy, preto cieľom nie je kopírovať všetky eGOV služby do aplikácie, ale poskytnúť len vybrané služby. Vybrané služby budú však pokryté E2E, tj od požiadavky na podanie, doplnenie údajov, cez zaplatenie poplatku a podpísanie podania. Celý proces vychádza od OVM a dáta, ktoré štát o používateľovi eviduje, sú automaticky vypĺňané. Používateľ tak pri podaní dopĺňa len vybrané dáta a potvrdzuje podanie.

Nasledujúci diagram porovnáva AS-IS a TO-BE proces a poukazuje na šetrenie času občana pri vybavovaní podania cez aplikáciu SVM (podproces „Prihlásenie na portál“ je popísaný vyššie).

AS-IS

TO-BE

Celý proces podania je založený na princípe modernej interaktívnej komunikácie občana a štátu vďaka vlastnostiam a všeobecnej dostupnosti mobilných zariadení s pripojením na dátové služby. Proaktívna a hlavne interaktívna komunikácia s občanom predstavuje nový spôsob vyžadujúci zmenu, resp. doplnenie nových biznis procesov na strane OVM/Poskytovateľov služby. Nový spôsob neobmedzuje súčasný biznis proces, ale predstavuje modernú alternatívu pre vybrané podania a komunikáciu so štátom. Ambíciou riešenia je poskytnúť užitočné a najčastejšie používané služby cez mobilné zariadenie.

V rámci štúdie sú riešené nasledovné konkrétne podania:

1. poskytnuie informovaného súhlasu
2. potvrdenie prítomnosti pacienta
3. doplnenie žiadosti o nemocenskú dávku (ePN)

Celkovo projekt SVM poskytne centrálne riešenie mobilného podania pre budúcu integráciu OVM, ktoré bude využívať mobilné podanie prostredníctvom SVM. Nižšie uvedené podania sú konkrétnymi príkladmi, ale nelimitujú celkové riešenie mobilného podania.

(1) Poskytnutie informovaného súhlasu

Každý zdravotnícky pracovník je povinný poučiť pacienta pred poskytnutím zdravotnej starostlivosti o účele, povahe, následkoch a rizikách poskytovanej zdravotnej starostlivosti, o možnostiach voľby navrhovaných postupov a rizikách odmietnutia poskytnutia zdravotnej starostlivosti. Potvrdenie o poučení dáva pacient prostredníctvom podpisu tzv. informovaného súhlasu (papierová A4).

Nasledujúci proces TO-BE popisuje proces s využitím SVM:

1. Lekár vyhľadá pacienta cez RČ cez svoj ambulantný informačný systém (integrovaný a overený v Systéme ezdravie)
2. Lekár vyžiada cez svoj ambulantný informačný systém Potvrdenie informovaného súhlasu
3. Ambulantný informačný systém zasiela request do ezdravie
4. ezdravie posiela request na podpis do SVM
5. Pacient na svojom mobilnom zariadení otvorí push notifikáciu o potrebe potvrdenia Informovaného súhlasu
6. Prihlási sa do aplikácie SVM a potvrdí Informovaný súhlas
7. SVM zašle informáciu do ezdravie a pribalí podpis pacienta (podpis klikom)
8. ezdravie zašle notifikáciu lekárovi o potvrdení Informovaného súhlasu

9. Pacient má zoznam svojich Informovaných súhlasov vo svojej elektronickej knižke (EZKO)

(2)Potvrdenie prítomnosti pacienta

V prípade, ak chce lekár-špecialista, resp. zastupujúci lekár pristupovať k zdravotnej dokumentácii pacienta, musí mu pacient dať prístup k týmto dátam. V súčasnosti je jediná možnosť cez eID a čítačku priamo v ambulancii lekára. Nasadením MobileID pribudne možnosť autentifikácie pacienta cez mobilné zariadenie a lekár tak už nebude musieť mať eID čítačku.

Nasledujúci proces TO-BE popisuje proces s využitím SVM:

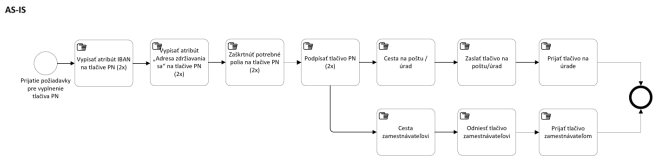
1. Lekár vyhľadá pacienta cez RČ cez svoj ambulantný informačný systém (integrovaný a overený v Systéme ezdravie)
2. Lekár vyžiada cez svoj ambulantný informačný systém prístup (tzv. Potvrdenie prítomnosti pacienta)
3. Ambulantný informačný systém zasiela request do ezdravie
4. ezdravie posiela request na podpis do SVM
5. Pacient na svojom mobilnom zariadení otvorí push notifikáciu o potrebe potvrdenia prístupu k zdravotnej dokumentácii
6. Prihlási sa do aplikácie SVM a potvrdí súhlas s prístupom
7. SVM zašle informáciu do ezdravie a pribalí podpis pacienta (podpis klikom)
8. ezdravie poskytne lekárovi cez jeho ambulantný systém náhľad k zdravotnej dokumentácii (časovo obmedzený, pacient vie manažovať prístup)
9. Pacient má zoznam svojich „potvrdených prístupov“ vo svojej elektronickej knižke (EZKO)

(3) Doplnenie žiadosti o nemocenskú dávku (ePN)

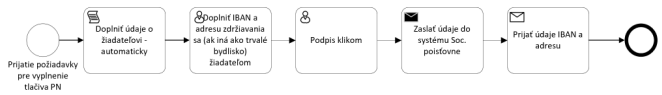
Digitalizácia procesu vystavenia práce neschopnosti (PNky) podporuje projekt elektronických PN, kedy nástrojom na zadanie miesta zdržiavania sa a číslo účtu pre PN zapíše pacient priamo v aplikácii SVM. Aplikácia SVM bude v procese vystavenia PN poskytovať možnosť zadania údajov PN priamo v ambulancii lekára bez toho, aby pacient musel navštíviť Sociálnu poisťovňu alebo zaslať údaje poštou. Šetrenie času a nákladov na tlačivá spočíva v odstránení nutnosti vypisovať papierové tlačivo PN.

Nasledujúci diagram znázorňuje postavenie SVM na strane občana pri doplnení údajov:

AS-IS



TO-BE



Nasledujúci proces TO-BE popisuje proces s využitím SVM:

1. Pacient prijme request z ambulantného systému na doplnenie žiadosti o nemocenskej dávky
2. Pacienta doplní adresu zdržiavania sa a IBAN cez SVM
3. Pacient podpíše žiadosť cez SVM
4. Žiadosť je následne zaslaná z SVM do systému Sociálnej poisťovne

Konkrétne mobilné podania (1) Poskytnutie informovaného súhlasu, (2)Potvrdenie prítomnosti pacienta, (3) Doplnenie žiadosti o nemocenskú dávku (ePN) vyvolávajú úpravu na strane IS PZS ako aj systému ezdravie. Uvedené zmeny budú zaradené do roadmap systému ezdravie a budú súčasťou releasu managementu dotknutých systémov. Zmeny podliehajú pravidlám release managmentu definovaným NCZI, rovnako ako zmeny core funkcionalít ezdravie (napr. erecept, evysetrenie, elab apod.).

Dizajn systém - implementácia back-end komponentov

V súčasnosti neexistuje dizajn systém pre natívne mobilné aplikácie, ale len pre webové aplikácie, resp. web stránky. Cieľom nasadenia dizajn systému pre natívne mobilné aplikácie je poskytnúť nielen framework vizuálnych komponentov aplikácii, ale rovnako poskytnúť back-endové komponenty, ktoré si môže akákoľvek iná mobilná aplikácia poskytujúca eGOV služby implementovať a výrazne znížiť náklady na práce programátora v situácii, keby si museli tieto komponenty vyvíjať sami.

Nasledujúci diagram porovnáva AS-IS a TO-BE stav s tým, že pre AS-IS stav je popísaný proces, ktorý znázorňuje situáciu bez implementácie Dizajn systému, tj. keby projekt SVM zahŕňal len produkt MobileID spolu s mobilnou aplikáciou.

AS-IS

TO-BE

4.2 Aplikačná vrstva

4.2.1 Popis aplikačnej architektúry aktuálneho stavu (AS-IS)

Aplikácia Slovensko v mobile je novo budovaná aplikácia ktorá v aktuálnom stave neexistuje, preto z hľadiska aplikačnej architektúry ide o nový komponent v celkovej architektúre slovenského eGovermentu. Cieľom aplikácie nie je budovať nové služby eGovermentu, ale sprístupňovať existujúce elektronické služby novým kanálom v rámci multikanálového prístupu, a to prostredníctvom mobilného zariadenia.

SVM bude využívať funkcionalitu existujúcih spoločných modulov ÚPVS, ktoré sú uvedené v popise aplikačnej architektúry riešenia. Aby SVM, ako aj iné mobilné aplikácie mohli poskytovať služby eGovermentu prostredníctvom mobilného zariadenia, niektoré moduly UPVS musia byť upravené/doplnené o podporu tohto kanála. Tieto úpravy sú realizované v rámci projektu: projekt_514 - Centrálna API Manažment Platforma (Platforma pre publikovanie služieb štátu cez Open API) (CAMP):

- Rozšírenie IAM o OpenIDConnect/OAuth2 pre mobilnú autentifikáciu používateľa
- Vytvorenie API Gateway a transformovanie SOAP rozhraní existujúcich spoločných modulov na Open Rest API využiteľných mobilnými aplikáciami

Taktiež projekt využije výstupy projektu: projekt_307 - Zvyšovanie úžitkovej hodnoty digitálnych služieb pre občanov, podnikateľov a inštitúcie verejnej správy rozvojom ÚPVS a spoločných modulov (UPVS 3.0). Tento projekt rieši celkové zlepšenie eGov služieb a ich dostupnosť aj na mobilných zariadeniach prostredníctvom responzívneho designu webových aplikácií. Projekt SVM vytvára mobilný prístupový kanál cez natívnu mobilnú aplikáciu primárne určenú na aktívne vyvolanú interakciu FO s verejnou správou pre vybrané služby s priamym a opakovaným benefitom pre občana pri použití cez mobilné zariadenie. S projektom SVM sa tieto projekty vzájomne dopĺňajú, keďže výstupy týchto projektov sa následne využívajú v druhom projekte. Projekt UPVS 3.0 poskytne pre SVM modernizované služby spoločných modulov použiteľné natívnou mobilnou aplikáciou. Naopak, SVM poskytne pre projekt UPVS 3.0 mobilnú autentifikáciu pre prístup na portál UPVS ci už na PC, alebo na mobilnom zariadení.

Tvorba mobilnej aplikácie je aj predmetom projektu: projekt_346 - Rozvoj platformy integrácie údajov (centrálna integračná platforma) a Manažment osobných údajov (CIP a MOU). Projekty SVM ako aj MOU v rámci svojich zadaní majú definované vytvorenie mobilnej aplikácie. SVM svojou povahou, keďže bude poskytovať Mobile ID, nevie poskytovať svoje služby inak ako natívna aplikácia. MOU mobilná aplikácia je uväzovaná ako responzívna aplikácia. Z pohľadu občana môže byť používanie viacerých mobilných aplikácii na core funkcionalitu poskytovanú verejnou správou zmätočné a nepraktické. Projekty budú svoje aplikácie budovať vo vzájomnej spolupráci na základe metodických pokynov pre budovanie elektronických služieb a výhod jednotlivých prístupových kanálov od BRISK. Predpokladá sa vypracovanie používateľského prieskumu z ktorého vyplynú závery pre spôsob implementácie daných aplikácií. Alternatívne riešenia sú nasledovné:

- Samostatné aplikácie - aj v prípade budovania samostatných aplikácii je potrebné dodržať jednotný designe (mobilné ID-SK) a spoločné funkcionality (primárne Mobile ID) poskytované projektom SVM
- Spoločná aplikácia - tu sa ponúkajú 2 alternatívy riešenia:
    - Funkcionalita MOU bude vytvorená v SVM dodávateľom SVM, pričom sa využijú rozhrania OPEN API ktoré sú výstupom projektu MOU
    - Spoločný zdrojový kód - dodávatelia MOU aj SVM budú funkcionality tvoriť v spoločnom repozitári podľa definovaných pravidiel a požiadaviek na aplikáciu SVM

Projekt využije aj výstupy projektu: projekt_329 - Otvorené údaje 2.0 - Rozvoj centrálnych komponentov pre kvalitné zabezpečenie otvorených údajov. V rámci tohto projektu je budovaný GitLab pre publikáciu zdrojových kódov. Projekt SVM využije GitLab pre publikáciu zdrojových kódv Dizajn systému mobilných aplikácií.

Projekt nie je v konflikte s projektom: projekt_1067 - Rozvoj governance, dohľadu a bezpečnosti v podsektore VS. Projekt SVM rieši autentifikáciu G2B /G2C, kým projekt_1067 rieši autentifikáciu G2E.

4.2.2 Popis aplikačnej architektúry riešenia na úrovni modulov ISVS a vzťahov medzi nimi (TO-BE)

Navrhovaná aplikačná architektúra zabezpečuje poskytovanie 2 koncových a 5 integračných aplikačných služieb:

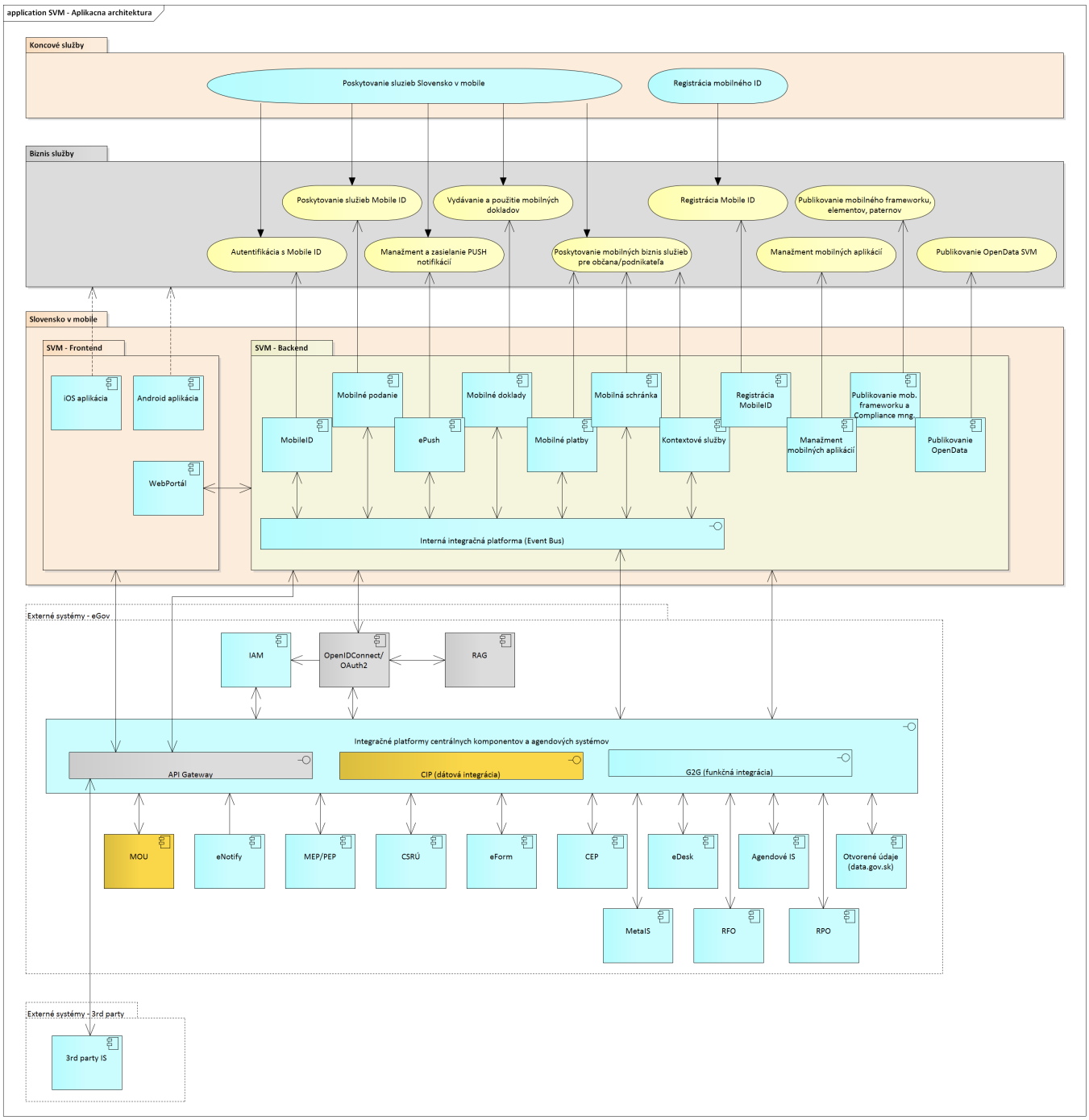
ISVS	*Koncová služba*		*Aplikačné služby*	
Slovensko v mobile	ks_339655	Registrácia mobilného ID	as_60921	Registrácia mobilného ID (registrovanie/odregistrovanie Mobile ID)
	ks_339656	Poskytovanie sluzieb Slovensko v mobile	as_60922	Poskytovanie služieb Slovensko v mobile
	N/A		as_60923	Registrácia Mobile ID pre externé aplikáce
			as_60924	Vyžiadanie interakcie FO prostredníctvom SVM (požiadavka na potvrdenie súhlasu, podpísanie dokumentu /podania, doplnenie údajov podania, prehľadu informácií)
			as_60925	Prijatie a distribúcia notifikácie
			as_60926	Vydanie mobilného dokladu
			as_60927	Poskytnutie údajov pre data.gov.sk
			as_60939	Integrácia SVM na spoločné moduly eGov

Kód služby	*Názov služby*	*Popis služby*
ks_339655	Registrácia mobilného ID	Koncová služba umožní prostredníctvom webového rozhrania na Portáli ÚPVS registrovanie a odregistrovanie mobilného ID pre používateľa FO prihláseného s eID.
ks_339656	Poskytovanie služieb Slovensko v mobile	Koncová služba zabezpečuje poskytovanie služieb mobilnej aplikácie Slovensko v mobile. Služba na Portáli ÚPVS poskytuje referenciu na app store pre stiahnutie mobilnej aplikácie SVM. V rámci samotnej mobilnej aplikácie sú poskytované služby mobilnej autentifikácie, mobilných podaní a potvrdení, zasielania PUSH notifikácií, vydávania a použitia mobilných dokladov, prezerania eDesku, platby poplatkov v súvislosti s mobilnými podaniami a kontextové služby.
as_60921	Registrácia mobilného ID	Aplikačná služba realizuje Koncovú službu Registrácia mobilného ID.

as_60922	Poskytovanie služieb Slovensko v mobile	Aplikačná služba realizuje Koncovú službu Poskytovanie služieb Slovensko v mobile.
as_60923	Registrácia Mobile ID pre externé aplikáce	Aplikačná služba umožní registráciu Mobile ID prostredníctvom rozhrania vypublikovaného na API GW. Služba je určená pre asistovanú registráciu Mobile ID.
as_60924	Vyžiadanie interakcie FO prostredníctvom SVM (požiadavka na potvrdenie súhlasu, podpísanie dokumentu/podania, doplnenie údajov podania, prehľadu informácií)	Aplikačná služba umožní integrovaným systémom vyžiadať interakciu FO prostredníctvom SVM (požiadavka na potvrdenie súhlasu, podpísanie dokumentu/podania, doplnenie údajov podania, zobrazenie prehľadu informácií). Služba notifikuje FO na jeho registrovaných mobilných zariadeniach o prijatej požiadavke. Po realizácii interakcie FO, SVM zašle výsledok interakcie, resp. timeout do zdrojového IS.
as_60925	Prijatie a distribúcia notifikácie	Aplikačná služba zabezpečuje príjem notifikácie zo zdrojového IS a ich následnú distribúciu na jednotlivé mobilné zariadenia FO.
as_60926	Vydanie mobilného dokladu	Aplikačná služba je určené pre IS VS, ako aj pre informačné systémy komerčných subjektov. Účelom služby je umožniť zdrojovému IS bezpečným a štandardným spôsobom doručiť mobilný doklad fyzickej osobe do mobilného zariadenia. Predpokladá sa sada metód na oboch stranách rozhrania, podporujúca celý proces vydania mobilného dokladu, od registrácie typu dokladu, zaslanie požiadavky o vydanie dokladu až po prijatie mobilného dokladu do mobilného zariadenia.
as_60927	Poskytnutie údajov pre data.gov.sk	Služba je určená na poskytovanie otvorených údajov SVM pre data.gov.sk
as_60939	Integrácia SVM na spoločné moduly eGov	Služba je určená na integráciu SVM na spoločné moduly eGovermentu

4.2.2.1 Model navrhovanej aplikačnej architektúry

Nasledujúci diagram vizuálne popisuje model navrhovanej aplikačnej architektúry na úrovni modulov ISVS a vzťahov medzi nimi, vrátane vzťahov na iné komponenty architektúry eGov.



Návrh aplikačnej architektúry systému Slovensko v mobile pokrýva požiadavky z biznis architektúry a je rozdelený na dve vrstvy:

- **SVM-Frontend** - ktorá predstavuje prezentačnú vrstvu primárne v podobe iOS a Android aplikácie na mobilných zariadeniach používateľa a WebPortál, ktorý zabezpečuje prezentačnú vrstvu pre administrátorov a používateľov backendových komponentov
- **SVM-Backend** - ktorá zabezpečuje biznis logiku na serverovej strane mobilnej aplikácie, ako aj funkcionality komponentov, ktorých prezentačnú vrstvu zabezpečuje WebPortál

Návrh architektúry dokreslujú väzby na existujúce a plánované komponenty eGoverment architektúry a externé systémy tretích strán:

- **Externé systémy – eGOV** – integrované centrálne komponenty eGOV, ako aj agendové IS orgánov verejnej moci. Farebne sú rozlíšené systémy, ktoré aktuálne neexistujú, ale sú plánované v rámci iných projektov
- **Externé systémy – 3rd party** – integrované systémy tretích strán (napr. banky, poisťovne a pod.), ktoré využívajú služby SVM

Slovensko v mobile

SVM-Frontend komponenty predstavujú samotnú mobilnú aplikáciu používateľa a sú uvedené pre úplnosť aplikačnej architektúry.

SVM-Backend komponenty poskytujú aplikačné služby a realizujú nasledovné funkcionality:

- MobileID
  - Autentifikácia a autorizácia prostredníctvom Mobile ID (UPVS, Agendové IS, 3rd party IS)
    - Autentifikácia a prihlásenie do slovensko.sk a do integrovaných portálov (Agendové IS/špecializované portály, 3rd party IS)
    - Autorizácia voči službe, ktorú chce občan/podnikateľ použiť
  - Mobilné podania
    - Poskytnutie súhlasu na používanie mobilného dokladu
      - UI v kontexte príslušného mobilného dokladu, ktorým používateľ poskytne súhlas na používanie mobilného dokladu inou osobou
      - Funkcionalita pre presun mobilného dokladu do SVM inej osoby (odobratie dokladu z SVM držiteľa dokladu, bezpečné prevzatie dokladu inou osobou)
      - Vygenerovanie elektronického potvrdenia, jeho podpísanie a doručenie do schránok poskytujúcich a prijímajúcich osôb
    - Potvrdenie súhlasu/oboznámenia sa s podmienkami alebo informáciou (informovaný súhlas)
      - Rozhranie pre IS VS a 3rd party IS pre zasielanie požiadaviek na potvrdenie súhlasu/oboznámenia sa s podmienkami alebo informáciou
      - Vygenerovanie push notifikácie o požiadavke na potvrdenie súhlasu/oboznámenia
      - UI pre zobrazenie požiadavky na potvrdenie a samotné potvrdenie súhlasu/oboznámenia
      - Vygenerovanie elektronického potvrdenia, jeho podpísanie a doručenie žiadajúcemu IS a do schránok žiadajúcich subjektov ako aj poskytovateľa súhlasu
    - Vygenerovanie elektronického podania
    - Podpísanie klikom (autorizačná doložka) elektronického podania/dokumentu
    - Zaslanie elektronického podania do centrálnej podateľne
  - Mobilné doklady
    - Prehľad mobilných dokladov
    - Vydanie mobilného dokladu – podpora procesu získania mobilného dokladu zo zdrojovej evidencie
    - Predloženie mobilného dokladu na overenie
      - Vizualizácia mobilného dokladu
      - NFC overenie mobilného dokladu
        - Evidencia logu NFC overení mobilného dokladu (kto, kedy, z akého zariadenia overoval doklad)
  - Mobilné platby
    - Platba správnych a súdnych poplatkov integráciou tzv. Virtuálneho kiosku systému eKolok
    - Automatické vyvolanie platby v kontexte prijatého platobného príkazu v schránke správ
    - Poskytnutie podporných funkcií pre kontextové služby v prípade ak bude potrebné poplatok zaplatiť pred zaslaním podania (zautomatizovanie činností pre používateľa)
  - Mobilná schránka
    - Mobilný prístup k eDesk schránke občana/podnikateľa
    - Potvrdenie prijatia správy v schránke správ
  - Kontextové služby
    - Vyhľadávanie elektronických služieb v kontexte údajov používateľa SVM (nad mobilnými dokladmi, prijatými správami v schránke správ, dátami poskytnutých prostredníctvom projektu MOU)
    - Inicializácia podania – informovanie používateľa o dostupných kontextových službách
    - Príprava a spustenie podania s využitím spoločných funkcií ostatných komponentov SVM
  - ePush
    - Prijatie a distribúcia push notifikácie na registrované zariadenia občana/podnikateľa
    - Manažment mobilných zariadení občana/podnikateľa (registrovanie/zrušenie registrácie zariadení na ktoré budú distribuované push notifikácie)
    - Manažment odoberaných tém (občan/podnikateľ si môže sám manažovať, pre ktoré témy chce dostávať push notifikácie a pre ktoré nie)
    - Manažment aplikácií (správca komponentu bude manažovať ktoré aplikácie IS VS, resp. 3rd party môžu posielať push notifikácie a v ktorých témach)
  - Registračný komponent – systém bude slúžiť pre zabezpečenie procesu registrácie Mobile ID a jeho spárovania s eID používateľa, poskytnutia autorizačných certifikátov a zaevidovania identity pre používanie Mobile ID
  - Manažment mobilných aplikácií – web portál pre evidenciu a správu mobilných aplikácií verejnej správy, regitráciu 3rd party aplikácií pre bezpečné využívanie spoločných a znovupoužiteľných komponentov mobilného frameworku
    - Zoznam overených mobilných aplikácií IS VS ako aj 3rd party
    - Verifikácia mobilných aplikácií (Verify by MIRRI) – web s údajmi o každej mobilnej aplikácii
    - Registrovanie mobilných aplikacii s vygenerovaným UID pre znovupoužitie mobilných serverových komponentov poskytnutých v rámci design platformy (napr. MobileId, Kontextové služby, ePush atď.)
    - Správa mobilných aplikácií (vymazanie, update údajov o aplikácii, compliance informácie)
    - Konfigurácia mobilných aplikácií (využitých komponentov design platformy)

- Publikovanie mobilného frameworku a Compliance management
    - Publikovanie mobilného frameworku – webový portál pre zverejňovanie komponentov, dokumentácie pre 3rd party developerov (verzionovanie, diskusia, blog). Pre zverejňovanie zdrojových kódov bude použitý GitLab vytvorený v rámci projektu Otvorené údaje 2.0. Zdrojové kódy budú odovzdané a tým bude splnená požiadavka EUPL podľa § 15, odsek (2) bod d) EUPL a naplnené zabránenie vendor - lock podľa Zákona 95/2019.
    - Compliance management – workflow systém pre príjem, posúdenie a informovanie 3rd party developera o zhode mobilnej aplikácie alebo jej časti s definovanými pravidlami
- Publikovanie OpenData - publikovanie otvorených údajvo z projektu SVM na portál data.gov.sk. Očakávané je publikovanie predovšetkým štatistických datasetov o využití mobilnej aplikácie SVM.
- Interná integračná platforma (Event Bus) – integračná platforma zabezpečujúca príjem a distribúciu udalostí pre registrované systémy. SVM bude primárne využívať udalosti prichádzajúce z RFO a RPO.

Externé systémy – eGOV

Centrálne moduly eGOV, ktoré sú využívané pri poskytovaní služieb SVM a agendové IS, ktoré budú využívať služby a funkcie SVM:

- IAM (isvs_8846) – kľúčový centrálny modul, ktorý poskytuje služby autentifikácie používateľa
    - OpenIDConnect/OAuth2 – ide o rozšírenie centrálneho IAM modulu pre potreby mobilných aplikácií, ktoré využívajú OAuth2 protokol. Pôvodný modul IAM ostáva nezmenený, pričom OAuth2 s ním bude priamo integrovaný a využije jeho existujúce rozhrania.
    - RAC - centrálny register autentifikačných certifikátov pre Mobile ID, perzistencia certifikátov používateľa
- eNotify (isvs_9370) – centrálny notifikačný modul bude integrovaný pre zasielanie emailových alebo SMS notifikácií
- MOU (isvs_8705) – modul osobných údajov je plánovaný projekt, ktorý poskytne služby prístupu k dátam občana, ako aj služby Consent managementu pre potvrdenie prístupu k osobným dátam občana tretími stranami. Z hľadiska aplikácie SVM budú využité služby prístupu k dátam občana v moduloch kontextových služieb a mobilných dokladov
- CSRÚ (isvs_5836) - centrálny systém referenčných údajov bude využitý pre získanie referenčných údajov pri tvorbe a generovaní podaní v SVM
- MEP(isvs_8850)/PEP(isvs_5585) – modul elektronických platieb a systém pre evidenciu správnych a súdnych poplatkov bude využitý pri riešení mobilných platieb poplatkov za elektronické podania, predpokladané je využitie funkcionalít tzv. Virtuálneho kiosku
- CEP (isvs_9368) – centrálna elektronická podateľna bude využitá pri podaní podania vytvoreného v SVM
- eForm (isvs_8848) – modul elektronických formulárov bude využitý pre vizualizáciu elektronických podaní podľa transformačných schém registrovaných v tomto module
- eDesk (isvs_8847) – elektronická schránka občana/podnikateľa, SVM použije rozhrania modulu pre prístup používateľa do eDesk prostredníctvom jeho mobilného zariadenia
- Agendové IS – jednotlivé agendové IS môžu využívať služby SVM ako napríklad notifikácie, alebo autentifikáciu mobilným ID
- RFO (isvs_191) – ide o agendový IS, samostatne je uvedený pretože udalosti o zmenách v tomto IS sú nevyhnutné pre správne fungovanie Mobile ID
- RPO (isvs_420) - ide o agendový IS, samostatne je uvedený pretože udalosti o zmenách v tomto IS sú nevyhnutné pre správne fungovanie Mobile ID
- Meta IS (isvs_63) – výmena informácii o IS VS, primárne v oblasti mobilných aplikácií
- Modul Otvorené dáta (isvs_9342) – modul pre publikovanie otvorených údajov. SVM bude publikovať primárne štatistické údaje o používaní mobilnej aplikácie SVM.
- Integračné platformy centrálnych komponentov a agendových systémov – systém SVM využije existujúce a plánované centrálne integračné platformy ako sú G2G, CIP (dátová integrácia)
    - API GW (isvs_9514) – API Gateway ktorá bude publikovať rozhrania komponentov eGov v štandarde OpenAPI

Externé systémy – 3rd party

- 3rd party IS – ide o informačné systémy tretích strán, napr. OVM, banky, poisťovne a pod., ktoré majú záujem využívať služby SVM ako napríklad notifikácie, alebo autentifikáciu mobilným ID

4.2.2.2 Vyjadrenie k mandatórnym požiadavkám

Tabuľka mandatórne požiadavky:

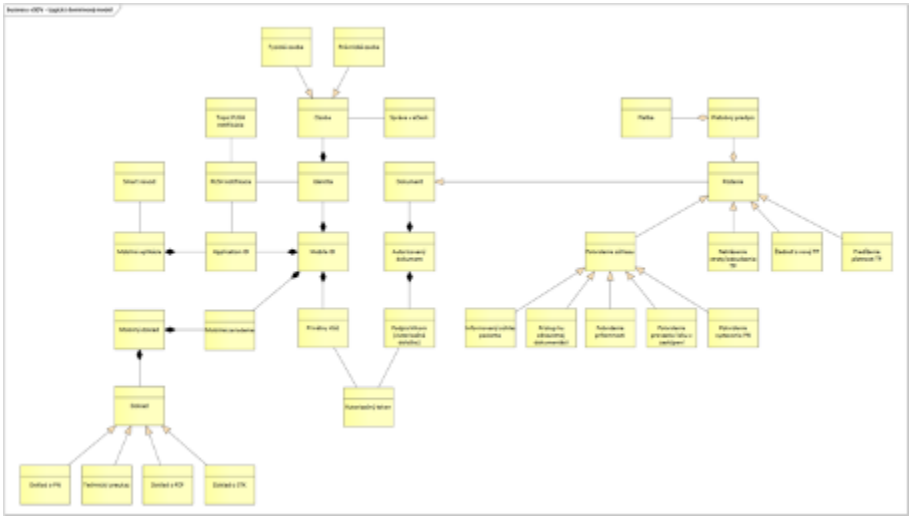
Požiadavka	***Požiadavka zahrnutá v projekte***
Použitie, alebo poskytovanie referenčných údajov (§ 49 – 55 zákona 305/2013	*Áno*
Požiadavky na používanie registrovaných jednotných referencovateľných identifikátorov „URI“ (centrálny model údajov verejnej správy)	*Áno*
Požiadavky na riešenie nariadenia (EU) 2016/679 - GDPR o ochrane osobných údajov – spôsob riešenia služby „Moje dáta“ (podľa konceptu Strategická priorita Manažment údajov (https://www.mirri.gov.sk/sekcie/strategicke-priority-nikvs/index.html)	*Áno*

Požiadavky na riešenie zabezpečenia manažmentu zmluvných vzťahov pre poskytovanie služieb– vyplýva zo Zákona o ITVS 95/2019, §14, odsek 6 a automatizáciu monitorovania služieb a ich úrovne poskytovania	*Áno*
Požiadavky na časť "Zoznam CI položiek (HW a SW) pre import do Servicedesku" (CMDB)	*Áno*
Požiadavky "Automatizované monitorovanie služieb"– povinný výstup každého projektu.	*Áno*
Požiadavky na časť "Poskytovanie analytických údajov a otvorených údajov (Open Data – detaily pre publikovanie na https://data.gov.sk/) "	*Áno*
Požiadavky pre časť „aplikačné služby na externú integráciu" – prepájanie ISVS sa realizuje prostredníctvom vzťahu na úrovní 2 AS, ktoré nesmú poskytovať KS	*Áno*
Požiadavka aby služby boli implementované tak, aby aj po nasadení do prevádzky fungovalo testovacie prostredie pre konzumentov a aby si integráciu mohol konzument otestovať aj s eID	*Áno*
Požiadavky na návrh digitálnych služieb v súlade s Metodickým usmernením pre tvorbu používateľsky kvalitných elektronických služieb verejnej správy (https://www.mirri.gov.sk/wp-content/uploads/2020/10/Metodicke-usmernenie-pre-tvorbu-pouzivatelsky-kvalitnych-elektronickych-sluzieb-VS_7102020.pdf)	*Áno*
Požiadavky na publikovanie elektronických služieb ISVS - aplikáciu odporúčaní z dokumentu Pravidlá publikovania elektronických služieb do multikanálového prostredia verejnej správy (https://www.mirri.gov.sk/wp-content/uploads/2018/10 /Pravidla_Publikovania_Sluzieb_v1_0-1.pdf)	*Áno*

4.2.3 Popis dátovej architektúry riešenia na úrovni objektov evidencie a vzťahov medzi nimi

4.2.3.1 Logický dátový model

Nasledujúci diagram znázorňuje HighLevel logický doménový model. Zobrazuje hlavné entity vystupujúce v projekte Slovensko v Mobile a kľúčové väzby medzi nimi. Nepredstavuje finálny dátový model, ten bude vytvorený vo fáze detailnej funkčnej špecifikácie. Slúži na identifikáciu potrieb a závislostí voči iným projektom a ISVS a ako podklad pre posúdenie projektu z hľadiska bezpečnosti.



Tabuľka Entity LDM:

Doména	***Entita***	***Popis***
Mobile ID	*Mobile ID*	*Predstavuje mobilnú reprezentáciu identity osoby, ktorých môže mať občan viac čo je realizované kompozíciou Identity, Mobilného zariadenia, Application ID a Privátneho kľúča*
	Identita	*Elektronická reprezentácia identity osoby*
	Application ID	*Identifikátor mobilnej aplikácie*

	Mobilné zariadenie	*Mobilné zariadenie osoby*
	Privátny kľúč	*Privátny kľúč osoby generovaný pre dané Mobile ID*
	Osoba	*Predstavuje zovšeobecnenie právnickej, alebo fyzickej osoby*
	Právnická osoba	*Právnická osoba registrovaná v RPO*
	Fyzická osoba	*Fyzická osoba registrovaná v RFO*
	Autorizačný token	*Autorizačný token generovaný pre autorizáciu prístupu, resp. pre podpis klikom*
PUSH notifikácie	*Topic PUSH notifikácie*	*Téma PUSH notifikácií ktoré si môže používateľ aktivovať*
	PUSH notifikácia	*PUSH notifikácia distribuovaná na mobilné zariadenie používateľa*
eDesk	*Správa v eDesk*	*Prijatá, alebo odoslaná správa v eDesku používateľa*
Podania	*Podpis klikom*	*Predstavuje autorizačnú doložku priloženú k súboru informácií, ktoré používateľ autorizoval*
	Autorizovaný dokument	*Zovšeobecnenie súboru informácií ktoré používateľ autorizoval, vyjadril súhlas*
	Dokument	*Zovšeobecnenie pre súbor informácií, môže ísť napr. o PDF dokument, alebo eForm*
	Podanie	*Podanie k elektronickej službe eGovermentu*
	Nahlásenie straty /odcudzenia TP	*Špecifické podanie pre Nahlásenie straty/odcudzenia TP*
	Žiadosť o nový TP	*Špecifické podanie pre Žiadosť o nový TP*
	Predĺženie platnosti TP	*Špecifické podanie pre Predĺženie platnosti TP*
	Potvrdenie súhlasu	*Zovšeobecnenie pre Potvrdenie súhlasu*
	Informovaný súhlas pacienta	*Špecifické potvrdenie súhlasu pre Informovaný súhlas pacienta*
	Prístup ku zdravotnej dokumentácii	*Špecifické potvrdenie súhlasu pre Prístup ku zdravotnej dokumentácii*
	Potvrdenie prítomnosti	*Špecifické potvrdenie súhlasu pre Potvrdenie prítomnosti*
	Potvrdenie prevzatia lieku v zastúpení	*Špecifické potvrdenie súhlasu pre Potvrdenie prevzatia lieku v zastúpení*
	Potvrdenie vystavenia PN	*Špecifické potvrdenie súhlasu pre Potvrdenie vystavenia PN*
Platby	*Platobný príkaz*	*Štruktúrovaný platobný príkaz prijatý v eDesku z MEP*
	Platba	*Informácia o realizovanej platbe prostredníctvom Virtuálneho kiosku*
Mobilné doklady	*Mobilný doklad*	*Mobilná reprezentácia dokladu. Tvorená je kompozíciou dokladu a mobilného zariadenia. Doklad sa nemusí vždy viazať na identitu používateľa, napr. ak ide o doklad k veci, napr. vozidlu*
	Doklad	*Zovšeobecnenie pre doklad slúžiaci na preukazovanie určitých skutočností*
	Doklad o PN	*Doklad o Pracovnej Neschopnosti*
	Technický preukaz	*Technický preukaz (TP)*
	Doklad o PZP	*Doklad o Povinnom Zmluvnom Poistení*
	Doklad o TK a EK	*Doklad o Technickej Kontrole a Emisnej Kontrole*

Manažment mobilných aplikácií	*Mobilná aplikácia*	*Mobilná aplikácia*
Smart návody	*Smart návod*	*Návod pre používateľa*

4.2.3.2 Použité referenčné registre

Aplikácia bude používať nasledovné referenčné registre:

- Register právnických osôb, podnikateľov a orgánov verejnej moci
- Register fyzických osôb
- Register adries

4.2.3.3 Prístup k riešeniu konceptu „Moje Dáta“ a GDPR

Moje Dáta

Aplikácia Slovensko v mobile nebude vytvárať nové objekty evidencie pre koncept Moje Dáta. Ide o frontend aplikáciu, ktorú využijú agendové IS VS pre interakciu s občanom. Zdrojom objektov pre koncept Moje Dáta je v takomto prípade agendový systém ktorý využije aplikáciu Slovensko v mobile.

Koncept Moje Dáta bude využitý z pohľadu využitia služieb ktoré tento koncept zavádza pre pokročilejšie (kontextové) služby aplikácie Slovensko v mobile:

- Poskytnutie súhlasu na spracovanie Mojich Dát občana pre kontextové služby
- Získanie a spracovanie Mojich Dát občana v kontextových službách

Predpokladané rozhrania systému Manažment osobných údajov ktoré budú využité:

- Sprístupnenie dát na základe splnomocnenia a súhlasov (as_56448)
- Servisná zbernica integrácie údajov (as_56531)
- Poskytnutie údajov z IS Manažment osobných údajov (as_60009)

GDPR

V súvislosti s prevádzkovaním aplikácie bude dochádzať ku spracovaniu osobných údajov fyzických osôb, ktoré budú využívať aplikáciu. Projekt /dodávateľ na základe tejto skutočnosti musí zabezpečiť implementáciu všetkých požiadaviek v zmysle príslušných ustanovení Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES.

Osobné údaje je potrebné spracovávať iba pre odôvodnené účely spracúvania osobných údajov, po obmedzenú dobu a s využitím maximálnej možnej miery zabezpečenia. Pre dodržanie všetkých legislatívnych požiadaviek Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 je potrebné realizovať vo fáze vývoja a implementácie aplikácie analýzu organizačných a IT procesov, ktoré pokrývajú spracovateľské činnosti osobných údajov.

Aplikácia Slovensko v mobile sa bude riadiť národnou legislatívou, kde je ochrana osobných údajov fyzických osôb upravená:

- Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
- Vyhláška Úradu na ochranu osobných údajov SR č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov

4.2.3.4 Požiadavky na dátovú integráciu na CSRÚ (poskytovanie a konzumovanie údajov)

Poskytovanie údajov

Aplikácia Slovensko v mobile bude poskytovať nasledujúce údaje pre dátovú integráciu:

- Témy (topic) PUSH notifikácií
- Typy podporovaných mobilných dokladov
- Registrované mobilné aplikácie

Konzumovanie údajov

Aplikácia bude konzumovať z CSRÚ nasledovné údaje:

- Referenčné registre
- Údaje o vozidlách občana
- Údaje o emisnej a technickej kontrole
- Výhľadovo môže SVM pristupovať k ďalším objektom evidencie, podľa toho ako budú do aplikácie zaraďované ďalšie konkrétne eGov služby

4.2.3.5 Prístup k zabezpečeniu dátovej kvality a čistenie dát

Dátová kvalita a čistenie dát bude zabezpečené projektovými a procesnými aktivitami:

- Projektové aktivity
  - V rámci DFŠ budú definované vstupné objekty evidencie z iných informačných systémov, voči ktorým prebehne referencovanie
- Procesné aktivity
  - Pre oblasti kde vzniknú kmeňové údaje (PUSH notifikácie, Manažment mobilných aplikácií) budú zavedené princípy manažmentu kvality kmeňových údajov a návrh riešenia konfliktov do budúcnosti. V rámci procesov budú definované role zabezpečujúce správu týchto údajov a ich priradenie zodpovedným organizačným útvarom.

4.2.3.6 Prístup k príprave a zabezpečení testovacích dát

Testovacie dáta budú pripravované v spolupráci so zástupcami zdrojových IS VS, ktoré budú využívať funkcionality Slovensko v mobile:

- Mobile ID – pre túto oblasť je potrebné zabezpečiť dostatočné množstvo testovacích eID kariet, ako aj testovacích identít, čo bude riešené v spolupráci s NASES
- Pre ostatné funkcionality budú testovacie dáta vytvárané testovacím tímom manuálne/skriptom pre manuálne ako aj automatizované testy, keďže nepredpokladáme využitie napr. anonymizovaných dát z existujúcich IS

4.2.3.7 Návrh dát, ktoré budú publikované ako Open Data

Aplikácia Slovensko v mobile predstavuje spoločnú frontend vrstvu pre agendové IS VS, preto v oblasti Open Data sú uvažované primárne štatistické datasety o využívaní mobilnej platformy:

- Počet registrovaných Mobile ID
- Počet autorizácií s Mobile ID
- Počet podaní s Mobile ID
- Počet distribuovaných PUSH notifikácií
- Číselník mobilných aplikácii
- Číselník platforiem
- Číselník push notifikačných tém

4.2.3.8 Prístup k migrácii dát

Migrácia dát nie je požadovaná, keďže sa jedná o nový IS, ktorý nerieši biznis logiku aktuálnych agend.

4.3 Technologická vrstva

Pri technickej a systémovej architektúre budú dodržané všetky definované priority informatizácie VS a tiež všetky technologické a dátové princípy, ako sú najmä:

- Technologická interoperabilita – softvér a hardvér vo verejnej správe musí byť v súlade s definovanými štandardami, ktoré podporujú interoperabilitu údajov, aplikácií a technológií.
- Otvorené štandardy – prednostne sa budú používať otvorené štandardy a formáty a dôraz bude na zabezpečení technologickej neutrálnosti.
- Vládny cloud prednostne – informačné systémy a technológie, ktoré sa v rámci verejnej správy rozvíjajú alebo modifikujú, musia byť budované v kooperácii s poskytovateľmi cloudových služieb v zmysle ich nasadenia do Vládneho cloudu.
- Otvorenosť údajov – údaje otvorenej vlády musia byť dostupné a prehľadné. Vybrané množiny údajov nebudú podliehať princípom otvorených údajov. Tento princíp však nesmie byť v rozpore s princípom „jeden krát a dosť“.
- Údaje sú dostupné a zdieľané – používatelia majú prístup ku všetkým údajom, na ktoré majú legitímny nárok, či už pre informatívne účely alebo pre potreby naplnenia svojich povinností. Údaje sú a budú zdieľané naprieč verejnou správou v súlade s platnou legislatívou. - Jednoduché používanie aplikácií – aplikácie VS musia byť jednoduché na použitie pre koncového používateľa, či už z technického alebo z obsahového hľadiska.
- Bezpečnosť údajov – údaje budú chránené najmä pred neoprávneným prístupom, manipuláciou, použitím a zverejnením (zachovanie dôvernosti údajov), ich úmyselnou alebo neúmyselnou modifikáciou (zachovanie integrity údajov) a budú dostupné v požadovanom čase a v požadovanej kvalite (zachovanie dostupnosti údajov).
- Pravosť údajov – používateľ bude pracovať len s údajmi, ktorých hodnovernosť a pôvod sú zabezpečené napr. ich autorizáciou.
- Auditovateľnosť – riadenie informačnej bezpečnosti, rovnako ako aj iných aktivít vo VS, musí používať princípy a pravidlá, ktoré umožňujú výkon kontroly a zároveň umožňujú generovanie auditných a iných log záznamov s požadovanou úrovňou ich ochrany.

- Otvorené API – aplikačné rozhrania elektronických služieb sú verejné pre dôveryhodné aplikácie tretích strán. Aplikačné rozhrania v informačných systémoch sú budované spôsobom umožňujúcim ich použitie komukoľvek (po splnení určených podmienok). Špecificky všetky služby informačných systémov, ktoré sú dostupné grafickým rozhraním majú byť dostupné aj otvoreným aplikačným rozhraním.

Multikanálový prístup

Natívna mobilná aplikácia Slovensko v mobile bude mobilným prístupovým kanálom k službám štátu. Výhodami natívnej mobilnej aplikácie sú:

- Možnosť bezpečného uloženia privátnych kľúčov a pokročilé kryptovanie.
- Bezpečnosť položiek Keychain-ov a SecureStore-ov, ktoré sú prístupné len pre danú aplikáciu (Sandbox). V prípade internetových prehliadačov je to pre všetky aktuálne bežiace web aplikácie.
- Podpora systémového aj aplikačného autorizačného follback-u, pre potreby ochrany privátnych parametrov uložených v secure priestoroch (touchId/faceId – passcode - lock).
- Automatická podpora najnovších technológii mobilného zariadenia vo forme frameworkov, knižníc, príkladov a dokumentácie.
- Umožňujú priamy prístup k hardvéru zariadenia, ktorý je pre web aplikácie nedostupný (Bluetooth, NFC, Kamera, ...).
- Rýchlosť a výkon - Mobilné aplikácie pracujú s integrovanými funkciami telefónu, ako sú lokalizačné služby, mikrofón a kamera, takže aplikácie vytvorené pre mobilné zariadenie fungujú rýchlejšie.
- Push notifikácie - mobilné aplikácie umožňujú posielať používateľom pripomienky, čo zvyšuje zapojenie a zároveň otvára ďalší komunikačný kanál, jedným z cieľov je notifikovať občana prirodzeným spôsobom, na ktorý je zvyknutý z komerčného sveta a sveta dnes bežne dostupných a používaných aplikácií (mentálny model používateľa nechceme narušiť) .
- Offline prístup – podpora offline funkcionality nezávislej od dostupnosti pripojenia na sieť a dátové služby.
- UIX - Natívne aplikácie sú interaktívne, intuitívne a fungujú plynulejšie. Mobilné zariadenia Android a iOS (Apple) majú svoje špecifické usmernenia a štandardy používateľského rozhrania. iOS a Android majú typické menu, zoznamy, dizajnové prvky, tlačidlá atď. Preto sa užívateľovi v nich omnoho ľahšie orientuje.
- Podpora pre ľahšie vytváranie obrazoviek a aplikačných flowov. Množstvo rozlíšení obrazoviek mobilných zariadení komplikuje vývoj aj pre web aplikáciu. V tomto ohľade je vývoj natívnej aplikácie rýchlejší.
- Umožňujú používateľovi používať gestá ruky špecifické pre dané zariadenie. Android a iOS postupne vyvíjajú rôzne konvencie pre interakciu a natívna aplikácia reaguje tak, ako to používateľ očakáva.
- Distribúcia v rámci App Store alebo Google Play obchodov s aplikáciami pomáha pri vyhľadávaní a kontroluje kvalitu, bezpečnosť a kompatibilitu zariadení. Natívne aplikácie dostanú schválenie obchodu s aplikáciami, pre ktorý sú určené, čo znamená, že používateľ môže mať väčšinou istotu zlepšenia bezpečnosti a zabezpečenia aplikácie
- Propagačné možnosti - zaradenie aplikácie do obchodu App Store alebo Google Play rozšíri váš dosah na širšie publikum.

Z hľadiska technickej architektúry musí mať natívna mobilná aplikácia čo najnižšiu závislosť na frameworkoch pre tvorbu mobilných aplikácií a v čo najväčšej miere využívať platformové frameworky.

Technologická architektúra backend komponentov

Pri budovaní aplikačných komponentov v rámci navrhovaného riešenia sa predpokladá využitie služieb vládneho cloudu. Pôjde minimálne o model využívania dostupných služieb IaaS (teda využitie virtuálneho dátového centra), pri ktorom cloudovú službu predstavuje poskytovanie virtualizovanej infraštruktúry ako serverov, úložísk údajov a sieťovej infraštruktúry. Zároveň sa okrem vlastnej fyzickej lokality predpokladá aj využitie housingových služieb z DC vládneho cloudu.

Predpokladá sa využitie najmä nasledujúcich služieb typu IaaS:

- virtuálny server,
- diskový priestor,
- sieťové pripojenie,

Predpokladá sa využitie najmä nasledujúcich služieb typu PaaS:

- služby aplikačnej vrstvy,
- služby bezpečnosti,
- služby monitoringu a manažmentu.

Predpokladá sa využitie nasledujúcich služieb typu SaaS

- aplikácia pre správu webového obsahu,
- aplikácia pre zálohu a archiváciu dát
- Služby vládneho cloudu
    - Profil klienta
    - Portfólio klienta
    - eID CA

Riešenie Slovensko v mobile pre novovytvorené cloudove služby využije Kubernetes - CaaS (container as a service) ako orchestračný systém pre automatické nasadzovanie, škálovanie a manažment kontajnerových aplikácii. Pre kontajnerizáciu aplikácii, servisov a mikroservisov využije Docker technológiu.

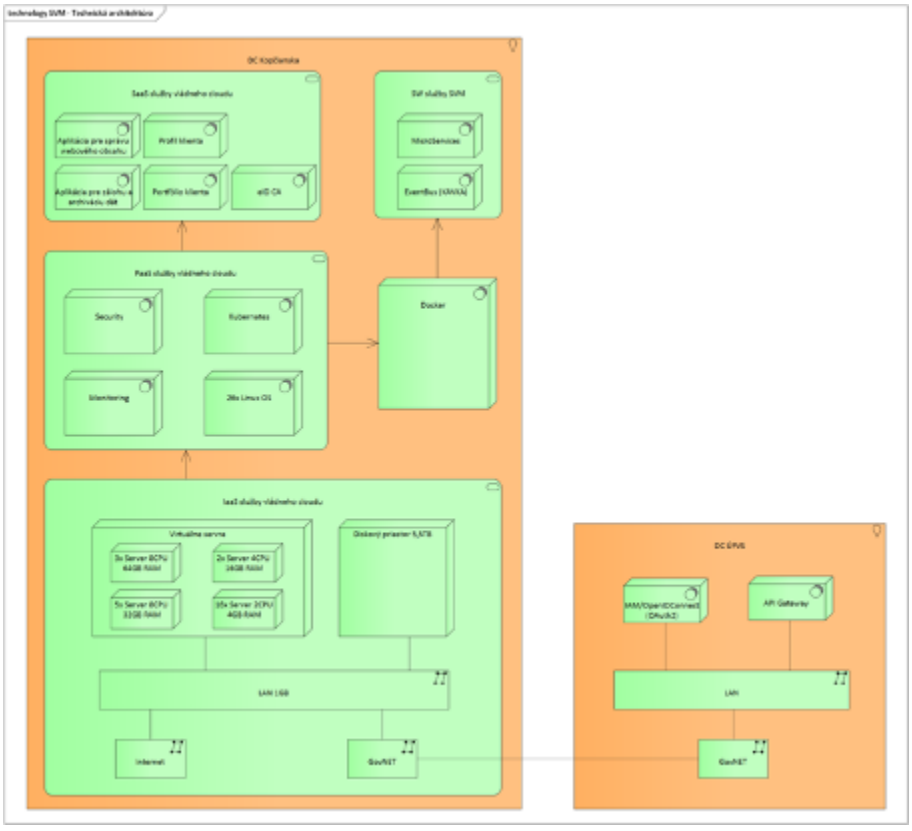
Keďže aktuálne vládny cloud neposkytuje služby typu CaaS, riešenie bude do prevádzky v prvej fáze nasadené bez orchestračnej platformy pre kontajnerové aplikácie. Riešenie ale bude pripravené na migráciu na takúto platformu po jej dobudovaní.

Návrh a riešenie aplikačnej časti bude orientované na rozšíriteľnosť, dynamickú škálovateľnosť a znovupoužiteľnosť jednotlivých servisov a komponentov.

Architektonický návrh a realizácia jednotlivých backendových komponentov bude v čo najväčšej miere zohľadňovať architektúru mikroslužieb s architektúrou riadenou udalosťami (Microservices architecture with Event-driven architecture). Tento návrh zohľadňuje princípy:

- **Princíp jednotnej zodpovednosti** - Každá mikroslužba musí byť zodpovedná za konkrétnu vlastnosť alebo funkčnosť alebo agregáciu spoločnej funkčnosti. Pravidlom, ktoré uplatňuje túto zásadu, je: „Zhromaždite veci, ktoré sa menia z rovnakého dôvodu, oddeľte veci, ktoré sa menia z rôzneho dôvodu“.
- **Návrh založený na doméne** - Návrh založený na doméne je architektonický princíp v súlade s objektovo orientovaným prístupom. Odporúča navrhovať systémy, ktoré odrážajú domény skutočného sveta. Berie do úvahy obchodnú oblasť, prvky a správanie a interakcie medzi obchodnými doménami.
- **Architektúra orientovaná na služby** - Service Oriented Architecture (SOA) je štýl architektúry, ktorý presadzuje určité princípy a filozofie. Nasledujú princípy SOA, ktoré treba dodržiavať pri navrhovaní mikroslužieb pre cloud:
    - **Zapuzdrenie** - Služby musia zapuzdrovať podrobnosti vnútornej implementácie, aby si externý systém využívajúci služby nemusel robiť starosti s vnútornými súčasťami. Zapuzdrenie znižuje zložitosť a zvyšuje flexibilitu (prispôsobivosť zmenám) systému.
    - **Voľné spriahnutie** - Zmeny v jednom mikrosystéme by mali mať nulový alebo minimálny vplyv na ostatné služby v ekosystéme. Tento princíp tiež navrhuje mať voľne spojené komunikačné metódy medzi mikroslužbami.
    - **Oddelenie rizík** - Vyvíjajte mikroslužby na základe odlišných funkcií s nulovým prekrytím s ostatnými funkciami. Hlavným cieľom je znížiť interakciu medzi službami tak, aby boli vysoko súdržné a voľne spojené.

Nasledujúci diagram zobrazuje navrhovanú technologickú architektúru:



4.3.1 Infraštruktúra

V rámci technických požiadaviek pre životný cyklus projektu Slovensko v mobile sú využívané 5 prostredia. Tieto prostredia sú oddelené a na sebe nezávisle.

- **DEV - vývojárske prostredie** na strane riešiteľa. Primárne určené pre prístup vývojárom softvéru, kde si vedia simulovať nasadenie aplikácie a chod v klastri.
- **INT - integračne prostredie** na strane riešiteľa. Toto prostredie je pre vývojárov softvéru s možnosťou napojenia na existujúce systémy, kde je možne overiť integračne funkcionality a scenáre.
- **QA – testovacie prostredie**. Toto prostredie je primárne určené pre testerov softvéru, kde po ukončení vývojového cyklu vedia testovať väčšie celky funkcionalít s napojením na externe existujúce systémy (integračné). Snaží sa v čo najväčšej miere kopírovať prostredie UAT na strane objednávateľa.
- **UAT** - testovacie prostredie objednávateľa na zabezpečenie používateľského akceptačného testovania.
- **PROD** - produkčné prostredie objednávateľa

V prvých fázach vývoja a nasadzovania produktu budú využité IaaS služby ako vládneho cloudu tak infraštruktúry UPVS/NASES. Pre plne nasadenie produktu, bude nevyhnutné rozšírenie služieb vládneho cloudu alebo infraštruktúry UPVS o služby orchestrácie novovzniknutých servisov (preferovaný Kubernetes a Docker).

Požiadavky na sizing

Prostredie DEV/INT

- Technologické požiadavky:
- Linux OS
- Kubernetes cluster ako služba
- Docker

- Hardvérové požiadavky:

Služba / Komponent	Počet inštancii	Požiadavky spolu pre všetky inštancie
Event Bus/Kafka	1x	4x CPU, 16GB RAM, 100GB disk
PosgreSQL/MobileID	1x	2x CPU, 4GB RAM, 100GB disk
ePush	1x	2x CPU, 4GB RAM, 20GB disk
Registračný komponent – Web Portál	1x	2x CPU, 4GB RAM, 20GB disk
Mobilné doklady	1x	2x CPU, 4GB RAM, 20GB disk
Mobilné platby/ Mobilná schránka	1x	2x CPU, 4GB RAM, 20GB disk
Mobilné podania	1x	2x CPU, 4GB RAM, 20GB disk
Kontextové služby	1x	2x CPU, 8GB RAM, 100GB disk
Manažment mobilných aplikácii/ Publikovanie mobile frameworku a complience management	1x	2x CPU, 4GB RAM, 20GB disk
Logging	1x	2x CPU, 4GB RAM, 100GB disk

Prostredie QA/UAT/ PROD

- Technologické požiadavky:
    - Linux OS (CentOS 8)
    - Kubernetes cluster ako služba
    - Docker

- Hardvérové požiadavky:

Služba / Komponent	Počet inštancii	Požiadavky spolu pre všetky inštancie
Event Bus/Kafka	3x	8x CPU, 64GB RAM, 500GB disk Tier 1
PosgreSQL	3x	8x CPU, 32GB RAM, 1TB disk Tier 1
MobileID	2x	2x CPU, 4GB RAM, 20GB disk Tier 2
ePush	2x	4x CPU, 16GB RAM, 20GB disk
Registračný komponent – Web Portál	2x	2x CPU, 4GB RAM, 20GB disk
Mobilné doklady	2x	2x CPU, 4GB RAM, 20GB disk
Mobilné platby	2x	2x CPU, 4GB RAM, 20GB disk
Mobilná schránka	2x	2x CPU, 4GB RAM, 20GB disk
Mobilné podania	2x	2x CPU, 4GB RAM, 20GB disk
Kontextové služby	2x	8x CPU, 32GB RAM, 100GB disk Tier 1
Manažment mobilných aplikácii	2x	2x CPU, 4GB RAM, 20GB disk
Publikovanie mobile frameworku a complience management	2x	2x CPU, 4GB RAM, 20GB disk
Logging	2x	2x CPU, 4GB RAM, 100GB disk

Predpokladané zaťaženie

- Počty používateľov 3,6 mil.
- Počet autentifikačných prístupov 20 mil./rok (podľa aktuálneho počtu prístupov na slovensko.sk)
- Počet podpisov podaní 3 mil./rok (približne 60% aktuálneho množstva podaní)
- Počet push notifikácii 25000/hod (podľa aktuálneho počtu notifikácii z eNotify modulu UPVS)

S predkladaným rastom využívania služieb aplikácie Slovensko k mobile určite porastie aj počty autorizácii, podaní a notifikácii. Návrh vytvára rezervu na HW požiadavky, avšak v budúcnosti je nutné rátať s navyšovaním výkonu a sizingu prostredí.

Komunikácia, sieťová a komunikačná infraštruktúra

Projekt využije public API Gateway projektu CAMP (projekt_514) zabezpečenú Revers Proxy, Firewal-om a load balancerami pre prístup z verejnej siete.

Projekt využije privátnu API Gateway projektu CAMP (projekt_514) zabezpečenú VPN prístupom pre prístup v rámci interných komponentov a spoločných modulov ÚPVS.

Interná asynchrónna komunikácia pomocou EvenBus zbernice medzi mikroservismi, komponentami a externými systémami bude taktiež v zabezpečenej sieti GovNET.

4.3.2 ICloud HW a SW

Viď Kapitoly infraštruktúra (sizing) a Technologická architektúra backend komponentov.

4.3.3 Softvérová systémová infraštruktúra

Preferovaný operačný systém je Linux (napr.. CentOS).

Pre uloženie dát to budú SQL DB – predbežne sa počíta s PostgreSQL, v prípade, že vládny cloud poskytne OracleDB ako jeden zo servisov, bude využitá, prípadne premigrovaná do tejto DB.

4.3.4 Databázová štruktúra

Pre uloženie dát sa počíta s využitím distribuovaných SQL databáz.

4.3.5 Hlavné riadiace toky

Jednotlivé aplikačné komponenty, servisy, mikroservisy budú medzi sebou komunikovať tak ako synchrónnou komunikáciou na báze OpenAPI3 protokolu (preferovaná JSON) a zároveň budú mať možnosť rozšírenej asyncrhónnej komunikácie prostredníctvom EvenBus KAVKA. EvenBus zároveň poskytne služby orchestrácie (riadenia flow-ov a stavov) a dočasnej databázy.

4.3.6 Iné hľadiská dizajnu

Popísané v Katalógu požiadaviek SVM.

4.3.7 Dátový model riešenia

Každý mikroservice bude mať svoju vlastnú DB. Dátový model bude bližšie špecifikovaný v DFŠ.

4.3.8 Licencie

Momentálne neexistujú požiadavky na licencie, keďže je celé riešenie stavané na OpenSource produktoch.

Pre zabezpečenie stabilnej prevádzky je odporúčané pre kľúčové komponenty (Kafka, PostgreSQL, Kubernetis) zabezpečiť support (vlastným odborným personálom prevádzkovateľa, alebo zakúpením supportu od dodávateľa komponentu).

4.3.9 Jazyková lokalizácia

Aplikácia SDV bude dostupná v rovnakom rozsahu funkcionalít pre slovenský ako aj anglický jazyk. Používateľ bude mať možnosť:

1. Nastaviť jazyk v rámci nastavení aplikácie pre prihláseného používateľa
2. Nastaviť jazyk ihneď po prvom spustení aplikácie.

4.4 Bezpečnostná architektúra

Základnými východiskami pre rozvíjané riešenie bezpečnosti IS sú rovnako ako v súčasnom stave právne predpisy ako zákon č. 122/2013 o ochrane osobných údajov, zákon č. 275/2006 o informačných systémoch VS a s ním súvisiaci výnos Ministerstva financií Slovenskej republiky č. 55/2014 o štandardoch pre informačné systémy verejnej správy a ďalej ISO/IES 27000, Common Criteria a OWASP Guides a dodatočných požiadaviek prevádzkovateľa systému - NASES.

Bezpečnostná architektúra bude vychádzať z týchto pravidiel a v rámci pripraveného Bezpečnostného projektu, ktorého vypracovanie a aplikovanie bude podmienkou sprevádzkovania navrhovaných nových, či rozvíjaných informačných systémov. Výstupmi Bezpečnostného projektu budú najmä návrhy postupov pre riadenie prístupov, výkon prevádzky, riešenia incidentov, havarijné plánovanie, implementácie bezpečných zmien a monitorovanie SLA. Návrhy postupov budú zosúladené s už aplikovanými postupmi informačných systémov NASES a ÚV SR. Samozrejme bude potrebné zohľadniť aj špecifiká vládneho cloudu, keďže je predpoklad, že riešenie bude využívať služby IaaS, PaaS aj SaaS.

V oblasti riadenia prístupov bude prístup používateľov do novej osobnej zóny mobilID (portfólio klienta), obdobne ako je to dnes pri prístupe k elektronickým schránkam, umožnený na základe overenia platného autentifikačného certifikátu uloženého na eID karte s čipom ako aj novo vybudovaným bezpečným autentifikačným prostriedkom mobileID vydaným MV SR (napr. v prípadoch prístupu cez mobilné zariadenie) na úrovni QAA3. Alternatívne bude možné pristupovať do portfólia, a tým aj do elektronických schránok PO a OVM, cez integračné rozhranie zabezpečené autentifikáciou pomocou mobileID autentizácie.

Všetky rozhrania si budú vyžadovať pripojenie pomocou SSL. V súlade s prijatím stratégie multikanálovosti bude navrhované riešenie, tam kde to bude možné a najmä bezpečné, podporovať prístup na vybrané služby VS prostredníctvom mobilného zariadenia, respektíve prístup na služby z tretích strán použitím Open API VS, na základe udelenej role a overeného oprávnenia. Bezpečná autentizácia a autorizácia API novovytvorených verejných služieb,

novovytvorených privátnych služieb ako aj služieb napojených tretích strán bude zabezpečovať OpenID Connect (OIDC) servis pomocou OAuth2 protokolu, prípadne aj s autorizačnými certifikátmi.

Ako základ pre bezpečnú autentizáciu a autorizáciu používateľov pre prístup mobilnej aplikácii bude využitá funkcionalita OpenID Connect (OIDC) servisov cez OAuth2 protokol. Registrácia požívateľov bude realizovaná OAuth2 Dynamic Client Registration protokolom. Samotná autentizácia a autorizácia požiadaviek mobilného používateľa využije metódu refresh tokenov v OAuth2 Authorization Code Flow s Proof Key for Code Exchange (PKCE). Privátne kľúče, tokeny a utajované identifikátory budú v mobilných zariadeniach uložené v bezpečných úložiskách poskytovaných mobilnými platformami.

Nakoľko riešenie ráta s pripojením k existujúcim službám a komponentom ISVS, novozavedené služby budú integrované s už ich zavedenou a schválenou autentizáciou a autorizáciou.

Pre bezpečnosť sietí, bezdrôtovej a mobilnej komunikácie, sa nastaví monitoring sieťových prístupov, DNS bezpečnosť, bezpečnosť vzdialenej práce a práce externistov, emailových sieťových brán, dôveryhodných sieťových a internetových spojení.

Riadenie kontinuity prevádzky bude budované na využití vlastností Kubernetes, virtualizačnej platformy a technológiou zberu monitorovaných dát určenou NASES.

Bezpečnosť mobilnej aplikácie a v nej uložených a spracovávaných dát bude zabezpečená platformovými bezpečnostnými prostriedkami (Keychain, SecureStore, Sandbox). Súkromné dáta uložené v aplikácii budú kryptované pokročilými kryptovacími algoritmami, ktoré dané platformy poskytujú. Čo sa týka autentifikácie, aplikácia využije metódy PINu a biometriou, pričom PIN nie je nikde ukladaný (ani na zariadení, ani na serverových komponentoch). Aplikácia podporí systémový aj aplikačný autorizačný follback pre potreby ochrany privátnych parametrov uložených v secure priestoroch (touchId/faceId – passcode - lock).

Aplikácia SVM nebude podporovať jailbraik-nuté a root-nuté mobilné zariadenia, keďže na nich nie je možné zabezpečiť bezpečnostné požiadavky kladené na aplikáciu.

4.5 SUMARIZÁCIA PREPOJENIA, INTEGRÁCIE a ROZHRANIA

MetaIS kód ISVS z projektu	Poskyt. Open data	Poskyt. ref. údajov	Konz. ref. údajov	Modul eSchránky	Platobný modul	Modul MED	Modul CEP	Modul MEF	Modul IAM
isvs_10684	Áno		Áno	Áno	Áno		Áno	Áno	

EXTERNÉ INTERFACES:

SVM bude využívať spoločné moduly UPVS a ich rozhrania nasledovne:

- OpenID Connect/OAuth2 – ide o rozšírenie centrálneho IAM modulu pre potreby mobilných aplikácií, ktoré využívajú OAuth2 protokol. Pôvodný modul IAM ostáva nezmenený, pričom OAuth2 s ním bude integrovaný a využije jeho existujúce rozhrania. SVM bude využívať služby pre autentifikáciu používateľa.
    - Autentifikácia používateľa na ÚPVS (BOK) (as_59698)
- eNotify (isvs_9370) – centrálny notifikačný modul bude integrovaný pre zasielanie emailových alebo SMS notifikácií
    - Zasielanie oznámení prostredníctvom elektronických komunikačných kanálov (sms, email) (as_59699)
- MOU (isvs_8705) – modul osobných údajov je plánovaný projekt, ktorý poskytne služby prístupu k dátam občana, ako aj služby Consent managementu pre potvrdenie prístupu k osobným dátam občana tretími stranami. Z hľadiska aplikácie SVM budú využité služby prístupu k dátam občana v moduloch kontextových služieb a mobilných dokladov
    - Sprístupnenie dát na základe splnomocnenia a súhlasov (as_56448)
    - Servisná zbernica integrácie údajov (as_56531)
    - Poskytnutie údajov z IS Manažment osobných údajov (as_60009)

- CSRÚ (isvs_5836) - centrálny systém referenčných údajov bude využitý pre získanie referenčných údajov pri tvorbe a generovaní podaní v SVM
- MEP(isvs_8850)/PEP(isvs_5585) – modul elektronických platieb a systém pre evidenciu správnych a súdnych poplatkov bude využitý pri riešení mobilných platieb poplatkov za elektronické podania, predpokladané je využitie rozhraní tzv. Virtuálneho kiosku
    - Realizácia platieb správnych a súdnych poplatkov (as_59700)
- CEP (isvs_9368) – centrálna elektronická podateľna bude využitá pri podaní podania vytvoreného v SVM
    - Overovanie elektronického podpisu (KEP) (as_59702)
- eForm (isvs_8848) – modul elektronických formulárov bude využitý pre vizualizáciu elektronických podaní podľa transformačných schém registrovaných v tomto module
- eDesk (isvs_8847) – elektronická schránka občana/podnikateľa, SVM použije rozhrania modulu pre prístup používateľa do eDesk prostredníctvom jeho mobilného zariadenia
    - Vytváranie, odosielanie a prijímanie elektronických správ (as_59630)
- Meta IS (isvs_63) – výmena informácii o IS VS, primárne v oblasti mobilných aplikácií
- API GW (isvs_9514) – API Gateway ktorá bude publikovať rozhrania komponentov eGov v štandarde OpenAPI
- Modul Otvorené dáta (isvs_9342) – modul pre publikovanie otvorených údajov. SVM bude publikovať primárne štatistické údaje a číselníky.
    - Zápis a aktualizácia údajov z dátového zdroja (sluzba_is_48063)

SVM vytvorí nové rozhrania ktoré budú publikované pre agendové IS, spoločné moduly UPVS ako aj externé 3rd party systémy. Rozhrania budú vystavené na API Gateway platforme pre integráciu externých IS a mobilných aplikácií s prepojením na G2G platformu pre prístup spoločných modulov UPVS a agendových IS. SVM vytvorí nasledovné rozhrania:

- **Registrácia Mobile ID** – rozhranie umožní registráciu Mobile ID prostredníctvom rozhrania vypublikovaného na API GW. Rozhranie je určené pre asistovanú registráciu Mobile ID.
- **Prijatie požiadavky na potvrdenie súhlasu** – rozhranie je určené pre IS VS, ako aj pre informačné systémy komerčných subjektov. Účelom rozhrania je umožniť vyžiadanie potvrdenia súhlasu s aktivitou OVM, resp. akéhokoľvek subjektu od fyzickej osoby ako napr. informovaný súhlas v ambulancii lekára. Pri prijatí požiadavky systém prostredníctvom PUSH notifikácie informuje fyzickú osobu o požiadavke na povolenie súhlasu. Následne si používateľ môže pozrieť detailné údaje daného súhlasu tento súhlas potvrdiť, alebo zamietnuť. Informácia o potvrdení, alebo zamietnutí je následne zaslaná volajúcemu systému, pričom bude autorizovaná klikom.
- **Prijatie požiadavky na podpísanie dokumentu/podania (autorizácia klikom)** – rozhranie je určené pre IS VS, ako aj pre informačné systémy komerčných subjektov. Účelom rozhrania je umožniť vyžiadanie podpísania dokumentu/podania fyzickou osobou. Pri prijatí požiadavky systém prostredníctvom PUSH notifikácie informuje fyzickú osobu o požiadavke na podpísanie dokumentu/podania. Následne si používateľ môže pozrieť detailné údaje daného dokumentu/podania a tento dokument/podanie podpísať. Podpísaný dokument/podanie je následne zaslané volajúcemu systému, pričom bude autorizované klikom. V ďalších fázach je možné doplnenie vyššej úrovne autorizácie, podpísanie dokumentu/podania kvalifikovaným elektronickým podpisom (eventuálne aj s časovou pečiatkou). Toto rozšírenie je závislé od projektu vydávania občianskych preukazov s NFC čipom, resp. od projektu vzdialeného podpisovania.
- **Prijatie požiadavky na doplnenie údajov podania** - rozhranie je určené pre IS VS, ako aj pre informačné systémy komerčných subjektov. Účelom rozhrania je umožniť vyžiadanie doplnenia údajov do podania od fyzickej osoby. Pri prijatí požiadavky systém prostredníctvom PUSH notifikácie informuje fyzickú osobu o požiadavke na doplnenie podania. Následne si používateľ môže pozrieť detailné údaje daného podania a doplniť požadované údaje. Podanie ktoré žiada zdrojový systém doplniť musí mať reprezentácia pre mobilné aplikácie v module eForm. Doplnené podanie je následne zaslané do centrálnej podateľne OVM, ktoré určil zdrojový systém, pričom bude autorizované klikom.
- **Prijatie notifikácie** – rozhranie umožní prijať notifikáciu pre fyzickú osobu, ktorá má registrované Mobile ID od IS VS ako aj informačného systému komerčných subjektov. Notifikácia z externého IS má informatívny charakter a nenasleduje po ňom žiadna aktivita používateľa v SVM. Ak externý IS očakáva od používateľa nejakú aktivitu, musí využiť iné poskytované rozhrania, v rámci ktorých je zahrnuté aj aktívne oslovenie používateľa notifikáciou.
- **Prijatie prehľadu informácií** - rozhranie je určené pre IS VS, ako aj pre informačné systémy komerčných subjektov. Účelom rozhrania je prijať a zobraziť používateľovi štruktúrovanú informáciu vo forme prehľadu (gridu) napr. prehľad platieb používateľa. Rozhranie bude využívané v opodstatnených prípadoch a po posúdení z hľadiska ergonómie používania aplikácie. Prehľad má čisto informatívny charakter a nenasleduje po ňom žiadna aktivita používateľa v SVM.
- **Prijatie mobilného dokladu** – rozhranie je určené pre IS VS, ako aj pre informačné systémy komerčných subjektov. Účelom rozhrania je umožniť zdrojovému IS bezpečným a štandardným spôsobom doručiť mobilný doklad fyzickej osobe do mobilného zariadenia. Predpokladá sa sada metód na oboch stranách rozhrania, podporujúca celý proces vydania mobilného dokladu, od registrácie typu dokladu, zaslanie požiadavky o vydanie dokladu až po prijatie mobilného dokladu do mobilného zariadenia.

INTERNÉ INTERFACES:

Bude definované v DFŠ projektu.

4.6 ZÁVISLOSTI NA OSTATNÉ IS / PROJEKTY

Nasledujúca tabuľka poskytuje

prehľad všetkých projektov a programov, ktoré sú v štádiu vývoja a v korelácii s pripravovaným projektom:

Stakeholder	Názov projektu	MetaIS Kód projektu	Termín ukončenia	Popis závislosti
MIRRI SR	Rozvoj platformy integrácie údajov (centrálna integračná platforma) a Manažment osobných údajov (CIP a MOU)	projekt_346	22.01.2021	Projekt SVM predpokladá využitie funkcionalít CIP a MOU: · Evidencia poskytnutia súhlasu na spracovanie Mojich Dát občana pre kontextové služby · Získanie a spracovanie Mojich Dát občana v kontextových službách · Vzájomné zosúladenie mobilných aplikácií MOU a SVM
NASES	Centrálna API Manažment Platforma (Platforma pre publikovanie služieb štátu cez Open API) (CAMP)	projekt_514	30.06.2022	Projekt SVM predpokladá využitie funkcionalít UPVS 2.0: · OpenIDConnect/OAuth2 pre mobilnú autentifikáciupoužívateľa · API Gateway a transformovanie SOAP rozhraní existujúcich spoločných modulov na Open Rest API využiteľných SVM
NASES	Zvyšovanie úžitkovej hodnoty digitálnych služieb pre občanov, podnikateľov a inštitúcie verejnej správy rozvojom ÚPVS a spoločných modulov (UPVS 3.0)	projekt_307	14.02.2021	Projekt UPVS 3.0 rieši celkové zlepšenie eGov služieb a ich dostupnosť aj na mobilných zariadeniach prostredníctvom responzívneho designu webových aplikácií. Projekt SVM vytvára mobilný prístupový kanál cez natívnu mobilnú aplikáciu primárne určenú na aktívne vyvolanú interakciu FO s verejnou správou pre vybrané služby s priamym a opakovaným benefitom pre občana pri použití cez mobilné zariadenie. S projektom SVM sa tieto projekty vzájomne dopĺňajú, keďže výstupy týchto projektov sa následne využívajú v druhom projekte. Projekt UPVS 3.0 poskytne pre SVM modernizované služby spoločných modulov použiteľné natívnou mobilnou aplikáciou. Naopak, SVM poskytne pre projekt UPVS 3.0 mobilnú autentifikáciu pre prístup na portál UPVS ci už na PC, alebo na mobilnom zariadení.
NCZI	Elektronizácia dávok z nemocenského poistenia	projekt_708	30.11.2021	Projekt SVM predpokladá poskytnutie: · Rozhraní pre systém Sociálnej poisťovne, ktorý sa integruje na rozhrania SVM pre doplnenie podania o údaje k PN [Adresa zdržiavania sa pacienta počas PN; Číslo účtu pacienta]
MIRRI SR	Otvorené údaje 2.0 - Rozvoj centrálnych komponentov pre kvalitné zabezpečenie otvorených údajov	projekt_329	17.08.2022	Projekt SVM predpokladá využitie výstupov projektu OU 2.0: • GitLab pre sprístupnenie zdrojových kódov frontendových a backendových komponentov vytvorených v rámci Dizajn systému pre mobilné aplikácie

5 ZDROJOVÉ KÓDY

Všetky zdrojové kódy a vykonávanie majetkových práv k celému dielu ale aj jeho častiam, ktoré môžu byť dodávané ako čiastkové plnenia predmetu diela bude plne pod kontrolou objednávateľa (štátu) bez licenčných obmedzení. Riešenie nebude obsahovať žiadne proprietárne technológie alebo technologické časti, ktoré nie sú voľne dostupné ako open-source riešenia alebo k nim dodávateľ neudelí nevýhradnú licenciu bez obmedzení.

Zdrojové kódy dodávaného riešenia budú uložené v centrálnom repozitári zdrojových kódov (GIT) a dodávateľ riešenia zabezpečí ich aktualizáciu s každým dodaním čiastkového plnenia predmetu diela. Zdrojové kódy pre časti riešenia, ktoré sú dostupné ako open-source dodávateľ nebude publikovať, ale iba popíše v administrátorskej dokumentácii k riešeniu alebo jeho časti čo a ako je využité alebo nakonfigurované.

Predpokladaná frekvencia dodávania častí predmetu diela a jeho uvedenia do produkčnej prevádzky je najviac 6 mesiacov. Harmonogram dodávok bude navrhnutý aj s ohľadom na technologické možnosti tak, aby boli dodávky čiastkových plnení realizované na kvartálnej báze. Predpokladom je riadne implementované a otestované riešenie. Uvedeniu príslušnej časti predmetu diela pre verejnosť (sprístupnenie funkcionality) bude predchádzať minimálne 30 dňové pilotné overenie s vybranými používateľmi.

Limitom pre používanie môže byť iba kapacita HW zariadení, na ktorých je možné riešenia prevádzkovať.

Ak bude pre prevádzkové prostredie dostupná infraštruktúra a technologické predpoklady pre prevádzku v režime **DevOps**, dodávateľ riešenia zabezpečí, aby bolo riešenia nasadzované a prevádzkované v súlade s očakávaným stavom.

6 PREVÁDZKA A ÚDRŽBA

Riešenie prinesie nové komponenty a služby, ku ktorým neexistuje súčasný stav. Budúca prevádzka bude vychádzať zo súčasného modelu prevádzky a podpory riešenia s ohľadom na best practice podľa bežných IT procesov (ITILv4).

Prevádzku riešenia bude podľa dodávateľom (víťazný uchádzač) dodanej technickej, prevádzkovej a administračnej dokumentácie zabezpečovať NASES. Pred preberaním diela alebo jeho časti do prevádzky prebehne zaškolenie určených administrátorov NASES a bude vykonaná kontrola dokumentácie a jej súladu s reálnym riešením.

Monitoring a podpora na úrovni L1 a L2 bude zabezpečená NASES a L3 bude zabezpečená cez SLA s dodávateľom (víťazný uchádzač), ktorú uzatvorí NASES a dodávateľ pri uvedení prvej časti predmetu diela do produkčnej prevádzky. Dodávať (víťazný uchádzač) zabezpečí L3 podporu počas prvých 6 mesiacov od uvedenia prvej časti predmetu diela do riadnej prevádzky diela bezodplatne.

Rozširovanie predmetu diela nad rámec požiadaviek špecifikovaných a schválených v katalógu požiadaviek bude realizované formou zmenových konaní v súlade s ITILv4 procesmi a príslušnými best practice. Objem človekodní vyčlenených na zmenové konania bude špecifikovaný v SLA ako služby rozširovania funkcionality s presne určenou dedikovanou kapacitou riešiteľského tímu dodávateľa (víťazný uchádzač) podľa riešiteľských rolí s vopred dohodnutými sadzbami sa jeden človekodeň práce riešiteľa.

V tejto kapitole sú uvedené minimálne požiadavky a očakávania na parametre SLA.

6.1 Požiadavky na dokumentáciu

V tejto kapitole sú vymenované požiadavky na dokumentáciu k riešeniu, ktoré budú použité pre uvedení diela alebo jeho časti do prevádzky a podľa ktorej bude riešenia vytvorené a následne prevádzkované:

- **Biznis architektúra** (Používatelia, funkcie, procesy, služby,...) - predstavuje základnú organizáciu fungovania Systému v naviazanosti na okolité IS v rámci rezortu ako aj mimo neho cez definovanie biznis procesov, používateľov a ich vzťahov, prostredí a princípov, ktoré riadia dizajn a evolúciu, podáva predstavu o tom, ako zdravotníctvo plní svoje biznis zámery
- **Aplikačná architektúra** (Komponenty, procesy, aplikácie, funkcie, služby,..) - musí znázorňovať principiálnu štruktúru informačného systému, ktorý sa musí skladať z aplikačných modulov spracovávajúcich informácie, zo vzájomných vzťahov a vzťahu k prostrediu, a z princípov, ktoré riadia jeho dizajn a rozvoj, pričom tento blok musí zachytávať to, ako informačný systém pomáha zdravotníctvu naplniť svoje biznis zámery
- **Architektúra dátová vrátane systémovej architektúry** (popisuje údajové entity a ich vzťahy, tok údajov, príslušnosť údajov, dekompozícia architektonických modulov, návrh ich väzieb,...)
- **Technologická architektúra vrátane architektúry za infraštruktúru** –(uzly, komunikácia medzi uzlami, systémový softvér, platformy, operačné systémy) - poskytne v projekte služby infraštruktúry s vysokou dostupnosťou a škálovateľnosťou. Tieto služby sú nevyhnutné pre chod aplikačných komponentov a budú realizované výpočtovým, sieťovým hardvérom a systémovým softvérom.
- **Integračná architektúra** - musí riešiť integráciu medzi aplikačnými komponentmi elektronického zdravotníctva a najmä systémami tretích strán a elektronickým zdravotníctvom na úrovni integrácie procesov a integrácie údajov. Definuje komunikačné štandardy.
- **Bezpečnostná architektúra** – musí riešiť systém ochrany implementovaný technickými prostriedkami t. j. dedikovanými bezpečnostnými prostriedkami ako aj prostriedkami tvoriacimi súčasť aplikačných komponentov a infraštruktúry a netechnickými prostriedkami pre manažment informačnej bezpečnosti.

Pri návrhu, implementácii a prevádzke riešenia dodržané a zároveň tvoria kritéria kvality pre aplikačnú, technologickú a prevádzkovú časť riešenia.

- Jeden repozitár zdrojového kódu pre jednu „aplikáciu",
- Explicitná deklarácia a izolácia závislostí aplikácie,
- Konfigurácia (aplikácie) súčasťou prostredia, nie aplikácie,
- Nezávislosť aplikácie od konkrétneho poskytovateľa podpornej služby „back-end“,
- Jasné oddeľovanie jednotlivých štádií transformácie zdrojového kódu na bežiacu aplikáciu,
- Spustená aplikácia beží ako jeden alebo viac bez-stavových procesov,
- Aplikácia je sama zodpovedná za publikáciu svojich komunikačných koncových bodov (portov),

- Jednoduché škálovanie výkonu pomocou spúšťania a zastavovania (paralelných) bez-stavových procesov,
- Okamžité reakcie procesov na požiadavky spustenia a zastavenia,
- Minimalizovať rozdiely medzi prostrediami (najmä vývojovým a produkčným),
- Aplikácia nikdy neriadi (a nespolieha sa na proprietárny) spôsob spracovania logov,
- Admin/manažment úlohy sú vyvíjané a vykonávané ako jednorazové procesy,
- Pre maximalizáciu robustnosti a minimalizáciu výpadkov aplikácie, je potrebné (tam, kde je to možné a efektívne) využívať tzv. „modro-zelený" systém nasadzovania. Jeho podstata spočíva v paralelnom behu (v okamihu nasadzovania novej verzie do produkcie) dvoch identických produkčných prostredí, pričom používateľov (alebo prichádzajúce požiadavky) obsluhuje vždy len jedno z nich. Postup pri nasadzovaní je taký, že na jednom sa vykoná finálna príprava a odladenie releasu nad konfiguráciou produkčného prostredia a následne sa prepne presmerovanie požiadaviek z doteraz obsluhujúceho (stará verzia aplikácie) na prostredie obsahujúce odladenú novú verziu (pričom staré prostredie je stále pripravené byť zapojené v prípade, že sa vyskytnú neočakávané chyby),
- Rovnaká dostupnosť a zrozumiteľnosť pre akéhokoľvek požívateľa - a teda aj pre určitým spôsobom znevýhodneného používateľa, napr. zrakovo, sluchovo postihnuté osoby a pod.

6.2 Prevádzkové požiadavky

Všetky Hlásenia a Požiadavky na služby budú evidované v jednotnom nástroji, ktorý určí verejný obstarávateľ. Presné pravidlá budú zachytené v PID a SLA. Minimálne očakávané parametre sú uvedení nižšie.

6.2.1 Úrovne podpory používateľov

Help Desk bude realizovaný cez 3 úrovne podpory, s nasledujúcim označením:

- **L1 podpory IS** (Level 1, priamy kontakt zákazníka) - jednotný kontaktný bod verejného obstarávateľa – IS Solution manager, ktorý je v správe verejného obstarávateľa a v prípade jeho nedostupnosti Centrum podpory používateľov (zabezpečuje prevádzkovateľ IS a DataCentrum).
- **L2 podpory IS** (Level 2, postúpenie požiadaviek od L1) - vybraná skupina dodávateľom riadne zaškolených garantov, so znalosťou funkcionality diela alebo jeho časti riadne uvedeného do prevádzky (zabezpečuje prevádzkovateľ IS – verejný obstarávateľ).
- **L3 podpory IS** (Level 3, postúpenie požiadaviek od L2) - na základe zmluvy o službách a podpore IS (zabezpečuje víťazný uchádzač) v súlade s procesmi ITILv4 a podľa pravidiel určených v budúcej SLA.

6.2.1.1 Definícia úrovní podpory

- Podpora L1 (podpora 1. stupňa) - začiatočná úroveň podpory, ktorá je zodpovedná za riešenie základných problémov a požiadaviek koncových užívateľov a ďalšie služby vyžadujúce základnú úroveň technickej podpory. Základnou funkciou podpory 1. stupňa je zhromaždiť informácie, previesť základnú analýzu a určiť príčinu problému a jeho klasifikáciu. Typicky sú v úrovni L1 riešené priamočiare a jednoduché problémy a základné diagnostiky, overenie dostupnosti jednotlivých vrstiev infraštruktúry (sieťové, operačné, vizualizačné, aplikačné atď.) a základné užívateľské problémy (typicky zabudnutie hesla), overovanie nastavení SW a HW atď.
- Podpora L2 (podpora 2. stupňa) – riešiteľské tímy s hlbšou technologickou znalosťou danej oblasti. Riešitelia na úrovni Podpory L2 nekomunikujú priamo s koncovým užívateľom, ale sú zodpovední za poskytovanie súčinnosti riešiteľom 1. úrovne podpory pri riešení eskalovaného hlásenia, čo mimo iného obsahuje aj spätnú kontrolu a podrobnejšiu analýzu zistených dát predaných riešiteľom 1. úrovne podpory. Výstupom takejto kontroly môže byť potvrdenie, upresnenie, alebo prehodnotenie hlásenia v závislosti na potrebách Objednávateľa. Primárnym cieľom riešiteľov na úrovni Podpory L2 je dostať Hlásenie čo najskôr pod kontrolu a následne ho vyriešiť - s možnosťou eskalácie na vyššiu úroveň podpory – Podpora L3.
- Podpora L3 (podpora 3. stupňa) - Podpora 3. stupňa predstavuje najvyššiu úroveň podpory pre riešenie zložitých Hlásení, vrátane prevádzania hĺbkových analýz a riešenie extrémnych prípadov pri riešení Incidentov a Problémov.

6.2.1.2 Pre služby podľa SLA sú definované takéto parametre

- Help Desk je dostupný minimálne v režime 12x5 cez verejným obstarávateľom určený jednotný nástroj a pre vybrané skupiny užívateľov vymenovaných v SLA cez telefón a email,
- Všetky Hlásenia sú evidované vo verejným obstarávateľom určenom jednotnom nástroji,
- Všetky Incidenty sú evidované vo verejným obstarávateľom určenom jednotnom nástroji,
- Dostupnosť L3 podpory pre IS je 12x5 (12 hodín x 5 dní od 6:00h do 18:00h počas pracovných dní),

6.2.1.3 Riešenie incidentov – SLA parametre

Za incident je považovaná chyba alebo neočakávané správanie IS alebo jeho časti, t.j. správanie sa v rozpore s prevádzkovou a používateľskou dokument áciou IS. Za incident nie je považovaná chyba, ktorá nastala mimo prostredia IS napr. výpadok poskytovania konkrétnej služby Vládneho cloudu alebo komunikačnej infraštruktúry.

Označenie naliehavosti incidentu:

Označenie naliehavosti incidentu	Závažnosť in cidentu	Popis naliehavosti incidentu
A	Kritická	Kritické chyby, ktoré spôsobia úplné zlyhanie systému ako celku a nie je možné používať ani jednu jeho časť, nie je možné poskytnúť požadovaný výstup z IS.
B	Vysoká	Chyby a nedostatky, ktoré zapríčinia čiastočné zlyhanie systému a neumožňuje používať časť systému.

C	Stredná	Chyby a nedostatky, ktoré spôsobia čiastočné obmedzenia používania systému.
D	Nízka	Kozmetické a drobné chyby.

Možné dopady incidentov:

Označenie závažnosti incidentu	**Dopad**	**Popis dopadu**
1	katastrofický	katastrofický dopad, priamy finančný dopad alebo strata dát,
2	značný	značný dopad alebo strata dát
3	malý	malý dopad alebo strata dát

Výpočet priority incidentu je kombináciou dopadu a naliehavosti v súlade s *best practices* ITILv4 uvedený v nasledovnej matici:

Matica priority incidentov		**Dopad**		
		Katastrofický - 1	**Značný - 2**	**Malý - 3**
Naliehavosť	Kritická - A	1	2	3
	Vysoká - B	2	3	3
	Stredná - C	2	3	4
	Nízka - D	3	4	4

Vyžadované reakčné doby (podľa určených prevádzkových hodín):

Označenie priority incidentu	**Reakčná doba[(1)] od nahlásenia incidentu po začiatok riešenia incidentu**	**Doba konečného vyriešenia incidentu od nahlásenia incidentu (DKVI) [(2)]**	***Spoľahlivosť* [(3)]** *(maximálny povolený počet incidentov za jeden mesiac)*
1	2 hod.	8 hodín	1
2	4 hod.	24 hodín	2
3	8 hod.	60 hodín	10
4	16 hod.	Vyriešené a nasadené v rámci plánovaných *releasov*, nie neskôr ako do 3 mesiacov o trvalého vyriešenia incidentu.	

Pojmy:

- (1) **Reakčná doba** je čas medzi nahlásením incidentu verejným obstarávateľom (vrátane užívateľov IS, ktorí nie sú v pracovnoprávnom vzťahu s verejným obstarávateľom) na helpdesk úrovne L3 a jeho prevzatím na riešenie.
- (2) **DKVI** znamená obnovenie štandardnej prevádzky - čas medzi nahlásením incidentu verejným obstarávateľom a vyriešením incidentu úspešným uchádzačom (do doby, kedy je funkčnosť prostredia znovu obnovená v plnom rozsahu). Doba konečného vyriešenia incidentu od nahlásenia incidentu verejným obstarávateľom (DKVI) sa počíta počas celého dňa. Do tejto doby sa nezarátava čas potrebný na nevyhnutnú súčinnosť verejného obstarávateľa, ak je potrebná pre vyriešenie incidentu. V prípade potreby je úspešný uchádzač oprávnený požadovať od verejného obstarávateľa schválenie riešenia incidentu.
- (3) **Maximálny počet incidentov** za kalendárny mesiac. Každá ďalšia chyba nad stanovený limit spoľahlivosti sa počíta ako začatý deň omeškania bez odstránenia vady alebo incidentu. Duplicitné alebo technicky súvisiace incidenty (zadané v rámci jedného pracovného dňa, počas pracovného času 8 hodín) sú považované ako jeden incident.
- (4) **Incidenty** nahlásené verejným obstarávateľom úspešnému uchádzačovi v rámci testovacieho prostredia:

1. Majú prioritu 3 a nižšiu,
2. Vzťahujú sa výhradne k dostupnosti testovacieho prostredia,
3. Za incident na testovacom prostredí sa nepovažuje incident vztiahnutý k práve testovanej funkcionalite (takého hlásenie sa bude nazývať defekt)

Vyššie uvedené SLA parametre nebudú použité pre nasledovné služby:

- Služby systémovej podpory na požiadanie (nad paušál alebo služby rozširovania funkcionality)
- Služby realizácie aplikačných zmien vyplývajúcich z legislatívnych a metodických zmien (nad paušál)

Pre služby rozširovania funkcionality budú dohodnuté osobitné pravidlá a parametre SLA. Ak ich dodávateľ odmietne vykonať bez uvedenia vecných argumentov, verejný obstarávateľ bude oprávnený takúto služby zabezpečiť u iného dodávateľa a pôvodný dodávateľ mu v tom nebude brániť ani jeho konanie obmedzovať.

6.3 Požadovaná dostupnosť IS

Popis	Parameter	Poznámka
Prevádzkové hodiny	24 hodín	00:00 hod. - do 23:59 hod. každý deň.
Servisné okno	10 hodín	od 19:00 hod. - do 5:00 hod. počas pracovných dní pre vopred naplánované a používateľom oznámené odstávky. Oznámenie prebehne minimálne 14 dní vopred.
	24 hodín	od 00:00 hod. - 23:59 hod. počas dní pracovného pokoja a štátnych sviatkov Servis a údržba sa bude realizovať mimo bežného pracovného času a iba počas vopred riadne nahlásených a schválených požiadaviek na plánovanú odstávku. Oznámenie prebehne minimálne 28 dní vopred.
Dostupnosť produkčného prostredia IS	98%	§ 98,5% z 24/7/365 t.j. max ročný výpadok je 66 hod. § Maximálny mesačný výpadok je 5,5 hodiny. § Vždy sa za takúto dobu považuje čas od 0.00 hod. do 23.59 hod. § Nedostupnosť IS sa počíta od nahlásenia incidentu Zákazníkom v čase dostupnosti podpory Poskytovateľa (t.j. nahlásenie incidentu na L3 v čase od 6:00 hod. - do 18:00 hod. počas pracovných dní). Do dostupnosti IS nie sú započítavané servisné okná a plánované odstávky IS. § V prípade nedodržania dostupnosti IS bude každý ďalší začatý pracovný deň nedostupnosti braný ako deň omeškania bez odstránenia vady alebo incidentu.
RTO (Recovery Time Objective)	24 hodín	§ doba obnovenia systému, t.j. za ako dlho po výpadku musí byť systém funkčný.
RPO (Recovery Point Objective)	10 minút	§ aké množstvo dát môže byť stratené od vymedzeného okamihu.
Odozva služieb	2 – 10 sekúnd	Čas odozvy musí splniť tieto pravidlá: § 80% z meraných testovacích volaní v pomere zápis a čítanie 1:2 má odozvu kratšiu alebo rovnú 2 sekundy, § 15% z meraných testovacích volaní v pomere zápis a čítanie 1:2 má odozvu kratšiu alebo rovnú 5 sekúnd, § 5% z meraných testovacích volaní v pomere zápis a čítanie 1:2 má odozvu najviac 10 sekúnd, § Simulácia sa vykonáva podľa dát z reálnej prevádzky existujúcich služieb UPVS, § Počet volaní a interakcia s koncovými používateľmi IS bude určená podľa špičiek v prevádzke Pondelok – Piatok, 07:00 – 13:00 prebehne 90% všetkých volaní služieb, z toho v pondelok prebehne 25% všetkých volaní (bude primerane upravené podľa reálnych štatistík pred podpisom Zmluvy o dielo)

6.4 Vymedzenie pojmov

6.4.1 Dostupnosť (Availability)

Dostupnosť (availability) znamená, že dáta alebo iné zariadenie sú prístupné v okamihu jej potreby. Vyjadruje sa v percentách dostupného času. Dostupnosť znamená, že dáta sú prístupné v okamihu jej potreby. Narušenie dostupnosti sa označuje ako nežiaduce zničenie (*destruction*) alebo nedostupnosť. Dostupnosť bude v SLA vyjadrená ako percento času v danom období za jeden kalendárny rok. Alternatívne možnosti sú:

- **90% dostupnosť**znamená výpadok 36,5 dňa,
- **95% dostupnosť**znamená výpadok 18,25 dňa,
- **98% dostupnosť**znamená výpadok 7,30 dňa [aktuálne zvolená dostupnosť IS],

- **99% dostupnosť**znamená výpadok 3,65 dňa,
- **99,5% dostupnosť**znamená výpadok 1,83 dňa,
- **99,8% dostupnosť**znamená výpadok 17,52 hodín,
- **99,9%**(“**tri deviatky**”) **dostupnosť** znamená výpadok 8,76 hodín,
- **99,99%**(“**štyri deviatky**”) **dostupnosť** znamená výpadok 52,6 minút,
- **99,999%**(“**päť deviatok**”) **dostupnosť** znamená výpadok 5,26 minút,
- **99,9999%**(“**šesť deviatok**”) **dostupnosť** znamená výpadok 31,5 sekúnd.

6.4.2 RTO (Recovery Time Objective)

RTO vyjadruje množstvo času potrebné pre obnovenie dát a celého prevádzky nedostupného systému (softvér). Preferovaný variant bude vytvorenie prostredí s minimálne 2 zastupujúcimi sa servermi v každej vrstve.

6.4.3 RPO (Recovery Point Objective)

RPO vyjadruje, do akého stavu (bodu) v minulosti možno obnoviť dáta. Preferovaný variant bude vytvárania synchrónnych replík dát.

7 POŽIADAVKY NA PERSONÁL

Projektový manažér za dodávateľa

Projektový manažér riadi projekt na strane Dodávateľa, zabezpečuje plánovanie, organizovanie a riadenie zdrojov a projektových aktivít a úloh tak, aby bol zrealizovaný projektový cieľ v dohodnutom rozsahu, stanovenom čase a za plánované náklady. Výsledkom jeho činnosti je dodanie produktu alebo nastavenie procesu.

Solution Enterprise architekt (IT architekt)

IT architekt na projekte zabezpečuje činnosti vychádzajúce z požiadaviek organizácie, transformuje ich do konkrétnej koncepcie architektúry IS/IT. Zodpovedá za návrh a implementáciu technológií predovšetkým z pohľadu udržateľnosti, kvality a nákladov. Jeho úlohou je vytvoriť návrh technologického riešenia SVM a odporúčanej infraštruktúry, analyzovať a navrhnúť vytvorenia služieb, definovať výstupy a postupy pre prípady použitia, navrhnúť zmeny procesov a využitie analytických metód pre lepšie rozhodovanie, analyzovať dátové potreby, definovať požiadavky na dátové zdroje, ako aj ďalšie činnosti vyplývajúce z požiadaviek na projekte SVM.

Analytik (IT analytik)

IT analytik na projekte zabezpečuje analyzovanie procesných a ďalších požiadaviek a špecifikácií súčasného alebo budúceho používateľa technického riešenia / informačného systému a následne navrhuje dizajn a programátorské riešenie. Aktívne sa zúčastňuje analytických stretnutí s kľúčovými používateľmi MIRRI k detailnej špecifikácii požiadaviek. Participuje na vývoji nových, ale i pri vylepšovaní existujúcich funkčností v rámci celého vývojového cyklu – systémová analýza, dizajn, kódovanie, integrácie na iné systémy, užívateľské testovanie, implementácia, podpora, dokumentácia. Úzko spolupracuje s IT architektom a vykonáva aj ďalšie činnosti vyplývajúce z požiadaviek na projekte SVM.

Developer (IT programátor/vývojár)

IT programátor/vývojár transformuje návrh technického riešenia, na základe jeho detailnej špecifikácie, vývojových diagramov a návrhu dátovej integrácie, do podoby fyzického, funkčného a overeného zdrojového kódu. Zabezpečuje alebo priamo vykonáva jednotkové a funkčné testovanie a asistuje IT testerom pri vyšších úrovniach testovania. Takisto je zodpovedný za dokumentáciu zdrojového kódu tak, aby tento mohol byť ďalej využívaný a rozvíjaný nezávisle od autora kódu (tzn. od konkrétnej osoby IT programátora/vývojára, ktorá kód vytvorila), ako i za ďalšie činnosti vyplývajúce z požiadaviek na projekte SVM.

Špecialista pre bezpečnosť (Špecialista pre bezpečnosť IT)

Špecialista pre bezpečnosť IT zabezpečuje definovanie a vykonávanie činností zabezpečujúcich ochranu IS a jeho zložiek proti bezpečnostným hrozbám a nepriateľským aktivitám, ktorých cieľom je krádež informácií, financií, zničenie dát, znefunkčnenie činnosti IS, špionážna činnosť prípadne iné činnosti s negatívnym dopadom, realizované prostredníctvom IS alebo na IS.

Databázový špecialista (Špecialista pre databázy)

Špecialista pre databázy zabezpečuje technickú podporu pre databázové systémy a chod databáz alebo databázového systému. Popisuje inštaláciu databáz, je konzultantom pre admina a správcu systému k aktualizácii na novšie verzie, prípadne aj dielčích častí systému. Sústreďuje ich požiadavky a podnety k databáze systému a následne ich rieši, ako aj ďalšie činnosti vyplývajúce z požiadaviek na projekte SVM.

Špecialista pre infraštruktúru (Špecialista pre infraštruktúry/HW špecialista)

Špecialista pre infraštruktúry/HW špecialista sa vyjadruje k požiadavkám na IT infraštruktúru a návrhom na IT infraštruktúru, zriaďuje/inštaluje, konfiguruje, diagnostikuje, opravuje, upgraduje/ rozširuje hardware a súvisiace technické zariadenia a spolupracuje pri nasadzovaní súvisiaceho SW. Zabezpečuje optimálnu prevádzku a výkon IT infraštruktúry. Rieši technické problémy a poskytuje technickú podporu v súvislosti s IT infraštruktúrou, ako aj ďalšie činnosti vyplývajúce z požiadaviek na projekte SVM.

Špecialista na integrácie

Špecialista na integrácie zabezpečuje definovanie spôsoby integrácie externých systémov a vykonávanie integrácie na iné systémy ISVS pre zabezpečenie riešenia SVM, ako i iné integrácie súvisiace so zabezpečením funkčnosti riešenia SVM. Zároveň je zodpovedný za definíciu Integračného manuálu, ktorý bude tvoriť súčasť Dizajn systému pre natívne mobilné aplikácie.

Konzultant (IT / IS konzultant)

IT/IS konzultant sa podieľa pri tvorbe riešenia a implementácii informačných technológií, resp. informačného systému. Konzultuje, analyzuje potreby, navrhuje riešenia a rieši potreby v rámci projektu. Spolupracuje pri implementácii konkrétneho informačného systému v rámci organizácie, ktorý integruje procesy vnútri organizácie a medzi organizáciami navzájom, ako aj ďalšie činnosti vyplývajúce z požiadaviek na projekte SVM.

QA špecialista (Odborník pre IT dohľad/Quality Assurance)

Špecialista kvality, resp. odborník pre IT dohľad/Quality Assurance navrhuje a implementuje do praxe také postupy, techniky, pravidlá, ktoré maximalizujú efektivitu práce a kvalitatívne parametre vývoja softvéru/produktu/IS, resp. IT projektu. Parametrami kvality sú napríklad funkcionalita softvéru, naplnenie požiadaviek zadania, spokojnosť klientov/užívateľov, výkonové parametre, efektívne procesy, produktivita, dodržanie časového a vecného rozsahu IT projektu. Zároveň definuje postupy, navrhuje a vyjadruje sa k plánom testov a testovacích scenárov. Analyzuje výsledky testovania. Komplexný prístup ku kvalite si vyžaduje jeho účasť vo všetkých fázach vývoja SW, resp. IS. To znamená pri definovaní a špecifikovaní požiadaviek klienta, ich analýze, pri vývoji produktu/softwaru/IS a tiež pri ich údržbe, ako aj ďalšie činnosti vyplývajúce z požiadaviek na projekte SVM.

Tester (IT tester)

IT tester na projekte hľadá chyby v zrealizovanom technickom riešení / softwarovej aplikácii, hľadáva prípadné chyby v kóde s cieľom dosiahnuť čo najvyššiu kvalitu dodávaného riešenia. Testovanie prebieha podľa prípadov použitia v analýze, testovacích prípadov a scenárov odsúhlasených MIRRI. Podľa typu a funkcionality riešenia / softvéru sa používajú rôzne druhy testovania, ako napr. funkčné, integračné, regresné, záťažové testovanie. Pri testovaní bezpečnosti a pri akceptačnom testovaní poskytuje IT tester potrebnú súčinnosť MIRRI. Okrem samotného testovania pripravuje IT tester dokumentáciu s testovacími scenármi a prípadmi a zabezpečuje ďalšie činnosti vyplývajúce z požiadaviek na projekte SVM.

8 IMPLEMENTÁCIA A PREBERANIE VÝSTUPOV PROJEKTU

Projekt bude realizovaný agilnými metódami s prihliadnutím na strategické priority podľa NKIVS a tiež v zmysle podnikateľského plánu a stratégie centra Slovensko IT, a.s. Centrum bude agilnými metódami realizovať projekty zamerané na vývoj a implementáciu front-end a back-end aplikácií, webových a natívnych mobilných aplikácií a web stránok. Centrum v rámci projektu bude zodpovedné za:

- analýzu zadaní – IT analytikom a IT architektom
- riadenie projektov a zákaziek, ktorý predstavuje rozdelenie úloh na kratšie segmenty práce s častým posudzovaním a prispôsobovaním plánov s aktívnou iteráciou koncového zákazníka,
- vypracovanie detailnej biznis a technickej špecifikácie riešenia pre každý projekt spolu so zákazníkom, ktorý je koncovým biznis vlastníkom riešenia, čím sa zabezpečí vývoj finálneho riešenia použiteľného v praxi bez nutnosti ďalších veľkých zmien či úprav.
- zabezpečenie jednotnej architektúry riešenia pre každý projekt s cieľom zachovať súlad s koncepciou architektúry štátnych IT riešení,

- vývoj a implementáciu riešenia (vrátane UX dizajnu a vývoja) na základe požiadaviek a detailných prípadov použitia (use cases)
- otestovanie riešenia z pohľadu záťaže, bezpečnosti a funkčnosti systému (vrátane UI a UX), kde finálnu podobu grafického rozhrania prekonzultuje s konečným odberateľom (užívateľské UAT testovanie) a po overení zapracuje pripomienky,
- nasadenie riešenia resp. jeho funkčných modulov do vývojového, testovacieho a produkčného prostredia a zmenových požiadaviek.
- poskytovanie kapacít pre vývoj a testovanie na iných projektoch podľa flexibilnej potreby pre iné organizácie štátu

Dodávka bude trvať 24 mesiacov, pričom predpokladaný termín začatia prác je termín zahájenia realizačnej fázy (označené ako „T“). Následne bude zabezpečená prevádzka IS v zmysle Podnikového zámeru spoločnosti Slovensko IT, a.s..

Nasledujúca tabuľka zobrazuje fakturačné míľniky jednotlivých fáz a produktov projektu:

Produkt/Aktivity	**Spôsob fakturácie**	**Termín fakturácie**
MobileID		
Analýza a dizajn: Analýza a špecifikácia požiadaviek	Schválený výstup	T+3m
Implementácia služieb	Schválený výstup	T+7m
Testovanie služieb	Schválený výstup	T+8m
Nasadenie	Schválený výstup	T+9m
ePush		
Analýza a dizajn: Analýza a špecifikácia požiadaviek	Schválený výstup	T+3m
Implementácia služieb	Schválený výstup	T+8m
Testovanie služieb	Schválený výstup	T+8m
Nasadenie	Schválený výstup	T+9m
Kontextové služby		
Analýza a dizajn: Analýza a špecifikácia požiadaviek	Schválený výstup	T+15m
Implementácia služieb	Schválený výstup	T+20m
Testovanie služieb	Schválený výstup	T+23m
Nasadenie	Schválený výstup	T+24m
Mobilná schránka		
Analýza a dizajn: Analýza a špecifikácia požiadaviek	Schválený výstup	T+9m
Implementácia služieb	Schválený výstup	T+14m
Testovanie služieb	Schválený výstup	T+17m
Nasadenie	Schválený výstup	T+18m
Mobilné podanie		
Analýza a dizajn: Analýza a špecifikácia požiadaviek	Schválený výstup	T+9m
Implementácia služieb	Schválený výstup	T+13m
Testovanie služieb	Schválený výstup	T+14m
Nasadenie	Schválený výstup	T+15m
Mobilné platby		
Analýza a dizajn: Analýza a špecifikácia požiadaviek	Schválený výstup	T+9m
Implementácia služieb	Schválený výstup	T+14m
Testovanie služieb	Schválený výstup	T+17m

Nasadenie	Schválený výstup	T+18m
Mobilné doklady		
Analýza a dizajn: Analýza a špecifikácia požiadaviek	Schválený výstup	T+15m
Implementácia služieb	Schválený výstup	T+20m
Testovanie služieb	Schválený výstup	T+23m
Nasadenie	Schválený výstup	T+24m
Smart návody		
Analýza a dizajn: Analýza a špecifikácia požiadaviek	Schválený výstup	T+15m
Implementácia služieb	T&M	Mesačne
Testovanie služieb	Schválený výstup	T+23m
Nasadenie	Schválený výstup	T+24m
Dizajn systém		
Analýza a dizajn: Analýza a špecifikácia požiadaviek	Schválený výstup	T+3m
Implementácia služieb	Schválený výstup	T+20m
Testovanie služieb	Schválený výstup	T+20m
Nasadenie	Schválený výstup	T+24m
Prierezové činnosti		
Podpora pri realizácii integrácií a migrácií IS VS	Schválený výstup	T+3m, T+14m
Publicita a informovanosť	Schválený výstup	T+14m, T+24m
Projektové riadenie	T&M	Mesačne
Testovanie: Bezpečnostné/Penetračné testy	Schválený výstup	T+9m, T+17m, T+21m

9 PRÍLOHY

Príloha 1: Katalóg požiadaviek (Excel)

- *Zoznam štandardov a požiadaviek na súlad diela s legislatívou*
- *Zoznam funkčných požiadaviek*
- *Zoznam nefunkčných požiadaviek*
- *Zoznam technických požiadaviek*