**PRÍSTUP K PROJEKTU**

Identifikovanie požiadaviek **na technickú časť riešenia**

**Identifikácia projektu**

|  |  |
| --- | --- |
| Povinná osoba | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky |
| Názov projektu | Slovensko v mobile |
| Identifikátor projektu: | MetaIS, projekt\_1060 |
| Zodpovedná osoba za projekt | Ing. Matej Maderič |
| Realizátor projektu | Slovensko IT, a.s. |
| Vlastník projektu | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky |

**Schvaľovanie dokumentu**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Položka | Meno a priezvisko | Organizácia | Pracovná pozícia | Dátum | Podpis  (alebo elektronický súhlas) |
| Vypracoval | Kevin Richter, Ján Tomášik | Slovensko IT, a.s. | Product Manager | 31.7.2022 |  |

**Obsah**

[1 POPIS ZMIEN DOKUMENTU 4](#_Toc110174679)

[1.1 História zmien 4](#_Toc110174680)

[2 ÚČEL DOKUMENTU 5](#_Toc110174681)

[2.1 Konvencie používané v dokumentoch – označovanie požiadaviek 5](#_Toc110174682)

[2.2 Použité skratky 5](#_Toc110174683)

[2.3 Slovník pojmov 6](#_Toc110174684)

[3 POPIS NAVRHOVANÉHO RIEŠENIA 9](#_Toc110174685)

[4 ARCHITEKTÚRA RIEŠENIA PROJEKTU 9](#_Toc110174686)

[4.1 Biznis vrstva 9](#_Toc110174687)

[4.1.1 Biznis architektúra 9](#_Toc110174688)

[4.1.2 Hlavné procesy riešenia 9](#_Toc110174689)

[4.2 Aplikačná vrstva 9](#_Toc110174690)

[4.2.1 Komponenty riešenia 10](#_Toc110174691)

[4.2.2 Komunikačné štandardy 12](#_Toc110174692)

[4.2.3 Mobile mID 15](#_Toc110174693)

[4.2.4 ePUSH notifikačné témy a notifikačné schémy 17](#_Toc110174694)

[4.2.5 Použité architektonické štandardy 18](#_Toc110174695)

[4.3 Dátová vrstva 19](#_Toc110174696)

[4.4 Technologická vrstva 20](#_Toc110174697)

[4.4.1 Popis vývojového prostredia (DEV) 21](#_Toc110174698)

[4.4.2 Popis testovacieho prostredia (UAT) 22](#_Toc110174699)

[4.5 Softvérové licencie 22](#_Toc110174700)

[4.6 Bezpečnostná architektúra 23](#_Toc110174701)

[4.6.1 Bezpečnosť prevádzky IS 23](#_Toc110174702)

[4.6.2 Zabezpečenie komunikácie 23](#_Toc110174703)

[4.6.3 Zabezpečenie integrity 25](#_Toc110174704)

[4.6.4 Riadenie prístupu 25](#_Toc110174705)

[4.6.5 Definícia používateľských rolí 26](#_Toc110174706)

[4.6.6 Manažment používateľov 27](#_Toc110174707)

[4.7 Ochrana osobných údajov 28](#_Toc110174708)

[4.7.1 Bezpečná autentifikácia používateľa 28](#_Toc110174709)

[4.7.2 Ukladanie a ochrana osobných údajov 28](#_Toc110174710)

[4.7.3 Komunikácia s tretími stranami 28](#_Toc110174711)

[5 ZÁVISLOSTI NA OSTATNÉ ISVS / PROJEKTY 32](#_Toc110174712)

[6 ZDROJOVÉ KÓDY 32](#_Toc110174713)

[7 PREVÁDZKA A ÚDRŽBA 33](#_Toc110174714)

[7.1 Prevádzkové požiadavky 33](#_Toc110174715)

[7.1.1 Úrovne podpory používateľov: 33](#_Toc110174716)

[7.1.2 Riešenie incidentov – SLA parametre 34](#_Toc110174717)

[7.2 Požadovaná dostupnosť IS 36](#_Toc110174718)

[7.2.1 Dostupnosť (Availability) 36](#_Toc110174719)

[7.2.2 RTO (Recovery Time Objective) 36](#_Toc110174720)

[7.2.3 RPO (Recovery Point Objective) 37](#_Toc110174721)

[7.3 Kontajnerizácia a orchestrácia 37](#_Toc110174722)

[7.4 CI/CD proces 37](#_Toc110174723)

[7.5 Využitie vládneho cloudu 38](#_Toc110174724)

[7.6 Záloha a obnova riešenia 38](#_Toc110174725)

[8 POŽIADAVKY NA PERSONÁL 38](#_Toc110174726)

[9 IMPLEMENTÁCIA A PREBERANIE VÝSTUPOV PROJEKTU 39](#_Toc110174727)

[10 PRÍLOHY 39](#_Toc110174728)

# POPIS ZMIEN DOKUMENTU

História zmien

|  |  |  |  |
| --- | --- | --- | --- |
| Verzia | Dátum | Zmeny | Meno |
| 0.1 | 31.7.2022 | Prvý návrh dokumentu. | Kevin RICHTER, Ján TOMÁŠIK |

# 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 z pohľadu budúceho stavu a navrhovaného riešenia.

Dokument má v zmysle vyššie uvedenej vyhlášky popisovať riešenie projektu v oblastiach:

* Požiadaviek na architektúru riešenia – biznis vrstva, aplikačná vrstva, technologická vrstva,
* Požiadaviek na dátový model, dátové konverzie a migrácie,
* Požiadaviek na vládny cloud, prípadne zdôvodnenie jeho použitia,
* Kapacitných požiadaviek na HW, SW a licencie,
* Požiadaviek na bezpečnosť riešenia,
* Požiadaviek na testovanie a akceptačné kritéria,
* Požiadaviek na prevádzku, výkonnosť, dostupnosť a zálohovanie,
* Požiadaviek na integrácie, rozhrania a spoločné komponenty,
* Požiadaviek na dokumentáciu a školenia,
* Konvencie používané v dokumente – označovanie požiadaviek.

Hlavné kategórie požiadaviek v zmysle katalógu požiadaviek, rozdeľujeme na **funkčné**, **nefunkčné** a **technické**. Katalóg požiadaviek je vedený v predpísanej štruktúrovanej podobe vo formáte MS Excel. **Zoznam požiadaviek tvorí Prílohu č.1. k Projektovému zámeru**.

Požiadavky sú číslované od 1 po N, každá je zaradené k príslušnému modulu, kde sa predpokladá jej realizácia. Nie sú používané verzie.

# Použité skratky

| ID | Skratka | Vysvetlenie / Popis |
| --- | --- | --- |
| 1. | A\_ALT | Alternatíva z pohľadu Aplikačnej vrstvy |
| 2. | AS-IS | Súčasný stav |
| 3. | B\_ALT | Alternatíva z pohľadu Biznis vrstvy |
| 4. | BCR | Z ang. Benefit-Cost Ratio, indikátor reprezentujúci vzťah medzi prínosmi a nákladmi predkladaného projektu |
| 5. | Compliance management | Z anglického Riadenie súladu/zhody, znamená proces overenia správnosti implementácie služby v aplikácii tretej strany podľa vopred určených a publikovaných pravidiel a požiadaviek na integráciu, napr. cez integračný manuál. |
| 6. | DCOM | Dátové centrum obcí a miest |
| 7. | DEUS | DataCentrum elektronizácie územnej samosprávy Slovenska |
| 8. | E2E | End to end |
| 9. | eGOV | Elektronické služby štátu |
| 10. | eID | Elektronický občiansky preukaz s čipom, fyzický predmet. |
| 11. | EK | Emisná kontrola |
| 12. | ePN | Elektronická PN (pracovná neschopnosť), resp. elektronické potvrdenie o dočasnej pracovnej neschopnosti. |
| 13. | ESB | Z ang. Enterprise Service Bus, znamená druh MiddleWare podporujúceho servisne orientované interakcie medzi podnikovými aplikáciami |
| 14. | SVM | Slovensko v mobile |
| 15. | FO | Fyzická osoba |
| 16. | IAM | Identity and Access Management (Správa identít) |
| 17. | ID | Identifikačné číslo |
| 18. | IdP | Identity provider |
| 19. | IOMO | Integrované obslužné miesto občana |
| 20. | ID-SK | Jednotný dizajn manuál elektronických služieb Slovenska |
| 21. | KEP | Kvalifikovaný elektronický podpis |
| 22. | KPI | Z anglického Key Performance Indicator, znamená Kľúčový ukazovateľ výkonnosti |
| 23. | mID, MeID | Mobilné ID |
| 24. | MOU | Moje osobné údaje |
| 25. | NKIVS | Národná koncepcia informatizácie verejnej správy Slovenskej republiky |
| 26. | OS | Operačný systém |
| 27. | OVM | Orgán verejnej moci |
| 28. | PO | Právnická osoba |
| 29. | QR kód | Z anglického označenia Quick Response, znamená dvojrozmerný čiarový kód |
| 30. | SIM | Z anglického Subscriber Identity Module, znamená Účastnícka identifikačná karta |
| 31. | T\_ALT | Alternatíva z pohľadu Technologickej vrstvy |
| 32. | TK | Technická kontroly |
| 33. | TO-BE | Budúci navrhovaný stav |
| 34. | UI | User Interface, Používateľské rozhranie pre vyplnenie elektronického formulára alebo jeho časti, ktorá je prezentovaná koncovému používateľovi alebo s ňou koncový používateľ interaguje. Používateľské rozhranie je aj časť elektronickej služby zobrazovaná koncovému používateľovi alebo inak slúžiaca na komunikáciu koncového používateľa so systémom pri jeho používaní. |
| 35. | UPVS | Ústredný portál verejnej správy |
| 36. | UX | User Experience, Používateľskou skúsenosťou sa rozumie celková skúsenosť koncového používateľa nadobudnutá pri všetkých interakciách s elektronickou službou alebo jej používateľským rozhraním. |
| 37. | VM | Z anglického Virtual Machine, znamená virtuálny stroj/server |
| 38. | QAA | Quality Authentication Assurance. |
| 39. | End User / end-user | Koncový používateľ je fyzická osoba, ktorá interaguje s elektronickou službou alebo informačným systémom. |
| 40. | UI Komponent | Funkčná časť používateľského rozhrania s definovanými vlastnosťami; najmä vizuálnymi, štruktúrou, stavmi zobrazenia na rôznych zariadeniach a technologických platformách. |

# Slovník pojmov

| Pojem | Vysvetlenie / Popis |
| --- | --- |
| Objednávateľ | Osoba alebo organizácia využívajúca definovaný súbor aplikácií podľa dohodnutých pravidiel a zmlúv. |
| Tretie strany | Komerčné subjekty alebo iné subjekty mimo prostredia VS (napríklad neziskové organizácie). |
| Zhotoviteľ, Poskytovateľ služby | Osoba alebo organizácia povinná Dielo vykonať a predmet Diela preukázateľne odovzdať Objednávateľovi. |
| Compliance management | Riadenie súladu/zhody, znamená proces overenia správnosti implementácie služby v aplikácii tretej strany podľa vopred určených a publikovaných pravidiel a požiadaviek na integráciu, napr. cez integračný manuál. |
| End User / End-user | Koncový používateľ je fyzická osoba, ktorá interaguje s elektronickou službou alebo informačným systémom. |
| UI Komponent | Funkčná časť používateľského rozhrania s definovanými vlastnosťami; najmä vizuálnymi, štruktúrou, stavmi zobrazenia na rôznych zariadeniach a technologických platformách. |
| Biometrické overenie | Biometrické overenie v kontexte tohto dokumentu sa používa ako odkaz na funkcionalitu mobilného zariadenia a jeho operačného systému, ktoré rozpoznaním na základe tvárovej biometrie prostriedkami príslušného zaradenia, kde si FO takúto možnosť zvolila, umožní zrýchliť zadanie PIN, ktorý je potrebný na odblokovanie aplikácie. Neslúži na identifikáciu osoby v procese aktivácie aplikácie, vytvorenia AC a jeho zápisu do registra autentifikačných certifikátov. |
| Elektronická identita osoby | Elektronická identita osoby sa deklaruje identifikáciou osoby a overuje sa autentifikáciou osoby. Pri prístupe osoby, k prístupovému miestu alebo spoločnému modulu sa identita deklaruje prostredníctvom identifikátora osoby. |
| Autentifikácia osoby (FO) | Autentifikácia FO vykonáva overením pravdivosti deklarovanej identity prostredníctvom overenia platnosti identifikátora osoby. |
| Autentifikačný certifikát (AC) | Druh certifikátu, ktorý slúži na identifikáciu osoby pri prístupe k elektronickej službe. Autentifikačný certifikát nie je určený pre vyhotovenie a overovanie elektronického podpisu alebo elektronickej pečate, ale slúži na prístup (identifikáciu a autentifikáciu osoby) k elektronickej službe. |
| Samoobslužný zápis autentifikátora FO (laicky: samoobslužná registrácia mID) | Samoobslužný zápis autentifikátora vytvoreného prostredníctvom mobilného zariadenia pre účely tohto dokumentu a procesov v ňom popísaných je postupnosť krokov, ktoré vedú k vytvoreniu a zápisu autentifikačného certifikátu FO do registra autentifikačných certifikátov mID.  FO identifikovaná a autentifikovaná pomocou úradného autentifikátora, požiada o vygenerovanie a zápis autentifikátora vytvoreného pomocou mobilného zariadenia do registra autentifikačných certifikátov mID. |
| Asistovaný zápis autentifikátora FO  (laicky: asistovaná registrácia mID) | Asistovaný zápis autentifikátora vytvoreného prostredníctvom mobilného zariadenia je pre účely tohto dokumentu a procesov v ňom navrhnutých postupnosť krokov, ktoré vedú k zápisu autentifikačného certifikátu FO do registra autentifikačných certifikátov mID.  FO na základe fyzickej prítomnosti požiada o identifikáciu a autentifikáciu osobu, ktorá je na vykonanie takého úkonu oprávnená a po potvrdení identity si žiadajúca FO proces dokončí v mobilnom zariadení. Oprávnená osoba, ktorú FO požiada na základe splnomocnenia alebo na základe dohody so Správcom ústredného portálu vykoná identifikáciu a autentifikáciu žiadajúcej FO a potvrdí to prostriedkami určenými príslušnými predpismi. |
| Registrácia mID, Aktivácia zariadenia | V kontexte tohto dokumentu “Samoobslužný zápis autentifikátora FO” alebo “Asistovaný zápis autentifikátora FO“. Každý autentifikačný certifikát sa registruje zvlášť. Proces v rámci ktorého sa vytvorí a zaregistruje autentifikačný certifikát ku ktorému je zariadenie nepriamo viazané privátnym kľúčom |
| Samoobslužné zrušenie zápisu autentifikátora FO (laicky: samoobslužná deaktivácia mID) | Samoobslužné zrušenie zápisu autentifikátora vytvoreného prostredníctvom mobilného zariadenia pre účely tohto dokumentu a procesov v ňom popísaných je postupnosť krokov, ktoré vedú k zrušeniu zápisu autentifikačného certifikátu FO z registra autentifikačných certifikátov mID.  FO identifikovaná a autentifikovaná pomocou úradného autentifikátora alebo prostredníctvom autentifikácie cez mobilné zariadenie, požiada o zrušenie zápisu autentifikátora vytvoreného pomocou mobilného zariadenia z registra autentifikačných certifikátov mID. |
| Asistované zrušenie zápisu autentifikátora FO (laicky: asistovaná deaktivácia mID) | Asistované zrušenie zápisu autentifikátora vytvoreného prostredníctvom mobilného zariadenia je pre účely tohto dokumentu a procesov v ňom navrhnutých postupnosť krokov, ktoré vedú ku zrušeniu zápisu autentifikačného certifikátu FO z registra autentifikačných certifikátov mID.  FO na základe fyzickej prítomnosti požiada o identifikáciu a autentifikáciu osobu, ktorá je na vykonanie takého úkonu oprávnená a po potvrdení identity si žiadajúca FO proces dokončí v mobilnom zariadení. Oprávnená osoba, ktorú FO požiada na základe splnomocnenia alebo na základy dohody so Správcom ústredného portálu vykoná identifikáciu a autentifikáciu žiadajúcej FO a potvrdí to prostriedkami určenými príslušnými predpismi. |
| Deaktivácia mID, Deaktivácia zariadenia | V kontexte tohto dokumentu “Samoobslužné zrušenie zápisu autentifikátora FO” alebo “Asistované zrušenie zápisu autentifikátora FO“.  Proces, pri ktorom je zrušený autentifikačný certifikát a odstránený privátny kľúč zo zariadenia. |
| Autentifikátor | Autentifikátor osoby je autentifikátor podľa Zákona 305 § 21 odsek 1, písmeno c). |
| Autentifikačný modul | Autentifikačný modul na základe identifikátora osoby a autentifikátora podľa Zákona 305, § 21 ods. 1 zabezpečuje autentifikáciu osoby podľa § 19 ods. 4 na účely elektronickej komunikácie, využitie elektronickej identity osoby pre všetky prístupové miesta na účely elektronickej komunikácie a prenos informácie o overenej identite.  Autentifikačný modul pozostáva z autentifikačnej časti a z komunikačnej časti. Autentifikačná časť autentifikačného modulu je určená na autentifikáciu a komunikačná časť autentifikačného modulu je určená na prenos informácie o overenej identite. Správcom autentifikačnej časti autentifikačného modulu je ministerstvo vnútra a správcom komunikačnej časti autentifikačného modulu je MIRRI. |
| Identifikátor FO | Identifikátorom osoby, ak ide o fyzickú osobu (FO), jej rodné číslo v spojení s menom a priezviskom alebo iný identifikátor, ak tak ustanoví osobitný predpis, a ak ide o zahraničnú fyzickú osobu, obdobné číslo alebo identifikátor, ktorý jej je pridelený alebo určený na účely jednoznačnej identifikácie podľa právneho poriadku štátu, ktorého je štátnym občanom, v spojení s menom a priezviskom; ak ide o medzi-systémovú identifikáciu, identifikátorom osoby je sada atribútov, ak tak ustanoví osobitný predpis.  Pre účely tohto dokumentu a služby popisovaných modulov je identifikátorom FO rodné číslo v spojení s menom a priezviskom. |
| Identifikátor PO | Identifikátorom osoby, ak ide o právnickú osobu (PO), fyzickú osobu podnikateľa alebo podnikateľa, ktorý nie je právnickou osobou ani fyzickou osobou (ďalej len „zapísaná organizačná zložka“), identifikačné číslo organizácie (IČO), a ak ide o obdobný zahraničný subjekt, obdobné číslo alebo iný identifikátor, ktorý je im pridelený alebo určený na účely jednoznačnej identifikácie podľa právneho poriadku štátu, v ktorom má sídlo alebo miesto podnikania.  Pre účely tohto dokumentu a služby popisovaných modulov je identifikátorom PO IČO. |
| Mobilné zaradenie FO | Zariadenie, ktoré FO používa ako technický prostriedok komunikácie pri využívaní mobilných služieb. |
| Registrované zariadenie FO | Je mobilné zariadenie FO, v ktorom si FO pomocou natívnej mobilnej aplikácie „Slovensko v mobile“ bezpečne vytvorila a uložila autentifikačný certifikát a príslušnú dvojicu public-private kľúčov, pričom verejný kľúč vygenerovaný na danom mobilnom zariadení FO je uložený v autentifikačnej časti Autentifikačného modulu. |
| Inkrement 1 | Označenie časti projektu “Slovensko v mobile”, ktorá u Zhotoviteľa Slovensko IT, a.s. bola obstaraná 1.9.2021 v rozsahu podľa opisu predmetu zákazky a katalógu požiadaviek, ktorí tvorí prílohy príslušnej zmluvy o dielo a návrh riešenia popísaný v tomto dokumente je v rozsahu a súlade s týmto katalógom požiadaviek. |
| Správca ÚPVS | MIRRI. |
| Mobilné služby | V kontexte tohto dokumentu ide o pojem, ktorý zahŕňa sústavu aplikácií, služieb a funkcionality, ktoré umožňuje používanie elektronických služieb na mobilných zariadeniach či už vo forme responzívnych webových sídiel, ich funkcionality alebo funkcionality natívnych mobilných aplikácií, ktoré tieto služby sprístupňujú cez používateľské rozhranie na mobilnom zariadení.  Súčasťou takejto sústavy sú štandardy, ktoré umožňujú vývoj, konfiguráciu a prevádzku mobilných aplikácií alebo sprístupnenie služieb na mobilných zariadeniach. |

# Popis navrhovaného riešenia

Navrhované riešenie zohľadňuje preferovanú alternatívu zvolenú pomocou MCA. Hlavným produktom je mobilná aplikácia Slovensko v mobile (MOA SVM), ktorá bude vytvorená ako nové riešenia v súlade s biznis požiadavkami a požiadavkami uvedenými v katalógu požiadaviek.

MOA SVM bude slúžiť ako autentifikačný prostriedok a bude postupne koncentrovať kľúčové služby štátu. Riešenie SVM bude integrované na vybrané OVM a zároveň podporí integráciu na pripravované zavedenie eID2.0 s NFC, ktoré bude po realizácii všetkých plánovaných inkrementov integrované cez mSDK poskytnuté MV SR do MOA SVM ako jednej štátnej aplikácie pre kľúčové služby.

SVM bude obsahovať tieto funkčné moduly rozdelené do štyroch (4) inkrementov:

1. **Registrácia a prihlasovanie cez mID** (mID) – vytvorenie natívnej mobilnej aplikácie SVM vrátane registrácie a autentifikácie osoby cez mID na úrovni „pokročilá“ (QAA3),
   1. Mobile ID (centrálny modul eGOV, pre-rekvizita pre ostatné moduly) - mobilný autentifikátor fyzickej osoby (rozhranie na Modul IAM a OAuth2), pre natívne mobilné aplikácie,
2. **Modul pre zasielanie PUSH notifikácií** (ePUSH) – modul slúži ako pre-rekvizita pre ostatné moduly, ktorým umožní zasielanie PUSH notifikácií na konkrétneho používateľa a na konkrétnu tému
   1. ePush (centrálny modul eGOV) - pre podporu interakcie štátu s občanom) bude využívaný ostatnými modulmi (napr. modulmi INNOCENT alebo MOCAL) pre zasielanie PUSH notifikácií používateľom a správu notifikačných tém
3. **Notifikačné centrum** (INNOCENT-BASIC) – umožní používateľom aktivovanej SVM aplikácie prijímať kontextové správy do notifikačného centra aplikácie. Prijaté správy budú v stave prečítaná / neprečítaná a budú uložené v pamäti zariadenia.
   1. Vytvorenie základu modulu, ktorý umožňuje vytvorenie a odoslanie kontextovej správy s preddefinovaným textom a možnou akciou (link na externú URL). Používateľ bude notifikovaný o prijatí kontextovej správy formou PUSH notifikácie vďaka integrácii na ePUSH modul. Používateľ bude schopný s prijatou kontextovou správou interagovať, pripnúť ju na začiatok zoznamu, alebo správu úplne a natrvalo vymazať.
4. **Statický kalendár udalostí** (MOCAL-BASIC) – statický zoznam kalendárových udalostí sumarizuje dôležité dátumy a udalosti o ktorých by mal občan vedieť. Používateľ aplikácie bude o blížiacej sa udalosti vopred notifikovaný formou PUSH notifikácie vďaka integrácii modulu KUKO na modul notifikácii ePUSH. Statický kalendár v tejto fáze poslúži ako základný stavebný kameň pre modul KUKO na ktorom sa v budúcnosti vybuduje interaktívny personalizovaný kalendár, ktorý bude dynamicky napĺňaný udalosťami pre každého používateľa osobitne, podľa toho, akú životnú situáciu aktuálne používateľ rieši.
5. **Registrácia a prihlasovanie pomocou eID 2.0 s NFC** (C3PO-EID20) – sprístupnenie procesu aktivácie aplikácie iba na mobilnom zariadení, bez potreby využitia počítača s pripojenou čítačkou a umožnenie prihlásenia prostredníctvom mobilnej aplikácie SVM k službe štátu na úrovni „vysoká“ (QAA4), vrátane použitia mobilného zariadenia FO s aktivovanou aplikáciou „Slovensko v mobile“ ako čítačky pre eID 2.0 s NFC.
6. **Integrácia Sociálnej poisťovne** (C3PO-SOCINS) – integrácia Sociálnej poisťovne na notifikačné centrum SVM systému umožní integrovaným zaslať predom nadefinované kontextové správy na určitú tému (topic) konkrétnemu používateľovi aktivovanej SVM identifikovanému prostredníctvom unikátneho identifikátora PČO,
7. **Integrácia 2 OVM** (C3PO-PBODY) – integrácia a podpora pripojenia dvoch (2) OVM (podľa určenia Objednávateľom) pre používanie mID v 1 procese ISVS alebo na zasielanie kontextových správ pre FO použitím existujúceho API vrátane pripojenia OVM ako ISVS tretej strany "spaghetti" spôsobom vrátane zapracovania Objednávateľom a Zhotoviteľom vzájomne pripomienok z rozhraniu pre zasielanie kontextových správ,
8. **Webový portálu pre uskutočnenie asistovanej registrácie** ( (mID-PREG)) – novovytvorený webový portál umožní oprávneným osobám vykonávať činnosti prezenčnej asistovanej registrácie a aktivácie aplikácie SVM a umožní tak rozšíriť základňu používateľov SVM o množstvo nových používateľov, ktorí by bez pomoci pri registrácii neboli ochotní alebo schopní aplikáciu SVM využívať.

ARCHITEKTÚRA RIEŠENIA PROJEKTU

Biznis vrstva

Biznis architektúra

Biznis architektúra vychádza zo základných cieľov projektového zámeru, ktorých spoločným prvkom je umožniť občanom SR a podnikateľom jednoduchým a prirodzeným spôsobom využívať elektronické služby verejnej správy SR s použitím registrovaného mobilného zariadenia. Zároveň zohľadňuje aktuálne a pripravované legislatívne rámce v oblasti eGOV na národnej, ako aj EÚ úrovni.

Nasledujúci diagram znázorňuje návrh budúcej architektúry biznis služieb SVM (high-level pohľad pre **všetky plánované inkrementy**, nie len v PZ a tomto PP uvedené časti). Primárnym cieľom je vytvorenie natívnej mobilnej aplikácie prostredníctvom ktorej bude môcť občan pristupovať k elektronickým službám eGovermentu.

Diagram

Description automatically generated

# Používatelia systému (aktéri)

Základnými používateľmi a aktérmi služieb SVM sú:

1. **Občan (fyzická osoba) –**  kľúčový aktér biznis architektúry, predstavuje hlavného príjemcu služieb natívnej mobilnej aplikácie SVM. Všetky služby SVM sú primárne zamerané na občana/podnikateľa, či už formou priameho poskytovania prostredníctvom mobilnej aplikácie, alebo prostredníctvom aplikácií a softvéru tretích strán, ktoré budú využívať jednotné služby a komponenty vybudované v rámci SVM,
2. **Občan (podnikateľ) –**  kľúčový aktér biznis architektúry, predstavuje hlavného príjemcu služieb natívnej mobilnej aplikácie SVM, vystupuje ako separátny typ používateľa, čiže fyzická osoba, ktorej rola je definovaná tak, že môže pristupovať k údajom právnickej osoby
3. **Správca obsahu registračného portálu –**  tento aktér zabezpečuje aktuálnosť textového a jazykového obsahu registračného portálu pomocou prístupu do CMS systému registračného portálu (DRUPAL),
4. **Správca prístupov –**  spravuje (prideľuje / odoberá) prístupy aplikácií tretích strán (alebo OVM), ktoré majú záujem o využívanie modulov SVM,
5. **Správca systému –**  zabezpečuje správu SVM systému a mobilných aplikácií a ich aktuálnych (podporovaných / nepodporovaných) verzií,
6. **Pracovník obslužného miesta –**  pracovník externej spoločnosti zmluvne sa zaväzujúcej poskytovať službu asistovanej (prezenčnej) registrácie zariadení SVM používateľov pre mID,
7. **Pracovník Kontaktného centra –**  pracovník prevádzkovateľa kontaktného centra (NASES), ktorý slúži ako prvá línia kontaktu pre používateľov, ktorí potrebujú pomoc. Jeho úlohou je poskytnúť používateľom (Občanom) potrebné informácie, prípadne ich previesť procesom asistovanej deaktivácie zariadenia,
8. **Konzument služby (OVM, tretia strana) –**  predstavuje prevádzkovateľa mobilnej aplikácie / informačného systému OVM alebo tretej strany, ktorý má záujem o využívanie modulov SVM. Konzument služby sa musí zaregistrovať a nechať posúdiť súlad aplikácie s podmienkami integrácie, predpokladá sa vytvorenie kostry Dohody o integračnom zámere v súčinnosti so Správcom komunikačnej časti.

# Hlavné procesy riešenia

V tejto časti sú spracované základné biznis procesy nahrnovaného riešenia. Jednotlivé procesy sú rozdelené podľa entít, ktoré sú prostredníctvom týchto procesov vytvárané a ďalej počas ich životného cyklu aktualizované. Biznis funkcie a služby sú popísané v PZ.

## Aktivácia zariadenia

Diagram popisuje aktivačnú fázu realizovanú pomocou webového registračného portálu (Enrollment portálu). Tento proces je iniciovaný pri prihlásení a zistení, že používateľ ešte nebol registrovaný.Diagram

Description automatically generated

Diagram

Description automatically generated

## Aktivačná fáza mobilnej aplikácie

Diagram popisuje proces aktivácie natívnej mobilnej aplikácie „Slovensko v mobile“ od jej prvého spustenia do ukončenia aktivačnej fázy tohto procesu.Diagram

Description automatically generated

## Konfirmačná fáza mobilnej aplikácie

Diagram popisuje proces aktivácie natívnej mobilnej aplikácie SVM od ukončenia aktivačnej fázy mobilnej aplikácie, inicializácie konfirmačnej fázy po úspešné ukončenie aktivácie natívnej mobilnej aplikácie SVM.Diagram

Description automatically generated

## Konfirmačná fáza Enrollment portálu

Diagram popisuje proces aktivácie natívnej mobilnej aplikácie SVM z pohľadu Enrollment portálu na ktorom prebieha konfirmačná fáza súbežne s priebehom konfirmačnej fázy mobilnej aplikácie.Diagram

Description automatically generated

## Prihlásenie k službe štátu

Služba predstavuje proces prihlasovania používateľa na webový portál ÚPVS prostredníctvom autentifikácie mobilnou aplikáciou SVM (mID) načítaním QR kódu.

Diagram

Description automatically generated

## Iniciačná fáza prihlásenia

Diagram popisuje inicializačnú fázu procesu prihlasovania používateľa pomocou QR kódu vo webovom prehliadači na počítači.Diagram

Description automatically generated

## Prihlásenie z pohľadu mobilnej aplikácie

Diagram popisuje proces prihlasovania používateľa pomocou QR kódu vo webovom prehliadači na počítači, z pohľadu mobilnej aplikácie, ktorá umožňuje verifikovanie používateľa.

Diagram

Description automatically generated

## Dokončenie prihlásenia

Diagram popisuje dokončovaciu fázu procesu prihlásenia pomocou QR kódu vo webovom prehliadači na počítači. Výstupom tohto procesu je prihlásený používateľ.

Diagram

Description automatically generated

## Prihlásenie k službe cez mID pomocou URL schémy

Služba predstavuje proces prihlasovania používateľa na webový portál ÚPVS prostredníctvom autentifikácie mobilnou aplikáciou SVM (mID) cez webový prehliadač v mobilnom zariadení.

Diagram

Description automatically generated

## Asistovaná registrácia zariadenia FO

Služba predstavuje asistovanú (prezenčnú) registráciu mobilného ID s pomocou asistenta (napr. na IOMO) v prevádzke.

Diagram

Description automatically generated

**FIGMA PROTOTYP:**

https://www.figma.com/file/OFZGUfcZor1ecJZVaRLmaP/SVM-Enrollment-(Development)?node-id=2622%3A9149

## Samoobslužná deaktivácia zariadenia FO cez webový portál

Proces samoobslužnej deaktivácie zariadenia fyzickej osobe cez webový portál.

Diagram

Description automatically generated

# Jazyková lokalizácia

MOA SVM aj webový portál budú dostupné v 2 jazykových lokalizáciách: Slovenský jazyk, Anglický jazyk. Používateľ bude mať možnosť nastaviť jazyk pri prvom prihlásení alebo kedykoľvek počas používania pomocou funkcie dostupnej v aplikácii.

Riešenie bude vytvorené tak, aby umožnilo pridať ďalšie jazykové mutácie doplnením prekladov jednotlivých kľúčov použitých v aplikácii.

# Aplikačná vrstva

Aplikačná architektúra definuje komponenty riešenia a väzby medzi nimi. V rámci architektúry riešenia sú definované aplikačné služby poskytované jednotlivými komponentami riešenia. Zámerom aplikačnej architektúry je pri riešení SVM používať moderné štandardy.

Aplikačné architektúra reprezentovaná komponentovým modelom, ktorý zobrazuje budúci stav (TO-BE) je uvedená na nasledujúcej schéme.

Graphical user interface, diagram

Description automatically generated

Komponenty riešenia

1. **ÚPVS NASES**  
   Prostredie a komponenty ÚPVS v správe NASES-u
   1. **Audit**  
      Auditný systém pre dlhodobé ukladanie auditných správ.
   2. **Logging**  
      Logovací systém pre krátkodobé uchovávanie systémových správ a biznisových metrík
   3. **Monitoring**  
      Monitorovací systém pre správu systému
2. **ÚPVS IAM**
   1. **Modul ÚPVS IAM**Identity access manažment modul UPVS poskytujúci služby autorizácie pomocou SAML2 tokenov, manažment identít a manažment ich zastupovaní v systému ÚPVS.
   2. **LDAP Mirror**Mirror LDAP servera s UPVS identít s jeho zastupovaniami, pre získanie zmien nad identitami, zastupovaniami a pre odľahčenie záťaže zo súčasného ÚPVS IAM.
3. **Identity Provider**Identity provider pre mID a systém SVM.
   1. **Registračný servis a LDAP mID** - Zabezpečuje registráciu a deaktiváciu mID identít do systému LDAP prevádzkovateľa systému.
   2. **OpenID Connect server** - pre zabezpečenie autorizácie a autentifikácie fyzickej osoby pomocou mID a OAuth2 protokolu
   3. **Device service** – správa a manažment autentifikačných certifikátov registrovaných v registri autentifikačných certifikátov mID
   4. **mID service** – servis pre prihlasovanie sa pomocou mID na portáloch s podporou jednotného prihlasovania sa pomocou ÚPVS.
   5. **LDAP Technických účtov** – zabezpečuje správu a autorizáciu servisov a mikroservisov pre pripojenie k interným servisom SvM a Kafke.
   6. **Audit**  
      Auditný proxi systém pre zber auditných správ a ich následne odosielanie do logging systému NASES.
   7. **Logging**  
      Logovací proxi systém pre krátkodobé uchovávanie systémových správ a biznisových metrík a ich následne odosielanie do logging systému NASES
   8. **Monitoring**  
      Monitorovací proxi systém pre správu systému a ich následne odosielanie do logging systému NASES
4. **Externá APIGW (Public)**  
   Verejná API gateway vystavená pre prístup v sieti verejného Internetu zabezpečuje:
   1. Správu verených REST API volaní (Open API 3 špecifikácia)
   2. Overenie autorizácie prístupu k verejným zdrojovým dátam systému SvM
   3. Prístup k autorizačným prostriedkom OIDC servera
   4. Prístup k modulom a zdrojom ÚPVS
5. **Interná APIGW (Private)**
   1. Správu neverejných a administrátorských REST API volaní (Open API 3 špecifikácia)
   2. Overenie autorizácie prístupu k interným zdrojovým dátam systému SVM
   3. Prístup k autorizačným prostriedkom OIDC servera
   4. Prístup k modulom a zdrojom ÚPVS
6. **Event/Message Bus (Kafka)**Event-message bus pre asynchrónnu komunikáciu medzi servismi a mikroservismi projektu SVM, publikovanie udalostí z SVM a  integrovaných systémov, modulov a servisov.
7. **Servisy a moduly SvM**
   1. **Registračný servis**  
      Servis pre zápis a zrušenie zápisu autentifikátora FO. Sprostredkúva samoobslužný ako aj asistovaný zápis či zrušenie zápisu autentifikátora FO do registra autentifikačných certifikátov mID.
   2. **Konfiguračný servis**Servis mobilných aplikácii pre manažovanie aplikačných a používateľských nastavení. Konfigurácii, profilov, force a soft update, podporu jazykov a jazykové lokalizácie, notifikačné schémy a profily.
   3. **ePush modul**Modul je zložený z mikroservisov poskytujúcich služby pre odosielanie push notifikácii, konkrétnej osobe alebo skupine osôb, pomocou manažmentu tém (topicov) a samotnú integráciu so službami Firebase pre odosielanie push notifikácii.
   4. **eDesk Event service**Servis zabezpečuje odchytávanie a spracovanie eventov z modulu ÚPVS eDesk pre ich následné odosielanie vo forme push notifikácií do aplikácie SVM.
   5. **Audit**  
      Auditný proxi systém pre zber auditných správ a ich následne odosielanie do logging systému NASES.
   6. **Logging**  
      Logovací proxi systém pre krátkodobé uchovávanie systémových správ a biznisových metrík a ich následne odosielanie do logging systému NASES
   7. **Monitoring**  
      Monitorovací proxi systém pre správu systému a ich následne odosielanie do logging systému NASES
8. **Enrollment portál**Informačný web portál používateľov neregistrovaných a registrovaných používateľov mID.  
   Poskytuje:
   1. Informačný web k mID
   2. Aktiváciu a registráciu mID
   3. Správu zariadení registrovaných mobilných zariadení
   4. Deaktiváciu mID aktivovaných zariadení
   5. Prihlasovanie na UPVS a portáloch integrujúcich jednotné prihlásenie pomocou ÚPVS
9. **Aplikácia SVM**Android aiOS verzie SVM aplikácie poskytujúcej identitu mID a služby aktivácie, deaktivácie a prihlasovanie sa pomocou mID.

# Komunikačné štandardy

Komunikačná architektúra zohľadňuje „API First“ princíp pre prístup k zdrojom dát. Pre **verejnú komunikáciu** je navrhnutá synchrónna komunikácia cez Layer7 APIGW rozhranie zabezpečenom s HTTPS protokolom (**TLS/SSL**). Preferovaným formátom REST API komunikácie je **JSON** formát. Jednotlivé API sú zašpecifikované a evidované v **OpenAPI 3** štandarde.

Pre **privátnu** **komunikáciu** je navrhnutá **synchrónna komunikácia** cez Layer7 APIGW rozhranie zabezpečenom HTTPS protokolom **(TLS/SSL**), ako aj **asynchrónna komunikácia** cez eventbus zbernicu (Apache Kafka) zabezpečená **ldap-ssl** v protokole **Avro**. Pri asynchrónnej komunikácii servisy na základe používateľských práv definovaných IdP LDAP-e, vytvoria permanentné spojenie z event brokerom na príslušné autorizované témy, čím sa vylúči z ďalšieho spracovania nutnosť realizovania autentifikačnej rutiny na jednotlivých servisoch prepojených event zbernicou.

Priame pripojenie servisov a mikroslužieb na IdP zabezpečí **mTLS** protokol.

## Autorizácia

Autorizáciu a autentifikáciu na verejnú API gateway zbernicu zabezpečuje **OpenID Connect** server pomocou OAuth2 protokolu a jeho tokenov v **JWT** formáte. Interná API GW je zabezpečená **OpenID Connect** serverom pomocou OAuth2 protokolu a **LDAP** serverom.

Pre potrebu integrácie a prístup k službám ÚPVS IdP integruje **WebSSO** autorizáciu cez **SAML2** protokol.

## OAuth2.0

OAuth 2.0 slúži na delegáciu prihlasovania (https://oauth.net/2/). Tento systém umožňuje poskytnúť obmedzený prístup k používateľskému účtu nachádzajúcemu sa v inej službe. Toto môže byť využité na overenie používateľa. Server inej služby autorizuje používateľa a poskytne túto informáciu službe, ktorá potrebuje overiť používateľa. Používateľ tak môže mať u služby používateľské konto, ale služba nemusí ošetrovať overovanie používateľa v rámci svojej funkcionality.

OAuth 2.0 je v štandarde Open API pre SVM využívaný na autentifikáciu používateľov.

Diagram, schematic

Description automatically generated

## OpenID Connect

OpenID Connect (https://openid.net/connect/) je otvorený štandard použiteľný bez obmedzení pri implementácii autorizácie prostredníctvom Oauth 2.0. OpenID je overený, otestovaný a funkčný spôsob jej nasadenia. Autorizácia v OpenID je uskutočňovaná prostredníctvom tokenov, ktoré sú vo formáte JSON Web Token.

Slovensko v mobile bude používať štandard OpenID Connect ako implementáciu Oauth 2.0 na autorizáciu používateľov. Jednotné prihlasovanie prostredníctvom modulu mID prebieha prostredníctvom autentifikácie používateľa v mobilnej aplikácii „Slovensko v mobile“, autentifikačného servera IdP (OIDC) mID a prostredníctvom rozšíreného modulu IAM ÚPVS.

Samotná autentifikácia bude riešená cez PKI typu sieť dôvery. IdP mID sa stáva IdP pre IAM ÚPVS kde v procese autentifikácie validuje požiadavku vo forme SAMLRequest z prihlasovacej stránky IAM ÚPVS a vracia ju podpísanú vo forme SAMLResponse do IAM ÚPVS, ktorý po autorizácii vydá WebSSO SAML token.

IdP (OIDC) mID identifikuje FO pomocou mobilnej aplikácie SVM, od ktorej vyžaduje opätovnej autentifikácie pomocou mID (privátnym kľúčom) na ľubovoľnom aktivovanom zariadení identity FO s následným potvrdením pomocou OTP vygenerovaným a zobrazeným vo forme passcodu resp. QR kódu v procese prihlasovania sa do portálu s integrovaným jednotným prihlásením pomocou WebSSO.

Pre vytvorenie sieť dôvery medzi IAM ÚPVS a IdP mID sa vymieňajú SAML2 Metadata s podpisovým a šifrovacím X.509 certifikátom s RSA 2056 bitovými kľúčmi.

## JSON Web Token

JavaScript Object Notation (JSON) Web Token (JWT, https://jwt.io/introduction/) je otvorený štandard (RFC751912), ktorý predstavuje kompaktný spôsob bezpečného prenosu informácií medzi rôznymi stranami vo forme JSON objektu. Digitálny podpis zabezpečuje overiteľnosť a dôveryhodnosť prenášaných informácií. Podpis tokenu párom verejného a súkromného kľúča zároveň dokladá, že podpis bol skutočne uskutočnený osobou držiacou osobný kľúč.

Dva hlavné scenáre využitia JWT sú autorizácia a výmena informácií. Autorizácia je realizovaná tak, že po prihlásení používateľa do systému jeho interakcie obsahujú JWT, ktoré ho jednoznačne identifikujú. Pri výmene informácií je využívaná vlastnosť, že vďaka podpisu je jasne určený skutočný pôvodca a zároveň JSON zaručuje, že obsah správy nebol modifikovaný.

Autentifikačný server (OIDC) mID autentifikuje používateľa pomocou autentifikačného certifikátu vo forme JWK, aktivovaného v procese zápisu autentifikátora FO vytvoreného pomocou mobilného zariadenia. V tomto prípade mobilná aplikácia „Slovensko v mobile“ plní úlohu jednotného mobilného autentifikátora mID.

Mobilná aplikácia v procese autentifikácie využíva privátny kľúč vygenerovaný v procese zápisu autentifikátora FO. Privátny kľúč je uložený v bezpečných úložiskách mobilných zariadení poskytovaných mobilnými platformami, chránené a šifrované pomocou používateľského (nie systémového, poskytovaného mobilnými zariadeniami) PIN zvoleného v procese zápisu. Zároveň s PIN má používateľ možnosť zvolenia ochrany privátneho kľúča pomocou biometrie poskytovanej výrobcom mobilného zariadenia.

Mobilná aplikácia pre autentifikáciu a overenie identity používateľa v autentifikačnom servery mID vytvára JWT s JWS signatúrou podpísanou privátnym kľúčom uloženým v procese zápisu autentifikátora FO. Autentifikačný server (OIDC) po overení signatúry vráti autorizačné JWT tokeny pre autorizovaný prístup k zdrojom cez API GW zbernicu.

Po úspešnej autentifikácii je mobilnej aplikácia „Slovensko v mobile“ umožnené autorizovane požiadať o vytvorenie overovacieho passcodu (OTP). Respektíve odoslať autorizovanú požiadavku o overenie QR kód (OTP) zo služby servis providera Enrollment portálu pre jednotné prihlásenie pomocou IAM ÚPVS.

## Mobile mID

Nakoľko bolo prijaté riešenie umožňuje vytvorenie a zápis autentifikátora FO na viacerých zariadeniach vlastnených FO. Aplikačná architektúra mID vytvára prostredie pre identifikačný pár identity mID FO a identity jej konkrétneho mobilného zariadenia. Identita mID FO je realizovaná pomocou bezrozmerného jedinečného identifikátora (UUID) a po procese zápisu autentifikátora je uložená v LDAP systéme mID. Priradený a uložený identifikátor mID FO sa už nikdy nemaže.

Nakoľko riešenie umožňuje FO mať zaktivované mID na viacerých vlastnených mobilných zariadeniach, samotná identita mID FO je zviazaná so zoznamom aktivovaných mobilných zariadení, identifikovaných pomocou vygenerovaného jednoznačného identifikátora mobilného zariadenia (UUID) a verejnej časti kľúčového páru pre potrebu overenia identity vo formáte JWK. Existencia týchto dvoch identifikátor závisí od aktivácie samotného zariadenia a v prípade deaktivácie mobilného zariadenia sa od danej identity mID zo systému vymazávajú.

Pre potreby deaktivácie mobilného zariadenia od identity mID FO, systém v procese zápisu identifikátora generuje jedinečný dezaktivačný token vo forme jedinečného identifikátora (UUID). Dezaktivačný token slúži pre deaktiváciu zariadenia aj v prípade, že FO zabudne PIN a nevie sa už autorizovať. Samotnú deaktiváciu zariadenia s týmto tokenom bude môcť FO zrealizovať autorizovane vo svojom mobilnom zariadení v aplikácii SVM, autorizovane pomocou mID, eID v Enrollment portáli ako aj asistovane pomocou služby poverenej MIRRI na základe jeho osobných údajov z občianskeho preukazu.

Ako kontajner autentifikačného certifikátu s verejnou časťou kľúčového páru bol zvolený formát JWK. Platnosť certifikátu je na obdobie 10 rokov. Pri súčasnom trende životnosti a používateľnosti mobilných zariadení FO nie je možné, aby aktivované certifikáty dosiahli životnosťou svoju expiračnú dobu. Preto nebude nutné ich obnovovanie.

## Autentifikácia mID

Ako základ autentifikácie sa zvolila podpis autentifikačnej požiadavky privátnou častou kľúčového páru a následné overenie podpísanej požiadavky pomocou verejnej časti kľúčového páru, vygenerovaného v procese zápisu autentifikátora, bezpečne uloženými v bezpečných úložiskách poskytovanými mobilnými platformami a v zabezpečenom úložisku identity providera.

Pre kryptografiu kľúčového páru bola vybraná na báze eliptických kriviek (ECC) s dĺžkou 256 bitov. Konkrétne krivka P-256 (Weierstrassova krivka hlavného poľa) umožňujúca podpisy NIST P-256 a overenie kľúčov, tak ako na mobilných platformách aj v backend systémoch.

Samotná autentifikačná požiadavka je realizovaná JWT tokenom podpísaného pomocou ECDSA podpisového algoritmu ES256 (ECDSA s použitím P-256 and SHA-256).

|  |  |  |
| --- | --- | --- |
| **Ekvivalentné veľkosti kľúčov (bity)** | | |
| Symetrický | **ECDSA** | **RSA** |
| 80 | 160 | 1024 |
| 112 | 224 | 2048 |
| 128 | 256 | 3072 |
| 192 | 384 | 7680 |
| 256 | 512 | 15360 |

Autentifikácia pomocou mID vyžaduje primárne ochranu samotný kľúčového páru ako v procese zápisu autentifikátora, kde sa v šifrovanom kanály prenáša verejná časť kľúča a bezpečne ukladá v LDAP systéme IdP mID. Prístup do LDAP-u mID má len IdP mID. Podobne najdôležitejšiu ochranu privátnej časti kľúčového páru v bezpečnom úložisku mobilného zariadenia (Apple secure enclave, Android key store) realizuje mobilná aplikácia SVM. Viac v odstavci *Privátna časť kľúčového páru v mobilnom zariadení*.

## Proces zápisu autentifikátora

Proces zápisu autentifikátora FO, teda identity mID, je realizovaný v pomocou techniky výmeny kľúčov ECDH a vytvorenia bezpečného kanála medzi registračnou službou IdP na báze JWE protokolu. Proces pozostáva z dvoch fáz a synchronizácie servisných služieb, ktoré sú súčasťou dodávky a to Enrollment portálu, registračnej servisy IdP a mobilnej aplikácie „Slovensko v mobile“:

1. Aktivačná fáza – slúži na identifikáciu osoby v systéme ÚPVS pomocou autentifikácie eID alebo mID (ak už bol realizovaný prvotný zápis) a následnú inicializáciu pre vytvorenie bezpečného kanála.
2. Konfirmačná fáza – slúži pre overenie ÚPVS identity voči IdP „Slovenska v mobile“ mID v procese zápisu, vytvorenie bezpečného kanála pre prenos údajov a samotnú výmenu údajov potrebných pre zápis identity mID.

## Aktivačná fáza

V aktivačnej fáze sa FO prihlási pomocou služby jednotného prihlasovania ÚPVS v Enrollment portáli cez eID alebo mID autentifikácie. Enrollment portál pomocou WebSSO tokenu ÚPVS získa aktivačný token pre začatie zápisu autentifikátora FO.

Mobilná aplikácia získa verejný aktivačný JWK RSA kľúč vytvorený a spravovaný registračnou službou IdP, vygeneruje dočasný pár EC kľúčov a získa aktivačný kód z Enrollment portálu pre zápis autentifikátora FO pre výmenu kľúčov a secretu medzi registračnou službou a mobilným zariadením s využitím ECDH protokolu. Secret je následne použitý pre vytvorenie bezpečného šifrovaného kanálu nad JWE protokolom.

## Konfirmačná fáza

V konfirmačnej fáze si mobilná aplikácia cez šifrovaný kanál požiada registračná služba o vygenerovanie konfirmačného kódu, ktorým je nevyhnutné prepísaním do Enrollment portálu opätovne potvrdiť identitu prihlásenej osoby v registračnej službe IdP a tým spustí samotný zápis autentifikátora FO v mobilnej aplikácii „Slovensko v mobile“. Tá po overení konfirmačného kódu registračnou službou spustí generovanie RSA páru privátneho a verejného kľúča, generovanie jedinečného identifikátora mobilného zariadenia a zozbiera dostupne informácie o mobilnom zariadení. Údaje nevyhnutné pre zápis autentifikátora FO pošle na zápis do registračnej servisy, ktorá po overení údajov, vygeneruje novú identitu a zapíše ju cez IdP SVM do LDAP-u mID.

## Privátna časť kľúčového páru v mobilnom zariadení

Samotný prístup k uloženým privátnym kľúčom je založený na sekvencii ochrany s podporou aplikačného PIN-u navoleného FO počas procesu zápisu autentifikátora, ktorý sa nikde neukladá. Veľkosť PIN bola určená ako 6 miestny numerický kód s pravidlami vytvárania znemožňujúcimi zadať viac ako 2 rovnaké čísla alebo vzostupnú a zostupnú sekvenciu čísel.

Aplikačný PIN identity, chráni 256 bitový šifrovací kľúč, vygenerovaným pri zápise autentifikátora, ktorým je zašifrovaný privátny kľúč uložený v bezpečnom úložisku. Aplikácia SVM zároveň umožňuje FO využiť možnosť systémovej biometrie poskytovanej výrobcami mobilných zariadení, ktorá v rovnakej sekvencii umožňuje prístup k privátnemu kľúču a následnej autentifikácie pomocou podpísanej požiadavky v IdP mID. Samotná biometriu nie možné použiť, pokiaľ si používateľ nezaktivuje systémový PIN mobilného zariadenia.

Samotná biometria je a PIN systém mobilného zariadenia zabezpečuje taktiež záložnou sekvenciou (fallback), kde v prípade 5-násobnej neúspešnej identifikácie pomocou biometrie sa automaticky systém mobilného zariadenia zablokuje biometriu a žiada o zadanie aplikačného PIN-u.

Samotná aplikácia zároveň kontroluje počet nesprávnych zadaní PIN a v prípade, že FO zadá 5 krát nesprávny PIN, automaticky odošle požiadavku o deaktivuje zariadenia v IdP mID a vymaže kľúče, tokeny a privátne dáta z mobilného zariadenia.

## ePUSH notifikačné témy a notifikačné schémy

Pre potrebu odosielania notifikácie skupine ľudí s konkrétnym záujmom sa zavádzajú do modulu **témy** (*topics*) reprezentujúce push notifikačnú správu pre skupinu používateľov a notifikačné schémy reprezentujúce push notifikačný model pre aplikačnú úroveň.

Podporované budú 2 typy tém:

1. **Statické** (Inkrement 1 a 2) – deklarované v priamo v schéme, ktoré budú inicializované aplikačným backend mobilnej aplikácie alebo externým IS.
2. **Dynamické** (Inkrement 5+, nie je predmetom tohto PP) – procesne určené IS, ktoré využívajú služby push notifikačného modulu. Sú definované a inicializované používateľom v mobilnej aplikácii.

Koncept tém bude tvorený **notifikačnou schémou** definovanou na základe biznis požiadaviek mobilnej aplikácie a premisy, že všetky témy sú si rovné. Notifikačná schéma bude podporovaná týmito stranami:

1. **ePush Modulom** – eviduje aplikačnú a používateľskú schému do registra tém pre používateľské, aplikačné a globálne push notifikácie
2. **Aplikačným backend mobilnej aplikácie** – backend služby, pre podporu mobilných aplikácii, udržujú a registrujú aplikačnú default schému. Aplikačná schéma bude rozšírená o aplikačné nastavenia potrebné pre ePush modul (ikonka, požadované APN a FCM konfigurácie pre konkrétnu mobilnú aplikáciu, ...). Taktiež udržiavajú používateľské schémy (notifikačné profily) vo svojom internom úložisku. Registrujú prístupy k notifikáciám pre používateľov na základe aplikačnej schémy na požadované notifikácie a odchytávajú zmeny nad požadovanými notifikáciami z ePush modulu.
3. **Mobilnou aplikáciou** – načítavajú a manažujú používateľskú notifikačnú schému, ktorá sa je súčasťou ich aplikačného profilu ako používateľský profil pre push notifikácie.

Schéma bude podporovať 3 typy top-level tém, ktoré môžu byt definované a požadované aplikáciou:

1. **Global** – témy, cez ktoré môže posielať push notifikácie štát do všetkých mobilných aplikácii registrovaných v ePush. Tieto témy budú súčasťou všetkých schém, automaticky, či už to aplikácia žiada alebo nie, teda povinné.
2. **Local** – témy, najmä pre podporu vlády, ministerstiev, parlamentu, organov vyšších územných celkov a vládneho cloudu. Budú podobne ako globálne témy predefinované a manažované v číselníkoch ePush modulu, avšak budú nepovinné a každá aplikácia si ich bude môcť notifikačnou schémou vyžiadať.
3. **Application** – tieto témy budú obsahovať vlastné témy pre mobilné aplikácie na základe biznis požiadaviek na tieto aplikácie ako aj predefinované témy externých inf. systémov, ak ich podporujú.

Inkrement 1 projektu „Slovensko v mobile“ implementuje požiadavky aplikácie „Slovensko v mobile“ a pripravuje architektúru riešenia tak, aby splnila požiadavky popísané v katalógu požiadaviek.

## Použité architektonické štandardy

Ako hlavný backend dizajn je navrhovaná mikroslužobvá architektúra s eventbus zbernicou.

Architektúra zohľadňuje princípy návrhu, ktoré sú:

1. **Princíp jednotnej zodpovednosti (Robert C Martin)**   
   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 rovnakého dôvodu“.
2. **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.
3. **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:
   1. **Zapuzdrenie** - Služby musia zapuzdrovať podrobnosti vnútornej implementácie, aby externý systém využívajúci služby nemusel robiť starosti s vnútornými súčasťami. Zapuzdrenie znižuje zložitosť a zvyšuje flexibilitu (prispôsobivosť zmenám) systému.
   2. **Voľné spriahnutie** - Zmeny v jednom mikrosystéme by mali mať nulový alebo minimálny vplyv na ostatné služby v ekosystéme. Tento princíp tiež navrhuje mať voľne spojenie komunikačné metódy medzi mikroslužbami.
   3. **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.
4. **Šesťhranná architektúra**   
   Tento štýl architektúry umožňuje aplikácii rovnako riadiť používateľov, programy, automatizované testovacie alebo dávkové skripty a vyvíjať a testovať ju izolovane od jej prípadných zariadení a databáz za behu. Nazýva sa to tiež „Architektúra portov-adaptérov“, kde porty a adaptéry zapuzdrujú základnú aplikáciu tak, aby fungovala jednomyseľne na externé požiadavky. Porty a adaptéry spracúvajú externé správy a prevádzajú ich na príslušné funkcie alebo metódy vystavené aplikácii vnútorného jadra. Typická mikroslužba vystavuje RESTful API pre externú vonkajšiu komunikáciu, rozhranie správ (napr. Kafka, RabbitMQ, HornetQ atď.) pre notifikáciu udalostí a databázové adaptéry pre perzistenciu robí z hexagonálnej architektúry vhodný štýl pre vývoj mikroslužby.

Aj keď existuje veľa architektonických štýlov a princípov, vyššie uvedené položky majú vysoký význam pre mikroslužby.

Jednotlivé mikroslužby budú spĺňať nasledovné:

1. **Bezpečnosť (Security)**
2. **Externalizovaná konfigurácia**(Configuration service)
3. **Health check**
4. **Log aggregation** (Correlation ID)
5. **Distributed tracing**
6. **Metrics**
7. **Exception tracking**
8. **Audit log**
9. **Monitoring:** s mikroslužbami rozmiestnenými po lokálnej alebo cloudovej infraštruktúre je schopnosť predvídať, detekovať a informovať o problémoch týkajúcich sa kritického stavu systému. K dispozícii je niekoľko monitorovacích nástrojov, napríklad New Relic, CloudWatch, Datadog, Prometheus a rafana.

# Dátová vrstva

High Level logický doménový model popisuje 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.

| ID | Doména | Popis |
| --- | --- | --- |
| DOM1 | Identita mID | Základné údaje o identite fyzickej osoby a jej registrovaných mobilných zariadení pre mID. Údaje sú budú uložené v LDAP service na MV SR. |
| DOM2 | Auditný záznam (audit\_data) | Základné údaje o zrealizovaných procesoch v aplikácii zaznamenávané v podobe auditných záznamov |
| DOM3 | Registrácia (registration\_data) | Základné údaje zaznamenávané v aplikácii počas procesu registrácie mobilného autentifikátora používateľa |
| DOM4 | Konfigurácia (conf\_data) | Základné údaje o nastaveniach aplikácie, ktoré sú poskytované mobilnej aplikácii prostredníctvom konfiguračnej servisy |
| DOM5 | Provider (provider) | Základné údaje o poskytovateľovi poskytujúcom push notifikácie prostredníctvom ePush modulu |
| DOM6 | Push notifikátor (push\_notifier) | Základné údaje o konfiguračných nastaveniach push notifikácii pre jednotlivé aplikácie |
| DOM7 | Príjemca (recipient) | Základné údaje o push notifikačnej identite. |
| DOM8 | Push notifikačná téma (push\_notification\_topic) | Základné údaje o formáte push notifikačnej témy a evidencie registrácie/deaktivácie sa na jednotlivé témy |
| DOM9 | Push notifikačná schéma (push\_notification\_app\_scheme) | Základné údaje o aplikačnej push notifikačnej schéme a používateľskej schéme používanej v používateľskom profile aplikácie konfigurovateľnej pomocou konfiguračnej servisy. |

Detailný popis dátových entít projektu „Slovensko v mobile“ bude vytvorený a popísané v Detailnom návrhu riešenia.

## 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:

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

Požiadavky na dátovú integráciu na CSRÚ

Poskytovanie údajov

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

1. Zoznam tém pre PUSH notifikácie.

Konzumácia údajov

Aplikácia SVM nebude v inkrementoch 1, 2, 3 a 4 konzumovať údaje z IS CSRÚ. Dáta o identite budú prevzaté z centrálneho IAM.

## Prístup k zabezpečeniu dátovej kvality

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

**Projektové aktivity:**

1. V rámci DNR budú definované vstupné objekty evidencie z iných informačných systémov, voči ktorým prebehne referencovanie (ak to bude potrebné).

**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.

Prístup k príprave a zabezpečení testovacích dát

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

1. Mobile ID – pre túto oblasť je potrebné zabezpečiť dostatočné množstvo testovacích eID kariet (minimálne 10), ako aj testovacích identít, čo bude riešené v spolupráci s NASES,
2. 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.

## Návrh dát pre publikovanie 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:

1. Počet registrovaných Mobile ID,
2. Počet autorizácií s Mobile ID,
3. Počet podaní s Mobile ID,
4. Počet distribuovaných PUSH notifikácií Číselník mobilných aplikácii,
5. Číselník platforiem,
6. Číselník push notifikačných tém.

## Prístup k migrácii

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

## Technologická vrstva

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

1. **Technologická interoperabilita** – softvér a hardvér vo verejnej správe musí byť v súlade s definovanými štandardami, ktoré podporujú interoperabilitu údajov, aplikácií a technológií.
2. **Otvorené štandardy** – prednostne sa budú používať otvorené štandardy a formáty a dôraz bude na zabezpečení technologickej neutrálnosti.
3. **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.
4. **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“.
5. **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.
6. **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.
7. **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.
8. **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:

1. Možnosť bezpečného uloženia privátnych kľúčov a pokročilé kryptovanie.
2. 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.
3. Podpora systémového aj aplikačného autorizačného follback-u, pre potreby ochrany privátnych parametrov uložených v secure priestoroch (touchId/faceId – passcode - lock).
4. Automatická podpora najnovších technológii mobilného zariadenia vo forme frameworkov, knižníc, príkladov a dokumentácie.
5. Umožňujú priamy prístup k hardvéru zariadenia, ktorý je pre web aplikácie nedostupný (Bluetooth, NFC, Kamera, ...).
6. 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.
7. 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).
8. Offline prístup – podpora offline funkcionality nezávislej od dostupnosti pripojenia na sieť a dátové služby.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.

## Technická 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:**

1. virtuálny server,
2. diskový priestor,
3. sieťové pripojenie,

**Predpokladá sa využitie najmä nasledujúcich služieb typu PaaS:**

1. služby aplikačnej vrstvy,
2. služby bezpečnosti,
3. služby monitoringu a manažmentu.

**Predpokladá sa využitie nasledujúcich služieb typu SaaS:**

1. aplikácia pre zálohu a archiváciu dát.

# Fyzická architektúra

Z dôvodu preferencie implementácie aplikácii ako mikroslužieb navrhujeme využitie otvorenej (open source) kontajnerizačnej platformy Kubernetes, ktorá automatizuje operácie s kontajnermi. Odstraňuje mnoho ručných procesov, ktoré sa týkajú nasadenia a zjednodušovania kontajnerových aplikácií. Z tohto dôvodu je Kubernetes ideálnou platformou pre hosťovanie aplikácií, ktoré vyžadujú rýchle škálovanie a časté upravovanie.

Jednotlivé moduly popísané v aplikačnej architektúre by boli v cieľovom riešení implementované a prevádzkované ako kontajnery, ktoré by vzájomne komunikovali prostredníctvom integračnej platformy. Zároveň aj integračnú platformu preferujeme prevádzkovať ako kontajnerové riešenie.

Nižšie uvedený obrázok schematicky popisuje použitie kontajnerizačnej platformy v prostredí NASES. Databázové systémy navrhujeme prevádzkovať mimo kontajnerizačnej platformy a to inštalované na samostatných nodoch (node). V prípade požadovanej vysokej dostupnosti je potrebné RDBMS SW inštalovať ako cluster.

Diagram

Description automatically generated

V prípade SVM bude riešenie nasadzované do vládneho cloudu. Riešenie bude pri návrhu architektúry vychádzať z poskytovaného katalógu služieb IaaS vládneho cloudu. Použije virtualizované serverové platformy x86 na báze Linuxu (https://www.sk.cloud).

Implementácia bude vyžadovať vytvorenie novej infraštruktúry projektu SVM vo vládnom cloude, ktoré bude zodpovedať výkonnostným nárokom budúcich SVM modulov, vrátane komponentov participujúcich na všetkých požadovaných integráciách. Vzhľadom na to, že architektúra informačného systému SVM je navrhnutá na princípoch mikroslužieb, tak ako najvhodnejšiu platformu súčasnej doby na prevádzkovanie mikroslužieb použijeme kontajnerizáciu na platforme Docker a ako orchestračný nástroj Kubernetes.

Všetky komponenty architektúry, sú navrhnuté s dôrazom na dostupnosť celého riešenia a teda redundantne. Toto riešenie poskytne efektívne využitie zdrojov, značnú mieru dostupnosti, menežovateľnosť a flexibilitu celkovej IT infraštruktúry.

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

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

1. DEV - vývojárske prostredie na strane Zhotoviteľa. Primárne určené pre prístup vývojárom softvéru, kde si vedia simulovať nasadenie aplikácie a chod v klastri.
2. INT - integračne prostredie na strane Zhotoviteľa. Toto prostredie je pre vývojárov softvéru s možnosťou napojenia na existujúce systémy, kde je možne overiť integračne funkcionality a scenáre.
3. QA – testovacie prostredie na strane Zhotoviteľa. 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 (NASES FIX prostredie).
4. UAT - testovacie prostredie Objednávateľa (FIX/UAT NASES) na zabezpečenie používateľského akceptačného testovania.
5. PROD - produkčné prostredie Objednávateľa (Správcu IS) prevádzkované určeným prevádzkovateľom.

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).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).

Popis vývojového prostredia (DEV)

Pre potreby implementácie mikroslužieb do vývojového prostredia je potrebné pripraviť infraštruktúru na zabezpečenie vývoja v Kubernetes clustri. Pre vývoj je potrebné zriadiť nástroj na správu verzií zdrojového kódu GitLab a zriadiť na ňom pre každú vývojársku skupinu extra prístup. Ďalej treba zabezpečiť nástroj na automatizovanú kompiláciu, spustenie automatizovaných testov a nasadenie do úložiska artefaktov GitLab-CI (Continuous Integration).

Prostredia DEV, Interný TEST a QA vytvorí Zhotoviteľ.

Table

Description automatically generated with medium confidence

Popis testovacieho prostredia (QA/UAT/PROD)

Riešenie bude nasadené a prevádzkované v QA, UAT a PROD prostredí rovnako ako na vývojovom prostredí s tým rozdielom, že v tomto prostredí budú niektoré uzly infraštruktúry posilnené o redundantné komponenty a namiesto úložiska v aplikačnom clustri bude zriadený v dátovej vrstve kubernetes cluster.

Vzhľadom na to, že sa aplikácie sú spúšťané v Kubernetes clustri, redundancia bude zabezpečená konfiguráciou deploymentu aplikácie v clustri (HAproxy load-balancing na nody aplikačného kubernetes clustra, HAproxy load-balancing na nody dátového clustra).

Table

Description automatically generated

## Predpokladané zaťaženie

Predpokladané zaťaženie bolo určení z dostupných dát a údajov, ktoré boli použité aj v CBA:

1. Počty používateľov 3,6 mil,
2. Počet autentifikačných prístupov 20 mil./rok (podľa aktuálneho počtu prístupov na slovensko.sk),
3. Počet podpisov podaní 3 mil./rok (približne 60% aktuálneho množstva podaní),
4. 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. Riešenie bude postavené ako autoškálovateľné a budúci prevádzkovateľ môže pridať potrebný výkon pridaním technických prostriedkov.

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 EventBus zbernice medzi mikroservismi, komponentami a externými systémami bude taktiež v zabezpečenej sieti GovNET.

Softvérové licencie

Pre vytvorenie modulov riešenia budú použité nasledujúce licencie. Zoznam môže byť v priebehu alebo po vykonaní Detailnej analýzy riešenia upravené. Pre perzistenciu biznis kritických dát je zvolený RDBMS Oracle, ktorý bude poskytnutý prevádzkovateľom.

| ID | Produkt – Software | Druh licencie |
| --- | --- | --- |
| 1 | PostreSQL | The PostgreSQL Licence (PostreSQL) |
| 2 | GitLab (CI/CD) | Open Source MIT Licence |
| 3 | Prometheus (monitoring) | Apache Licence 2.0 |
| 4 | Grafana (Logging, monitoring) | GNU Afero General Public Licence 3.0 |
| 5 | Drupal (Enrolment portál | GNU General Public Licence 3.0 |
| 6 | Loki (Logging) | Apache Licence 2.0 |
| 7 | Jaeger (Logging, tracing) | Apache Licence 2.0 |
| 8 | Layer7 (IdP, APIGW) | Komerčná licencia + Subscription (závislé na projekte “CAMP”). |
| 9 | Kafka (Confluent) | Apache Licence 2.0 |
| 10 | Kafka schema registry (Confluent) | Apache Licence 2.0 |
| 11 | Apache Hadoop | Apache Licence 2.0 |
| 12 | LDAP (technické účty) | Súčasť produktu Layer7 a jeho licencie |
| 13 | Oracle DB | Komerčná licencia + Subscription, súčasť služieb prostredí NASES |
| 14 | Kubernetes | Apache Licence 2.0, súčasť služieb prostredí NASES |
| 15 | Docker | Komerčná licencia + Subscription, súčasť služieb prostredí NASES |
| 16 | Firebase (Messaging, Analytics) | Komerčná licencia, Free spark plan |
| 17 | Helm (CD) | [BSD License](http://opensource.org/licenses/bsd-license.php) |
| 18 | Android studio (Development) | Android Software Development Kit License Agreement |
| 19 | xCode (Development) | Xcode and Apple SDKs Agreement |
| 20 | IntelliJ (Development) | Komerčná licencia + Subscription |
| 21 | Visual Studio Code (Development) | MICROSOFT SOFTWARE LICENSE TERMS |
| 22 | Slovensko v mobile (produkt) | Verejná open source softvérovú licencia Európskej únie (EUPL) |
| 23 | Nexus? LDAP (mID) | Komerčná licencia + Subscription |

# Bezpečnostná architektúra

Návrh na bezpečnostné opatrenia vychádza z platnej legislatívy a súčasného stavu. SVM vzniká ako nový ISVS a bude používaný ako spoločný komponent a rozširujúca funkcionalita v rámci modulov ÚPVS.

## Bezpečnosť prevádzky IS

Bezpečnostné požiadavky delíme na 3 časti:

* 1. Požiadavky na vývojové prostredie,
  2. Požiadavky na vyvíjaný produkt (vrátane konfigurácie a nastavení preexistentných diel),
  3. Požiadavky na produkčné prostredie, v ktorom je produkt prevádzkovaný.

Kapitola definuje primárne bezpečnostné opatrenia týkajúce sa prevádzky systému a konfigurácie prostredia, v ktorom sa systém bude prevádzkovať.

## Zabezpečenie komunikácie

Komunikácia bude prebiehať pomocou REST volaní, formát údajov JSON. Prenos dát bude prebiehať cez protokol HTTPS, certifikát bude vydaný dôveryhodnou certifikačnou autoritou. Služby vystavené navonok budú popísané podľa štandardu Open API Standard 3.0 (Swagger).

Dáta budú chránené pri uložení ale aj pri prenose symetrickým šifrovaním. Na prístup k službám je potrebná autentifikácia s použitím protokolu OAUTH 2.0.

Všetky komunikačné kanály budú známe a popísané. Jednotlivé komponenty systému budú oddelené podľa vrstiev plniacich špecifickú úlohu:

* 1. Prístupová vrstva,
  2. Aplikačná vrstva,
  3. Databázová vrstva.

Jednotlivé vrstvy budú umiestnené v separátnych, logicky oddelených sieťových segmentoch pričom komunikácia medzi nimi bude umožnená na základe pravidiel nastavených vo firewalle. Komunikácia bude kontinuálne monitorovaná a filtrovaná.

Za implementáciu monitoring eventov je v zmysle časti "K" prílohy č.2 vyhlášky 179/2020, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy Kategórie III, nesie zodpovednosť prevádzkovateľ ISVS a je povinný spomínané opatrenia nasadiť. Na serveroch bude host-based firewall nakonfigurovaný podľa princípu najmenšieho privilégia (least privilege).

Správcovské a monitorovacie rozhrania sieťových prvkov a serverov nesmú byť prístupné priamo z externej siete, internetu. Správcovské a monitorovacie rozhrania musia byť prístupné len z vopred špecifikovaných sietí (napr. administrátorská sieť) - viď časť "E" prílohy č.2 vyhlášky 179/2020.

Webový portál bude prístupný výlučne prostredníctvom protokolu HTTPS. S ohľadom na *best practices* sa k webovému portálu nebude pristupovať prostredníctvom HTTP.

Identita webového portálu bude zabezpečená platným, dôveryhodným certifikátom vydaným na doménu, na ktorej je dostupný. Identita webového portálu bude zabezpečená certifikátom s *Extended Validation*. Webový portál nesmie používať nedôveryhodné alebo vypršané SSL/TLS certifikáty.

Údaje, ktoré sú citlivé z hľadiska integrity alebo dôvernosti, sa musia prenášať iba prostredníctvom zašifrovaného spojenia SSL/TLS. Citlivé údaje a prihlasovacie údaje sa musia byť prenášané výhradne prostredníctvom zašifrovaného kanála. Webový portál nebude ukladať citlivé informácie v nezašifrovanej podobe na strane klienta, ani na strane servera. Webový portál nebude vkladať nešifrované zdroje bez SSL/TLS do stránok používajúcich SSL/ TLS.

Webový portál pre samoobslužnú registráciu bude:

1. podporovať TLS 1.2a TLS 1.3,
2. podporovať šifry, ktoré majú vlastnosť Perfect Forward Secrecy (PFS),
3. podporovať HTTP metódy OPTIONS, TRACK a TRACE,
4. dodržiavať negociačný postup negociácie TLS spojenia, popísaný v RFC 5746, kvôli zraniteľnosti Insecure renegociation a riziku útoku typu MitM,

Webový portál pre samoobslužnú registráciu **nebude** podporovať

1. SSLv2, SSLv3, TLS 1.0 a TLS 1.1,
2. šifry s kľúčom kratším ako 112 bitov a blokom kratším ako 64 bitov,
3. NULL ciphers a anonymný Diffie-Hellman algoritmus,
4. export (EXP) šifry,
5. RC4, DES a 3DES. Šifry s CBC módom by mali byť nahradené bezpečnejšími AEAD šiframi,
6. klientom iniciovanú SSL/TLS renegociáciu šifrovacích kľúčov (kvôli DoS útoku),

Použité šifry a protokoly SSL/TLS by mali byť odolné voči známym typom útokov, ako napríklad: FREAK, BEAST (používanie TLS 1.2, pri TLS 1.0 nepoužívanie šifry s AES), BREACH (Pri SSL/TLS musí byť vypnutá http kompresia), POODLE, LOGJAM, TLS Crime (TLS kompresia bude vypnutá).

Dĺžka kľúča asymetrickej šifry RSA, DSA v X.509 certifikáte musí byť aspoň 2048 bitov. Toto neplatí pre ECDSA, kedy na dosiahnutie vysokej bezpečnosti postačujú kratšie kľúče – napríklad 256 bitov. X.509 certifikáty musia byť hashované bezpečnými hashovacími funkciami (napr. kvôli možnosti kolíznych útokov nesmie byť použitý algoritmus MD5).

Pre všetky kryptografické operácie musia byť použité kryptograficky silné generátory pseudonáhodných čísel.

Webový server bude chránený WAF (web aplikačný firewall - viď časť "I" prílohy 2 vyhlášky 179/2020) minimálne s nasledujúcou funkcionalitou:

* 1. Detekcia a prevencia známych útokov (Code injection – SQL, XSS, Command, XPATH, ...),
  2. Kontrola používateľských vstupov prostredníctvom blacklistu a ich prekódovanie do HTML entít alebo podobných bezpečných náhrad.

Server bude pri SSL/TLS používať HSTS - HTTP Strict Transport Security. Nastavené by mali byť direktívy:

* 1. max-age=<číslo> – počet sekúnd, počas ktorých má prehliadač automaticky konvertovať všetky HTTP požiadavky do HTTPS
  2. includeSubDomains – indikuje, že všetky subdomény aplikácie musia používať HTTPS

V odpovediach webového servera sa nesmú nachádzať hlavičky prezrádzajúce použitú technológiu a / alebo jej verziu (Server, X-Powered-By, X-AspNet-Version a pod.).

Aplikácia musí korektne inštruovať prehliadač, aby neukladal citlivé informácie, prenášané prostredníctvom HTTPS, do cache (a aby neboli bez kontroly opäť prístupné z histórie prehliadania) minimálne v rozsahu: Cache-Control:no-cache,no- store,private,must-re-validate,max-age=0,no-transform; Expires:0; Pragma:no-cache

Webové správcovské rozhrania musia byť dostupné iba prostredníctvom SSL/TLS.

## Zabezpečenie integrity

Validácia vstupov bude vykonávaná na strane servera a bude vykonávaná aj na strane klienta. Všetky používateľské vstupy musia byť kontrolované na strane servera prostredníctvom whitelistov alebo regulárnych výrazov v kontexte, v ktorom sú použité.

Proces webového servera aj proces backendovej databázy musí byť konfigurovaný tak, aby bežal pod unikátnym používateľským kontom s limitovanou množinou privilégií (napr. v oddelenej schéme).

Webový server bude konfigurovaný tak, aby súbory s webovým obsahom boli procesom prislúchajúcim službe webového servera prístupné na čítanie, no nie na zápis. Procesy webového servera nebudú mať právo zápisu do priečinkov, kde je uchovávaný verejný obsah.

Operačný systém bude nakonfigurovaný tak, aby proces webového servera mohol vytvárať log záznamy, no nemohol ich čítať.

OS bude nakonfigurovaný tak, aby dočasné súbory vytvorené procesmi webového servera boli obmedzené na určený a vhodne zabezpečený priečinok. Ak je to možné, prístup k dočasným súborom by mal byť obmedzený na procesy, ktoré ich vytvorili.

Webový obsah a všetky logy ním vytvárané by mali byť umiestnené na separátnom pevnom disku alebo na inej logickej partícii, ako OS a webový server. Podľa tohoto pravidla bude požadovaná konfigurácia platformy v vládnom cloude.

Na systémoch bude nainštalovaný systém na kontrolu integrity konfiguračných súborov a narušenie integrity bude logované do centrálneho log manažmentu. Pre jednotlivé komponenty bude použitý zodpovedajúci mechanizmus popísaný v kapitole 4.4.

Integrita používateľských dát uložených v aplikácii musí byť zabezpečená pomocou vhodných kryptografických prostriedkov.

Integrita auditných záznamov a logov musí byť zabezpečená vhodnými kryptografickými prostriedkami a vynucovaná pomocou oddelenia právomocí. Bude použitý centrálny logovací a auditovací nástroj určený budúcim prevádzkovateľom (predpokladá sa ELK).

## Riadenie prístupu

Právo na vykonávanie privilegovaných operácií musí byť obmedzené na poverených administrátorov.

Privilegované prístupy (administrátorské prístupy) sa musia realizovať pomocou šifrovaných kanálov z vopred definovaných kontrolovaných pracovných staníc (viď časti "E" a "K" prílohy č.2 vyhlášky 179/2020 - jedná sa o súčinnosť prevádzkovateľa). Administrátori prostredia, v ktorom sa komponenty riešenia prevádzkujú, môžu vykonávať svoje aktivity len spôsobom, ktorý im neumožňuje vymazať stopy ich aktivít (viď časť "K" prílohy č.2 vyhlášky 179/2020). Na tento účel pristupujú na manažované systémy výhradne cez systém riadenia privilegovaného prístupu (PAM - privileged access management). Prístup môže byť realizovaný formou jump servera spravovaného nezávislým bezpečnostným oddelením, na ktorom sa nahrávajú všetky používateľské relácie (viď časť "E" prílohy č.2 vyhlášky 179/2020). Prístup na manažment rozhrania serverov riešenia je umožnený výhradne z PAM, nikdy nie z pracovných staníc používaných na bežnú prácu. Prístup na PAM by mal byť chránený dvojfaktorovou autentizáciou.

Lokálny administrátor web servera musí byť unikátny pre každý webový server.

Všetky servery a syslog servery musia byť synchronizované s dôveryhodným NTP serverom.

Pre každý virtuálny host na fyzickom web serveri musí existovať separátny log (viď časť "D" prílohy č.2 vyhlášky 179/2020).

V logoch musia byť uvedené:

1. timestamp - kedy udalosť nastala, vrátane určenia časovej zóny,
2. verejná IP adresa používateľa,
3. dopytovaná stránka/URL,
4. HTTP kód odpovede servera,
5. veľkosť odpovede servera v bytoch,
6. obsahy hlavičiek User-Agent a Referrer,
7. V prípade záznamov o udalostiach súvisiacich s autentifikáciou alebo s činnosťou autentifikovaného používateľa je nutné zaznamenať účet a akciu aká bola vykonaná.

Logy musia byť uchovávané na separátnom zariadení, resp. na separátnej logickej partícii (viď časť "D" prílohy č. 2 vyhlášky 179/2020). Na uchovávanie logov musí byť vyhradená dostatočná kapacita, vrátane monitoringu voľnej kapacity, ktorý v prípade dosiahnutia hraničnej hodnoty spoľahlivo notifikuje príslušné oddelenie správcov systému. Logy musia byť archivované po dobu stanovenú pravidlami budúceho prevádzkovateľa, minimálne však počas 6 mesiacov.

Logy musia byť prezerané v pravidelných intervaloch v závislosti od politiky budúceho prevádzkovateľa a požiadaviek Správu IS, minimálne však raz týždenne. V prípade služieb, ktoré spracúvajú citlivé údaje alebo ich správna činnosť ovplyvňuje kritické aktíva Správcu IS, by mali byť logy kontrolované denne (viď časť "K" prílohy č.2 vyhlášky 179/2020 - jedná sa o súčinnosť prevádzkovateľa ISVS).

Je nutné vytvárať log záznamy všetkých pokusov o autentifikáciu (log-in, log-out, neúspešný log-in, lockout konta, žiadosť o zmenu hesla). Toto platí rovnako pre aplikáciu ako aj pre všetky technologické komponenty, na ktorých aplikácia beží a systém pre riadenie privilegovaného prístupu (PAM) - viď časť "K" prílohy č.2 vyhlášky 179/2020.

Logy budú zaznamenávať minimálne:

* 1. (Úspešné aj neúspešné) Prihlásenie a odhlásenie,
  2. (Úspešné aj neúspešné) Vytvorenie, modifikáciu alebo zmazanie používateľa alebo skupiny (Úspešné aj neúspešné) Pokusy pristúpiť k citlivým údajom a osobným údajom,
  3. (Úspešné aj neúspešné) Pokusy o kritické operácie.

Logovacie súbory musia byť čitateľné len administrátorom. Nemôžu byť prepisovateľné a vymazateľné (možný je iba zápis na koniec súboru). Riešenie bude integrované na centrálny systém na zber a uchovávanie logov, do ktorého sa v reálnom čase prenášajú generované logy (viď časť "K" prílohy č.2 vyhlášky 179/2020).

## Definícia používateľských rolí

Používateľské role rozlišujeme v dvoch oblastiach:

* 1. Role definované v samotnej aplikácii,
  2. Role definované v prostredí, v ktorom sa aplikácia prevádzkuje.

V rámci aplikácie sú definované nasledovné role (podľa identifikovaných aktérov v tejto fáze uvedených Projektovom zámere najmä z pohľadu Správcu a Prevádzkovateľa).

V rámci prostredia, v ktorom je aplikácia prevádzkovaná, je možné definovať nasledovné role:

* 1. Správca operačného systému
  2. Správca databázy
  3. Administrátor bezpečnosti
  4. Administrátor siete

Pre potreby prevádzkového prostredia je nutné udržiavať aspoň nasledovnú dokumentáciu:

* 1. Matica prístupov jednotlivých rolí k systémom – ktorá rola má kam prístup s akými oprávneniami,
  2. Dokumentácia o pridelených roliach jednotlivým používateľom,
  3. Matica nezlučiteľných rolí aby sa zabránilo možnosti jednotlivca vykonať sériu operácií predstavujúcich zneužitie privilégií, umožňujúcich únik dát, znefunkčnenie systému alebo bezpečnostný incident.

Základné pravidlo pre definovanie používateľských rolí je pravidlo nezlučiteľnosti rolí a oddelenia právomocí. Žiadna osoba nesmie disponovať takou kombináciou právomocí, ktorá by jej umožnila vykonať na systémoch operácie vedúce k narušeniu dostupnosti, dôvernosti alebo integrity dát. Toto platí rovnako pre dáta uložené v aplikácii ako aj prevádzkové dáta technológie, na ktorej aplikácia beží.

## Manažment používateľov

V tejto kapitole je popísaná všeobecná metodika manažmentu používateľov.

Musia byť odstránené všetky testovacie a pôvodné účty z produkčných systémov. Každý používateľ a administrátor musia mať jedinečné ID.

Základné pravidlá pre manažment používateľov v prostredí, v ktorom sa riešenie prevádzkuje, sú nasledovné:

* 1. Privilégiá sa prideľujú podľa princípu need-to-know,
  2. Privilégiá sa prideľujú podľa princípu least privilege,
  3. Privilégiá sa prideľujú tak, aby sa neporušili pravidlá nezlučiteľnosti privilégií a oddelenia právomocí,
  4. Administrátori siete a operačných systémov nesmú byť zároveň administrátori bezpečnosti,
  5. Žiadatelia o prístup nesmú byť schopní schváliť si vlastné žiadosti,
  6. Žiadatelia o prístup si nesmú byť schopní sami vytvárať účty.

Vývojári a testeri nesmú mať za normálnych okolností prístup na produkčné systémy. Existujú však výnimočné prípady kedy takéto prístupy môžu byť poskytnuté - viď časť "J" písmeno g) prílohy č.2 vyhlášky 179/2020.

Tvorcovia reportov nesmú byť zároveň ich schvaľovateľmi.

Dokumentácia k prideleným roliam musí byť pravidelne kontrolovaná a pridelené role prehodnocované. Dokumentácia prístupu rolí k systémom musí byť pravidelne kontrolovaná a pridelené prístupy prehodnocované. O vykonaní kontroly musí byť vedený záznam.

Používateľské a administrátorské prístupy môžu byť pridelené len na základe schválených žiadostí. Prístupové údaje (meno a heslo) používané pre bežnú prácu sa nesmú používať pre vykonávanie privilegovaných operácií.

Prvotné heslá musia byť komunikované bezpečným spôsobom a musí byť vynútená ich zmena pri prvom prihlásení. Kvalita hesiel vyžadovaná aplikáciou ako aj podpornou infraštruktúrou musí byť v súlade s heslovou politikou organizácie.

Aplikácia musí pre všetky autorizačné mechanizmy implementovať politiku, pri ktorej je zakázané všetko, čo nie je explicitne povolené (default-deny). Aplikácia musí vyžadovať autentizáciu pre každú privilegovanú operáciu (napr. meno a heslo na prvotné prihlásenie, token). Aplikácia musí implementovať autentizáciu a autorizáciu na strane servera.

## Ochrana osobných údajov

V návrhu riešenia SVM sú zahrnuté v tejto kapitole popísané požiadavky.

## Bezpečná autentifikácia používateľa

Používateľ pristupuje k funkcionalite cez mobilnú, webovú aplikáciu alebo integrovaný ISVS (tretia strana). Pre prácu v musí byť používateľ autentifikovaný. Predpokladáme nasledujúce alternatívy autentifikácie (neplatí pre API, ktoré budú verejne prístupné a nebudú požadovať autentifikáciu):

1. **Autentifikácia cez mID** - Autentifikácia používateľa bude primárne riešená použitím riešenia mobilnej identity (mID). mID bude použité pri autentifikácii používateľa, ktorý bude pracovať s mobilnou aplikáciou „Slovensko v mobile“, prípadne s aplikáciou tretej strany, ktorá je s aplikáciou „Slovensko v mobile“ integrovaná priamo (deepLink / URL Schema). Pri autentifikácii cez mID je úroveň eIDAS „pokročilá“.
2. **Autentifikácia cez eID kartu** - v prípade, že bude používateľ pracovať s portálom, môže použiť na autentifikáciu eID kartu s kontaktnou čítačkou kariet, v prípade dostupnosti riešenia pre bezkontaktné eID 2.0 s NFC čipom, aj to. Autentifikácia cez eID kartu je EIDAS registrovaná schéma autentifikácie s vysokou úrovňou bezpečnosti. Rovnako to bude platiť aj pri pripravovanej eID2.0 karte.

## Ukladanie a ochrana osobných údajov

SVM nebude ukladať žiadne osobné údaje. Dáta budú prenášané v zašifrovanej forme a rozšifrovanie sa udeje až v aplikácii tretej strany (konzument).

## Komunikácia s tretími stranami

Na komunikáciu s tretími stranami sa využije API Gateway. API GW vytvorí bezpečnostnú vrstvu pre komunikáciu s riadne integrovanými tretími strany (ISVS, komerčné subjekty). Integrované tretie strany sa budú k publikovaným službám pripájať cez REST API publikovanými a dokumentovanými v súlade so štandardom OAS3.0.

Integrované tretie strany budú volať metódy príslušných API vystavené na zabezpečených end-pointoch zo siete internet, ku ktorým budú mať povolený prístup. Zabezpečenie komunikácie bude:

1. HTTPS spojenie je zabezpečené TLS minimálne vo verzii 1.2 a vyššej s použitím AEAD šifier
2. pomocou klientskeho certifikátu,
3. HTTP basic authentication (ako všeobecné označenie pre autentifikačný mechanizmus, ktorý je použitý aj pre HTTPS protokol, a ktorý bude použitý aj v komunikácii s tretími stranami kde systém primárne využíva klientsky certifikát na zabezpečenie autentifikácie) s prihlasovacími údajmi.

Komunikácia bude na báze REST a formáty budú, nie výlučne, XML a JSON.

## Zabezpečenie serverov

V závislosti na realizácii projektu CAMP, na ktorom je publikovanie a sprístupnenie služieb SVM tretím stranám závislé (CAMP: Modul API GW, Modul Manažment tretích strán).

Server API GW aj server tretej strany musí:

* 1. podporovať SSL/TLS spojenie s klientskym certifikátom. Na serveri musí byť možnosť pridať klientsky certifikát, ku ktorému je možné priradiť povolené prístupové údaje z HTTP basic authentication,
  2. podporovať možnosť odstrániť / revokovať klientsky certifikát a prihlasovacie údaje,
  3. zamietnuť všetky spojenia, ktoré nevyužívajú klientsky certifikát alebo klientsky certifikát nie je zaregistrovaný alebo nie je platný alebo prihlasovacie údaje v HTTP basic authentication nekorešpondujú s použitým certifikátom,
  4. bežať na vlastnom doménovom mene,
  5. mať platný SSL/TLS certifikát vydaný autorizovanou certifikačnou autoritou,
  6. mať zo siete internet otvorený iba port pre HTTPS (443). Všetky ostatné porty zo siete internet musia byť zatvorené firewallom,
  7. integrovať vhodnú formu ochrany voči DoS útokom.

## Integrácia tretej strany

V závislosti na realizácii projektu CAMP, na ktorom je publikovanie a sprístupnenie služieb SVM tretím stranám závislé (CAMP: Modul API GW, Modul Manažment tretích strán).

Pri integráciu IS VS tretej strany bude potrebné, aby si jednotlivé strany vymenili metadáta. Tretia strana poskytne API GW nasledujúce informácie:

1. Klientsky certifikát s verejným kľúčom (môže byť self-signed), pomocou ktorého sa bude pripájať na end-pointy API Gateway.

API Gateway poskytne tretej strane nasledujúce informácie:

* 1. Klientsky certifikát s verejným kľúčom (môže byť self-signed), pomocou ktorého sa bude pripájať na end-pointy tretej strany,
  2. Prihlasovacie údaje, ktoré bude používať API Gateway pre autentifikáciu pomocou http basic authentication pri volaní endpointov tretej strany (ak bude potrebné),
  3. Prihlasovacie údaje, ktoré bude používať tretia strana pre autentifikáciu pomocou http basic authentication pri volaní endpointov API Gateway.

Bezpečnostné požiadavky na prevádzku systému

* 1. Všetky certifikáty musia poskytovať dostatočnú mieru bezpečnosti,
  2. Certifikáty bude možné vymeniť po exspirácii,
  3. Celá sieťová aktivita na end-pointoch musí byť logovaná,
  4. Certifikáty musia byť bezpečne generované len na strane ktorá ich vydáva,
  5. Musia byť použité dostatočne bezpečné generátory pseudonáhodných čísel.

Detailný popis rozsahu integrácie bude popísaných v Dohode o integračnom zámere, ktorý uzatvorí Prevádzkovateľ IS a tretou stranou v súlade s pravidlami podľa Integračného manuálu pre služby, ktorý bude súčasťou dokumentácie ku CAMP a bude vytvorený vo fáze Implementácia a testovanie a bude validovaný vo fáze Nasadenie a post-implementačná podpora s jedným vybraným subjektom (jeden IS VS alebo jedna aplikácia ISVS).

Do spustenia príslušných modulov CAMP bude integrácia tretích strán realizovaná podľa pokynov Správcu IS dostupnými technickými prostriedkami, ktoré umožnia udržať požadovanú úroveň bezpečnosti.

## Pravidlá pre bezpečnú komunikáciu pre vývoj

Pri konfigurácii a vývoji súčasní riešenia budú aplikované tieto pravidlá (a musí ich primerane implementovať aj integrovaná tretia strana):

1. **Ukladanie dát a súkromie:**
   1. Pre integrované mobilné aplikácie sa na ukladanie citlivých údajov (prihlasovacie údaje, šifrovacie kľúče) sa použije “bezpečné úložisko“ daného systému na to určené (Keychain/Keystore), prípadne sa mobilná aplikácia pripája cez svoj backend,
   2. Citlivé údaje nebudú ukladané mimo aplikačný kontajner a bezpečného úložiska,
   3. Citlivé údaje sa nebudú zapisovať do logov, záloh aplikácie ani zdieľané s tretími stranami ak to nie je súčasťou funkcionality,
   4. UI neumožní zobraziť heslo alebo PIN,
   5. Citlivé údaje budú odstránené z náhľadu obrazovky, ak ide aplikácia do pozadia,
   6. Citlivé údaje nebudú uložené lokálne na zariadení, v prípade potreby sú získavané zo služby a uložené iba v pamäti,
   7. Citlivé údaje sú odstránené z pamäte bezprostredne po použití,
   8. Lokálne úložisko je vymazané po väčšom počte neúspešných pokusov prihlásenia do aplikácie,
2. **Šifrovanie**:
   1. Aplikácia nevyužíva ten istý šifrovací materiál na rôzne účely,
   2. Pri generovaní náhodných hodnôt sa použije dostatočne bezpečný generátor,
3. **Autentifikácia pre tretie strany**:
   1. Na prístup k vzdialenej službe je potrebná autentifikácia,
   2. Autentifikačná služba vydá podpísaný prístupový token (JWT) s krátkou životnosťou.
   3. Po odhlásení užívateľom je prístupový token odstránený z pamäte aplikácie,
   4. Po exspirácii platnosti tokenu sa relácia ukončí a dôjde k odhláseniu užívateľa,
   5. Spôsoby prihlásenia sú definované a vynútené na strane služby,
4. **Sieťová komunikácia:**
   1. Prenášané dáta sú šifrované s TLS, aplikácia overuje X.509 certifikáty a akceptuje iba vydané dôveryhodnou CA,
   2. Aplikácia používa najnovšie bezpečnostné knižnice,
5. **Interakcia**:
   1. Aplikácia neumožní spustiť JavaScript kód z neznámych zdrojov,
   2. Aplikácia používa safe-serialization API pri object deserializácií,
   3. Používa sa mechanizmus CORS,
6. **Kvalita a nastavenie buildov aplikácií a ich súčastí:**
   1. Všetky developerské pomocné kódy, nastavenia, back-door sú odstránené
   2. Aplikácia neloguje detailné chyby,
   3. Všetky použité knižnice tretích strán sú identifikované, overené a skontrolované že neobsahujú známe zraniteľnosti,
   4. Aplikácia správne narába s výnimkami a ich odchytávaním,
   5. Pri release zostavení sa použijú nástroje na obfuskáciu kódu, tak aby základná statická analýza kódu neodhalila dôležitý kód alebo dáta.
7. **Implementácia OWASP TOP 10 primerane aplikované pre webové rozhranie**:
   1. Broken Access Control,
   2. Cryptographic Failures,
   3. Injection,
   4. Insecure Design,
   5. Security Misconfiguration,
   6. Vulnerable and Outdated Components,
   7. Identification and Authentication Failures,
   8. Software and Data Integrity Failures,
   9. Security Logging and Monitoring Failures,
   10. Server-Side Request Forgery.

# ZÁVISLOSTI NA OSTATNÉ ISVS / PROJEKTY

Navrhované riešenie bude integrované s už existujúcimi ISVS. Aktuálne nie sú plánované integrácie na projekty, ktoré by aktuálne boli v realizácii.

Table 1 Prehľad existujúcich ISVS, ktoré bude potrebné integrovať.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Stakeholder** | **Kód ISVS**  *(z MetaIS)* | **Názov projektu** | **Termín ukončenia projektu** | **Popis závislosti** |
| MIRRI | isvs\_62 | Ústredný portál verejnej správy | N/A | Integrácia na centrálne komponenty ÚVPS, IAM (isvs\_8846) – poskytovanie služieb autentifikácie FO a vydávanie SAML tokenov. |
| MIRRI | isvs\_9342 | Otvorené dáta | N/A | Publikovanie dát o službách. |
| MIRRI | isvs\_63 | MetaIS | N/A | Publikovanie informácií o projekte, službách a hlásenie SLA parametrov služieb zo strany Prevádzkovateľa. |

Pri implementácia a integrácii je potrebné zohľadniť projekty uvedené v tabuľke nižšie:

Table 2 Prehľad projektov, ktoré sú v príprave alebo prebiehajú a je potrebné zosúladiť výstupy s projektom SVM.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Stakeholder** | **Kód ISVS**  *(z MetaIS)* | **Názov projektu** | **Termín ukončenia projektu** | **Popis závislosti** |
| MIRRI | isvs\_9514  projekt\_514 | Centrálna API manažment platforme (CAMP) | September 2023 | Publikovanie služieb dodaných projektom na centrálne API GW.  Manažment tretích strán pre prístup ku službám projektu a jeho modulov (integrácia OVM, pripojenie tretích strán). |
| MIRRI | isvs\_8705 | Manažment osobných údajov | September 2023 | Poskytnutie integrácie App2App pre mobilnú aplikáciu MOU v PoC verzii. |

# ZDROJOVÉ KÓDY

Predpokladá sa, že riešenie bude dodané ako unikátne SW dielo na základe zmluvy o dielo vyvinuté pre potreby MIRRI SR. Zdrojový kód, vytvorený počas zhotovovania, bude otvorený v súlade s licenčnými podmienkami verejnej softvérovej licencie Európskej únie podľa osobitného predpisu a to v rozsahu, v akom zverejnenie tohto kódu nemôže byť zneužité na činnosť smerujúcu k narušeniu alebo k zničeniu informačného systému. Zmluva s dodávateľom bude pripravená tak, aby po skončení zmluvného vzťahu, v rámci ktorého bolo unikátne SW dielo vytvorené a po istú dobu prevádzkované pôvodným dodávateľom, disponovalo MIRRI všetkými oprávneniami potrebnými pre ďalšiu prevádzku a rozvoj tohto diela bez závislosti na pôvodnom dodávateľovi, teda i prostredníctvom nového dodávateľa vybraného v neobmedzenej súťaži dodávateľov.

V prípade, že súčasťou dodávky bude aj tzv. špecializované konfigurovateľné riešenie[[1]](#footnote-1), resp. špecializovaný SW, pokiaľ pôjde o licenciu špecializovaného SW, obstaranie a užívanie špecializovaného SW sa bude riadiť štandardnými zmluvnými podmienkami dodávateľa. Pokiaľ ide o prispôsobenie a nadstavbu nad špecializovaným SW, ktoré bude zohľadňovať špecifické potreby a podmienky MIRRI SR, zdrojový kód, vytvorený počas zhotovovania, bude otvorený v súlade s licenčnými podmienkami verejnej softvérovej licencie Európskej únie podľa osobitného predpisu a to v rozsahu, v akom zverejnenie tohto kódu nemôže byť zneužité na činnosť smerujúcu k narušeniu alebo k zničeniu informačného systému. Požadovaná bude podrobná dokumentácia, aby bolo možná prevádzkovanie a rozvoj aj inými dodávateľmi.

# PREVÁDZKA A ÚDRŽBA

## Prevádzkové požiadavky

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 (MIRRI SR)

**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.

**L2 podpory IS** (Level 2, postúpenie požiadaviek od L1) - vybraná skupina garantov, so znalosťou IS na základe zmluvy o podpore IS (zabezpečuje verejný obstarávateľ v spolupráci s úspešným uchádzačom).

**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.

**L3 podpory IS** (Level 3, postúpenie požiadaviek od L2) - na základe zmluvy o podpore IS (zabezpečuje úspešný uchádzač).

**Podpora L3 (podpora 3. stupňa)** - Podpora 3. stupňa predstavuje najvyššiu úroveň podpory pre riešenie tých najzložitejších Hlásení, vrátane prevádzania hĺbkových analýz a riešenie extrémnych prípadov.

**Pre služby sú definované takéto SLA:**

Help Desk je dostupný cez SW nástroj pre nahlasovanie a riešenie incidentov a pre vybrané skupiny užívateľov (používatelia verejného portálu) cez telefón a email,

Dostupnosť L3 podpory pre IS je 8x5 (8 hodín x 5 dní od 8:00h do 16:00h počas pracovných dní).

Podporu úrovne L1 a L2 bude vykonávať budúci prevádzkovateľ riešenia (NASES) existujúcimi prostriedkami cez Kontaktné centrum a pracovníkov podpory.

Podpora úrovne L3 sa bude riadiť pravidlami SLA, ktorú Správca IS uzatvorí s Zhotoviteľom najneskôr pred ukončením termínu post implementačnej podpory pre Inkrement 1. Minimálne požiadavka na SLA sú uvedené nižšie v tejto kapitole.

## Riešenie incidentov – SLA parametre

Za incident je považovaná chyba IS, t.j. správanie sa v rozpore s prevádzkovou a používateľskou dokumentáciou 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 incidentu** | **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. |

**Možný dopad:**

|  |  |  |
| --- | --- | --- |
| **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 ITIL V3 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:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Označenie priority incidentu** | **Reakčná doba(1) od nahlásenia incidentu po začiatok riešenia incidentu** | **Doba konečného vyriešenia incidentu od nahlásenia incidentu (DKVI) (2)** | **Spoľahlivosť (3)**  (počet incidentov za mesiac) |
| **1** | 4 hod. | 1 pracovný deň | 1 |
| **2** | 8 hod. | 3 pracovné dni | 2 |
| **3** | 16 hod. | 10 pracovných dní | 10 |
| **4** | 24 hod. | Vyriešené a nasadené v rámci plánovaných releasov | |

**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.

**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.

**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.

Incidenty nahlásené verejným obstarávateľom úspešnému uchádzačovi v rámci testovacieho prostredia

Majú prioritu 3 a nižšiu

Vzťahujú sa výhradne k dostupnosti testovacieho prostredia

Za incident na testovacom prostredí sa nepovažuje incident vztiahnutý k práve testovanej funkcionalite.

Vyššie uvedené SLA parametre nebudú použité pre nasledovné služby:

Služby systémovej podpory na požiadanie,

Služby realizácie aplikačných zmien vyplývajúcich z legislatívnych a metodických zmien.

Pre tieto služby budú dohodnuté osobitné parametre dodávky.

## Požadovaná dostupnosť IS

| **Popis** | **Parameter** | **Poznámka** |
| --- | --- | --- |
| **Prevádzkové hodiny** | 12 hodín | od 6:00 hod. - do 18:00 hod. počas pracovných dní |
| **Servisné okno** | 24 hodín | od 00:00 hod. - 23:59 hod. počas dní pracovného pokoja a štátnych sviatkov  Servis a údržba sa bude realizovať mimo pracovného času. |
| **Dostupnosť produkčného prostredia IS** | 99,9% | 1. 99,9% z 24/7/365 t.j. max ročný výpadok je 61 hod. 2. Maximálny mesačný výpadok je 5,1 hodiny. 3. Vždy sa za takúto dobu považuje čas od 0.00 hod. do 23.59 hod. počas pracovných dní v týždni. 4. Nedostupnosť IS sa štandardne 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. 5. V prípade nedodržania dostupnosti IS bude každý ďalší začatý pracovný deň nedostupnosti braný ako deň omeškania bez odstránenia vady alebo incidentu. |

### Dostupnosť (Availability)

Dostupnosť (Availability) znamená, že dáta alebo iné zariadenie sú prístupné v okamihu ich 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 je zvyčajne vyjadrená ako percento času v danom období, obvykle za rok. Pre riešenie sa vyžaduje dostupnosť 99,9%.

### RTO (Recovery Time Objective)

**RTO** (Recovery Time Objective) je jeden z ukazovateľov dostupnosti dát. RTO vyjadruje množstvo času potrebné pre obnovenie dát a celého prevádzky nedostupného systému (softvér). V rámci projektu sa očakáva tradičné zálohovanie a nie je k dispozícii druhá lokalita. Nakoľko však bude systém v cloude, ktorý je možný zálohovať ako celok, obnova z katastrofického výpadku by mala byť realizovaná do 48 hodín.

**Finálne RTO nastaví Správca IS s budúcim prevádzkovateľom.**

### RPO (Recovery Point Objective)

**RPO** (Recovery Point Objective) je jeden z ukazovateľov dostupnosti dát. RPO vyjadruje, do akého stavu (bodu) v minulosti možno obnoviť dáta. V rámci projektu je potrebné nastaviť zálohovanie tak, aby maximálna strata údajov bola 2 hodiny.

**Finálne RPO nastaví Správca IS s budúcim prevádzkovateľom.**

# Riadenie zmien

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.

# 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:

1. **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,
2. **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,
3. **Architektúra dátová vrátane systémovej architektúry** (popisuje údajové entity a ich vzťahy, tok údajov, príslušnosť údajov, dekompozícia architektonických modulov, návrh ich väzieb,...),
4. **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.
5. **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,
6. **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.

## Kontajnerizácia a orchestrácia

Kontajnerizácia mikroslužieb je virtualizačná metóda na úrovni OS, ktorá sa používa na nasadenie a spúšťanie distribuovaných mikroslužieb bez potreby spúšťania celého virtuálneho počítača pre každú mikroslužbu. Na jednom hostiteľovi tak môžeme bežať viac izolovaných mikroslužieb a pristupovať k rovnakému jadru OS.

Jednou z najväčších výhod kontajnerizácie oproti virtualizácii je, že kontajnerovaná aplikácia (uložená v docker image) je oveľa prenosnejšia, pretože odstraňuje požiadavky na predinštalovaný softvér, služby alebo operačné systémy v cieľovom počítači. Okrem toho môžu byť aplikácie na kontajneri prevádzkované na holých kovových hostiteľoch a vzdialených alebo cloudových serveroch s neznámymi prostrediami.

Ďalšou výhodou pre kontajnerizáciu je to, ako blízkosť služieb operačného systému k mikroslužbám, ktoré ich potrebujú v rámci kontajnera, často znamená, že môže koncovým používateľom dodávať rýchlejšie časy odozvy ako typický virtuálny server. V sieti nám spôsobí menej záťaží potrebných na doručenie kontajnerovej aplikácie, ako na prevádzkovanie, manažovanie alebo nasadzovanie cez VPN prístup k virtuálnym serverom.

Kubernetes sa stáva najviac používanou platformou na orchestráciu kontajnerov, rieši automatizáciu nasadzovania a škálovania kontajnerizovaného pracovného zaťaženia. Umožňuje nám spravovať zhluk izolovaných kontajnerov ako celok a poskytuje mechanizmy pre nasadenie, údržbu a škálovanie aplikácií, ktoré bežia v kontajneroch. Podporuje väčšie rozmedzie využití a najmä vďaka jeho rozšíriteľnosti nám prináša na projekte väčšiu komplexnosť. Na testovacom a produkčnom prostredí predpokladáme prevádzkovať 1 Kubernetes cluster.

## CI/CD proces

V riešení predpokladáme automatizované nasadzovanie nových verzií po schválení a UAT testoch. Na automatizáciu bude použitý Docker registri v kombinácií s Helm charts. Z uvedeného dôvodu je aj v technickej architektúre uvedený dedikovaný server pre Docker registri, na ktorý budú umiestňované nové verzie kontajnerov.

Na strane dodávateľa bude vykonané testovanie nových verzií. Na strane MIRRI/NASES prebehnú len UAT testy a nasadenie na produkčné prostredie. UAT testy vykonáva a potvrdzuje MIRRI, NASES zabezpečuje nasadenie odsúhlasenej verzie aplikácie na produkčného prostredie.

V prípade mobilnej aplikácie, správu na aplikačných obchodoch realizuje v rámci SLA podpory L3 Zhotoviteľ v dohodnutom rozsahu a publikovaniu verzie na príslušný aplikačný obchod Apple alebo Google predchádza riadne UAT testovanie a prevzatie verzie. Publikovanie aplikácie – release – je potom manuálne a vykoná ho oprávnená osoba na príslušnom aplikačnom obchode po revízii, ktoré vykonáva Apple alebo Google v súlade so všeobecným podmienkami aplikačných obchodov.

## Využitie vládneho cloudu

V prípade využitia vládneho cloudu nasadenie Kubernetes clustera pomocou RKE binary je v prevažnej miere o konfigurácii pomocou cluster.yml súboru, ktorým zadefinujeme parametre Kubernetes clustera (nodes, IP addresses, ports, roles, docker socket, network plugin atď. ) na danom prostredí.

Z toho dôvodu je potrebné pred vytváraním Kubernetes clustera navrhnúť iniciálny počet nodov, na ktorých bude Kubernetes cluster prevádzkovaný, následne požiadame o zriadenie rovnakého počtu virtuálnych serverov s požadovanými výkonnostnými parametrami (veľkosť HDD, RAM a počet CPU), ale s prihliadnutím na postupné čerpanie zdrojov z vládneho cloudu, t.j. až s narastajúcou záťažou budeme žiadať o ďalšie zdroje a aplikovať horizontálne škálovanie. Zadaním, schválením a nasadením požiadaviek pomocou nástroja vládneho cloudu CSP (Cloud Service Provisioner) budú na jednotlivých prostrediach vytvorené nové virtuálne serveri. Na týchto serveroch bude potrebné vykonať inštalačné požiadavky nutné pre spustenie Kubernetes clustera podľa dokumentácie RKE.

# Záloha a obnova riešenia

Zálohovanie na Projekte v mID a ePUSH je realizované využitím cloud-native mechanizmov pre zálohovanie dát s využitím prostriedkov poskytnutých IaaS služieb.

Konfigurácia aplikácií bude uložená do systému pre správu zdrojových kódov (GitLab), v súlade s best practices GitOps. Toto riešenie umožňuje v spolupráci s Continuous Delivery (GitLab) použiť rollback predchádzajúcej verzie, testovacie nasadenie vo forme A/B testu, deployment alebo canary deployment podľa finálne dohody s NASES.

Databázy majú vlastný cluster a mikroslužby k nim pristupujú každá do vlastnej schémy. DB engine je podľa usmernenia NASES použitý ORACLE.

Zálohovanie a správa DB clustra bude spravovaná operátorom na správu zálohy pre Oracle, ktorý umožní:

1. Update a zmenu clustra,
2. Zmenu veľkosti úložiska bez zastavenia clustra.

Zálohovanie Kafka clustra bude zabezpečená cez HDFS 2 sink konektora pomocou Apache Hadoop nástroja. Správa clustra Kafky bude spravovaná operátorom pomocou Confluent Control Centrum, ktorý okrem iného umožní aj:

• Update a zmenu Kafka clustra.

Zálohovanie bude riešiť prevádzkovateľ podľa príručiek (vytvorenie dokumentácie R3-4, príloha č. 1, Vyhláška 85/2020).

# POŽIADAVKY NA PERSONÁL

Projekt bude realizovaný agilnými metódami s prihliadnutím na strategické priority podľa NKIVS a tiež v zmysle podnikateľského plánu a stratégie Zhotoviteľa Slovensko IT, a.s. (SKIT).

SKIT v roli Zhotoviteľa bude agilnými metódami realizovať aktivity zamerané na vývoj a implementáciu front-end a back-end aplikácií, webových a natívnych mobilných aplikácií a web stránok. SKIT v rámci projektu bude zodpovedný za:

1. Riadenie projekt na strane Zhotoviteľa, ktorý predstavuje rozdelenie úloh na kratšie segmenty práce s častým posudzovaním a prispôsobovaním plánov s aktívnou iteráciou koncového zákazníka,
2. Analýzu a návrh riešenia – IT analytikom a IT architektom,
3. Vypracovanie detailného návrhu riešenia a technickej špecifikácie riešenia pre každý modul spolu s Objednávateľom, ktorý je koncovým biznis vlastníkom riešenia, čím sa zabezpečí vývoj finálneho riešenia použiteľného v praxi bez nutnosti ďalších veľkých zmien či úprav,
4. Zabezpečenie jednotnej architektúry riešenia v súlade s inými projektami realizovanými SKIT alebo MIRRI alebo NASES s cieľom zachovať súlad s koncepciou architektúry štátnych IT riešení,
5. Vývoj a implementáciu objednaných súčasti alebo modulov riešenia (vrátane UX dizajnu a vývoja) na základe požiadaviek a detailných prípadov použitia v rozsahu podľa objednávky alebo Zmluvy o dielo (položky v katalógu požiadaviek alebo v OPZ popísané prípady použitia)
6. 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,
7. Nasadenie riešenia resp. jeho funkčných modulov do DEV, TEST a QA prostredia,
8. Poskytnutie súčinnosti pri nasadení riešenia do UAT a produkčného prostredia,
9. Poskytnutie súčinnosť pre vytvorenie Bezpečnostného projektu a vykonanie penetračných testov nezávislou inštitúciou zvolenou Objednávateľom (MIRRI ako Správca IS),
10. Komunikáciu s partnermi a ich dodávateľmi ISVS alebo častí ISVS, ktoré sa priamo integrujú na služby SVM poskytované cez API alebo tvoria súčasť riešenia (SDK poskytnuté treťou stranou).

Požiadavky na riešiteľské role sú podrobne uvedené v Projektovom zámere.

# IMPLEMENTÁCIA A PREBERANIE VÝSTUPOV PROJEKTU

Harmonogram projektu je uvedený v Projektovom zámere.

Projekt bude realizovaný metódou agile, ktorý sa uplatňuje v projektoch, u ktorých je jasný rámcový cieľ, ale z najrôznejších dôvodov je nemožné presne definovať všetky dlhodobé požiadavky bez priebežných prototypov. Pri agilných metódach práce sa realizujú malé porcie výsledkov v každom vývojovom cykle, iterácii, v tesnej spolupráci so zákazníkom.

Zhotoviteľ aplikuje metodológiu SAFe (https://www.scaledagileframework.com).

# PRÍLOHY

Príloha 1: Katalóg požiadaviek (Excel) je zhodná s prílohou č. 1 k Projektovému zámeru.

1. Koncepcia nákupu IT vo verejnej správe, https://sp.vicepremier.gov.sk/verejne-obstaravanie-IKT/Verejn/2019\_05\_16\_Koncepcia\_nakupu\_IT\_s%20prilohami\_schvalene\_znenie.pdf [↑](#footnote-ref-1)