Detailný návrh riešenia

- Časť 1: Detailný návrh riešenia pre **Funkčné** a**Nefunkčné požiadavky**.
- Časť 2: Detailný návrh riešenia pre **Technické požiadavky**.
- Časť 3: Detailný návrh postupov a produktov pre fázy Testovanie a Nasadenie do produkcie.

Názov projektu

Verzia dokumentu:	
Projektový manažér - objednávateľa:	
Projektový manažér - dodávateľa:	
Predseda Riadiaceho výboru projektu:	

Obsah

1 ÚVOD 4
1.1 IDENTIFIKÁCIA A URČENIE 4
1.1.1 Zmenový list 4
1.1.2 Referencia na dokumenty 4
1.1.3 Skratky 4
1.1.4 Slovník pojmov 5
1.1.5 Zoznam obrázkov 5
1.1.6 Zoznam tabuliek 5
2 MANAŽÉRSKE ZRHNUTIE 5
2.1 Mimo rozsah projektu 5
2.1.1.1.1.1.1.1.1 Časť 1: Funkčná špecifikácia a detailný návrh riešenia 5
3 ZÁMER RIEŠENIA 6
3.1 CIELE A PRÍNOSY NAVRHOVANÉHO RIEŠENIA 6
3.2 POPIS NAVRHOVANÉHO RIEŠENIA 6
3.3 MERATEĽNÉ A VÝKONNOSTNÉ UKAZOVATELE (KPI) 6
3.4 AKCEPTAČNÉ KRITÉRIÁ 6
3.5 KATALÓG POŽIADAVIEK 6
4 POPIS POSTUPU ANALÝZY 6
4.1 POSTUP PRI VÝVOJI ARCHITEKTÚRY 6
4.2 DESIGN APLIKÁCIE PREPOJENÝ NA ARCHITEKTÚRU 7
5 PROCESY PODPOROVANÉ NAVRHOVANÝM RIEŠENÍM 7
6 BIZNIS ARCHITEKTÚRA RIEŠENIA 7
7 POPIS DÁTOVÝCH ENTÍT 7
8 NÁVRH RIEŠENIA DIZAJNU KONCOVÝCH SLUŽIEB 7
8.1 Modul 7
9 PRÍPADY POUŽITIA 8
9.1 NÁVRH VIZUÁLOV OBRAZOVIEK, PODPORENÝCH E2E PROCESOM 8
9.2 POUŽÍVATEĽSKÉ ROLY – AKTÉRI 8
9.3 VŠEOBECNÉ PRÍPADY POUŽITIA 8
9.4 SEKVENČNÉ DIAGRAMY 8
9.4.1.1.1.1.1.1.1 Časť 2: Technická špecifikácia a detailný návrh riešenia 8
10 APLIKAČNÁ ARCHITEKTÚRA 8
11 FYZICKÁ ARCHITEKTÚRA 8
11.1 CI/CD PROCES 9
11.2 KONTAJNERIZÁCIA A ORCHESTRÁCIA 9
11.3 POPIS TESTOVACIEHO PROSTREDIA 9
11.4 POPIS PRODUKČNÉHO PROSTREDIA 9
12 SOFTVÉROVÉ LICENCIE 9
13 ZÁLOHOVANIE A OBNOVA RIEŠENIA 9
13.1 POPIS RIEŠENIA PRE ZÁLOHOVANIE 9
13.2 POPIS RIEŠENIA PRE OBNOVU 10
14 ZABEZPEČENIE DOSTUPNOSTI 10
14.1 POPIS RIEŠENIA NA DOSTUPNOSŤ SYSTÉMU IS 10

15 BEZPEČNOSŤ, AUTORITY MANAŽMENT 10
15.1.1 Zásady bezpečného vývoja 10
15.2 DEFINOVANIE POUŽÍVATEĽSKÝCH ROLÍ 12
15.3 ZABEZPEČENIE KOMUNIKÁCIE A INTEGRITY 12
15.3.1 Zabezpečenie integrity 12
15.3.2 Zabezpečenie komunikácie 12
15.4 RIADENIE PRÍSTUPU (AUDIT TRAILS – SLEDOVANIE LOGOVANIA DO SYSTÉMU) 13
15.4.1 Riadenie prístupu 13
15.4.2 Logovanie systému a zber auditných záznamov 13
15.5 METODIKA MANAŽMENTU POUŽÍVATEĽOV 13
16 KONVERZIE DÁT, MIGRÁCIA DÁT, DÁTOVÝ MODEL A NÁVRH RIEŠENIA 13
16.1 POSTUP VYKONANIA MIGRÁCIE DÁT 13
16.2 OVERENIE MIGRÁCIE DÁT 13
16.2.1.1.1.1.1.1.1 Časť 3: Detailný návrh postupov a produktov pre fázy Testovanie a Nasadenie do produkcie 14
17 FÁZY PROJEKTU A ČASOVÝ HARMONOGRAM – KONSOLIDOVANÝ PREHĽAD . 14
17.1 Fáza - Analýzy a Dizajnu 14
17.2 Fáza - Implementácie a Testovania 14
17.3 Fáza - Nasadenia a Post-Implementačnej podpory – príprava a nasadenie do prevádzky 14
17.4 Ukončenie projektu 14
18 ZÁVISLOSTI A NÁVRH RIEŠENIA 14
18.1 ZÁVISLOSTI (PROJEKTOVÉ/MEDZIPROJEKTOVÉ) 14
18.2 ĎALŠIE (DOPLŇTE PODĽA POTREBY) 14
19 DOKUMENTÁCIA 15
20 OTVORENÉ OTÁZKY 15
21 PRÍLOHY 15
21.1.1.1.1.1.1.1.1 Príloha 1 - Katalóg požiadaviek 15

1 ÚVOD

1.1 IDENTIFIKÁCIA A URČENIE

1.1.1 Zmenový list

Verzia	Dátum	Autor	Dôvod zmeny	Kapitola, bod
1.0	24.6.2025	BrainIT	Iniciálna verzia dokumentu	

1.1.2 Referencia na dokumenty

Identikácia	Názov dokumentu
Príloha 1	Katalóg požiadaviek
Príloha 2	Zoznam obrázkov

Tento dokument je vypracovaný v zmysle QA riadenia kvality podľa pravidiel uvedených vo Vyhláške 85/2020 Z.z. a podľa odporúčanej šablóny MIRRI SR. Zmluvná štruktúra/šablóna DNR bola navrhnutá zákazníkom podľa vyhlášky 85/2020 Z.z. a podľa potrieb zákazníka.

1.1.3 Skratky

Skratka	Vysvetlenie
IS	Informačný systém
DNR	Detailný návrh riešenia
API	Application programming interface, rozhranie aplikačnej platformy

1.1.4 Slovník pojmov

Pojem	Vysvetlenie
Aplikačné rozhranie	Programovacie rozhranie informačného systému, ktorým je umožnené pre autorizovaného používateľa používať elektronickú službu
Rola	Štandardná aplikačná rola, ktorá bude evidovaná v systéme
Číselník	Množina údajov vo forme jednotlivých položiek číselníka, ktoré sú opísané najmenej dvojicou dátových prvkov "kód položky" a "názov položky"

1.1.5 Zoznam obrázkov

Zoznam obrázkov je uvedený v Prílohe 2 tohoto dokumentu.

1.1.6 Zoznam tabuliek

2 MANAŽÉRSKE ZRHNUTIE

Doplniť popis kapitoly Manažérske zhrnutie.

2.1 Mimo rozsah projektu

Mimo rozsah projektu sú identifikované aktivity ako:

- Implementačné pokrytie požiadaviek, schválených ako zmenové požiadavky.
- Implementačné pokrytie požiadaviek, ktoré sú rozhodnutím Riadiaceho výboru projektu označené ako ZRUŠENÉ.
- Implementačné pokrytie akýchkoľvek požiadaviek mimo schválený zoznam požiadaviek (definované príslušnými dokumentami DNR (detailného návrhu riešenia) z etapy Analýza a dizajn.
- Tvorba interných smerníc Objednávateľa.
- Školenia nad rámec definovaný v tomto dokumente.
- Legislatívna a organizačná príprava spustenia systému do prevádzky.
- SLA a prevádzka riešenia.

2.1.1.1.1.1.1.1 Časť 1: Funkčná špecifikácia a detailný návrh riešenia

Cieľom tejto časti dokumentu je popísať systém z pohľadu architektúry na úrovni biznis, aplikácií a technológií. Jednotlivé časti ukazujú kľúčové entity a ich vzťahy, resp. závislosti.
Pri opise architektúry boli použité ArchiMate 3.1 diagramy vytvorené podľa zásad uvedených v dokumente "Architektonické rámce verejnej správy, Enterprise architektúra VS SR 2014-2020".
Dôležité linky:
Hlavná stránka pre ArchiMate: https://pubs.opengroup.org/architecture/archimate3-doc/.

3 ZÁMER RIEŠENIA

Doplniť popis ku kapitole Zámer riešenia.

3.1 CIELE A PRÍNOSY NAVRHOVANÉHO RIEŠENIA

Doplniť popis ku kapitole Ciele a prínosy navrhovaného riešenia.

3.2 POPIS NAVRHOVANÉHO RIEŠENIA

Doplniť popis ku kapitole Popis navrhovaného riešenia.

3.3 MERATEĽNÉ A VÝKONNOSTNÉ UKAZOVATELE (KPI)

Merateľné avýkonnostné ukazovatele (KPI) sú súčasťou tabuľky vkapitole 3.1 Ciele a prínosy navrhovaného riešenia tohto dokumentu.

3.4 AKCEPTAČNÉ KRITÉRIÁ

Doplniť popis ku kapitole Akceptačné kritériá.

3.5 KATALÓG POŽIADAVIEK

Táto kapitola je súčasťou dokumentu DNR ako Príloha 1 dokumentu DNR.

4 POPIS POSTUPU ANALÝZY

Pri vývoji architektúry je v rámci tohoto projektu použitý rámec TOGAF a jazyk Archimate. Využívanie komponentov rámca TOGAF bolo pre účely tohoto projektu prispôsobené. Z rámca bola predovšetkým prevzatá časť metódy pre vývoj architektúry (Architecture Development Method) týkajúca sa vývoja architektúry vo všetkých štyroch architektonických doménach. Metóda pre vývoj architektúry predstavuje proces s doporučenými krokmi a aktivitami, ktoré boli nastavené s prihliadnutím na ciele a charakter tohoto projektu.

4.1 POSTUP PRI VÝVOJI ARCHITEKTÚRY

Projekt je vyvíjaný dvomi vývojovými tímami riadenými metodikou Scrum s dvojtýždňovým cyklom dodávania naplánovaných prírastkov. Od samotného začiatku sú nastavené pravidelné každotýždenné spoločné stretnutia architektov a ďalších expertov z obidvoch tímov. Každý týždeň sú aj stretnutia produktových vlastníkov (product ownerov), na ktorých dochádza k základným výmenám informácií a synchronizácii prác na projekte.

Pre vývoj architektúry majú zásadný význam spomínané stretnutia architektov a jednotlivých IT expertov. Každému stretnutiu predchádza príprava a sumarizácia aktuálnych otázok, ich rýchle posúdenie a prioritizácia s cieľom zaradenia na aktuálne stretnutie témy s najvyššou prioritou apotenciálnym dopadom.

4.2 DESIGN APLIKÁCIE PREPOJENÝ NA ARCHITEKTÚRU

Pre dizajn vyvíjaných aplikačných komponentov je použitý nástroj Enterprise Architect. Dizajn aplikačného rozhranie je vytvorený použitím nástroja Figma.

5 PROCESY PODPOROVANÉ NAVRHOVANÝM RIEŠENÍM

Doplniť popis ku kapitole Procesy podporované navrhovaným riešením.

6 BIZNIS ARCHITEKTÚRA RIEŠENIA

Kapitola popisuje biznis architektúru riešenia.

7 POPIS DÁTOVÝCH ENTÍT

Kapitola popisuje návrh nových entít tak, aby bola pokrytá požadovaná funkčnosť.

Každá entita obsahuje:

- Definíciu entity
- Zoznam základných atribútov
- Názov atribútu
- Dátový typ
- Popis – buď vysvetlenie čo atribút vyjadruje, ak to z názvu nie je zrejmé, prípadne popis validácie.

8 NÁVRH RIEŠENIA DIZAJNU KONCOVÝCH SLUŽIEB

8.1 Modul

9 PRÍPADY POUŽITIA

Jedným z cieľov návrhu riešenia je vyzbieranie požiadaviek zákazníka pre Klientsku zónu. Na zachytenie funkčných požiadaviek sa používajú prípady použitia, ktoré opisujú vzťahy medzi systémom a používateľom systému.

Používateľ systému, nazývaný aj aktér, vyvoláva interakciu so systémom s cieľom dosiahnuť určitý účel. Každý prípad použitia predstavuje sériu činností a udalostí z pohľadu aktéra, ktorý má definované oprávnenia na realizáciu danej činnosti.

9.1 NÁVRH VIZUÁLOV OBRAZOVIEK, PODPORENÝCH E2E PROCESOM

Kapitola popisuje štruktúrovaný návrh obsahu obrazoviek na základe identifikovaného procesu a údajov, obsiahnuté v tomto procese.

Kapitola je popísaná v kapitole Návrh riešenia dizajnu koncových služieb.

9.2 POUŽÍVATEĽSKÉ ROLY – AKTÉRI

Kapitola prezentuje časť návrhu používateľských rolí a oprávnení, ktoré sú následne priradené prípadom použitia v nasledujúcej kapitole. V nasledujúcich odsekoch je uvedený stručný popis konvencií používaných pre znázornenie modelu prepojenia používateľských rolí.

9.3 VŠEOBECNÉ PRÍPADY POUŽITIA

V ďalšom texte sú uvedené jednotlivé používateľské scenáre pre...

9.4 SEKVENČNÉ DIAGRAMY

V kapitole sa popisujú sekvenčné diagramy.

9.4.1.1.1.1.1.1 Časť 2: Technická špecifikácia a detailný návrh riešenia

10 APLIKAČNÁ ARCHITEKTÚRA

Kapitola popisujúca Aplikačnú architektúru.

11 FYZICKÁ ARCHITEKTÚRA

Kapitola popisuje fyzickú architektúra a definuje požiadavky pre testovacie a produkčné prostredie.

Navrhovaná prevádzka je plánovaná na dvoch identických prostrediach líšiacimi sa len množstvom a typom zdrojov:

- **PROD** prostredie – prevádzkové prostredie s reálnymi dátami a prevádzkou verejného portálu.
- **TEST** prostredie – testovacie, školiace, pred produkčné prostredie. Celé TEST prostredie je dostupné prostredníctvom VPN pre privilegovaných používateľov.

11.1 CI/CD PROCES

Doplniť popis ku kapitole CI/CD proces.

11.2 KONTAJNERIZÁCIA A ORCHESTRÁCIA

Doplniť popis ku kapitole Kontajnerizácia a orchestrácia.

11.3 POPIS TESTOVACIEHO PROSTREDIA

Doplniť popis ku kapitole Popis testovacieho prostredia.

11.4 POPIS PRODUKČNÉHO PROSTREDIA

Doplniť popis ku kapitole Popis produkčného prostredia.

12 SOFTVÉROVÉ LICENCIE

Komponent	Popis	Typ licencie	Licenčné podmienky	Poznámka

13 ZÁLOHOVANIE A OBNOVA RIEŠENIA

13.1 POPIS RIEŠENIA PRE ZÁLOHOVANIE

Doplniť popis ku kapitole Popis riešenia pre zálohovanie.

13.2 POPIS RIEŠENIA PRE OBNOVU

Doplniť popis ku kapitole Popis riešenia pre obnovu.

14 ZABEZPEČENIE DOSTUPNOSTI

Parametre prevádzky jednotlivých modulov:

Popis	Parameter	Poznámka
Prevádzkové hodiny		
Servisné zásahy		
Dostupnosť produkčného prostredia		

14.1 POPIS RIEŠENIA NA DOSTUPNOSŤ SYSTÉMU IS

Doplniť popis ku kapitole Popis riešenia na dostupnosť systému IS.

15 BEZPEČNOSŤ, AUTORITY MANAŽMENT

15.1.1 Zásady bezpečného vývoja

Požiadavky stanovené v tomto dokumente musia byť splnené pre všetky komponenty, ktoré sú používané v priebehu vývoja a všetky artefakty, ktoré sa považujú za produkty vývoja.

Pod produktami vývoja máme na mysli najmä:
- High-level Design (HLD), Low-level Design (LLD), Entity Relationship Diagram (ERD), procesné diagramy apodobne
- zdrojové kódy softvéru
- spustiteľné programy ktoré sú súčasťou dodávky
- konfigurácie
- databázové schémy
- testovacie sady údajov

Bezpečnostné požiadavky je vhodné rozdeliť do troch častí:
- Požiadavky na vývojové prostredie
- Požiadavky na samotný vyvíjaný produkt – aplikáciu
- Požiadavky na produkčné prostredie, v ktorom je produkt prevádzkovaný.

Cieľom týchto opatrení je znížiť pravdepodobnosť a dopad hrozieb spojených s vývojom a dodávkou softvéru a to predovšetkým:
- zanesenie zraniteľností v dôsledku zlých programátorských techník,
- zanesenie zraniteľností v dôsledku používania nebezpečných a nepodporovaných frameworkov,
- zanesenie nežiadúcej funkcionality do kódu či už v dôsledku nedbalosti alebo úmyselne,
- oneskorenie dodávky z dôvodu výpadku vývojárskych prostredí,
- porušenie zásad ochrany osobných údajov z dôvodu nesprávnej manipulácie s nimi,

- zanesenie zraniteľností z dôvodu nesprávnej konfigurácie prostredí,
- trestnoprávna zodpovednosť v dôsledku porušovania autorských práv,
- únik citlivých údajov, strata citlivých údajov,
- nemožnosť zabezpečiť dôkazný materiál v prípade bezpečnostného incidentu ako vo vývoji tak v prevádzke a podobne.

Počas vývoja projektu je potrebné zamedziť a vyhnúť sa zaneseniu najbežnejších implementačných chýb, zraniteľností arizík na základe dodržiavania bezpečného životného cyklu vývoja, best-practices avhodne zvoleného bezpečnostného štandardu a/alebo metodiky. Pri implementácii navrhovaného riešenia sapočas vývoja softvér verifikuje voči well-known zraniteľnostiam abezpečnostným odporúčaniam, ktoré sú obsahom dodržiavania bezpečného vývoja pre zamedzenie vzniku najčastejších bezpečnostných rizík pre webové aplikácie.

Pod komponentami používanými v priebehu vývoja máme na mysli najmä:
- pracovné stanice používané pri vývoji
- virtualizačné prostredie
- servery používané pri vývoji (vývojové, testovacie)
- sieťové prostredie používané pri vývoji, vrátane domácich sietí
- tlačiarne a ostatné aktívne prvky
- fyzické prostredie v ktorom prebieha vývoj, vrátane domácich kancelárií
- podporné služby používané pri vývoji ako sú komunikačné nástroje (MS Teams, Jira, email...)
- vývojové nástroje (editory, kompilátory)
- vývojové frameworky
- middleware (webservery, proxy servery, aplikačné servery)
- úložiská zdrojových kódov a konfigurácií (github)
- zálohovacie aplikácie/služby/systémy a zálohované dáta
- autentizačné mechanizmy (AD, AAD, LDAP, Radius, Kerberos, SAML, cloud access security broker a podobne)

Zabezpečenie vývojového prostredia
Pri vývoji sa dodržujú zásady najlepšej bezpečnostnej praxe vrátane bezpečnej správy, konfigurácie, patchovania a hardeningu pracovných staníc a serverov, antimalvérovej ochrany, segregácie fyzických a logických prostredí, politík pre účty, správy prihlasovacích údajov, bezpečných prihlasovacích postupov, napr. v súlade s ISO/IEC 27001.

Všetky zariadenia používané pri vývoji budú chránené firewallom a to ako na sieťovom perimetri (rozhraní medzi sieťami) tak aj lokálne pomocou host firewallu, ktorý povoľuje len nutné spojenia. V sieťach, v ktorých prebieha vývoj, smú byť zapojené len zariadenia, ktoré sú pre vývoj potrebné.
Koncové stanice, na ktorých prebieha vývoj, nesmú byť prístupné a používané inými osobami. Vprípade počítačov bude zabezpečená avyžadovaná nutnosť mať nastavené automatické uzamykanie obrazovky chránené heslom.
Počítač sa nebude automaticky pripájať k iným wifi sieťam než ku chráneným sieťam používaným pri vývoji. Wifi SSID, v ktorom je pripojený vývojársky počítač, musí mať prístup riadený WPA2 a komplexné heslo, ideálne autentizáciu cez WPA2 Enterprise. V prípade používania fyzickej LAN, je potrebné používať ochranu prístupu.
Všetky zariadenia používané pri vývoji, vrátane OS sieťových a bezpečnostných prvkov (routre, switche, firewally, wifi accesspointy) musia mať nainštalované aktuálne bezpečnostné záplaty a verzia firmvéru musí byť najmenej N-1.

Všetka sieťová komunikácia do internetu a z internetu musí prechádzať zariadením filtrujúcim nebezpečný a škodlivý obsah. Všetka komunikácia z počítačov používaných na vývoj, ktoré sa nachádzajú mimo chránené interné siete (napríklad sú na homeoffice), musí prechádzať cez firemnú VPN bránu kontrolujúcu a filtrujúcu nebezpečný obsah.
Pri vývoji sa bude používať len legálny, podporovaný a aktuálny softvér. Disky všetkých prenosných zariadení musia byť šifrované (notebooky). Je potrebné šifrovať aj disky neprenosných pracovných staníc a serverov, ktoré nie sú umiestnené v dostatočne chránených priestoroch dátových centier a serverovní.

Všetky konfigurácie musia byť chránené proti neautorizovaným zmenám. Všetky zmeny v konfigurácii budú automaticky detegované a reportované.

Na prihlasovanie sa k systémom je povolené používať len osobné účty. Osobné účty používané na bežnú prácu musia byť oddelené od osobných účtov na administráciu. Používanie generických a zdieľaných účtov (root, administrator) je zakázané s výnimkou disaster recovery. Všetky účty musia byť chránené pomocou SSH kľúčov, vo výnimočných prípadoch, ak je to potrebné dostatočne silným heslom alebo frázou s vysokou mierou entropie.
Na všetkých systémoch používaných pre vývoj je povolené inštalovať len minimálnu nutnú množinu softvéru potrebnú pre konkrétnu činnosť.

Všetky testovacie dáta, citlivé dáta, heslá a podobne sa ukladajú na definované miesta.
i

15.2 DEFINOVANIE POUŽÍVATEĽSKÝCH ROLÍ

Samotné práva, či už pre prístup k informáciám, oprávnenia pre prácu s údajmi, ako aj pre prístup k jednotlivým modulom, funkcionalitám budú riadené oprávneniami definovanými v centrálnej správe používateľov a správe identít, tzv. IAM (Identity and Access Management) pomocou oAuth s využitím 2FA na základe čoho sa budú prideľovať jednotlivé používateľské roly.

15.3 ZABEZPEČENIE KOMUNIKÁCIE A INTEGRITY

15.3.1 Zabezpečenie integrity

Validácia všetkých používateľských vstupov a akcií bude vykonávaná na strane servera a pre vhodné operácie aj na strane klienta. Všetky používateľské vstupy musia byť kontrolované na strane servera prostredníctvom whitelistov (ak je to možné a vhodné) alebo regulárnych výrazov v kontexte, v ktorom sú použité.
Proces webového servera aj proces backend databázy musí byť konfigurovaný tak, aby bežal pod unikátnym používateľským kontom s limitovanou množinou privilégií.
Webový server bude konfigurovaný tak, aby súbory s webovým obsahom boli procesom prislúchajúcim službe webového servera prístupné iba na čítanie, no nie na zápis (ak si to samotná služba a proces nevyžaduje).
Webový obsah a všetky logy ním vytvárané budú umiestnené na separátnom pevnom disku alebo na inej logickej partícii, ako OS a webový server.
Na zabezpečenie požiadaviek na bezpečnosť spojených s vývojom projektu TatraLeasing – klientská zóna bude použitý vhodný nástroj poskytujúci priebežnú kontrolu kvality kódu, validáciu bezpečného životného cyklu akontrolu, ktorá odhaľuje chyby, duplikovaný kód a bezpečnostné diery.

15.3.2 Zabezpečenie komunikácie

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

- Prístupová vrstva
- Aplikačná vrstva
- Databázová vrstva

Jednotlivé vrstvy budú umiestnené v separátnych, logicky oddelených sieťových segmentoch pričom komunikácia medzi nimi bude umožnená na základe pravidiel firewallu a navyše bude sústavne monitorovaná a filtrovaná.
Správcovské a monitorovacie rozhrania sieťových prvkov a serverov nie sú prístupné priamo z externej siete, internetu. Správcovské a monitorovacie rozhrania sú prístupné len z vopred špecifikovaných sietí (napr. administrátorská sieť).
Webový server bude prístupný výlučne prostredníctvom protokolu HTTPS. S ohľadom na best-practices sa k webovému portálu nemá pristupovať prostredníctvom HTTP.
Identita webového portálu bude zabezpečená platným, dôveryhodným certifikátom vydaným na doménu, na ktorej je dostupný predmetný portál. 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 (zvlášť prihlasovacie údaje) musia byť prenášané výhradne prostredníctvom zašifrovaného kanála. Webový portál nebude ukladať citlivé informácie v nezašifrovanej podobe na strane klienta, ani na strane servera.
Webový server bude podporovať TLS 1.2, TLS 1.3 a novšie. Nebude podporovať staré verzie SSLv2, SSLv3, TLS 1.0 a TLS 1.1.
Webový server nemá podporovať šifry s kľúčom kratším ako 112 bitov a blokom kratším ako 64 bitov. Webový server nesmie podporovať (musia byť vypnuté) HTTP metódy OPTIONS, TRACK a TRACE.
Webová aplikácia bude čo v najväčšej miere zohľadňovať a aplikovať odporúčania na elimináciu well known zraniteľností podľa best practices.

15.4 RIADENIE PRÍSTUPU (AUDIT TRAILS – SLEDOVANIE LOGOVANIA DO SYSTÉMU)

Základná logická topológia riešenia systému bude rozdelená na tri časti vprostredí AWS, a to:

1. Transfer – komunikácia cez F5 zabezpečená firewallom ale nie smerom do internetu
2. Internal – aplikačná vrstva
3. Restricted – databáza a celkovo storage

15.4.1 Riadenie prístupu

Na riadenie prístupu k aplikácií sa využíva IAM, ktorý na základe definovaných oprávnení vcentrálnej správe používateľov na základe oAuth a2FA prideľuje používateľské roly.
Riadenie prístupu medzi jednotlivými zónami je zabezpečené pomocou firewallov, ktoré využívajú definované security groupy pre definíciu práv jednotlivých rolí. Zóny rozdelené na 3 časti predstavujú virtuálne oblasti vprostredí AWS ktoré využívajú Fargate ECS network ACL pre riadenie prístupu a komunikácie medzi nimi.

15.4.2 Logovanie systému a zber auditných záznamov

Logovanie a monitorovanie systému bude zabezpečené technológiou AWS Fargate, ktorá monitoruje a poskytuje prehľad o využívaných zdrojoch pre jednotlivé účty. Je odporúčanie nastaviť vhodné metriky pre monitorovanie využiteľnosti a kapacity zdrojov pre každé monitorované zariadenie/system.
Monitorovanie a logovanie systému bude zahŕňať upozornenia, ktoré by mali byť poskytované systémovému administrátorovi v prípadoch ako napríklad: blížiace sa zaplnenie kapacity úložného priestoru, neštandardne vysoká záťaž systému, detegovaná neobvyklá bezpečnostná udalosť.
Logy aauditné záznamy budú obsahovať konkrétne informácie odátume, čase apoužitej časovej zóne, budú prenášané zabezpečeným kanálom agranularita logovania bude zodpovedať požiadavkám danej služby. Uchovávanie logov bude nastavené tak, aby sa predišlo prípadnému zaplneniu logovacieho miesta aneovplyvnilo stabilitu zdrojov, napríklad svyužitím AWS EFS, pričom táto služba bude využívaná aj ako backup.

15.5 METODIKA MANAŽMENTU POUŽÍVATEĽOV

Samotné práva, či už pre prístup k informáciám, oprávnenia pre prácu s údajmi, ako aj pre prístup k jednotlivým modulom, funkcionalitám budú riadené oprávneniami definovanými v centrálnej správe používateľov a správe identít, tzv. IAM (Identity and Access Management) pomocou oAuth s využitím 2FA na základe čoho sa budú prideľovať jednotlivé používateľské roly. Pomocou IAM bude taktiež zabezpečené definovanie spôsobu akým môžu jednotlivý používatelia narábať so systémom (CRUD operácie).

16 KONVERZIE DÁT, MIGRÁCIA DÁT, DÁTOVÝ MODEL A NÁVRH RIEŠENIA

V rámci riešenia sa nebude vykonávať migrácia dát.

16.1 POSTUP VYKONANIA MIGRÁCIE DÁT

-

16.2 OVERENIE MIGRÁCIE DÁT

-

16.2.1.1.1.1.1.1 Časť 3: Detailný návrh postupov a produktov pre fázy Testovanie a Nasadenie do produkcie

17 FÁZY PROJEKTU A ČASOVÝ HARMONOGRAM – KONSOLIDOVANÝ PREHĽAD

ČASOVÝ HARMONOGRAM PROJEKTU

Aktivita projektu	Od	Do
Analýza adizajn		
Implementácia atestovanie		
Nasadenie		

ČASOVÝ HARMONOGRAM DIELA – časť M4 a VÝSTUPY

17.1 Fáza - Analýzy a Dizajnu

17.2 Fáza - Implementácie a Testovania

17.3 Fáza - Nasadenia a Post-Implementačnej podpory – príprava a nasadenie do prevádzky

17.4 Ukončenie projektu

18 ZÁVISLOSTI A NÁVRH RIEŠENIA

18.1 ZÁVISLOSTI (PROJEKTOVÉ/MEDZIPROJEKTOVÉ)

Doplniť popis ku kapitole Závislosti.

18.2 ĎALŠIE (DOPLŇTE PODĽA POTREBY)

19 DOKUMENTÁCIA

V rámci projektu a diela budú dodané nasledujúce dokumenty

Dokument	Vytvorený vrámci projektu
Technická dokumentácia	Áno
Prevádzková dokumentácia	Áno
Používateľská dokumentácia	Áno

20 OTVORENÉ OTÁZKY

Z nasledujúceho riešenia nevyplynuli otvorené otázky.

21 PRÍLOHY

Identikácia	Názov dokumentu
Príloha 1	Katalóg požiadaviek
Príloha 2	Zoznam obrázkov

21.1.1.1.1.1.1.1 Príloha 1 - Katalóg požiadaviek

Táto kapitola obsahuje prehľad funkčných, nefunkčných a integračných požiadaviek.