

## PRÍSTUP K PROJEKTU

### Manažérsky výstup I-03

podľa vyhlášky MIRRI č. 401/2023 Z. z.

Povinná osoba	Národná agentúra pre sieťové a elektronické služby
Názov projektu	Modernizácia Platformy pre rozvoj a riešenie prioritných životných situácií (SVK3 – NASES)
Zodpovedná osoba za projekt	Projektová kancelária
Realizátor projektu	Národná agentúra pre sieťové a elektronické služby
Vlastník projektu	Národná agentúra pre sieťové a elektronické služby

#### Schvaľovanie dokumentu

Položka	Meno a priezvisko	Organizácia	Pracovná pozícia	Dátum	Podpis (alebo elektronický súhlas)
Schválenie		NASES	GR NASES		

## 1. HISTÓRIA DOKUMENTU

Verzia	Dátum	Zmeny	Meno
0.1	12.10.2024	Pracovný návrh	NASES
0.2	24.10.2024	Aktualizácia, doplnenie	NASES
0.3	6.11.2024	Aktualizácia	NASES
1.0	7.11.2024	Finalizácia dokumentu	NASES

## 2. ÚČEL DOKUMENTU

V súlade s Vyhláškou 401/2023 Z.z. dokument I-03 Prístup k projektu rozpracováva detailné informácie prípravy projektu z pohľadu aktuálneho stavu, budúceho stavu a navrhovaného riešenia na úrovni biznis vrstvy, aplikačnej vrstvy, dátovej vrstvy, technologickej vrstvy, infraštruktúry navrhovaného riešenia, bezpečnostnej architektúry, špecifikáciu údajov spracovaných v projekte, čistenie údajov, prevádzku a údržbu výstupov projektu, prevádzkové požiadavky, požiadavky na zdrojové kódy. Zároveň opisuje aj implementáciu projektu a preberanie výstupov projektu.

Účelom dokumentu je teda na technickej úrovni popísať cieľ projektu „Modernizácia Platformy pre rozvoj a riešenie prioritných životných situácií (SVK3 – NASES)“, ktorého zámerom je optimalizácia prevádzkovej platformy pre podporu životných situácií. Požiadavky vychádzajú od používateľov a ich role v rámci využívania zákazníckej cesty v príslušnej ŽS.

Detailné funkčné a nefunkčné požiadavky, ich rozsah, požadované technické, bezpečnostné a iné vlastností sú uvedené v **Prílohe č.2 Katalóg požiadaviek**.

Popisované riešenia sa vypracujú pomocou spoločnej platformy IT nástrojov potrebných na vybudovanie a poskytovanie zrozumiteľných a používateľsky ústretových digitálnych služieb zahŕňajúcich postup ucelenej životnej situácie.

Cieľom projektu je zjednodušenie zákazníckej cesty, ktorá rieši životné situácie občana a podnikateľa. Zákaznícka cesta (customer journey), zachytáva sled aktivít a udalostí životnej situácie týkajúcich sa fyzickej osoby.



Obrázok 1 Zákaznícka cesta (ŽS)

Podrobnosti sú uvedené v **Prílohe č.8 Závislosti na úrovni dopadov na externé systémy a ŽS**.

## 2.1. Použité skratky a pojmy

Jednotlivé skratky a pojmy sa nachádzajú v **Prílohe č.1 Zoznam skratiek a pojmov**.

## 2.2. Konvencie pre typy požiadaviek (príklady)

Hlavné kategórie požiadaviek v zmysle katalógu požiadaviek rozdeľujeme podľa funkčných modulov.

Požiadavky majú nasledovnú konvenciu:

### REQ\_MODULE\_xx

- MODULE – modul Slovensko 3.0
  - o IAM – Autentifikácia, autorizácia a správa identít
  - o PAP – Portfólio a Profil klienta
  - o FDES – Dizajnovanie elektronických formulárov
  - o FFIL – Vyplňovanie elektronických formulárov
  - o KS – Konštruktor správy
  - o LS – Lokátor služieb
  - o EDESK – Elektronická schránka
  - o EDESK\_US – Úložisko správ
  - o CNM – Centrálny notifikačný modul
  - o CEP – Centrálna elektronická podateľňa
  - o COP – Centrálna orchestračná platforma pre životné situácie
  - o CZU – Centrálna zbernica udalostí
  - o SNCA – Konsolidácia kvalifikovaných dôveryhodných služieb štátu v NASES
  - o PR – Prierezové
  - o BEZ – Bezpečnostné
- xx – číslo požiadavky (dvojmiestne)

Požiadavky majú určené ID, kategóriu (funkčné, nefunkčné), oblasť, názov, popis, modul, release.

Ostatné typy požiadaviek môžu byť ďalej definované objednávateľom/PM.

Zoznam požiadaviek je uvedený v **Prílohe č.2 Katalóg požiadaviek**.

### 3. POPIS NAVRHOVANÉHO RIEŠENIA

Cieľom projektu „Modernizácia Platformy pre rozvoj a riešenie prioritných životných situácií“ je zamerať sa na vybudovanie a modernizáciu platformy, ktorá by mala fungovať aj v mobilnej verzii, pričom používatelia by mali k dispozícii prehľad o stave spracovania podaní, prislúchajúce notifikácie a platby online. Modernizácia a rozšírenie platformy a aplikačného portfólia ÚPVS sa bude primárne zameriavať na znižovanie zastaranosti, optimalizáciu základných procesov a centrálnych komponentov ÚPVS, čo prispeje k zjednodušeniu riešenia životných situácií, vytvorenie dostupnej, efektívnej a transparentnej komunikácie voči konzumentom centrálnych komponentov, t.j. aj k modernizácii integračných a komunikačných rozhraní.

Výsledkom zmien plánovaných v tomto projekte bude nahradenie vybraných aplikačných komponentov Ústredného portálu verejnej správy (UPVS), modernizácia kvalifikovaných dôveryhodných služieb štátu a zavedenie nových modulov do ekosystému UPVS, ktoré budú zabezpečovať centrálnu orchestráciu životných situácií pre občanov.

Z pohľadu používateľa (koncového zákazníka) budú najviac viditeľné zmeny v aplikačnej vrstve, a to vo forme zavádzania nových funkčných komponentov a aktualizácií existujúcich komponentov v rámci UPVS. Tieto zmeny sú navrhnuté tak, aby zlepšili užívateľskú skúsenosť a zároveň umožnili integráciu so širším ekosystémom verejných služieb.

Z možných variantov riešenia tento dokument na detailnejšej úrovni popisuje Optimálny (želaný) variant v zmysle záverov Multikriteriálnej analýzy (MCA). Tento variant pokrýva požiadavky všetkých stakeholderov.

Ide o

#### Alt 4 – TO BE STAV Optimálny (želaný)

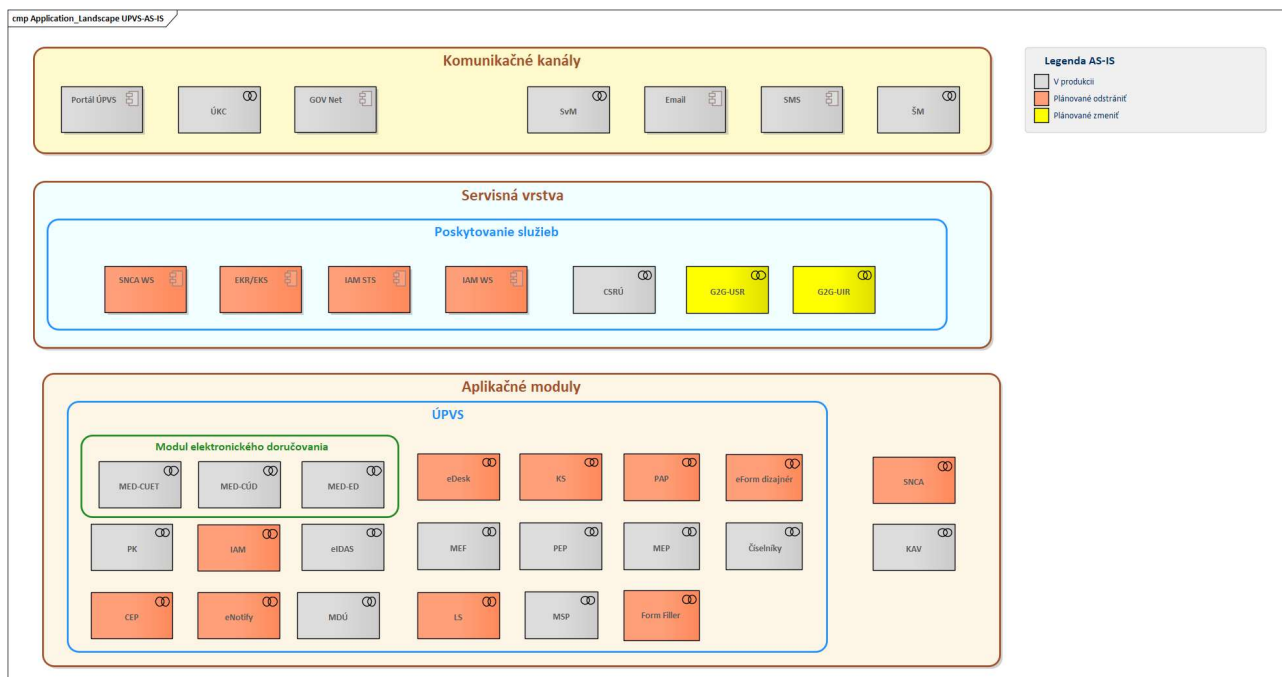
- Celá platforma rozdelená a dodávaná ako samostatné veci – nie jeden dodávateľ
  - Realizované všetky požiadavky zo ŽS a prevádzky NASES pre centrálné komponenty
- Nová architektúra rešpektujúca požiadavku na:
- Efektívnejšia prevádzka
    - o kubernetes (kontajnerizácia)
    - o automatizácia DevOps prevádzky
    - o zvýšenie performance (CEP)
    - o inhouse riešenie prevádzkových procesov L2 a NASES zabezpečuje podporu
    - o podpora klientov (SSOZ – Systém starostlivosti o zákazníkov, podpora UKC)
    - o administratívne moduly pre L2 prevádzku
  - Benefits pre používateľov
    - o lepšia používateľská prívetivosť (eDESK, SNCA 5, PAP, DWH reporting pre používateľov v NASES)
    - o zlepšenie používateľského zážitku (dizajner, lokátor a konštruktor, IAM a eIDAS3 pre jednoduchšie prihlasovanie)
    - o podpora pre proaktívne služby (notifikácie, orchestrácia platforma, mobilné rozhrania, asynchrónne služby)
  - OVM – jednoduchšie integrácie na centrálné komponenty (skrátene čas na integráciu OVM systémov)

### 4. ARCHITEKTÚRA RIEŠENIA PROJEKTU

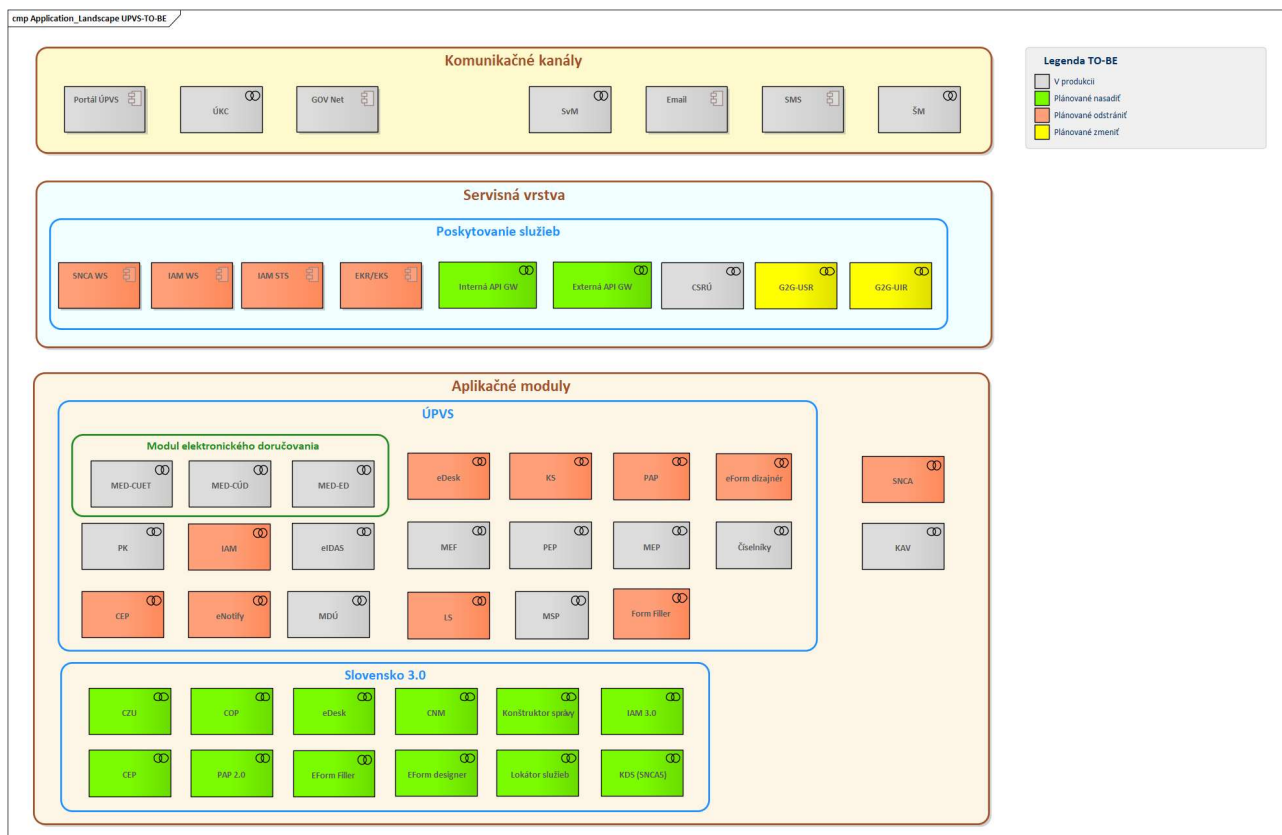
Architektúra riešenia popisuje kľúčové komponenty, ktoré budú upravené, sú navrhnuté tak, aby spĺňali najnovšie požiadavky moderných aplikácií, v súlade s dizajnovými princípmi a štandardmi organizácie NASES. Tieto zmeny reflektujú aj potrebu udržania spätnej kompatibility, a to prostredníctvom zodpovedajúcich rozhraní tam, kde je to nevyhnutné.

Okrem úprav v aplikačnom portfóliu zahŕňa projekt aj rad technologických a organizačno-procesných zmien, ktoré majú za cieľ zvýšiť efektivitu prevádzky NASES. Táto optimalizácia prevádzkovej platformy je kľúčovým aspektom modernizácie infraštruktúry.

Pre názornosť zmeny v aplikačnom portfóliu NASES, ktoré prinesie projekt „Modernizácia Platformy pre rozvoj a riešenie prioritných životných situácií (SVK3 – NASES)“ je schematicky znázornený na nasledovných obrázkoch, ktorý zobrazuje rozdiel medzi stavom pred (AS IS) a po (TO BE) realizácií projektu.



Obrázok 2 Zmeny v aplikačnom portfóliu NASES - AS IS stav



Obrázok 3 Zmeny v aplikačnom portfóliu NASES – TO BE stav

#### 4.1. Biznis vrstva

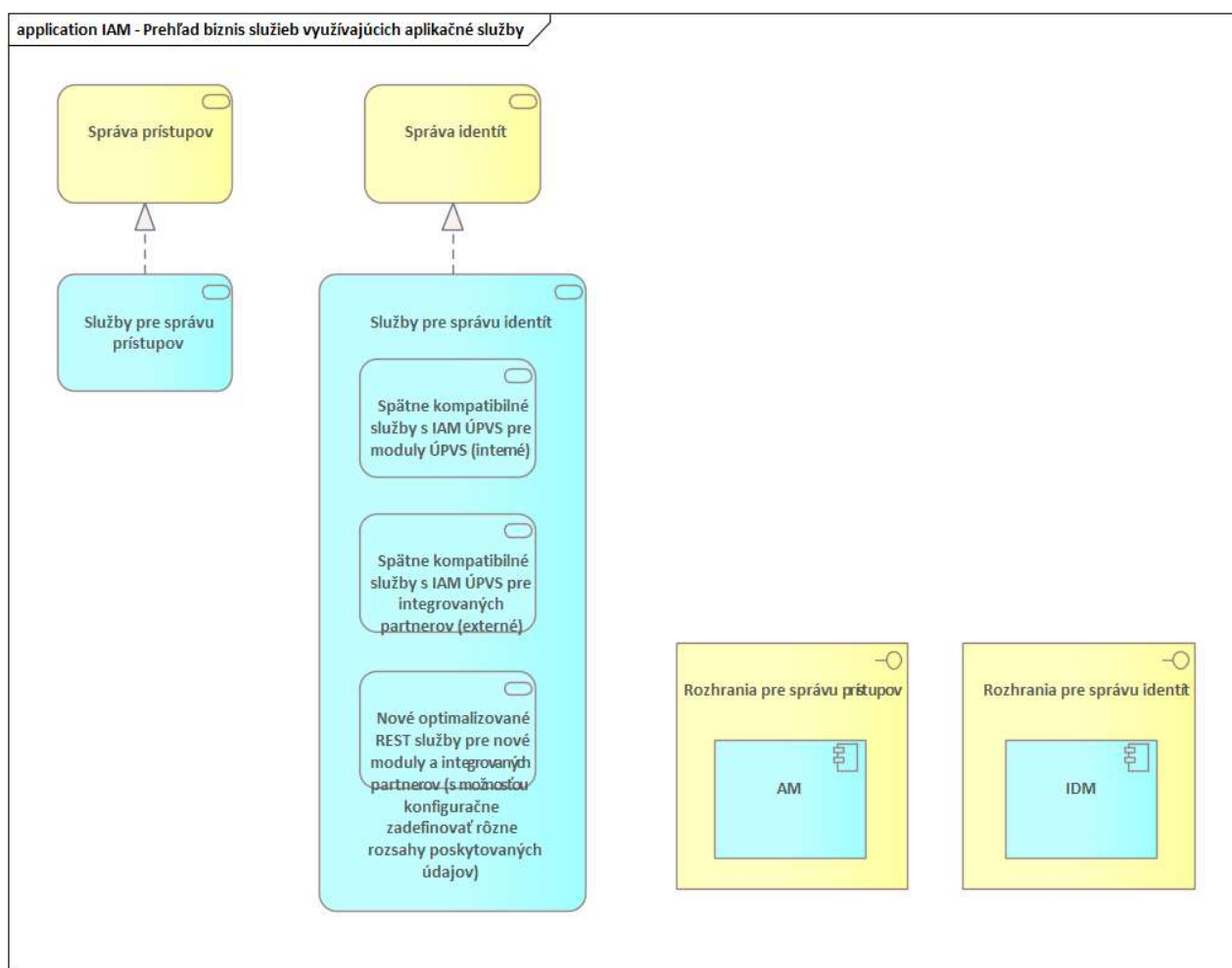
Kapitola popisuje jednotlivé moduly, ktorých modernizácia je predmetom projektu „Modernizácia Platformy pre rozvoj a riešenie prioritných životných situácií“.

#### 4.1.1. IAM - IDENTITY ACCESS MANAGEMENT

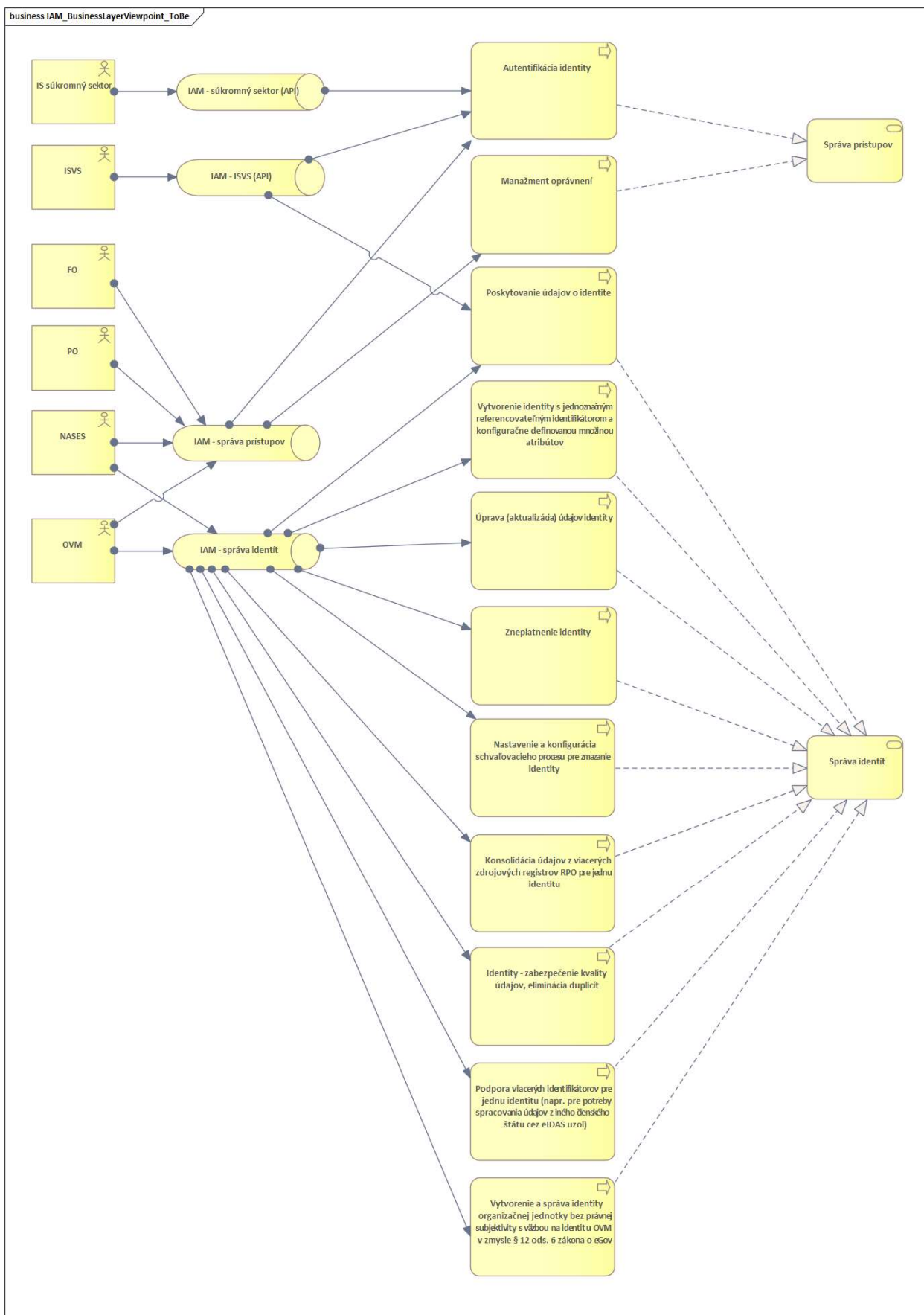
**IAM** - Identity Access Management / Autentifikačný Modul definovaný v zákone 305/2013 Z.z. ako komunikačná časť autentifikačného modulu slúžiaca na overenie identity používateľa a odovzdanie identifikačných údajov ostatným zapojeným systémom. Modul pre autentifikáciu používateľa slúži v rámci ÚPVŠ a celej verejnej správy na overenie identity používateľa a odovzdanie identifikačných údajov ostatným zapojeným systémom. **IAM 3.0** - Nové riešenie modulu IAM ktorého cieľom je do prostredia NASES inštalovať a konfigurovať dielo, ktoré umožní evidenciu identít vrátane cezhraničných používateľov a ich alternatívnych identifikátorov a tak im umožní jednoduchší prístup k elektronickým službám štátu.

Ďalším cieľom IAM 3.0 je zjednodušiť prevádzkovanie a rozvoj modulu pre správu prístupov a identít (modulu IAM ÚPVŠ) vrátane rozširovania jeho služieb vertikálnym a horizontálnym smerom. Nové riešenie musí mať funkčnosť, používateľskú prívetivosť a výkon minimálne na úrovni súčasného riešenia. Riešenie musí spĺňať požiadavky na rozšírenú funkčnosť, ktoré vznikli pri používaní súčasného IAM ÚPVŠ. Riešenie musí obsahovať aj funkcionality, ktorá zahŕňa cezhraničných používateľov, alternatívne identifikátory a stotožňovanie. Taktiež musí obsahovať jednoduchší prístup k tvorbe reportov a štatistík.

Riešenie musí byť postavené na modernejších technológiách, musí poskytovať a preferovať štandardy REST a OpenID Connect. Zároveň musí riešenie podporovať aj štandardy SAML 2.0 a SOAP, aby bola možná spätná kompatibilita s modulmi ÚPVŠ a systémami OVM, ktoré sa budú meniť postupne.



Obrázok 4 Modul IAM - Prehľad biznis služieb využívajúcich aplikačné služby



Obrázok 5 Modul IAM - Biznis služby a rozhrania modulu

#### 4.1.2. eIDAS 3/ STOTOŽŇOVACÍ MODUL - SYSTÉMU NA STOTOŽNENIE OSÔB

**eIDAS 3/ Stotožňovací modul** - Účelom systému je zabezpečiť stotožnenie osôb s viacerými identifikátormi a/alebo prostriedkami elektronickej identifikácie a ich zápis do registra fyzických osôb, vrátane informácie o stotožnení. Modul bude za týmto účelom vyhľadávať dostatočnú zhodu údajov o identite a v prípade výraznejšej zmeny umožní stotožnenie aj pomocou stotožňovacieho kódu. Výsledkom stotožnenia bude, že sa osoba s rôznymi identifikátormi alebo prostriedkami elektronickej identifikácie bude môcť prihlásiť do rovnakej elektronickej schránky a vystupovať v rámci eGovernmentu a v registroch ako pôvodná osoba.

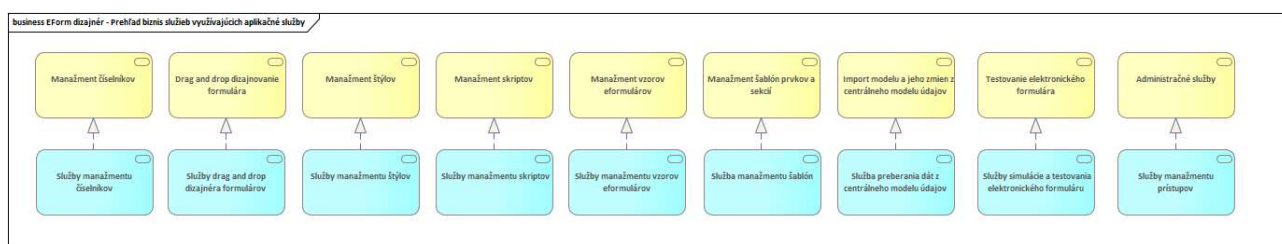
**eIDAS Node / (eIDAS uzol)** - Uzol je súčasťou architektúry interoperability elektronickej identifikácie členských štátov EÚ v zmysle Nariadenia Európskeho parlamentu a Rady EÚ č. 910/2014 (eIDAS) a Vykonávacieho nariadenia Komisie EÚ č. 2015/1501. Umožňuje cezhraničnú autentifikáciu prostriedkami elektronickej identifikácie posúdenými a notifikovanými členskými štátmi EÚ predpísanou procedúrou a zverejnenými vo Vestníku EÚ. Členské štáty majú povinnosť akceptovať pri prístupe k službám online svojho verejného sektora autentifikáciu prostriedkami elektronickej identifikácie minimálne na úrovni „pokročilá“.

#### 4.1.3. eFORM DIZAJNÉR - ELEKTRONICKÝ DIZAJNÉR

**eDizajnér** Elektronický dizajnér (e-dizajnér) je softvérový nástroj alebo platforma, ktorá umožňuje užívateľom vytvárať, upravovať a spravovať elektronické formuláre a dokumenty bez potreby rozsiahlych technických znalostí. Tento nástroj je zameraný na zjednodušenie a automatizáciu procesu dizajnovania elektronických formulárov, pričom poskytuje širokú škálu funkcií a možností prispôbenia.

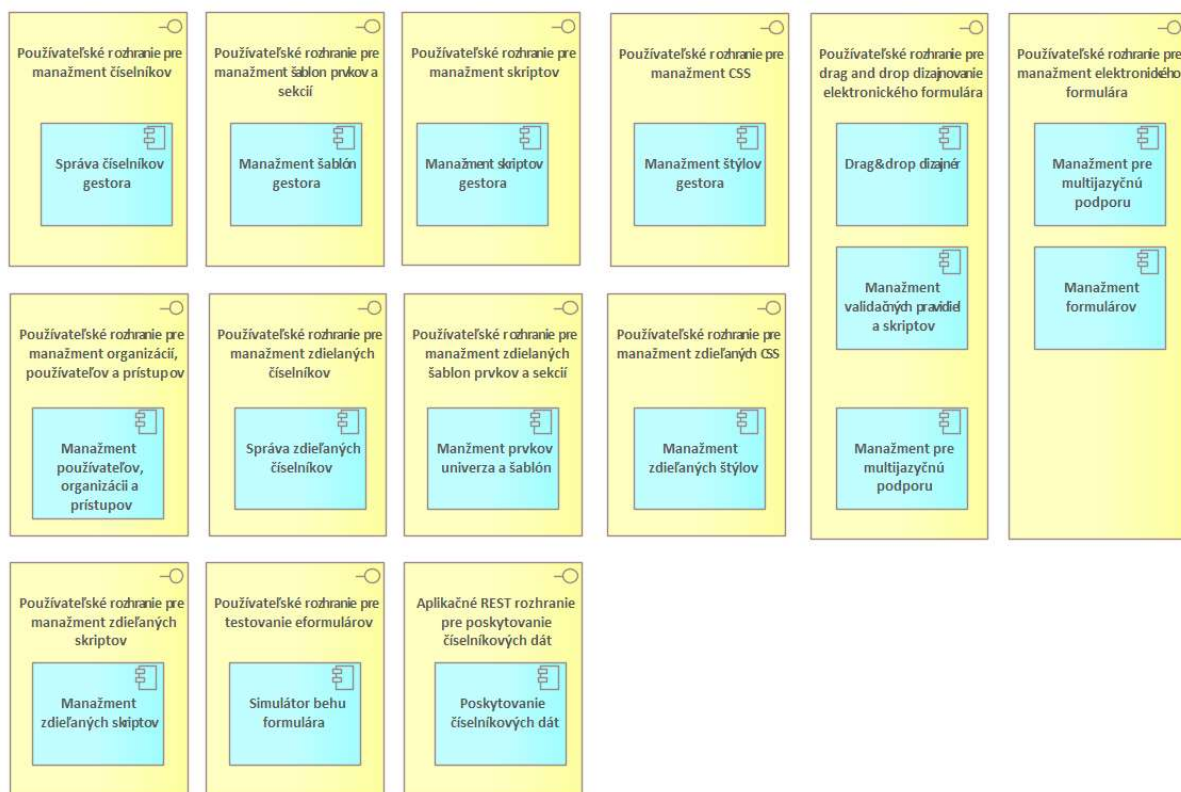
Medzi hlavné funkcie nového e-dizajnéra patria:

- Získanie licencií pre OVM
- Preddefinované šablóny a vizualizácia primárne v PDF
- Responzívny dizajn
- Drag & Drop dizajnér
- Podpora predvypĺňania údajov
- Podpora rôznych prvkov formulárov (textové polia, rozbaľovacie zoznamy, zaškrŕtávacie políčka, rádiové políčka a.i.)
- Podpora hybridných číselníkov
- Kompatibilita s IDSK 3.0.



Obrázok 6 Modul eForm dizajnér - Prehľad biznis služieb využívajúcich aplikačné služby

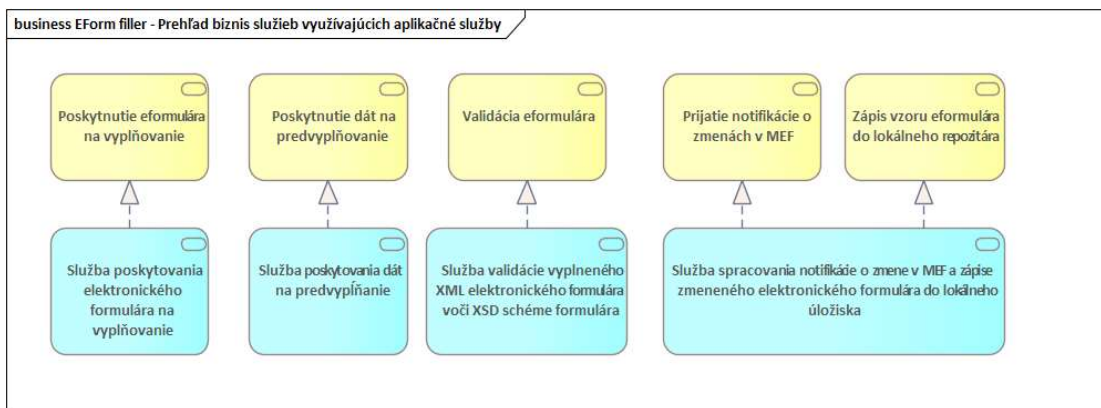




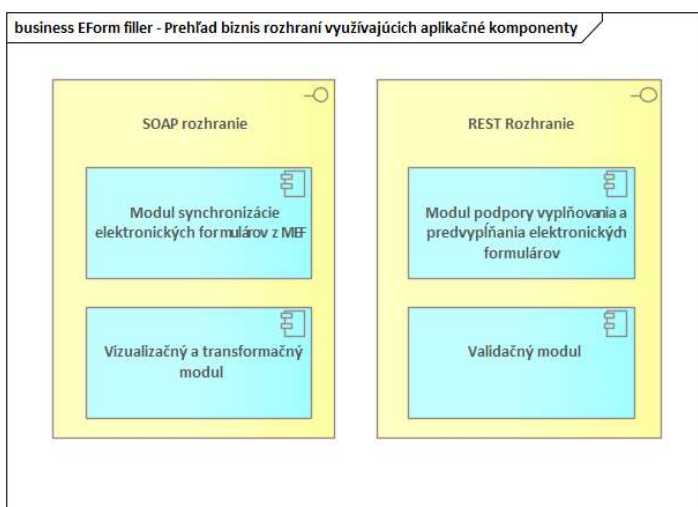
Obrázok 7 Modul eForm dizajnér - Prehľad biznis rozhraní využívajúcich aplikačné komponenty



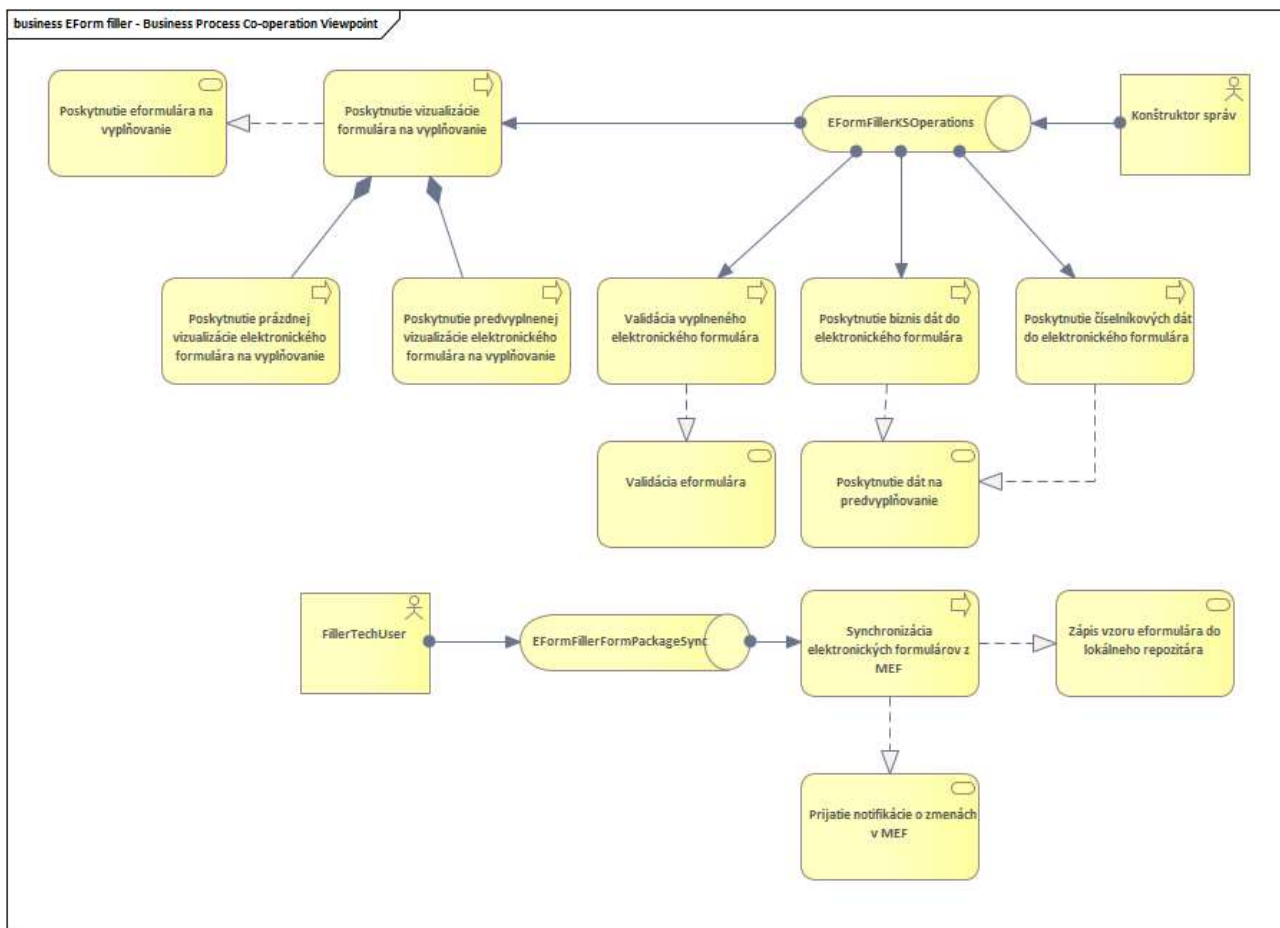




Obrázok 9 Modul eForm filler – Prehľad biznis služieb využívajúcich aplikačné služby



Obrázok 10 Modul eForm filler - Prehľad biznis rozhraní využívajúcich aplikačné služby



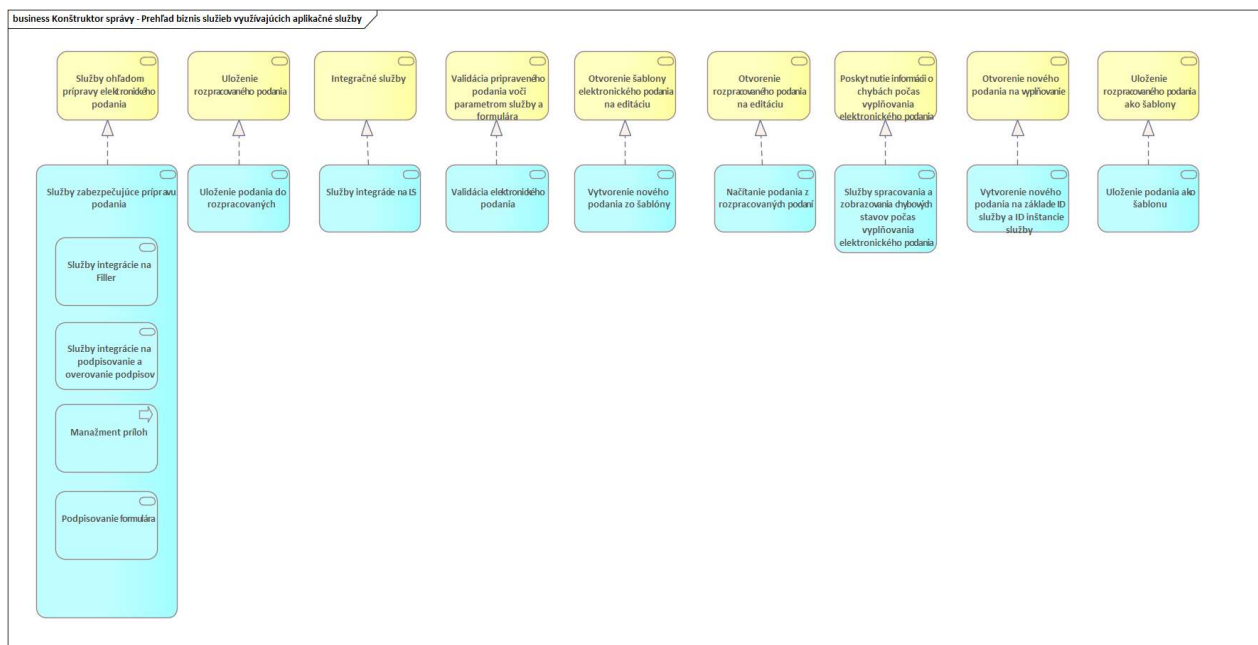
Obrázok 11 Modul eForm filler - Biznis služby modulu

#### 4.1.5. Konštruktor správ - VYTVORENIE ELEKTRONICKÉHO PODANIA

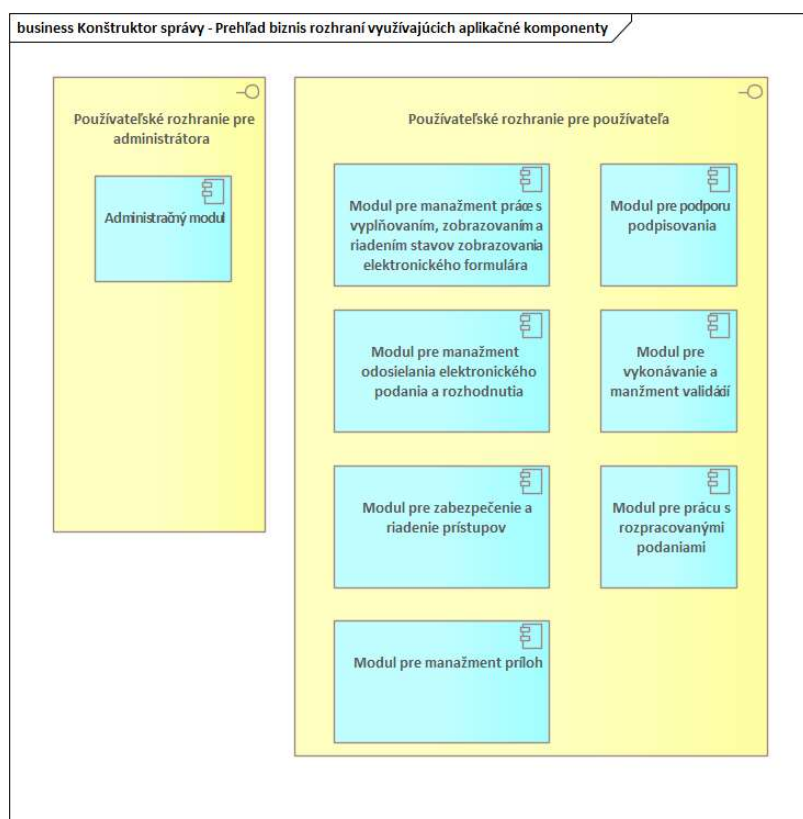
**Konštruktor správ** - slúžiaci na vytvorenie elektronického podania pozostávajúceho z častí elektronického formulára a príloh k podaniu s funkcionalitou práce s rozpracovanými podaniami.

**Konštruktor správ 3.0** - Nový responzívny konštruktor správ a rozpracovaných podaní, ktorý zabezpečí:

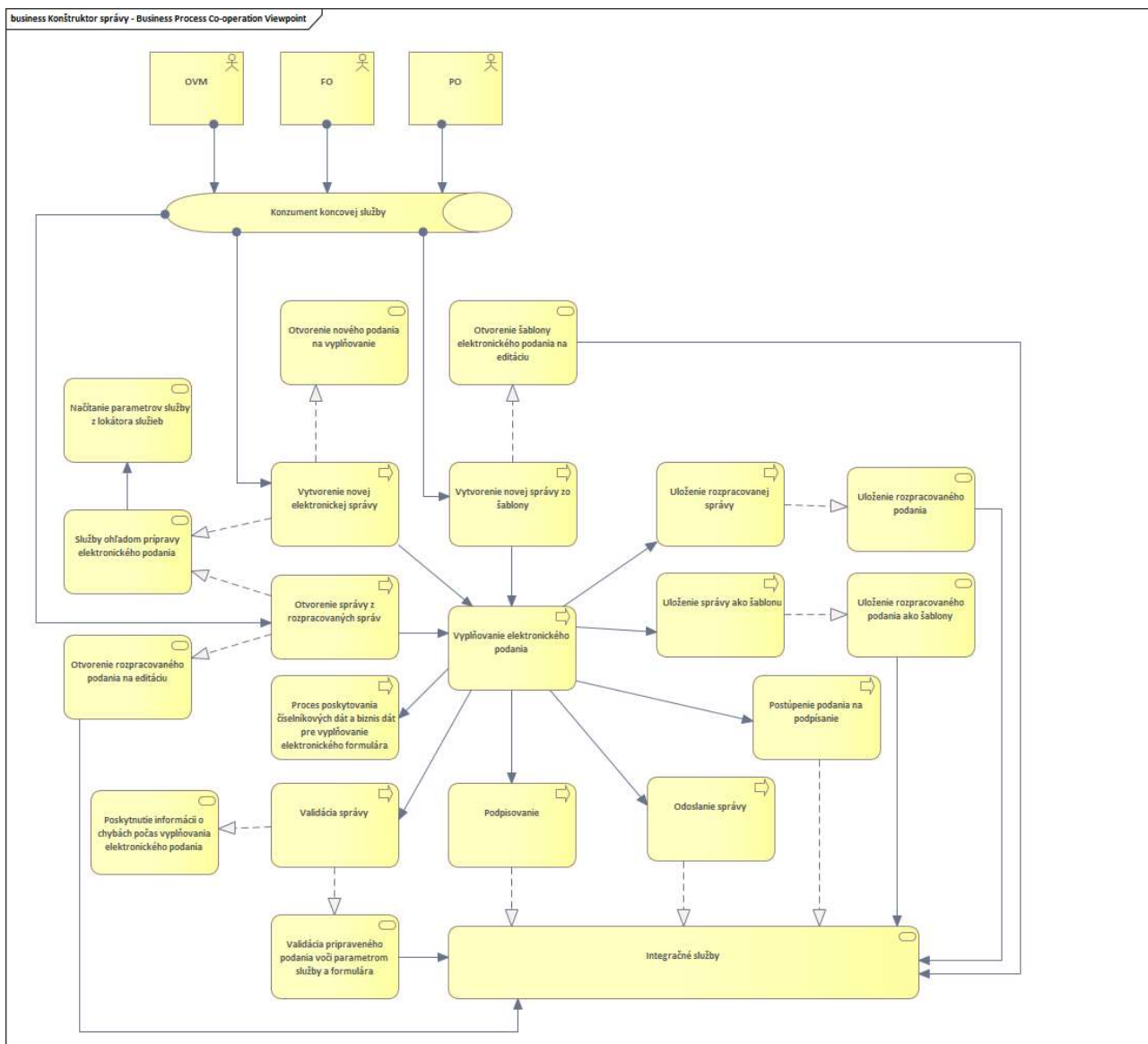
- Plne responzívnym rozhraním vytvorenie elektronického podania pozostávajúceho z častí elektronického formulára a príloh k elektronickému podaniu.
- Pre OVM plne responzívnym rozhraním vytvorenie elektronického úradného dokumentu, najmä však rozhodnutia alebo notifikácie, pozostávajúceho z častí elektronického formulára a jednotlivých príloh.
- Podpisovanie elektronického formulára a elektronických príloh prostredníctvom centrálného podpisového komponentu.
- Funkcionalitu práce s rozpracovanými podaniami.
- Vybrané kolaboračné práce nad elektronickým podaním podľa katalógu požiadaviek.
- Validácie vyplňovaného elektronického podania voči konfigurácii služby v METAIS.
- Odoslanie elektronického podania na centrálné komponenty ÚPVS.



Obrázok 12 Modul Konštruktor správ - Prehľad biznis služieb využívajúcich aplikačné služby



Obrázok 13 Modul Konštruktor správ - Prehľad biznis rozhraní využívajúcich aplikačné komponenty

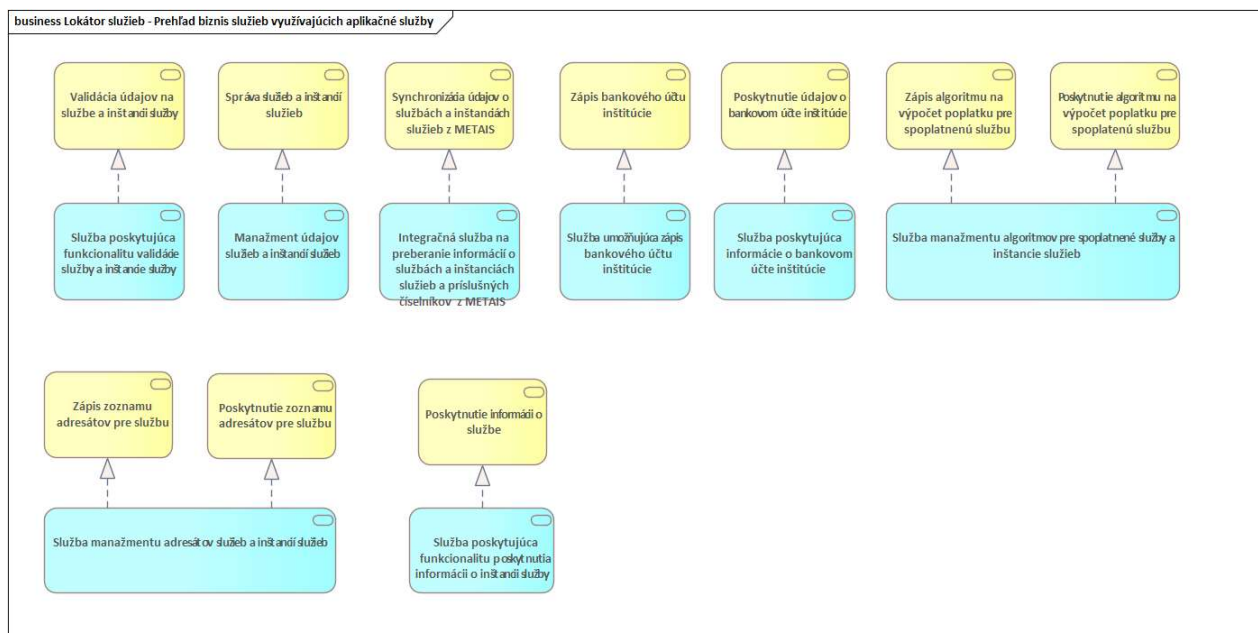


Obrázok 14 Modul Konštruktor správ - Biznis služby modulu

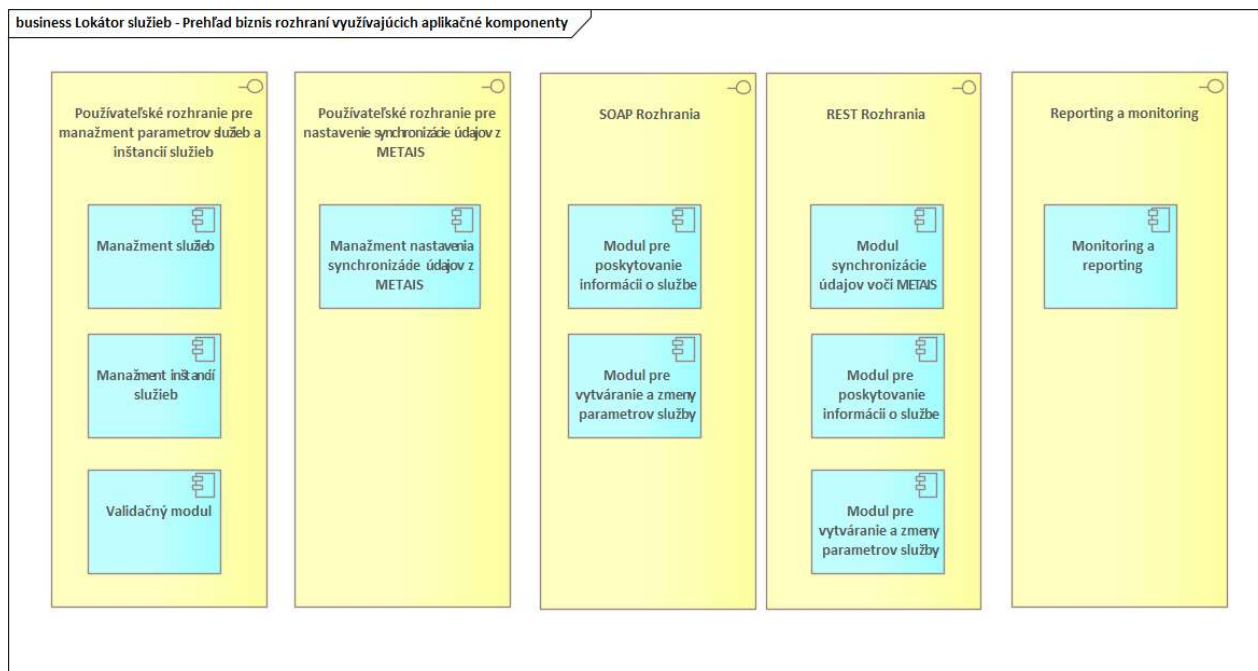
#### 4.1.6. Lokátor služieb A JEHO FUNKCIA

**Lokátor služieb 3.0** - zabezpečí:

- Prostredníctvom aplikačných služieb prístup k parametrom elektronických služieb.
- Synchronizáciu konfigurácií elektronických služieb prevádzkovaných na ÚPVS voči METAIS.
- Prostredníctvom používateľského rozhrania evidenciu služieb a parametrov služieb, vrátane takých, ktoré nie sú registrované v METAIS.
- Aplikačné rozhranie na vyhľadávanie elektronických služieb.
- Kompatibilitu rozhraní s aktuálne prevádzkovaným komponentom lokátor služieb.

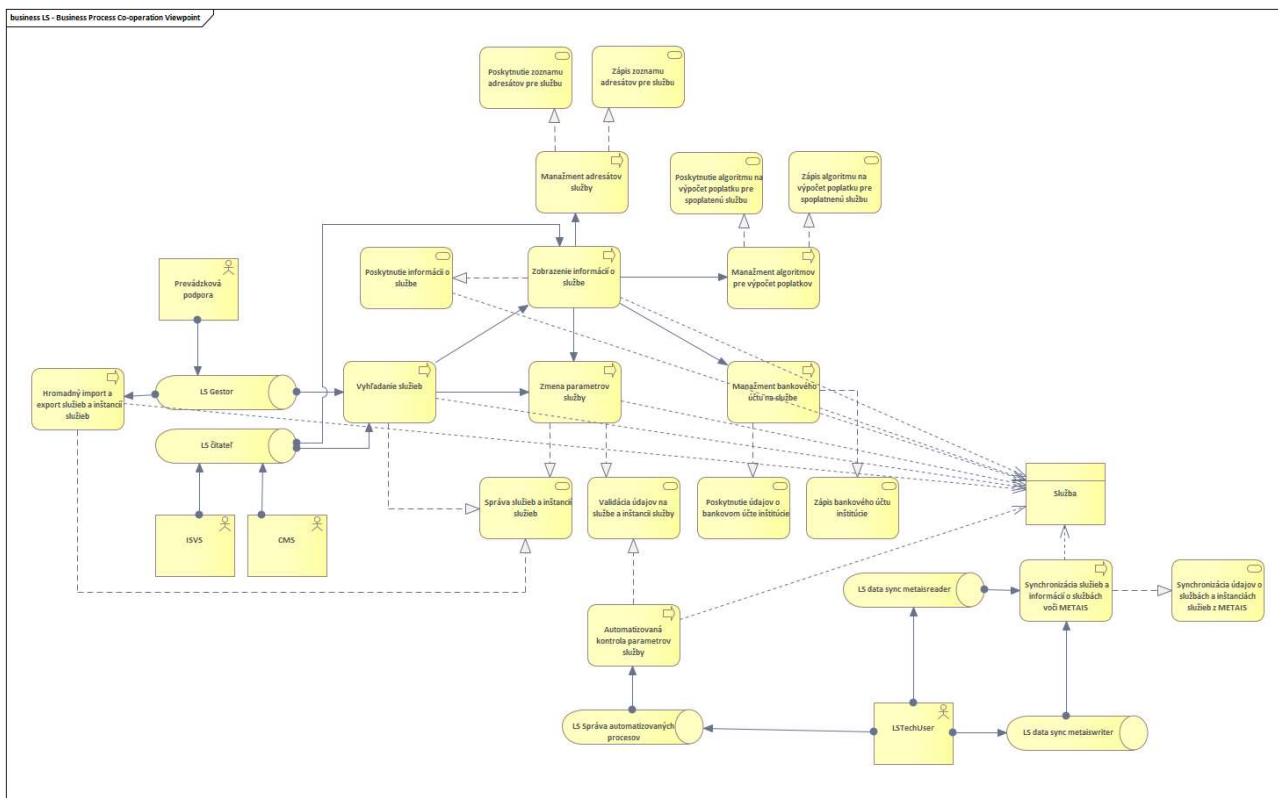


Obrázok 15 Modul Lokátor služieb - Prehľad biznis služieb využívajúcich aplikačné služby



Obrázok 16 Modul Lokátor služieb - Prehľad biznis rozhraní využívajúcich aplikačné komponenty





Obrázok 17 Modul Lokátor služieb - Biznis služby modulu

#### 4.1.7. eDesk - ELEKTRONICKÁ SCHRÁNKA

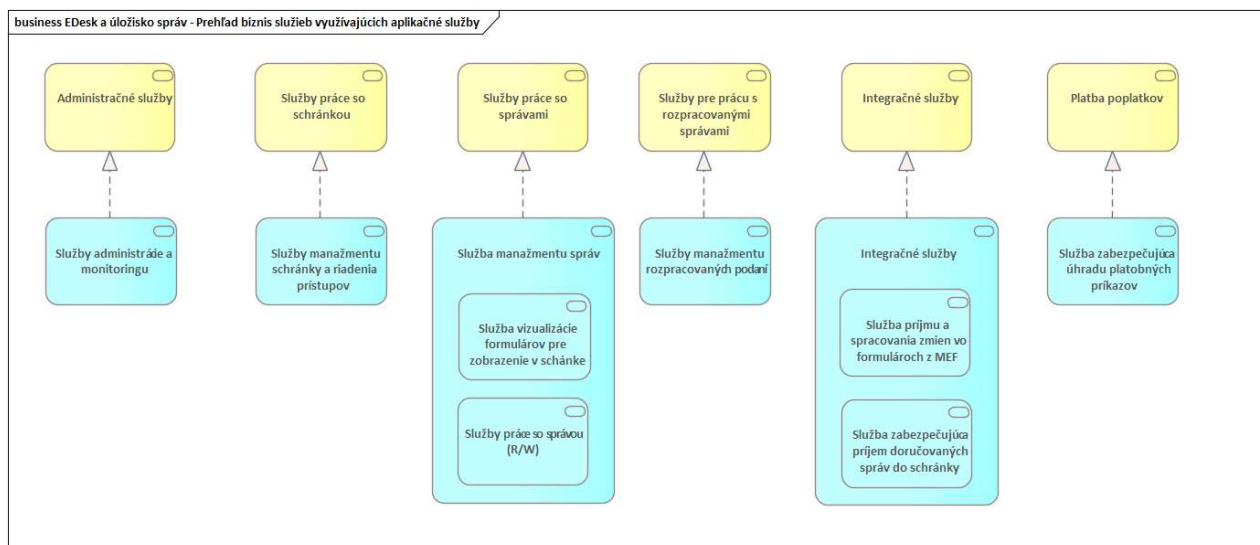
**eDesk - Elektronická schránka** slúžiaca na komunikáciu medzi občanmi, podnikateľmi a verejnou správou. Služi na prijímanie elektronických správ a úradných dokumentov, ukladanie a sprístupňovanie elektronických správ, vrátane ich súčastí. **eDesk 3.0** - Nové riešenie eDesk má umožniť bezpečnú komunikáciu medzi občanmi, podnikateľmi a verejnou správou. Služiť má na prijímanie a odosielanie elektronických správ a úradných dokumentov. Tiež má zabezpečiť dôvernoscť a integritu komunikácie a umožniť zobrazovať a archivovať všetky aktivity, vrátane dátumu a času prístupu a prijatia správ. Riešenie musí umožniť spravovať oprávnenia na prístup, vďaka čomu k citlivým informáciám majú prístup len oprávnené osoby.

Súčasťou riešenia je aj úložisko elektronických správ (Úložisko správ), ktoré umožní ukladanie a sprístupňovanie elektronických správ, vrátane ich súčastí. Správy môžu byť väčšie ako je súčasne podporovaných 50 MB. Riešenie obsahuje aj natívnu/hybridnú aplikáciu pre mobilné zariadenia s vybranými funkcionalitami webovej aplikácie, primárne na zobrazovanie a čítanie správ. Cieľom je celkovo zjednodušiť a zefektívniť komunikáciu v elektronickej verejnej správe. Zároveň bude poskytovať natívny prístup do elektronickej schránky správ prostredníctvom optimalizovaného GUI pre mobilne zariadenia. Ponúkne tak množstvo funkcií pre pohodlnú a efektívnu prácu s elektronicou schránkou správ na mobilných zariadeniach.

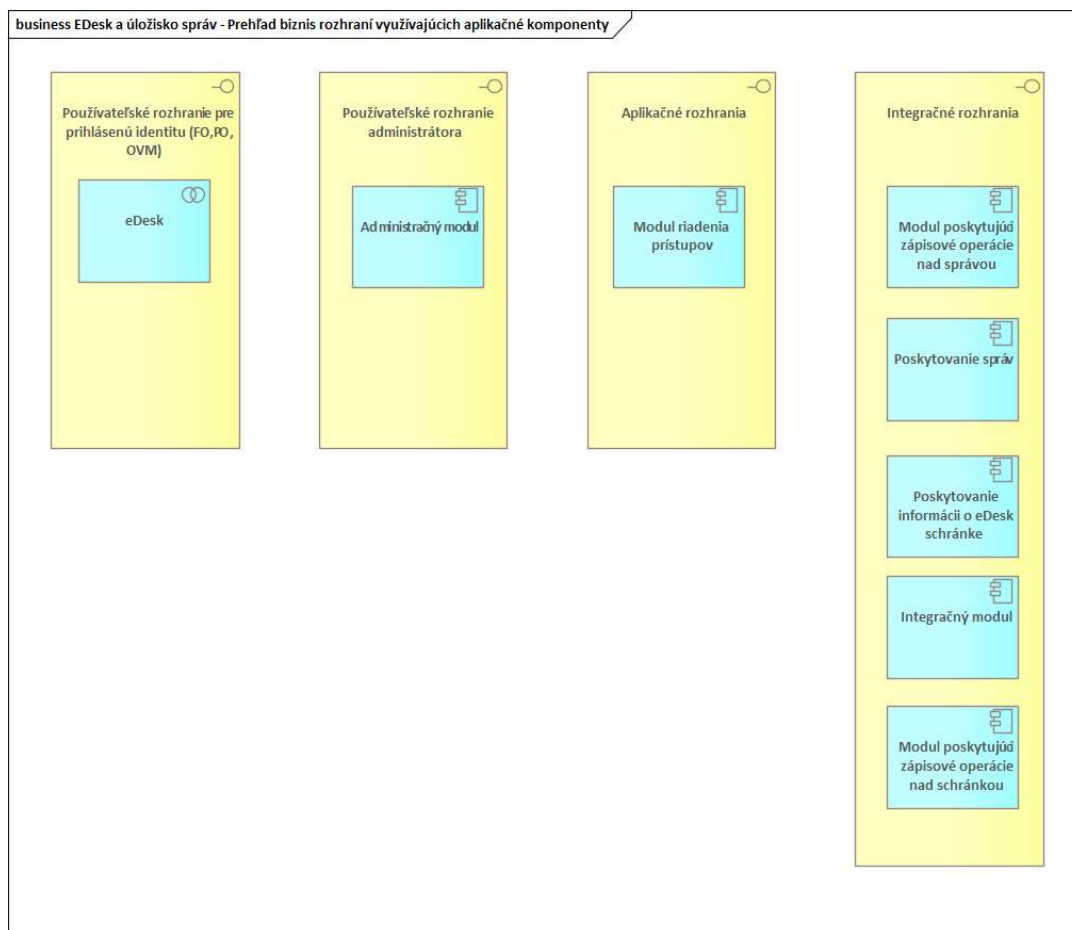
Funkcionalita eDesk:

- Prístup do elektronickej schránky správ
- Aktivácia schránky na doručovanie
- Notifikácie o novej správe
- Vytváranie a odosielanie podaní

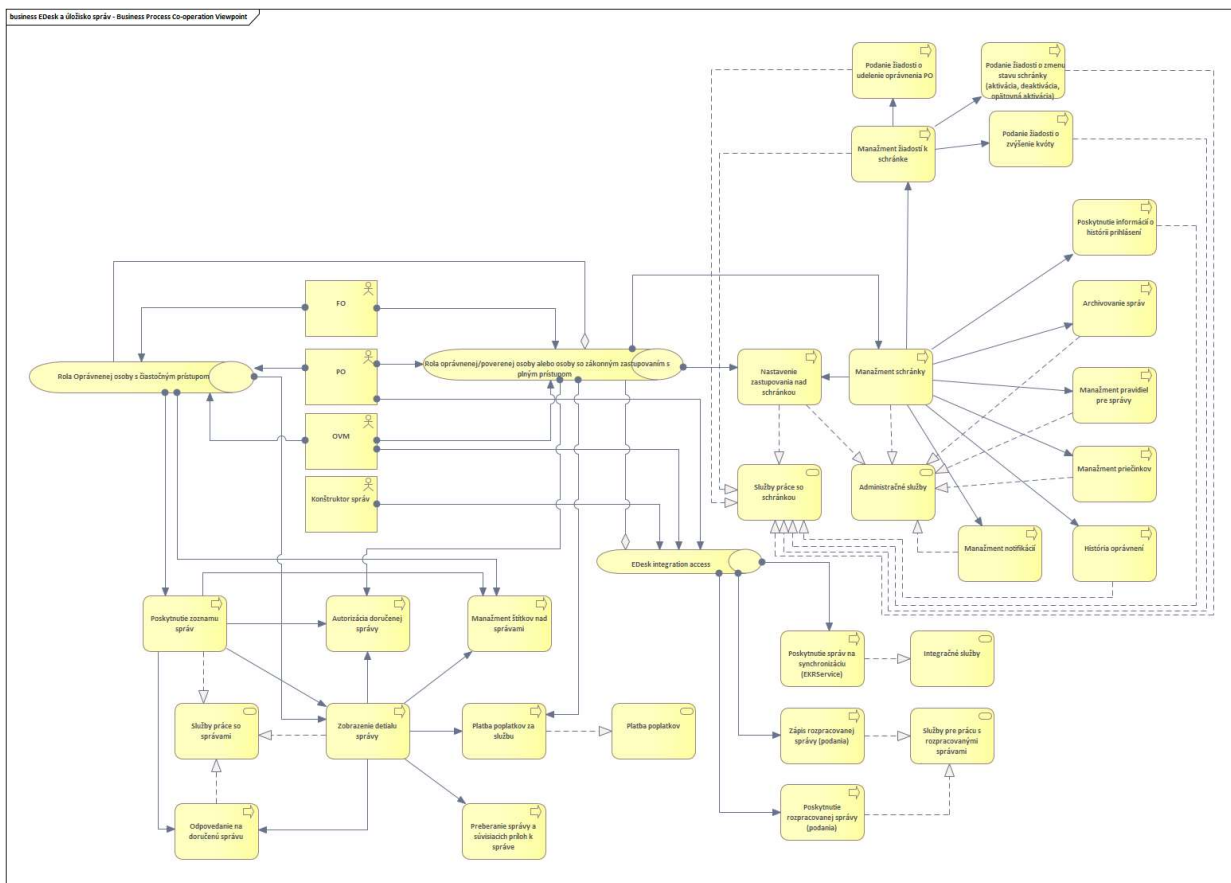




Obrázok 18 Modul eDesk a úložisko správ - Prehľad biznis služieb využívajúcich aplikačné služby



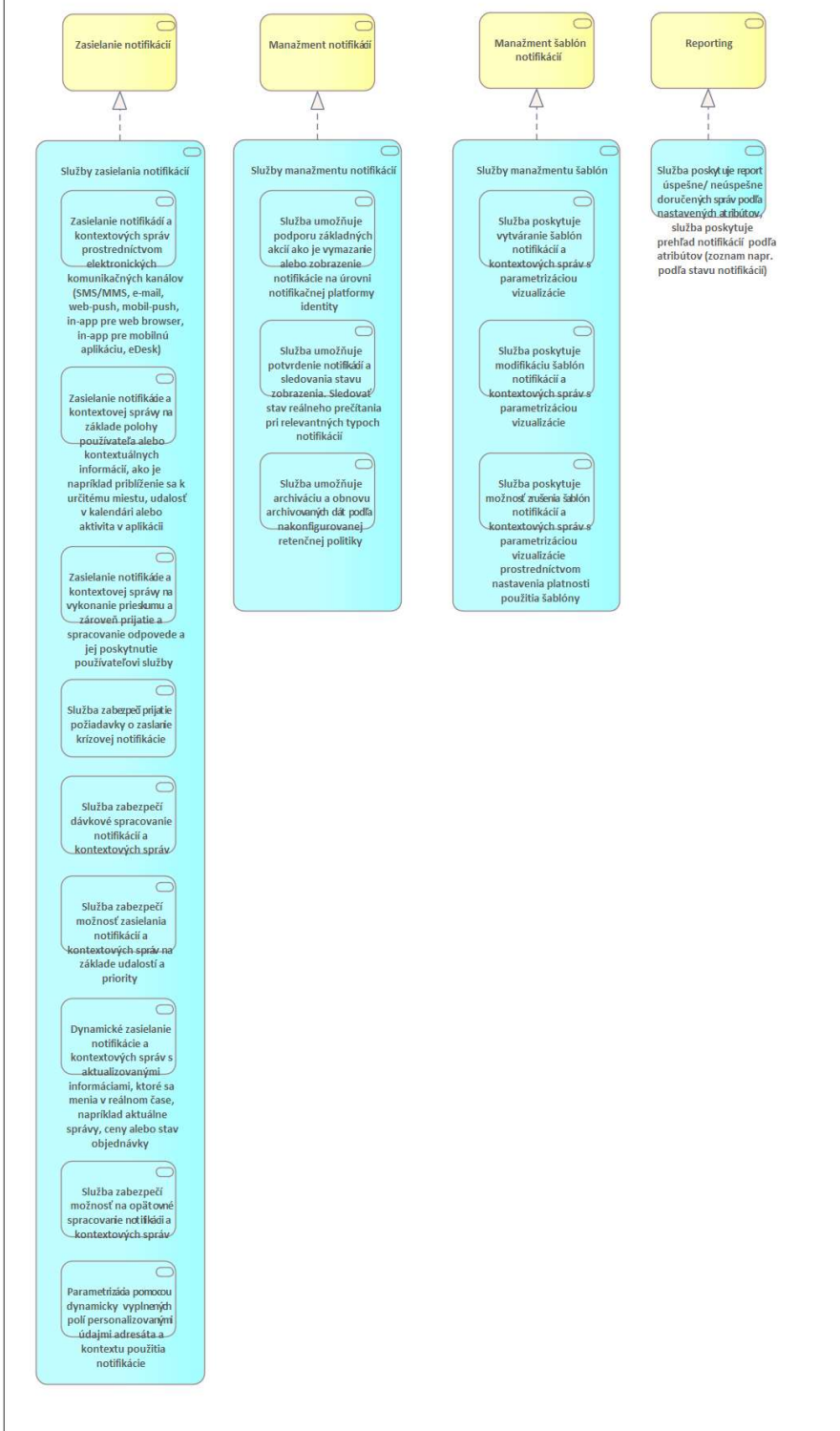
Obrázok 19 Modul eDesk a úložisko správ - Prehľad biznis rozhraní využívajúcich aplikačné komponenty

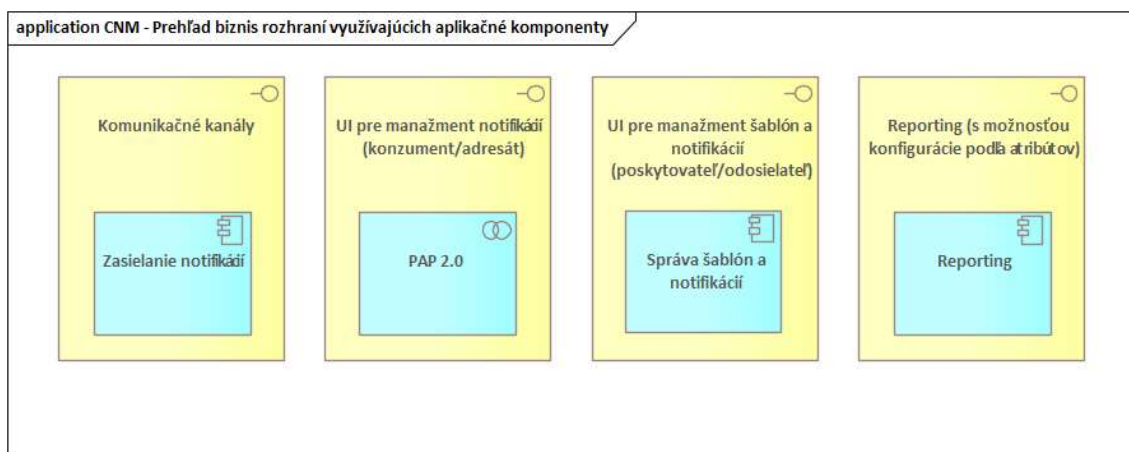


Obrázok 20 Modul eDesk a úložisko správ - Biznis služby modulu

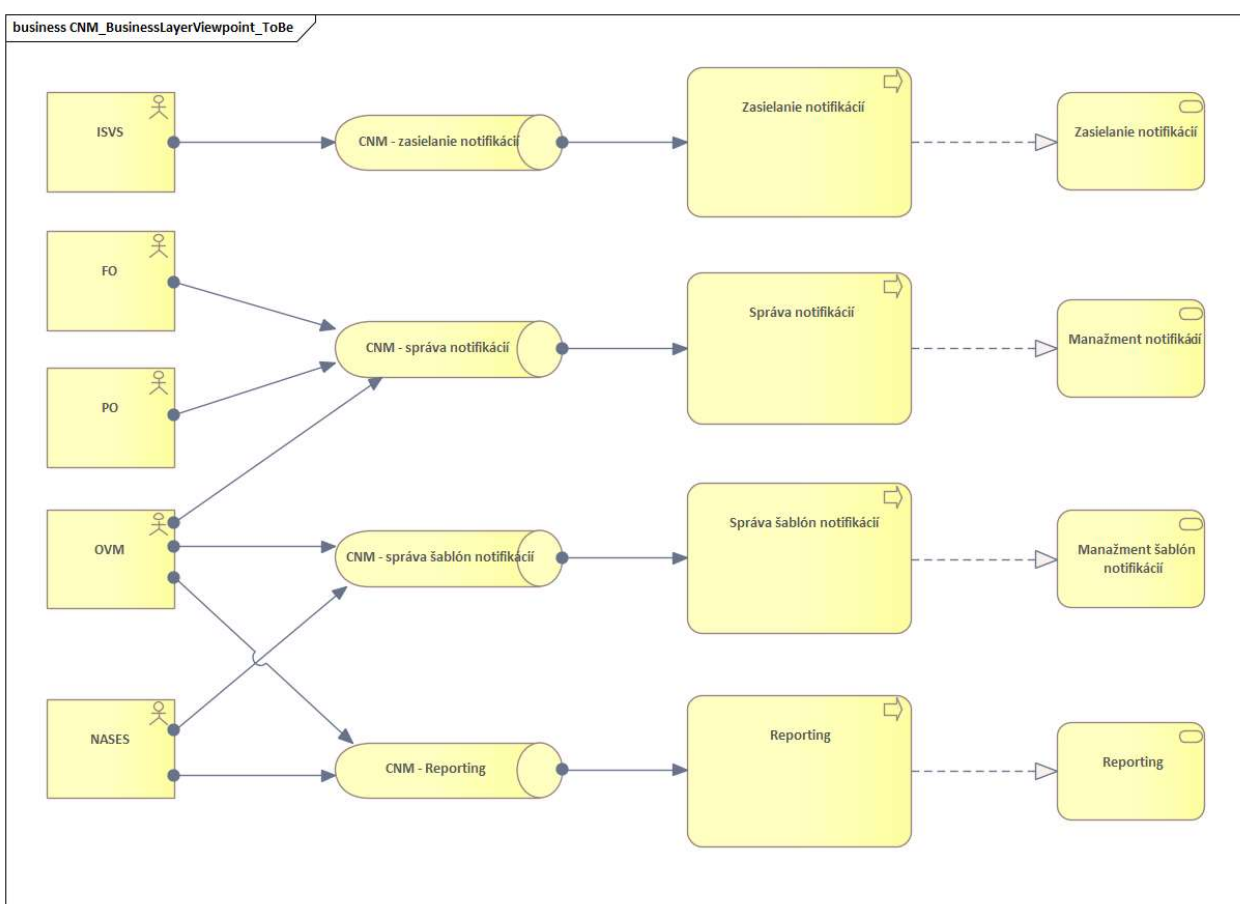
#### 4.1.8. Centrálny NOTIFIKAČNÝ MODUL - **NÁSTROJ NA ZLEPŠENIE KOMUNIKÁCIE ŠTÁTU S OBČANOM**

**Notifikačný modul** - nástroj pre zlepšenie komunikácie štátu s občanom, slúžiaci na poskytovanie informácií, upozornení a aktualizácií občanom a verejnosti, či už v komunikácii v rámci životných situácií alebo v rámci komunikácie iných orgánov verejnej moci.





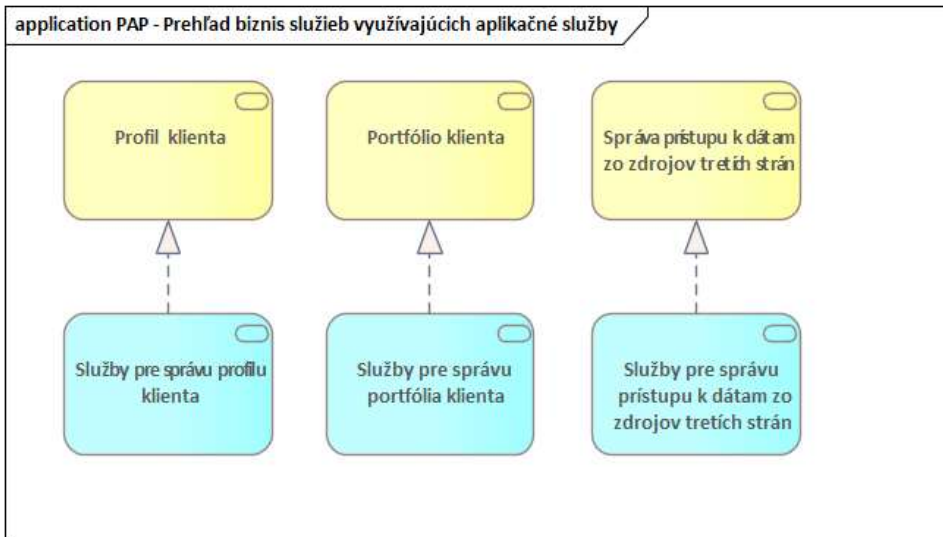
Obrázok 21 Notifikačný modul - Prehľad biznis rozhraní využívajúcich aplikačné komponenty



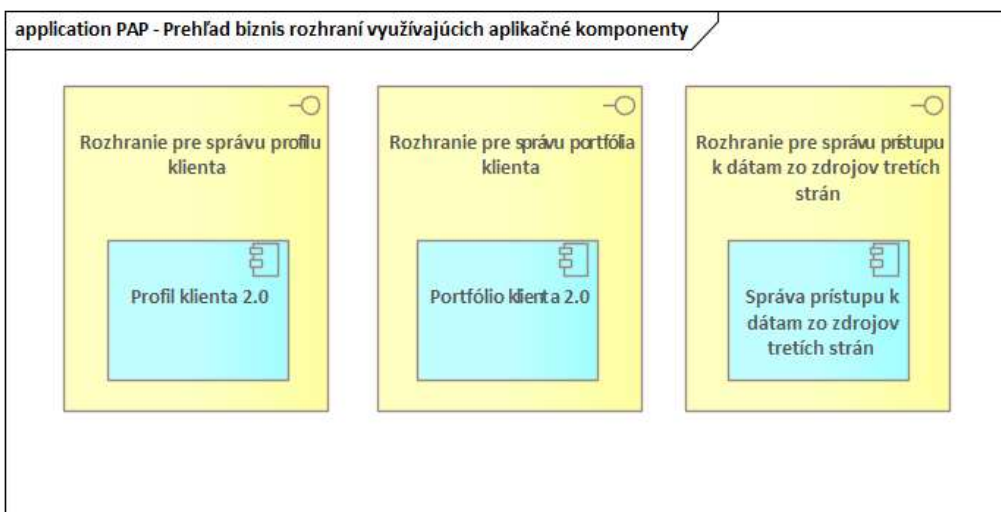
Obrázok 22 Notifikačný modul - Biznis služby modulu

#### 4.1.9. PaP - Portfólio a profil klienta (PaP) 2.0 - POUŽÍVATEĽSKÉ ROZHRANIE PRE OBČANA A PODNIKATEĽA

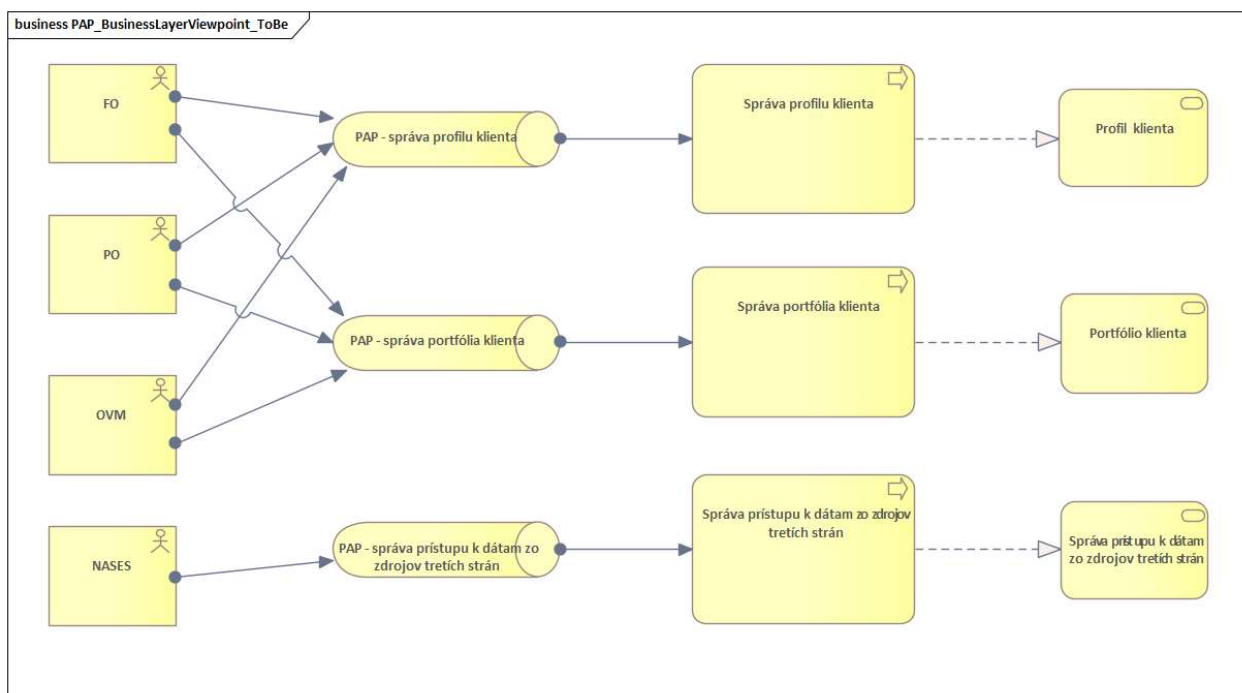
**Portfólio a profil klienta (PaP) 2.0** - Používateľské rozhranie optimalizované pre občana a občana podnikateľa. Modul používateľovi umožňuje vytvorenie si vlastných nastavení, reagovať na kontext v ktorom sa používateľ nachádza a poskytovať sady nastavení viazané podľa vzťahov medzi subjektami (zastupovanie) aj pre iné systémy tak, aby mal používateľ jedno miesto, kde nastaví svoje preferencie pre celý digitálny ekosystém.



Obrázok 23 Modul PaP 3.0 - Prehľad biznis služieb využívajúcich aplikačné služby



Obrázok 24 Modul PaP 3.0 - Prehľad biznis rozhraní využívajúcich aplikačné komponenty

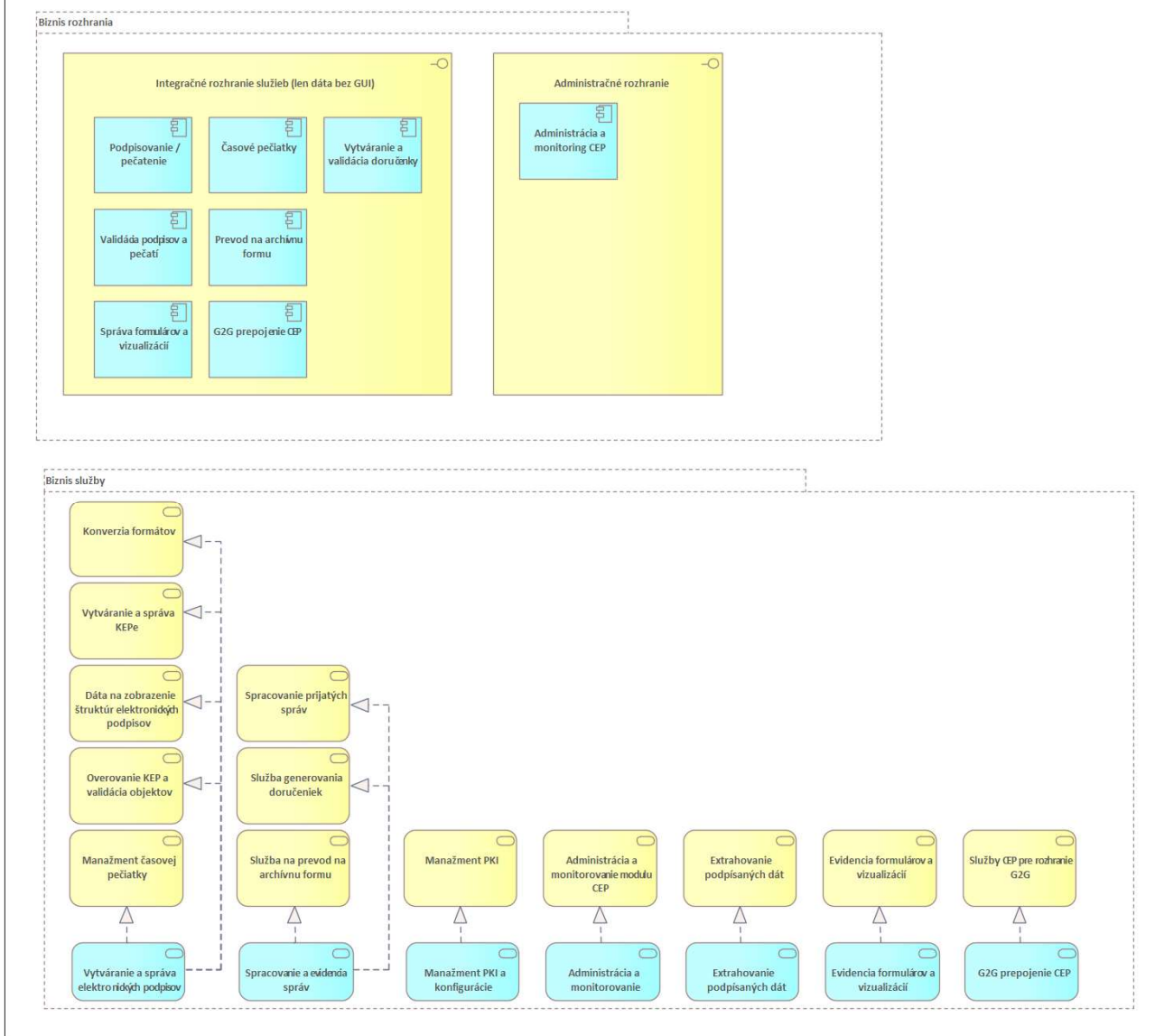


Obrázok 25 Modul PaP 2.0 - Biznis služby modulu

#### **4.1.10. CEP - CENTRÁLNA ELEKTRONICKÁ PODATEĽŇA**

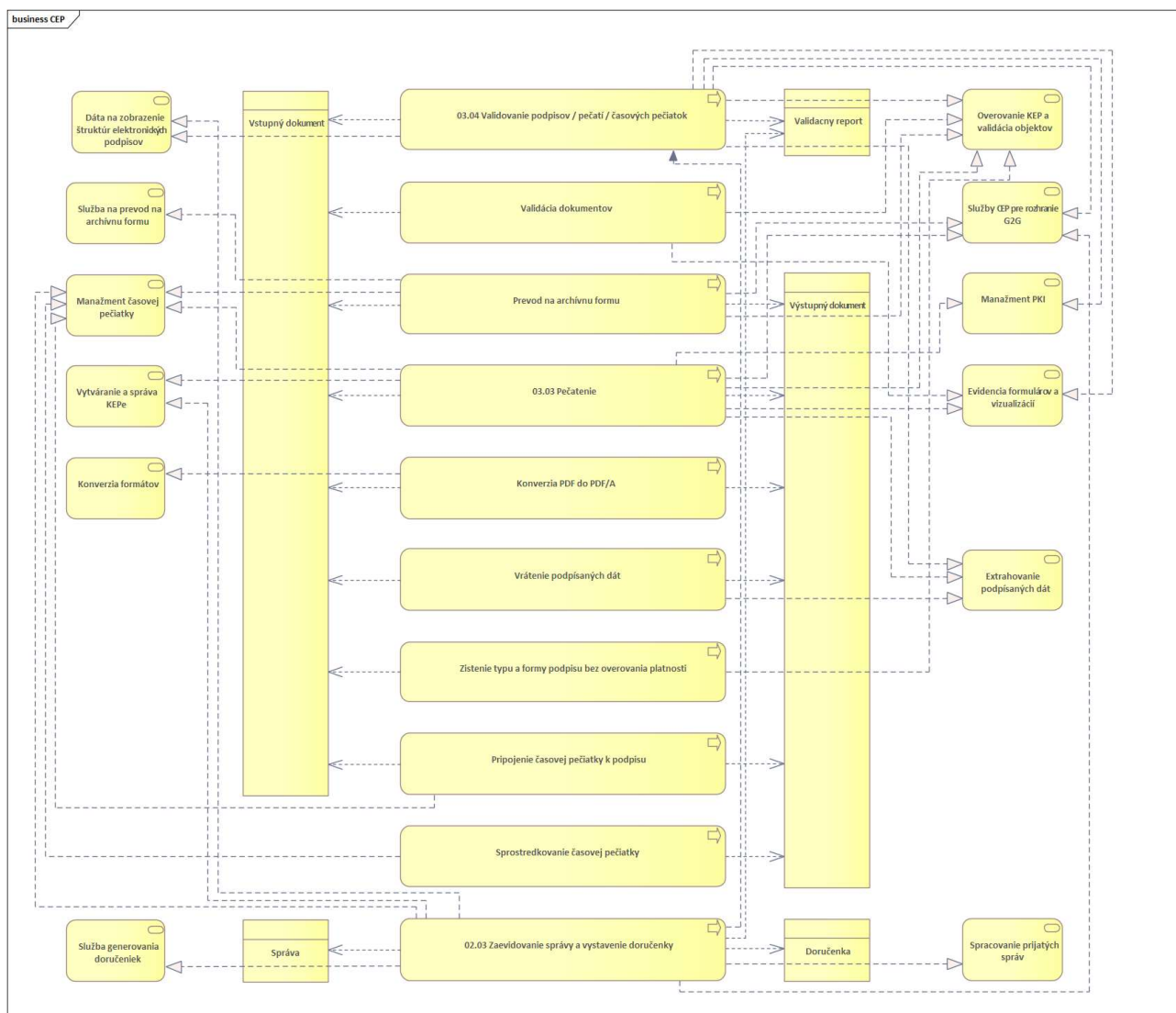
**Centrálnou elektronickou podateľňou (CEP)** rozumieme komplexný systém určený na prácu s elektronickými podpismi a potvrdzovanie prijatia správy doručenej orgánu verejnej moci podpísaných dokumentov. Tento systém je navrhnutý tak, aby spĺňal vysoké štandardy bezpečnosti a spoľahlivosti, pričom umožňuje efektívne vytvárať overovať elektronické podpisy, pečate a časové pečiatky. CEP zaisťuje integritu a právnu záväznosť elektronických dokumentov v súlade s platnou legislatívou a medzinárodnými normami, najmä nariadením eIDAS. Hlavné vylepšenia CEP 3.0.:

- Architektúra mikroslužieb
- Škálovateľnosť databázy
- Synchronná a asynchronná validácia podpisov a pečatí v súlade s legislatívou vrátane autorizácie funkciu prístupového miesta
- Remote sealing (Pečatenie na diaľku)
- Detekcia typu a formy podpisu
- Spájanie a rozdeľovanie podpisových kontajnerov
- Pokročilé logovanie a monitoring
- Konverzia medzi podpisovými formátmi EÚ



Obrázok 26 Modul CEP - Prehľad biznis služieb využívajúcich aplikačné služby modulu

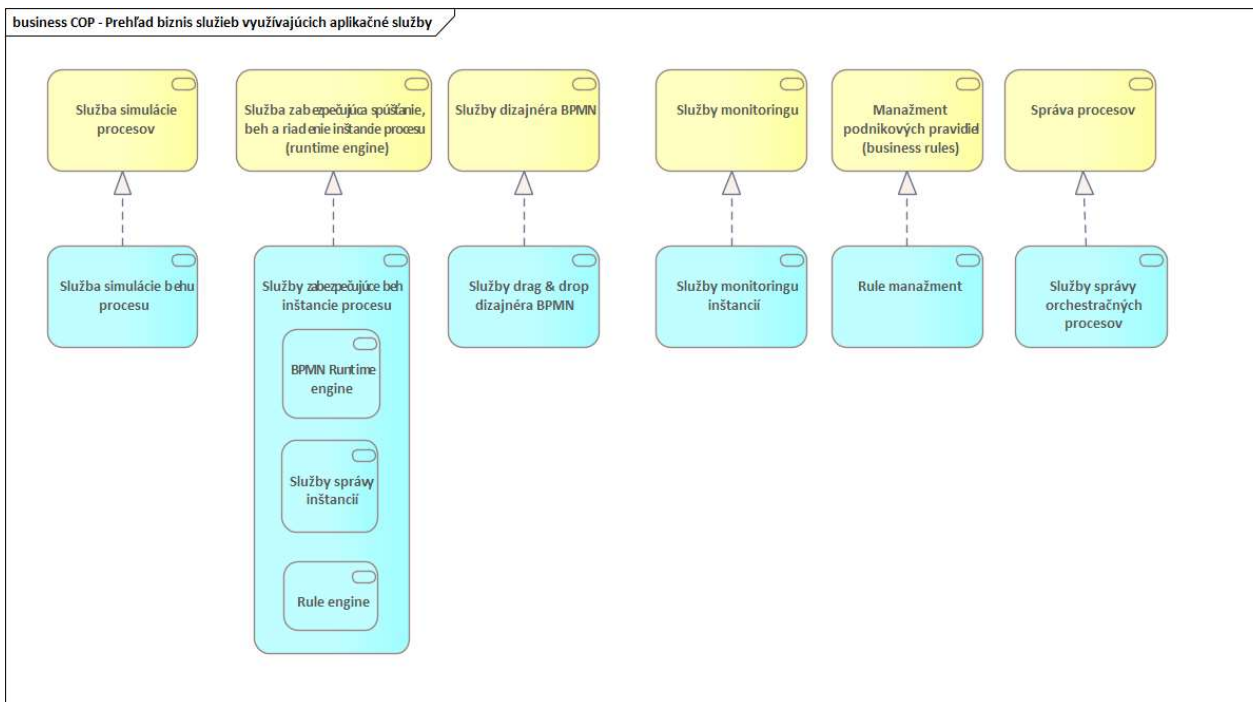




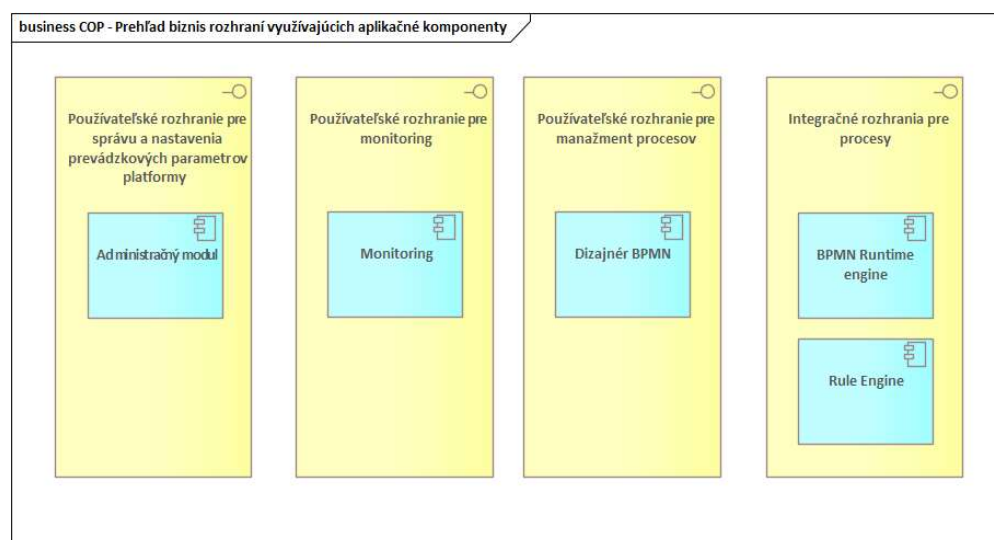
Obrázok 27 Modul CEP - Biznis služby modulu

#### 4.1.11. COP - CENTRÁLNA ORCHESTRAČNÁ PLATFORMA (COP)

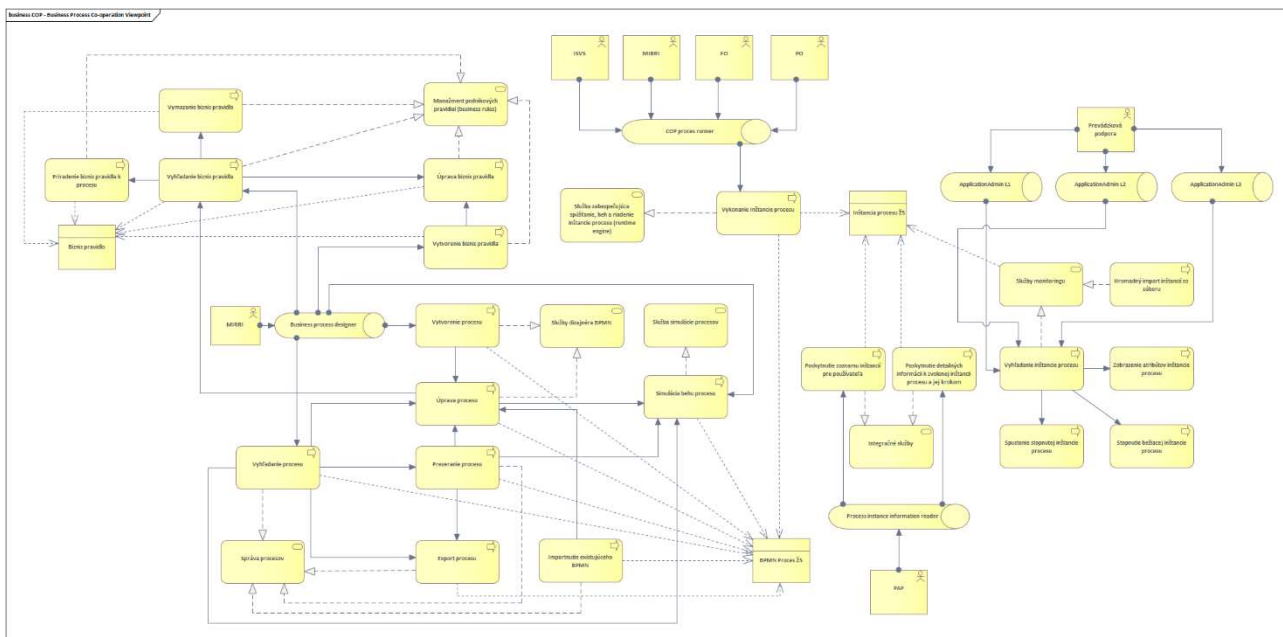
**Centrálna orchestračná platforma (COP)** – Konfigurovateľná platforma pre orchestráciu procesov pre životné situácie. Cieľom riešenia je umožniť modelovanie vybraných aktivít procesov životných situácií podľa štandardu BPMN 2.0 tak, aby následne bolo možné orchestrovať životné situácie. Orchestračná platforma pre životné situácie bude obsahovať procesy životných situácií, kde budú definované aktivity životnej situácie, ktoré vykonávajú jednotlivé OVM (resp. systémy OVM). Aktivity budú prepojené na elektronické služby štátu, na spoločné moduly ÚPVS, OVM. Súčasťou riešenia bude aj nástroj pre manažment pravidiel, podľa ktorých budú fungovať aktivity. Pravidlá bude možné prepojiť s aktivitami v procesoch. Procesy aj pravidlá pre ne bude možné modelovať a nastavovať priamo v riešení s použitím low code prístupu. Taktiež bude možný import a export v štandardizovaných formátoch, BPMN 2.0 pre procesy a DMN pre pravidlá. Namodelované procesy životných situácií budú nasadené v orchestračnej platforme, kde budú vytvárané jednotlivé inštancie procesov. Centrálna orchestračná platforma pre životné situácie na základe udalosti o stave riešenia životnej situácie (získanej z Centrálnej zbernice udalostí) aktualizuje stav riešenia príslušnej inštancie životnej situácie alebo zabezpečí aktiváciu ďalšieho komponentu (vykonanie ďalšej aktivity procesu životnej situácie).



Obrázok 28 Modul COP - Prehľad biznis služieb využívajúcich aplikačné služby



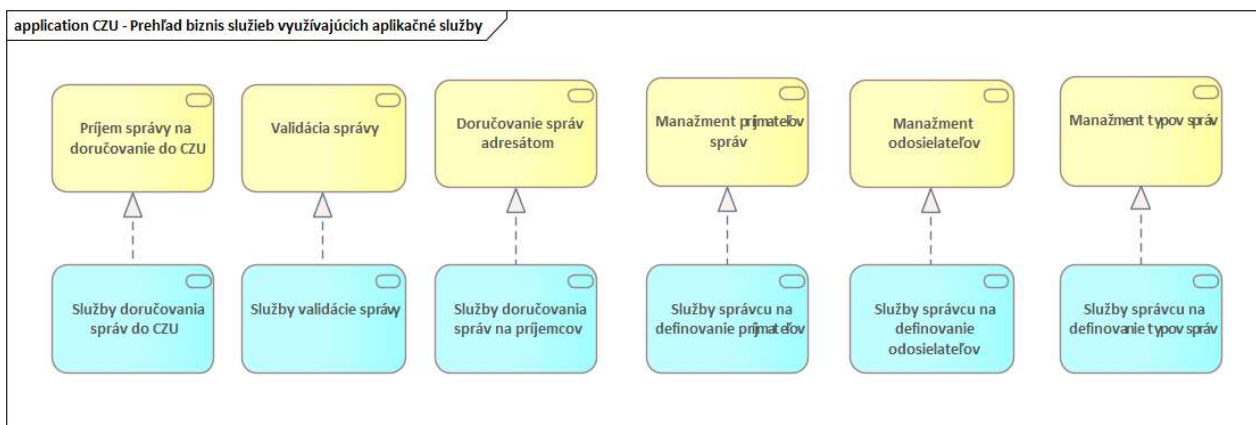
Obrázok 29 Modul COP - Prehľad biznis rozhraní využívajúcich aplikačné komponenty



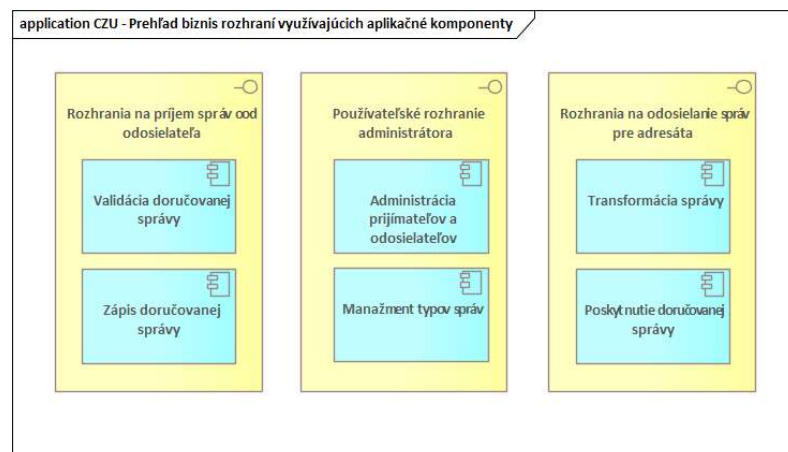
Obrázok 30 Modul COP - Biznis služby modulu

#### 4.1.12. CZU - Centrálna zbernica udalostí (CZU) - systém pre správu udalostí

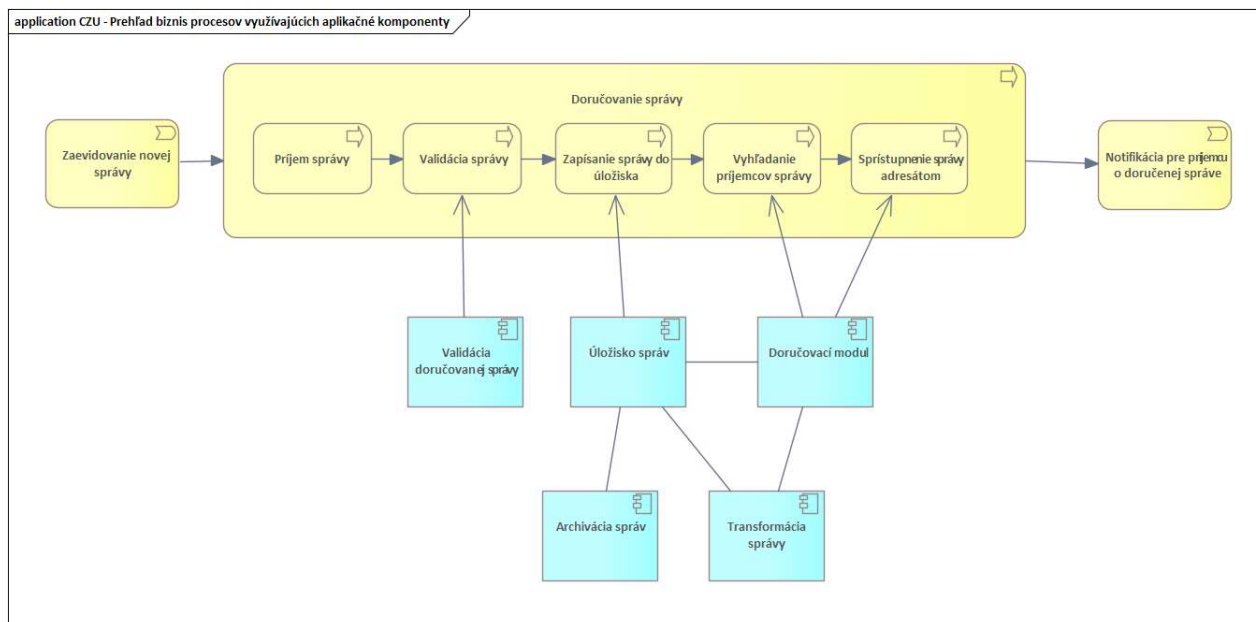
**Centrálna zbernica udalostí (CZU)** - Konfigurovateľný systém pre vytvorenie, nastavenie, prijímanie a sprístupňovanie udalostí procesov pre životné situácie. Cieľom riešenia je umožniť definovať udalosti o priebehu procesov životných situácií, prijímať takéto udalosti z jednotlivých OVM, vybraných subjektov a ÚPVŠ, a následne ich sprístupňovať pre iné OVM, vybrané subjekty alebo ÚPVŠ.



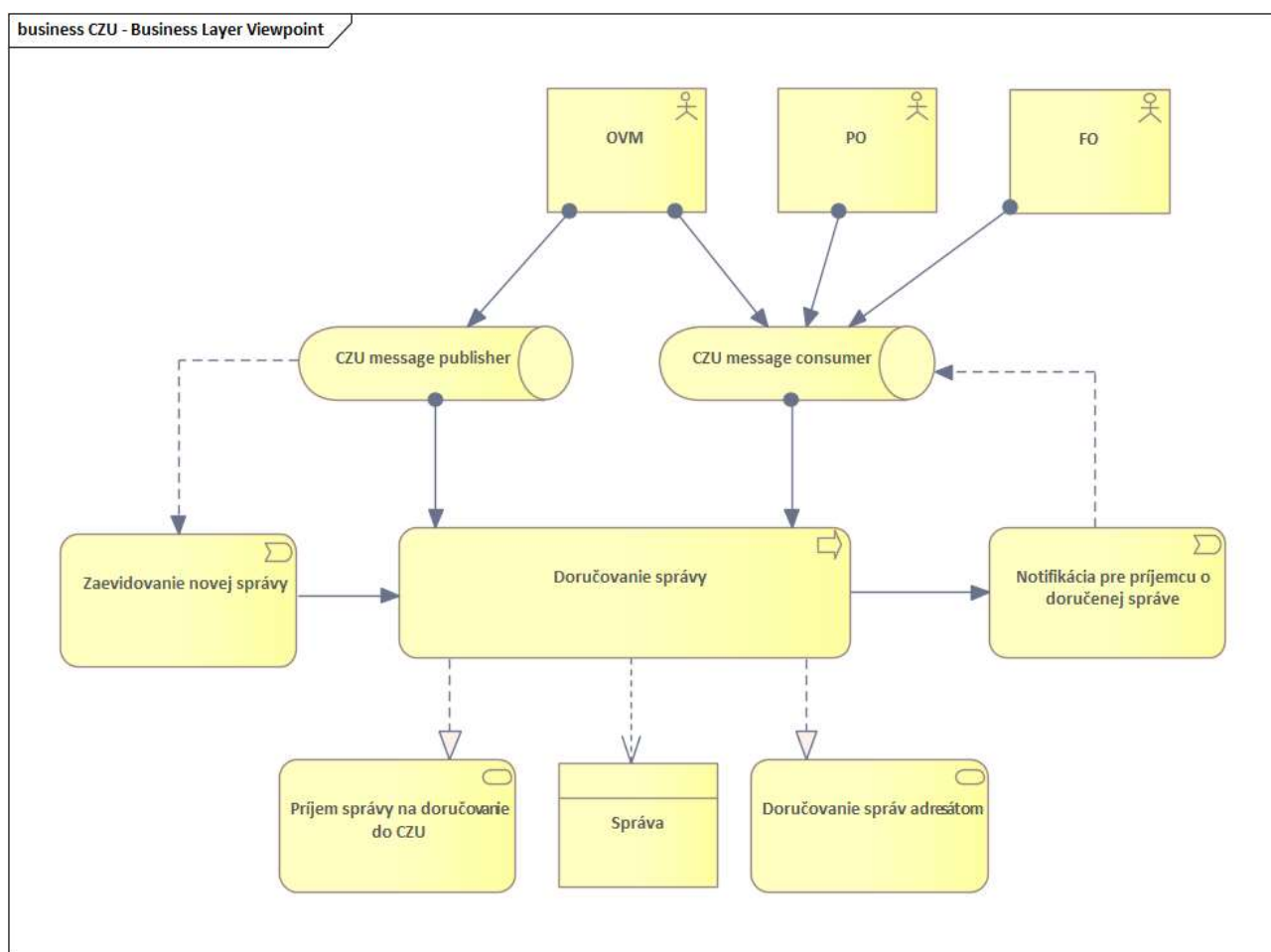
Obrázok 31 Modul CZU - Prehľad biznis služieb využívajúcich aplikačné služby



Obrázok 32 Modul CZU - Prehľad biznis rozhraní využívajúcich aplikačné komponenty



Obrázok 33 Modul CZU - Prehľad biznis procesov využívajúcich aplikačné komponenty



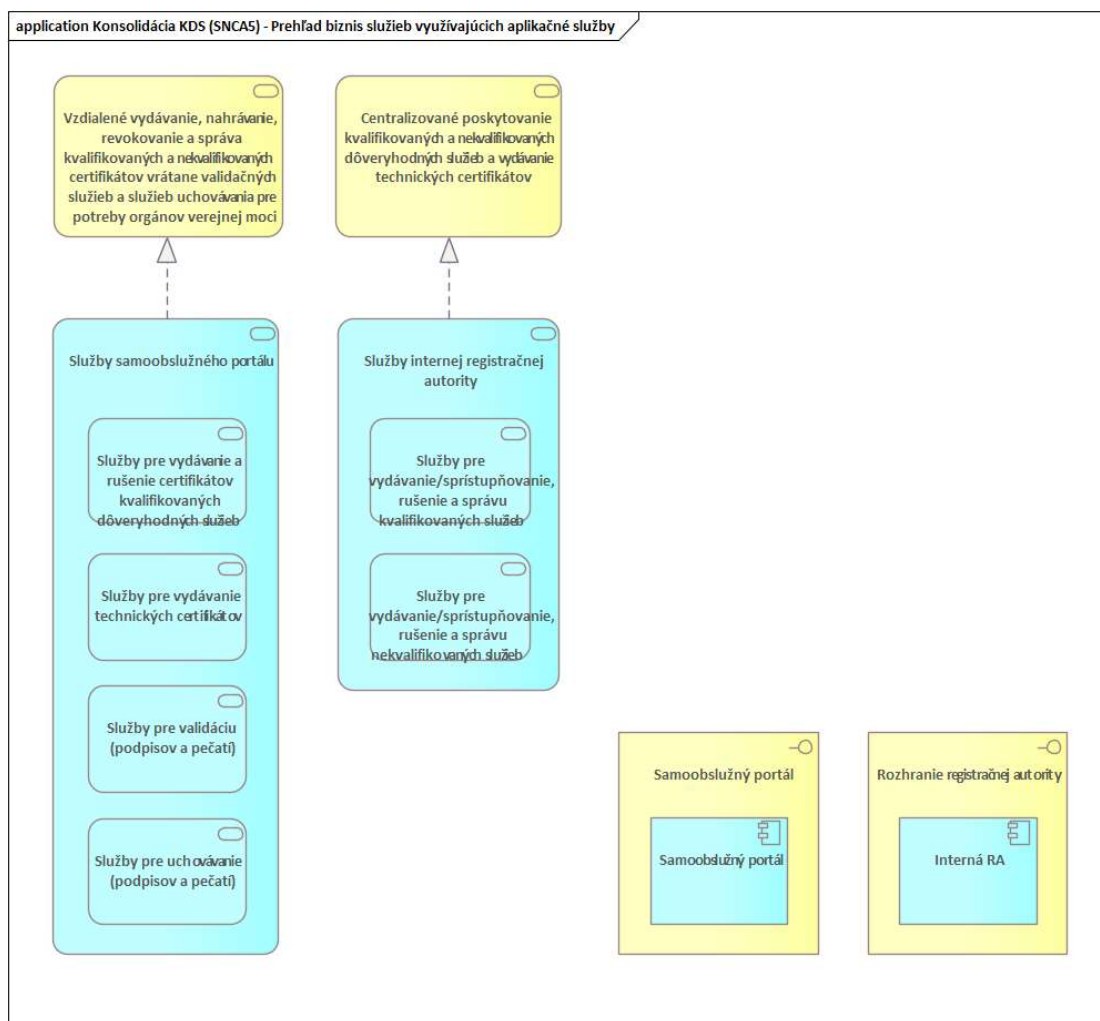
Obrázok 34 Modul CZU - Biznis architektúra modulu

#### 4.1.13. Konsolidácia certifikačných autorít

Zabezpečenie konsolidácie certifikačných autorít, ktorého cieľom je:

- Centralizácia **kvalifikovaných dôveryhodných služieb** a vytvorenie jednej kvalifikovanej dôveryhodnej certifikačnej autority v rámci informačných systémov:
  - Ústredný portál verejnej správy – NASES / MIRRI (existujúci remote sealing) – poskytovanie technickej časti vytvárania podpisu privátnym kľúčom z HSM serverov,
  - Slovenská národná certifikačná autorita – NASES (8 dôveryhodných služieb – vydávanie a overovanie kvalifikovaných mandátnych certifikátov, kvalifikovaných certifikátov pre elektronickú pečať, kvalifikovaných certifikátov pre autentifikáciu webových sídiel, vyhotovovanie kvalifikovaných časových pečiatok, validácia kvalifikovaných elektronických podpisov a pečatí, uchovávanie kvalifikovaných elektronických podpisov a pečatí),
- Centralizácia poskytovania **technických certifikátov** pre potreby štátu a vytvorenie jednej dôveryhodnej certifikačnej autority pre ich vydávanie (aktuálne si každé OVM stavia vlastnú certifikačnú autoritu na tento účel).
- Zavedenie **nových dôveryhodných služieb** pre zatraktívnenie a uľahčenie elektronickej komunikácie pre občanov a podnikateľov s orgánmi verejnej moci prostredníctvom služby vzdialeného podpisovania (Remote signing) a pečatenia (Remote sealing).
- Vytvorenie **samoobslužného portálu** pre vydávanie a administráciu kvalifikovaných dôveryhodných služieb a vydávanie technických certifikátov.

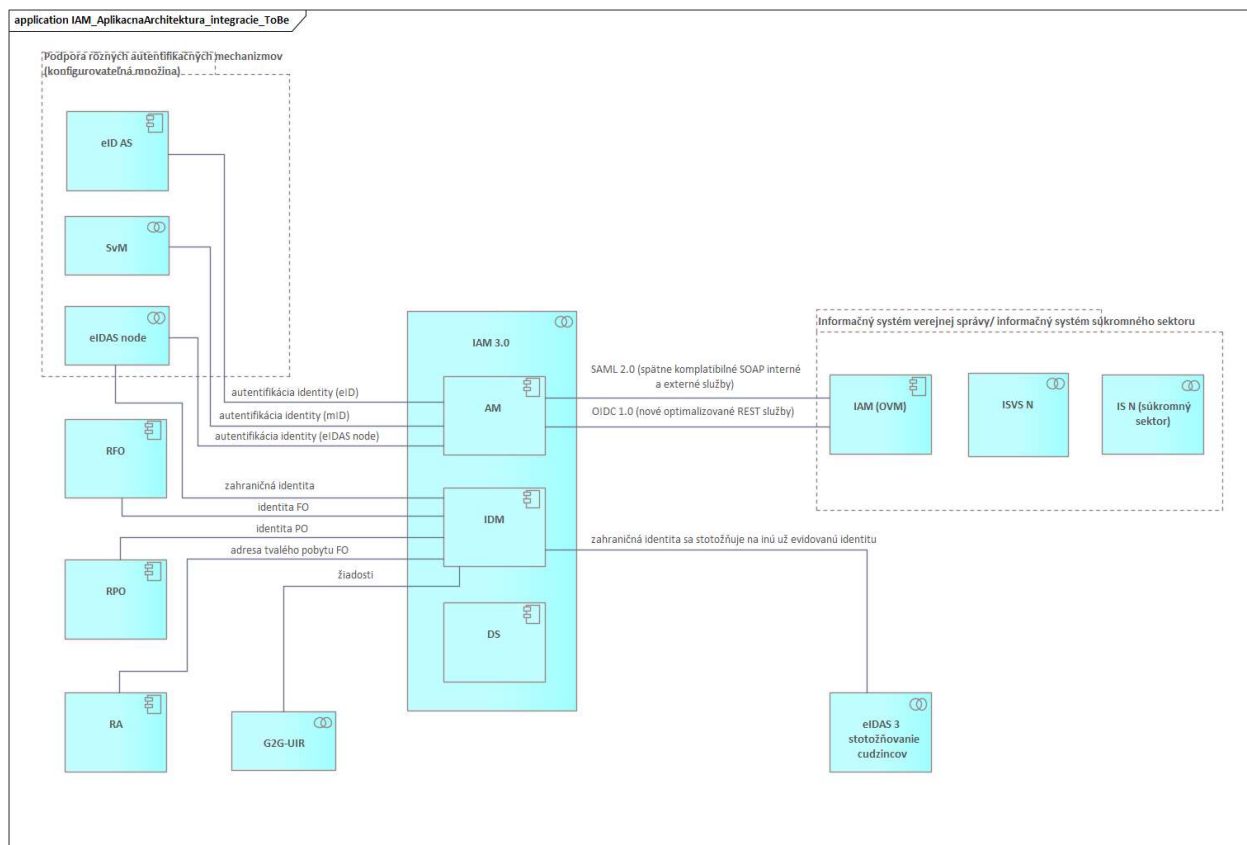
Riešenie musí byť postavené na moderných technológiách, musí zvládať požadované kapacity a zároveň mať dostatočnú rezervu aj pre ďalší predpokladaný nárast čerpania služieb a rozvoj.



Obrázok 35 Modul SNCA 5 - Prehľad biznis služieb využívajúcich aplikačné služby

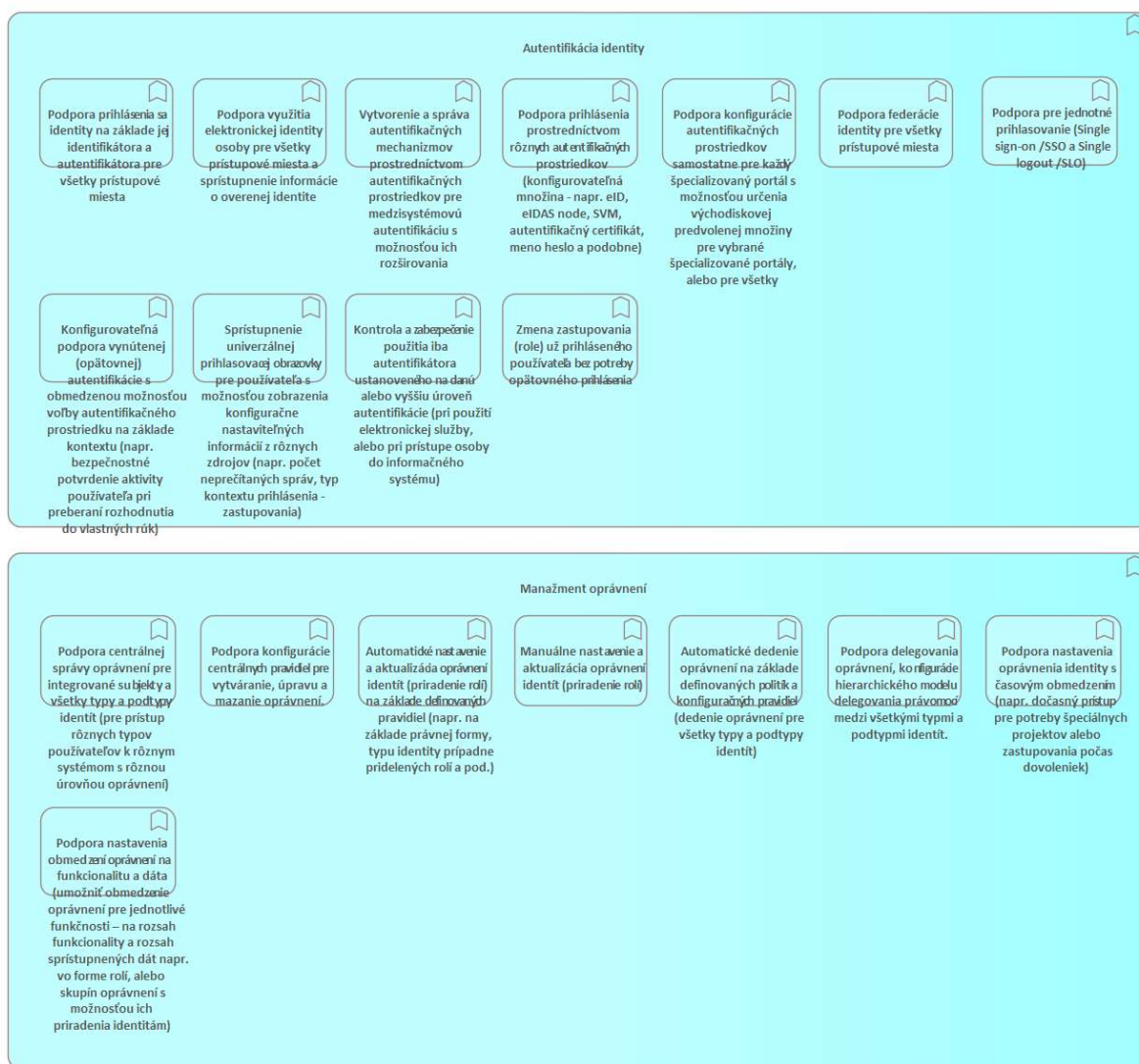




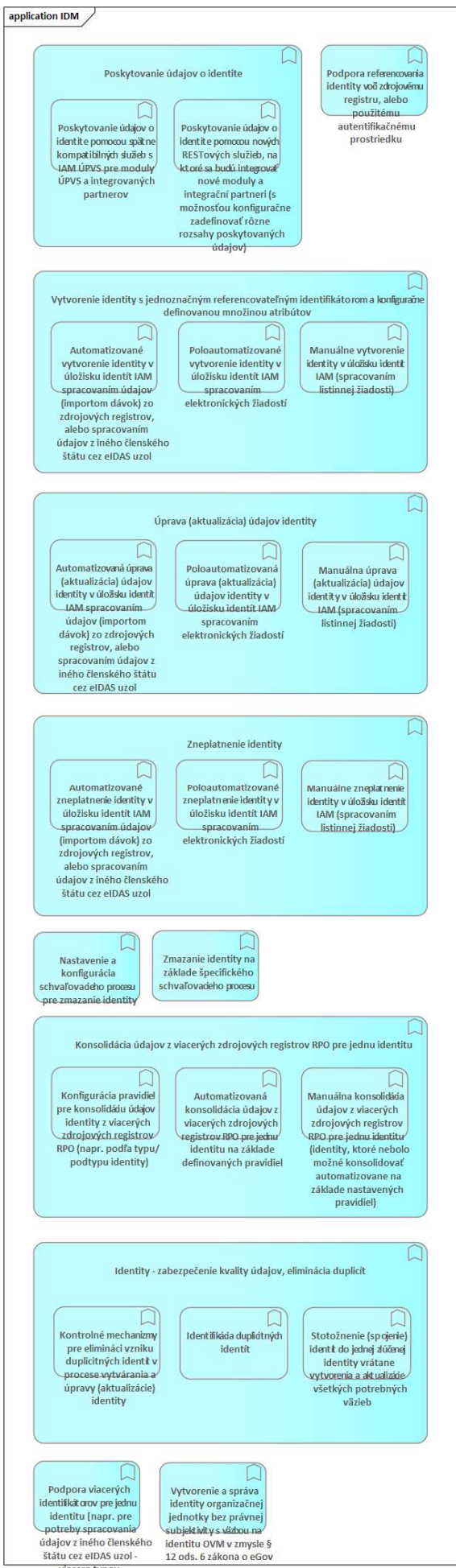


Obrázok 37 Modul IAM - Aplikačná architektúra modulu v TO BE stave



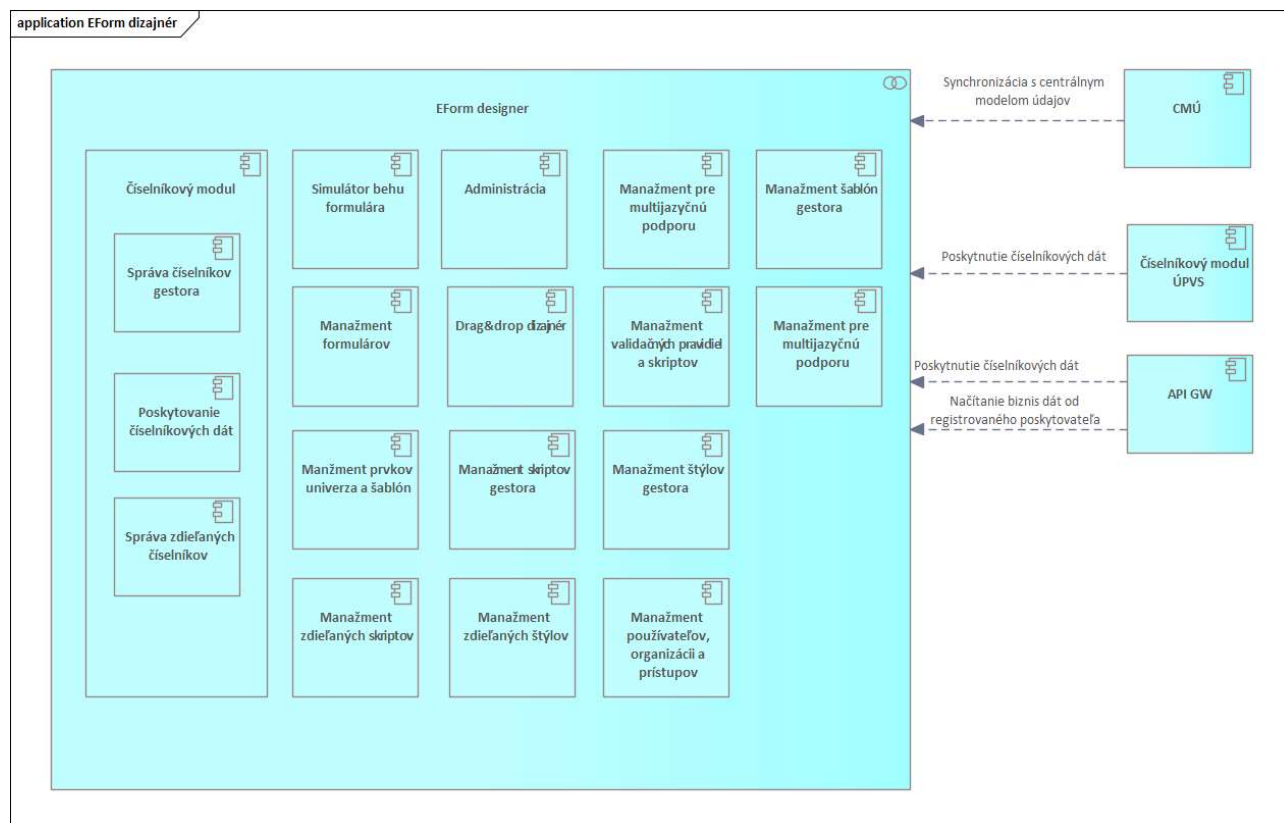


Obrázok 38 Modul IAM - Aplikačné funkcie modulu

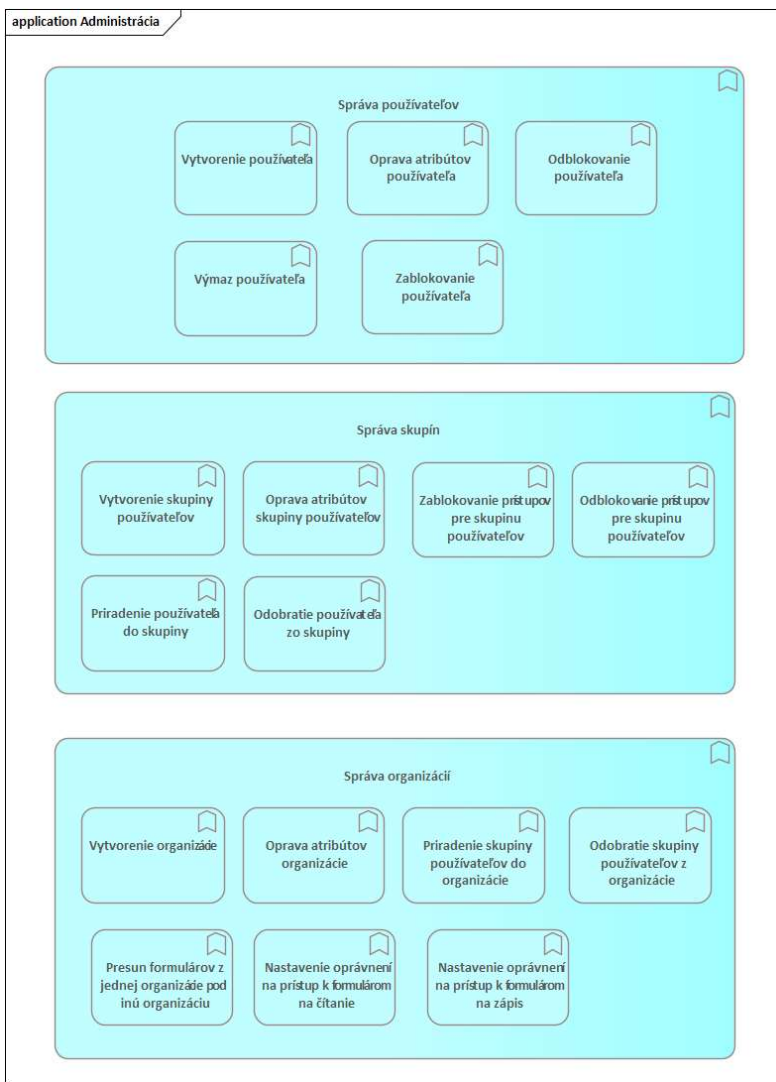


#### 4.3.2. eForm Dizajnér

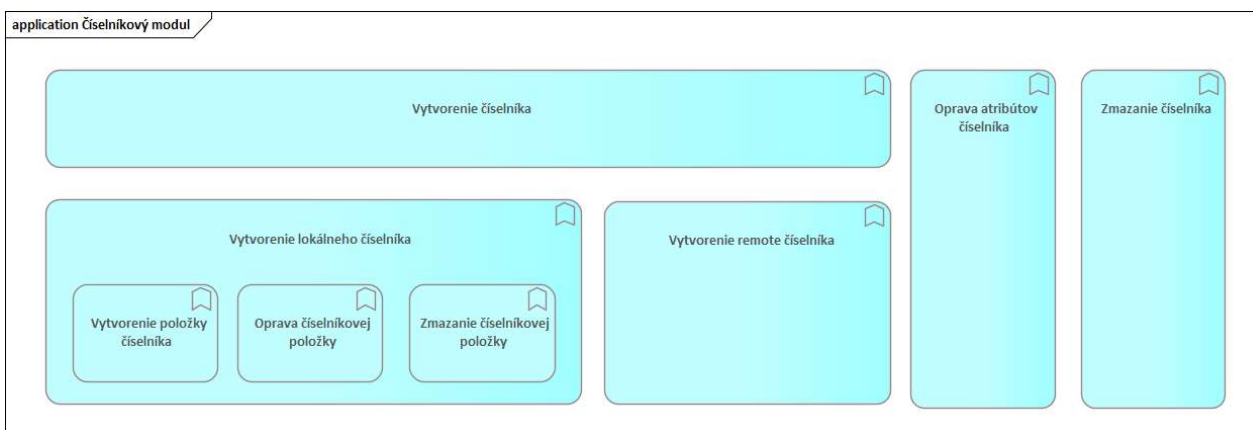
platforma, ktorá umožňuje používateľom vytvárať, upravovať a spravovať elektronické formuláre



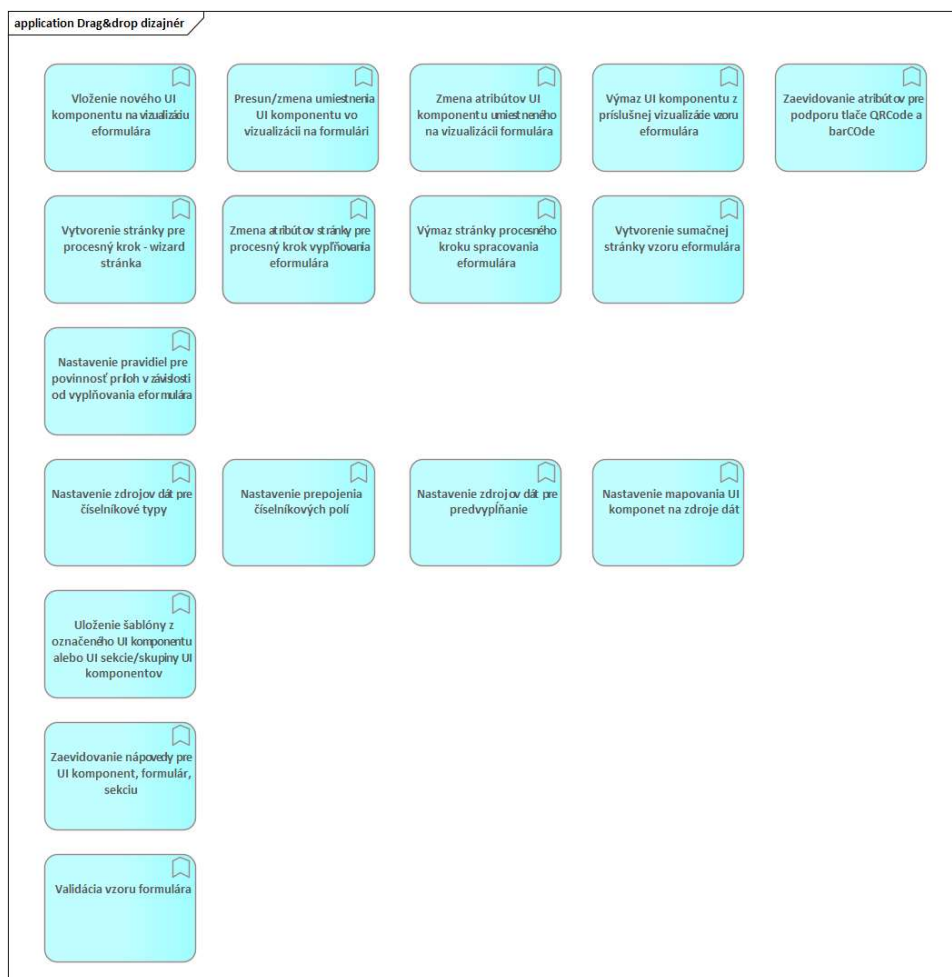
Obrázok 40 Modul eForm Dizajnér – Aplikačná architektúra modulu



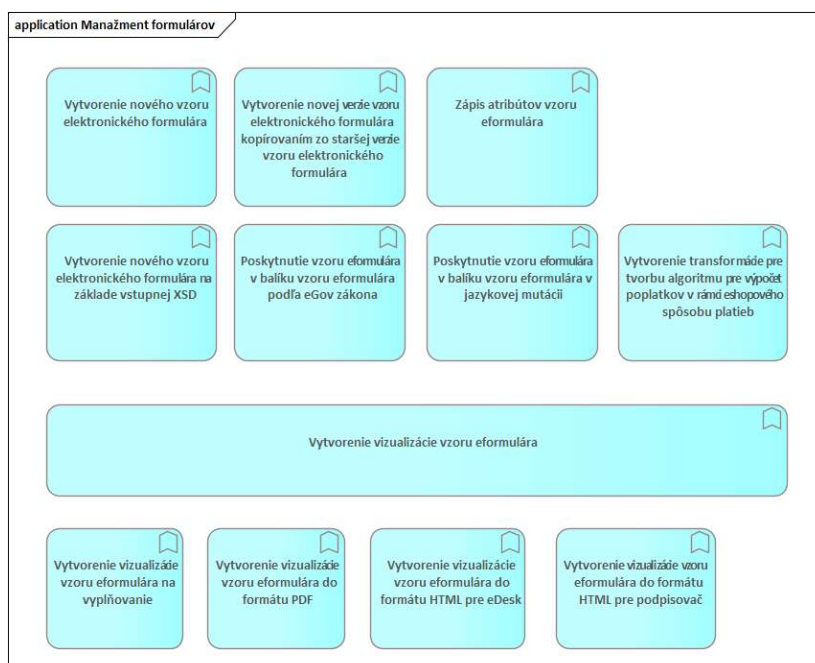
Obrázok 41 Modul eForm Dizajnér – Aplikačné funkcie pre Administráciu



Obrázok 42 Modul eForm Dizajnér - Číselníkový modul



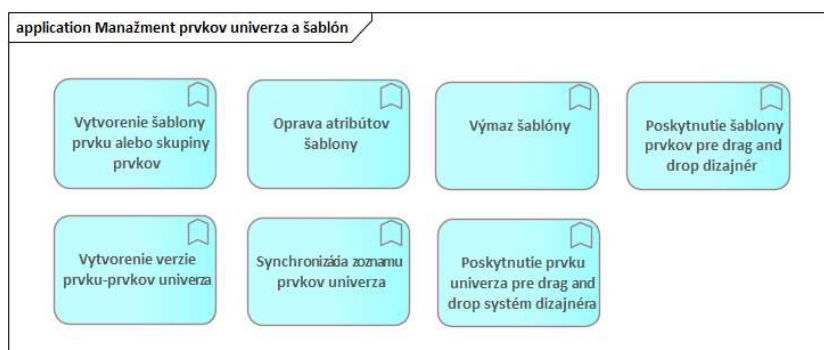
Obrázok 43 Modul eForm Dizajnér - Aplikačné funkcie pre Drag&Drop



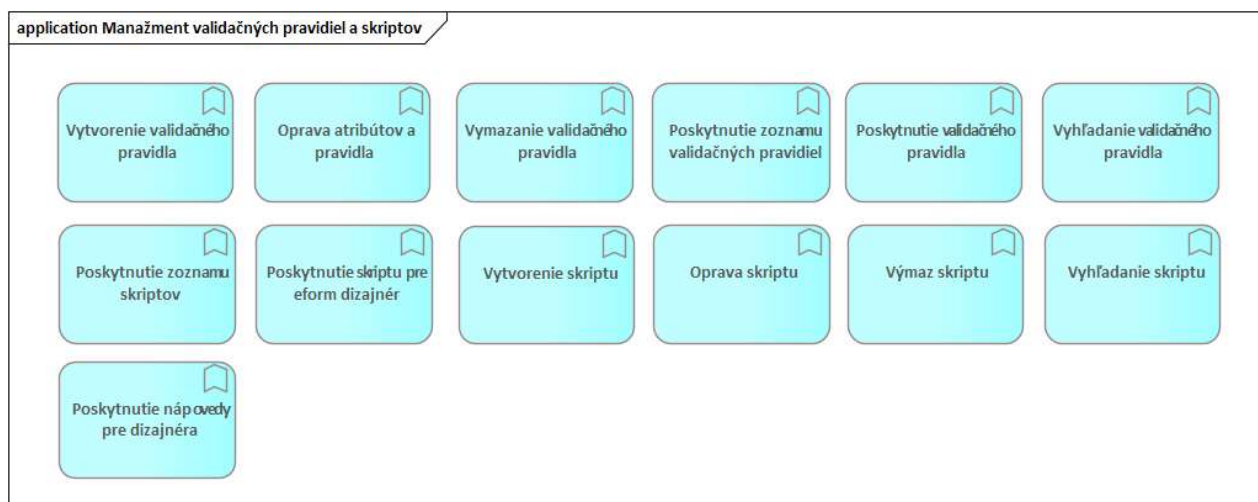
Obrázok 44 Modul eForm Dizajnér - Aplikačné funkcie pre Manažment formulárov



Obrázok 45 Modul eForm Dizajnér - Manažment pre multijazyčnú podporu



Obrázok 46 Modul eForm Dizajnér - Aplikačné funkcie pre Manažment prvkov univerza šablón

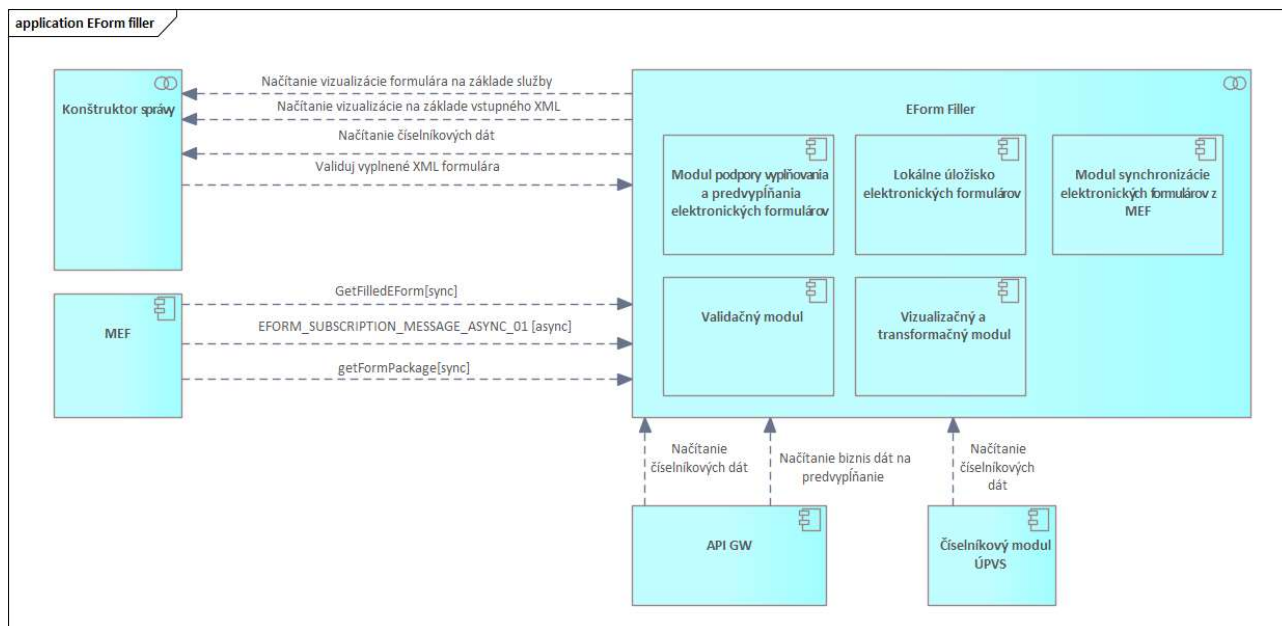


Obrázok 47 Modul eForm Dizajnér - Aplikačné funkcie pre Manažment validačných pravidiel a skriptov

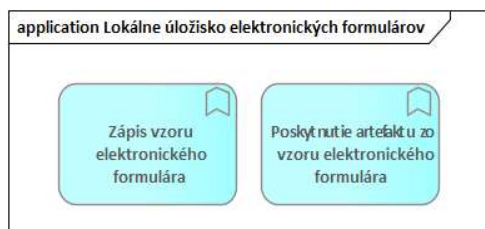
#### 4.3.3. Filler

nástroj na vyplňovanie elektronických formulárov





Obrázok 48 Modul Filler - Aplikačná architektúra modulu

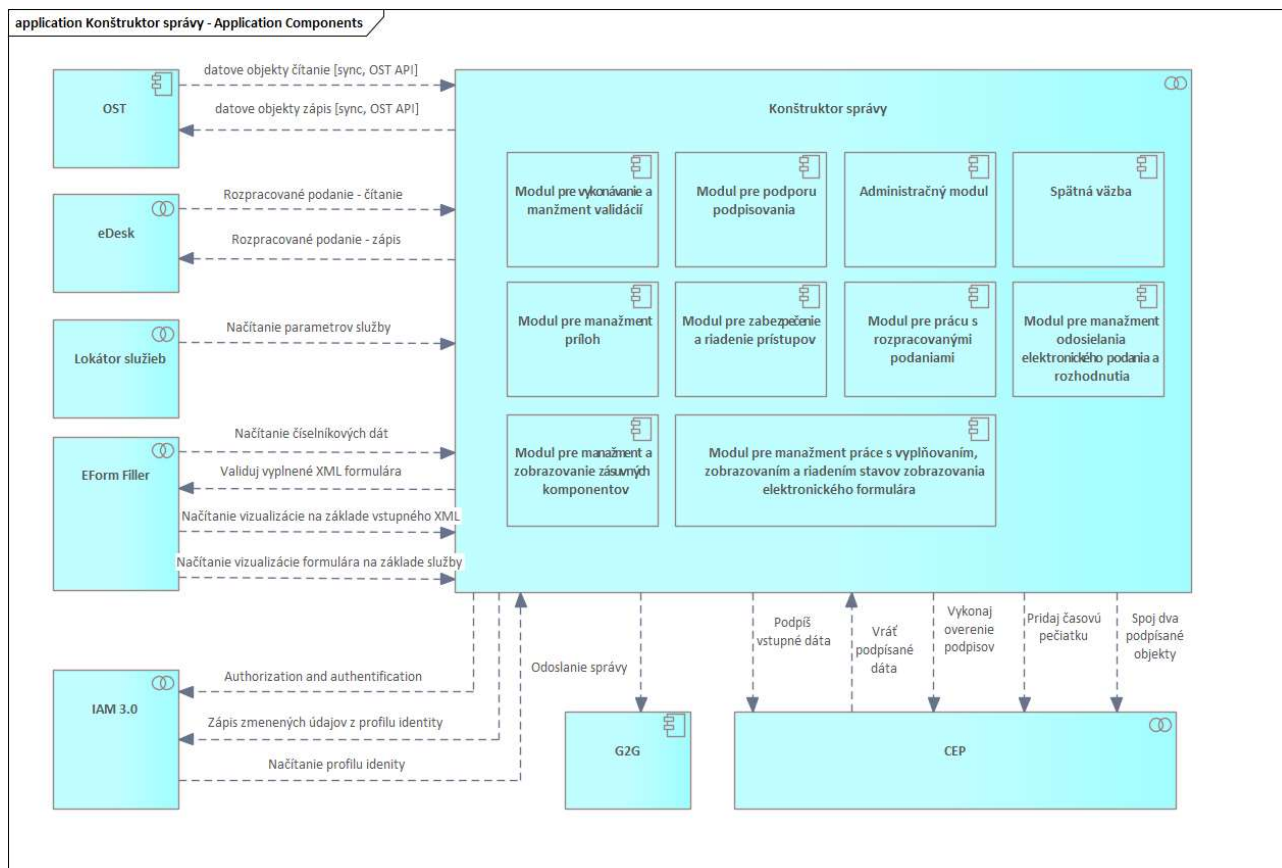


Obrázok 49 Modul Filler – Aplikačné funkcie pre Lokálne úložisko elektronických formulárov

#### 4.3.4. Konštruktor správ

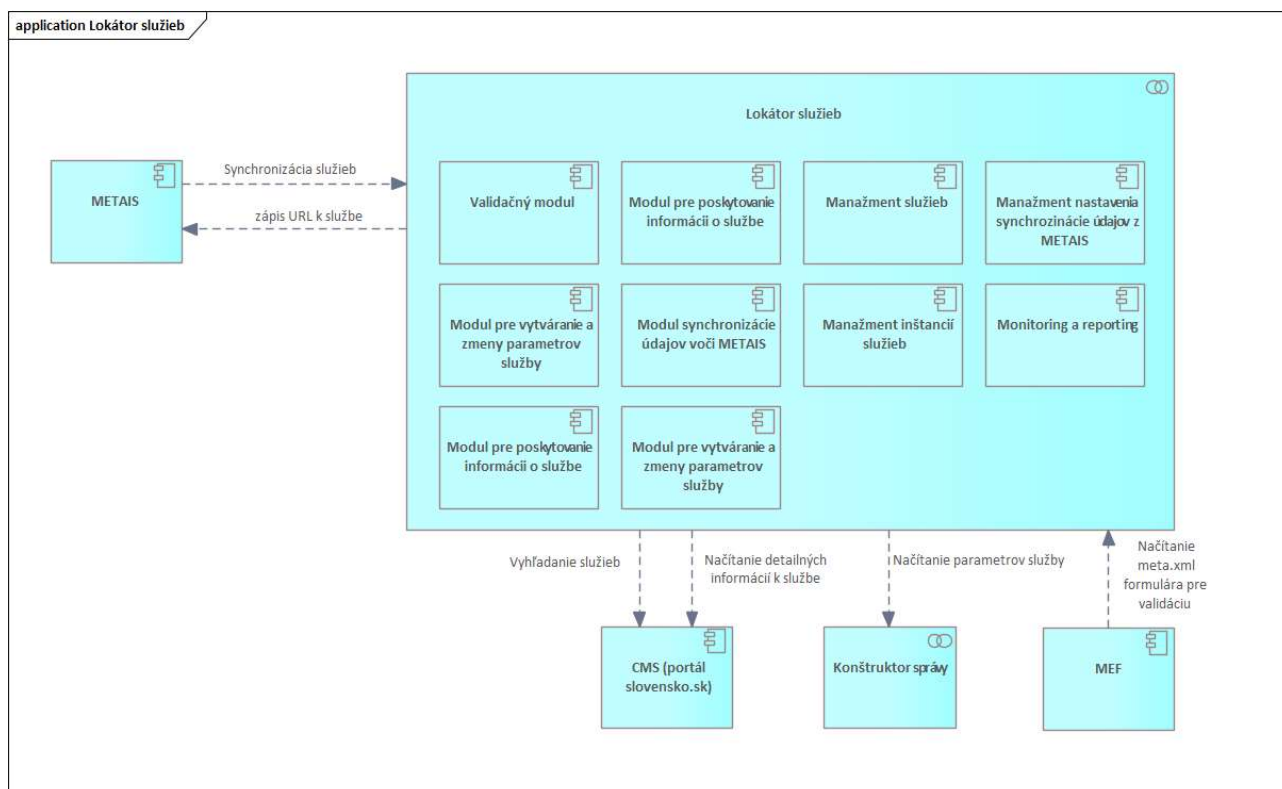
rozhranie slúžiace na vytvorenie elektronického podania





Obrázok 50 Konštruktor správ - Aplikačná architektúra modulu

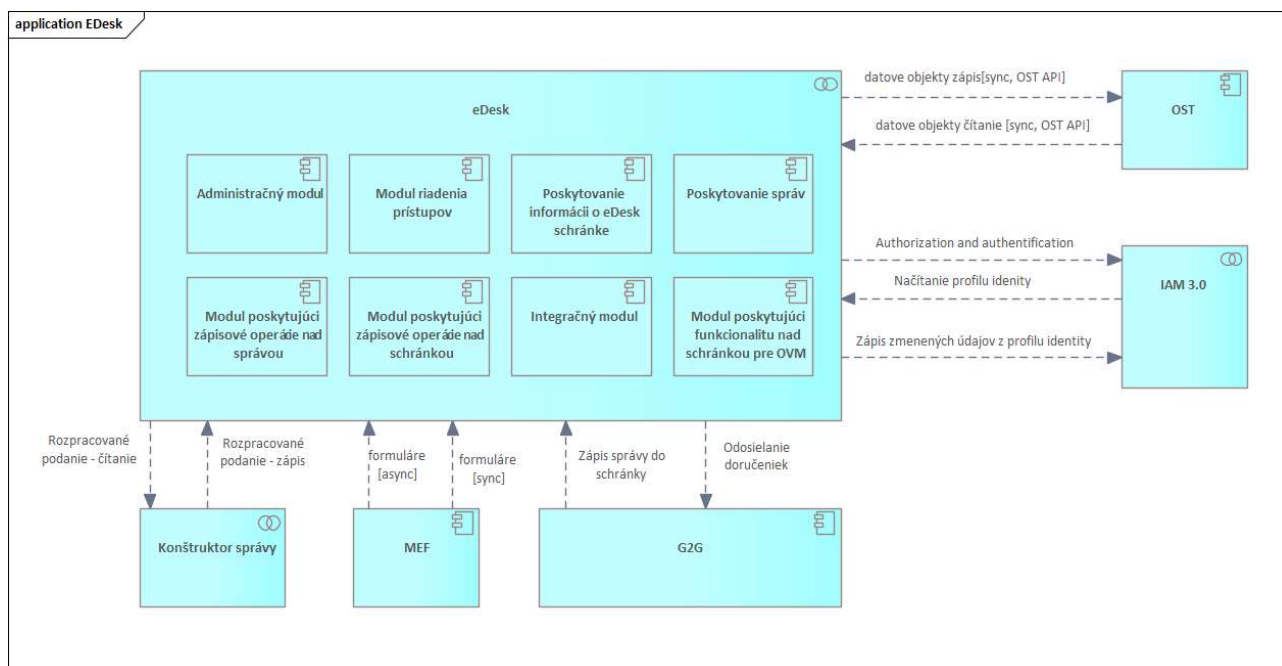
#### 4.3.5. Lokátor služieb a jeho funkcia



Obrázok 51 Lokátor služieb - Aplikačná architektúra modulu

#### 4.3.6. eDesk 2.0

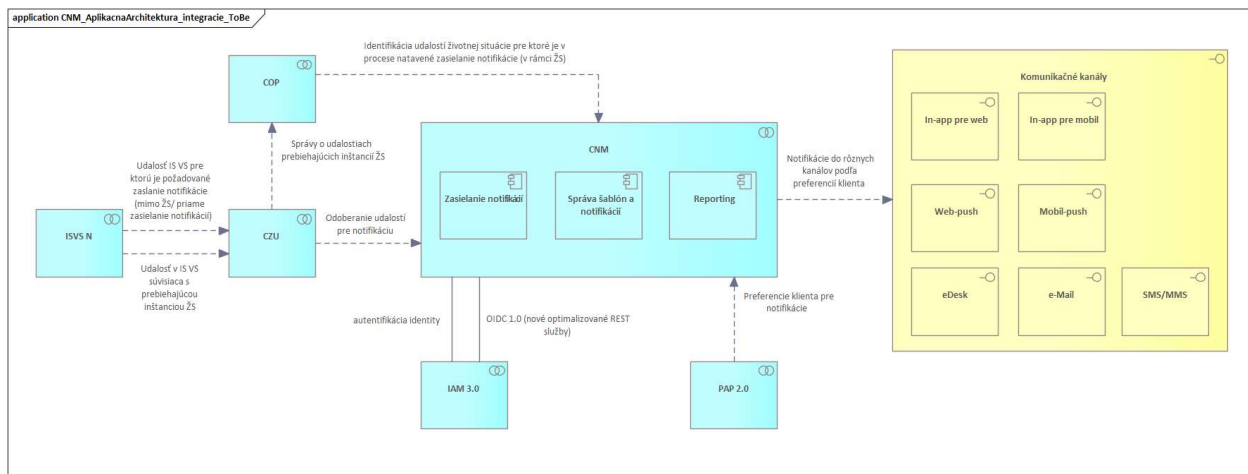
Elektronická schránka slúžiaca na občana, podnikateľa s verejnou správou



Obrázok 52 Modul eDesk - Aplikačná architektúra modulu

#### 4.3.7. Centrálny notifikačný modul (CNM)

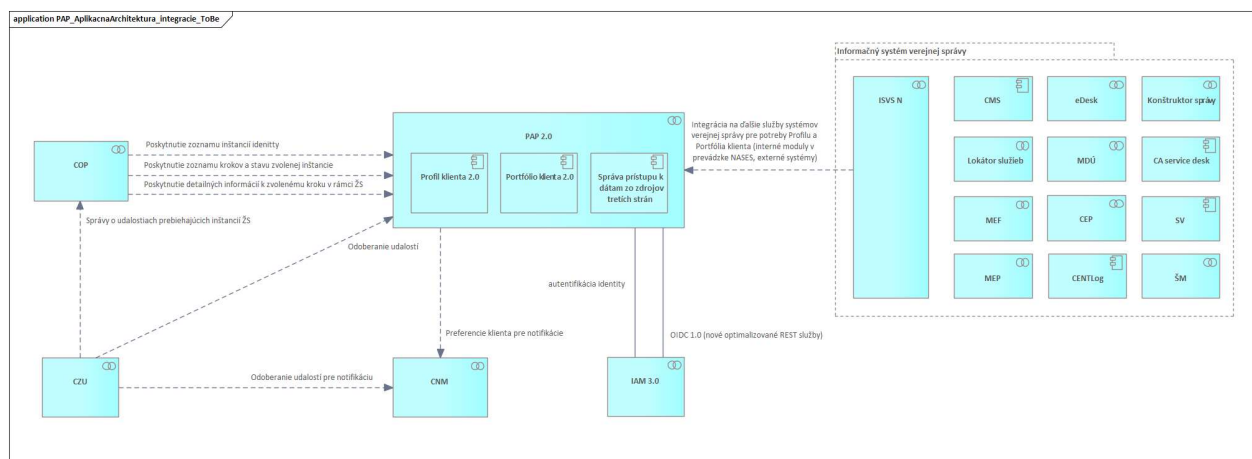
nástroj pre komunikácie štátu s občanom



Obrázok 53 Notifikačný modul - Aplikačná architektúra modulu

#### Portfólio a profil klienta (PAP2.0)

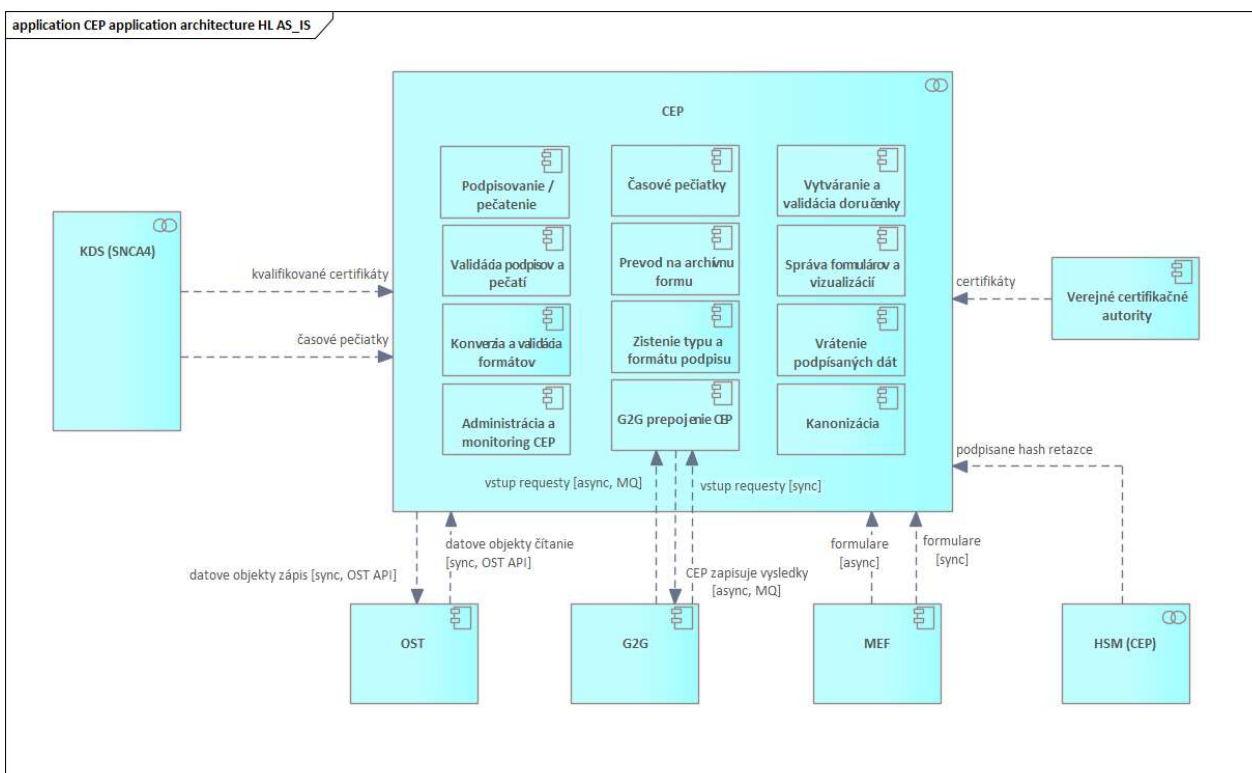
rozhranie pre občana a občana podnikateľa na personalizáciu



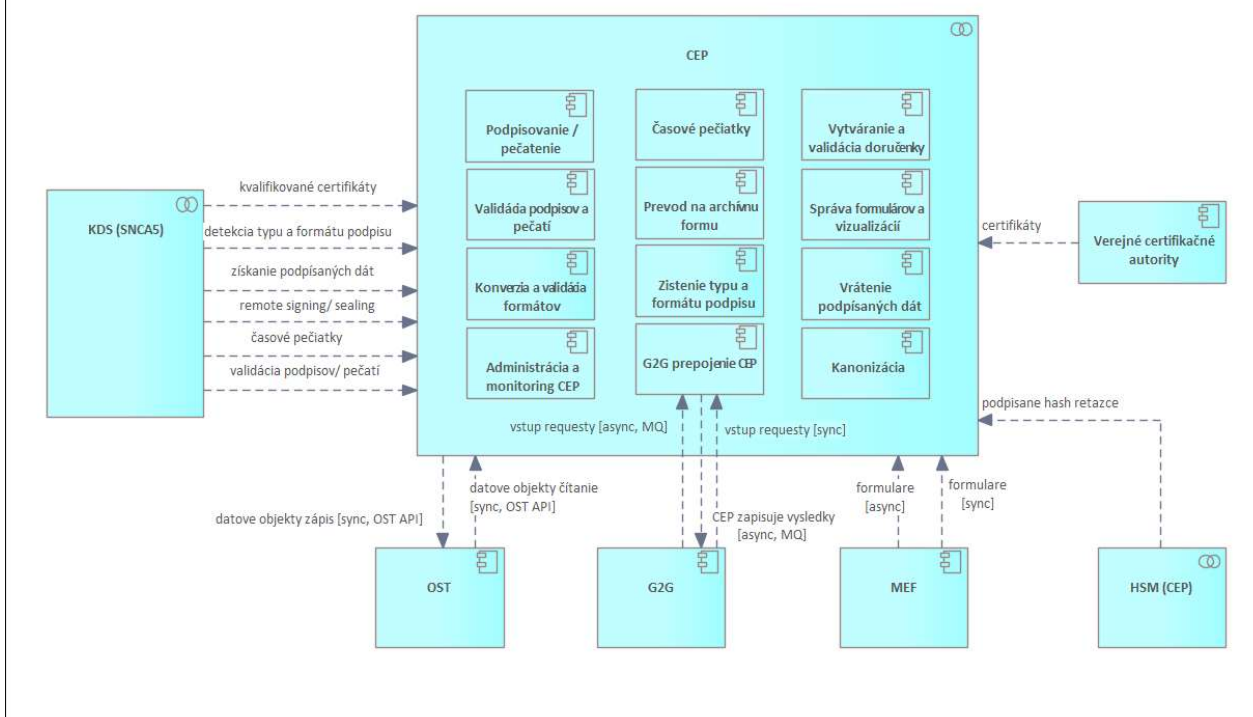
Obrázok 54 PaP - Aplikačná architektúra modulu

#### 4.3.8. Centrálna elektronická podateľňa (CEP)

práca s elektronickými podpismi a CÚD



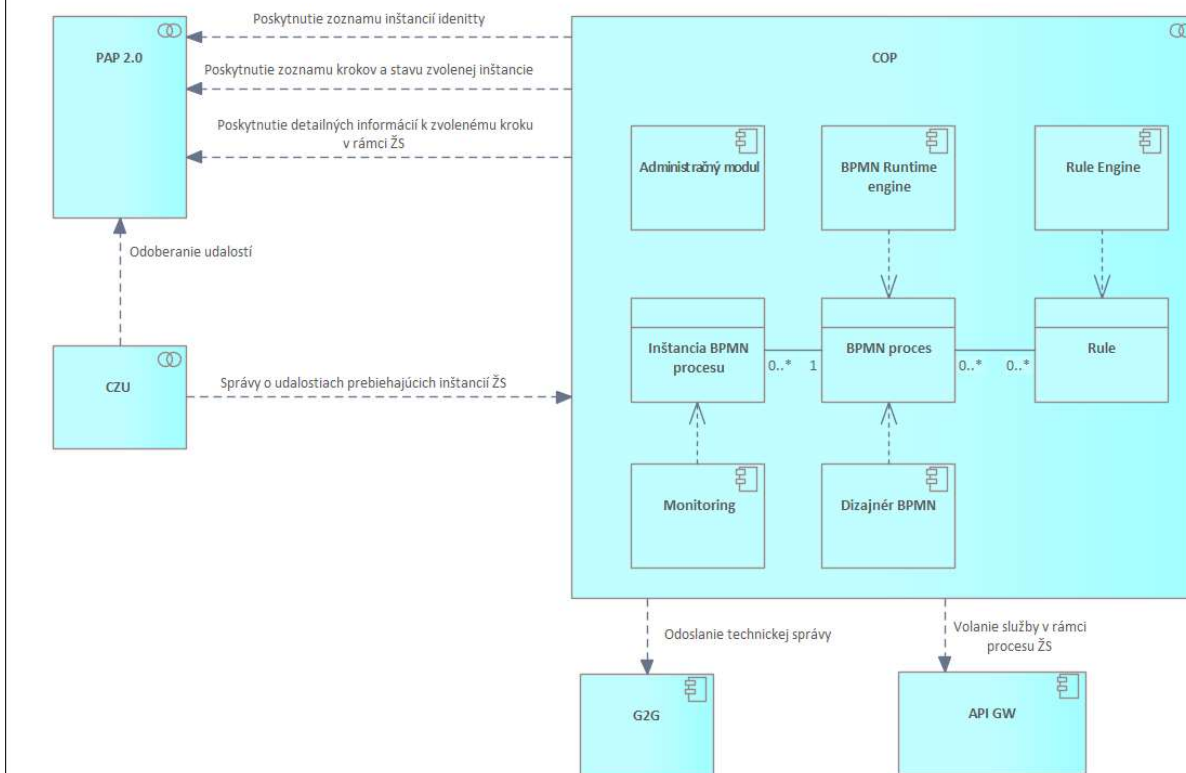
Obrázok 55 Modul CEP - Aplikačná architektúra modulu v AS IS stave



Obrázok 56 Modul CEP - Aplikačná architektúra modulu v TO BE stave

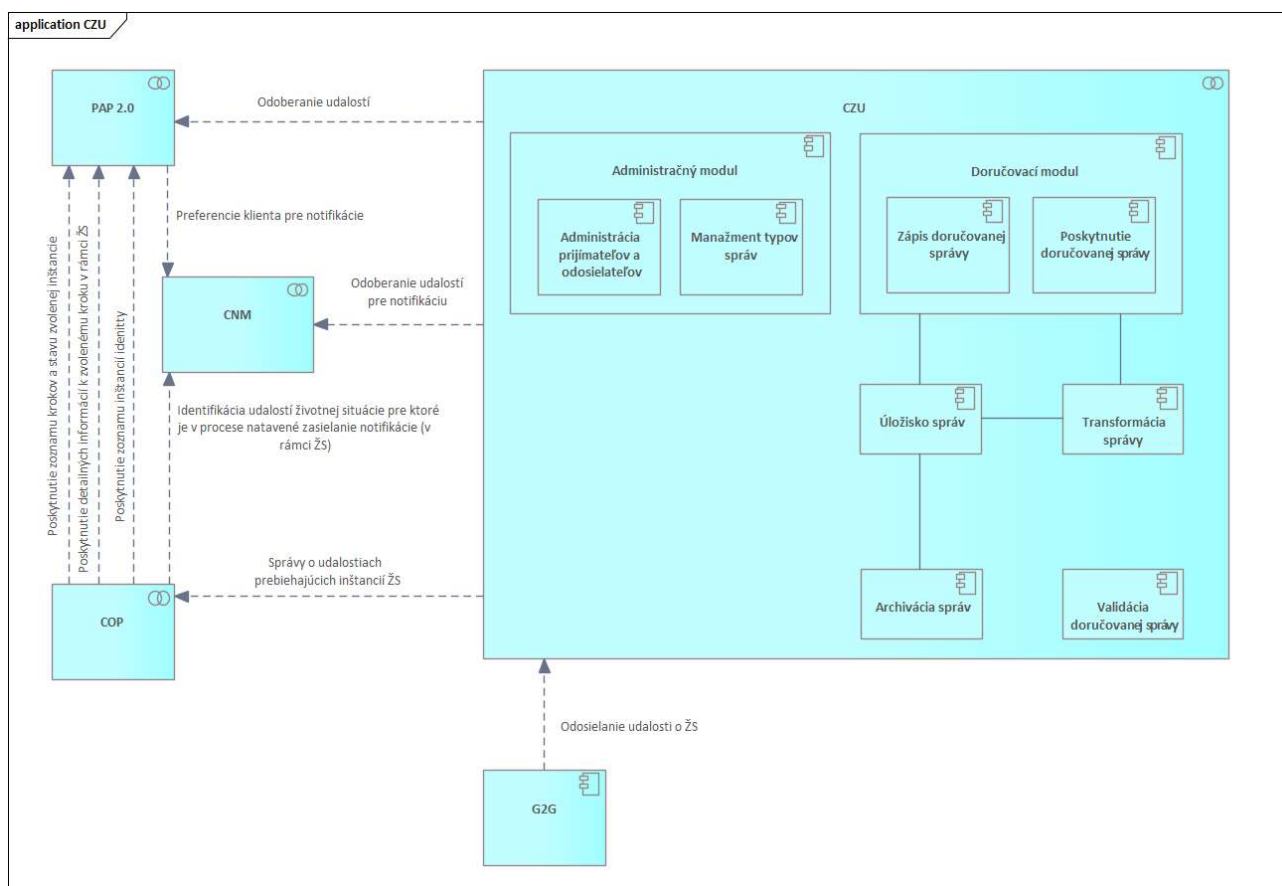
#### 4.3.9. Centrálna orchestračná platforma (COP)

platforma pre orchestráciu procesov pre životné situácie

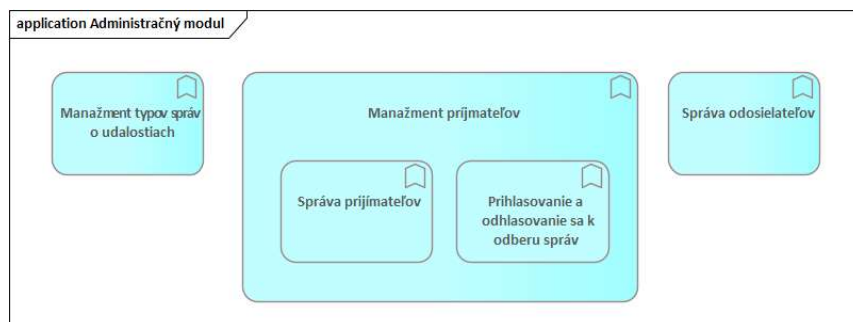


Obrázok 57 Modul COP - Aplikačná architektúra modulu

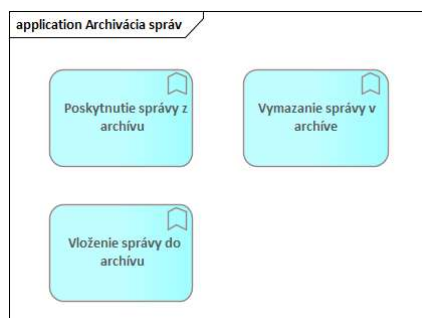
#### 4.3.10. Centrálna zbernica udalostí (CZU) systém pre správu udalostí procesov pre životné situácie



Obrázok 58 Modul CUZ - Aplikačná architektúra modulu



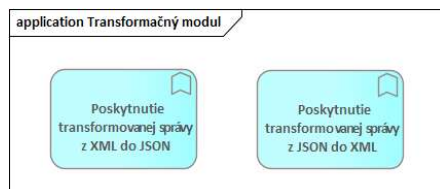
Obrázok 59 Modul CUZ - Aplikačné funkcie pre Administračný modul



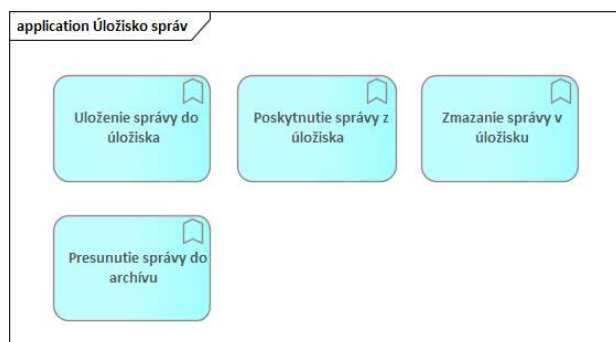
Obrázok 60 Modul CUZ - Aplikačné funkcie pre Archiváciu správ



Obrázok 61 Modul CUZ - Aplikačné funkcie pre Doručovací modul



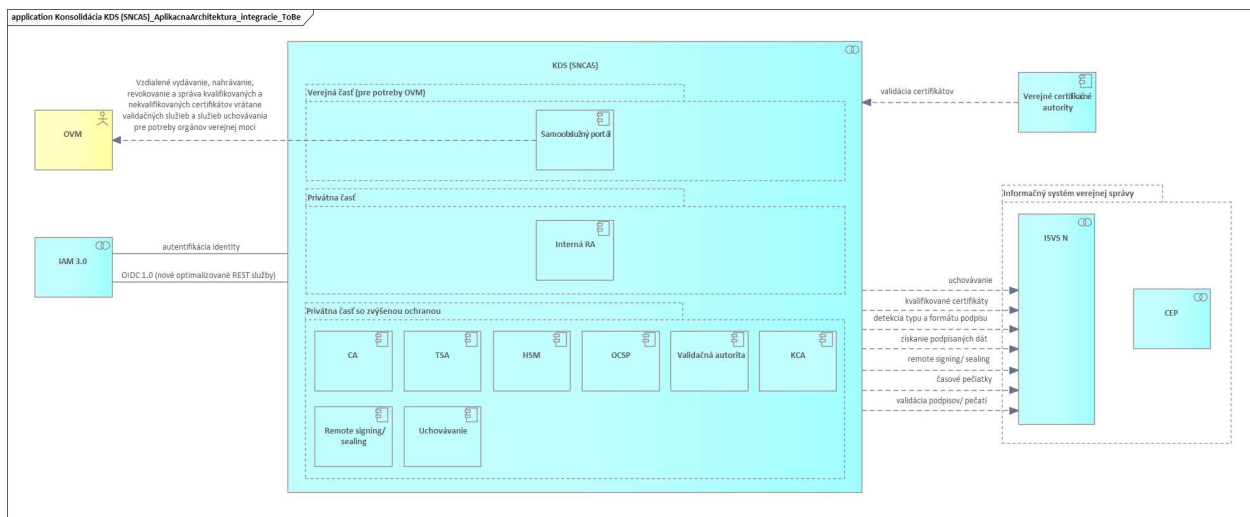
Obrázok 62 Modul CUZ - Aplikačné funkcie pre Transformačný modul



Obrázok 63 Modul CUZ - Aplikačné funkcie pre Úložisko správ

#### 4.3.11. Konsolidácia dôveryhodných služieb (KDS)

SNCA5 (Slovenská Národná Certifikačná Autorita)



Obrázok 64 Modul SNCA 5 - Aplikačná architektúra modulu

#### 4.4. Rozsah informačných systémov – AS IS

Podrobnosti sú uvedené v **Prílohe č.5 Zoznam IS v AS IS a TO BE.**

#### 4.5. Rozsah informačných systémov – TO BE

Podrobnosti sú uvedené v *Prílohe č.5 Zoznam IS v AS IS a TO BE*.

#### 4.6. Využívanie nadrezortných a spoločných ISVS – AS IS

Podrobnosti sú uvedené v *Prílohe č.5 Zoznam IS v AS IS a TO BE*.

#### 4.7. Prehľad plánovaných integrácií ISVS na nadrezortné ISVS – spoločné moduly podľa zákona č. 305/2013 e-Governmente – TO BE

Podrobnosti sú uvedené v *Prílohe č.5 Zoznam IS v AS IS a TO BE* a v Prílohe č.8 Závislosti na úrovni dopadov na externé systémy a ŽS

#### 4.8. Prehľad plánovaného využívania iných ISVS (integrácie) – TO BE

Podrobnosti sú uvedené v *Prílohe č.5 Zoznam IS v AS IS a TO BE*.

#### 4.9. Aplikačné služby pre realizáciu koncových služieb – TO BE

Podrobnosti sú uvedené v *Prílohe č.4 Zoznam KS a AS služieb*.

#### 4.10. Aplikačné služby na integráciu – TO BE

Podrobnosti sú uvedené v *Prílohe č.4 Zoznam KS a AS služieb*.

#### 4.11. Poskytovanie údajov z ISVS do IS CSRÚ – TO BE

N/A

#### 4.12. Konzumovanie údajov z IS CSRÚ – TO BE

Uvedte v tabuľke prehľad konzumovaných údajov z IS CSRÚ v TO BE stave. Súčasné dostupné objekty evidencie a údaje v IS CSRÚ sú uvedené v integračnom manuáli IS CSRÚ.

ID OE	Názov (konzumovaného) objektu evidencie	Kód a názov ISVS konzumujúceho OE z IS CSRÚ	Kód zdrojového ISVS v MetaIS
1	Register právnických osôb (RPO)		isvs_5836
2	Register fyzických osôb (RFO)		isvs_5836
3	Register adries (RA)		isvs_5836
4	Číselníky		isvs_5836

### 5. DÁTOVÁ VRSTVA

Kapitola popisuje dátovú architektúru jednotlivých modulov, ktoré sú predmetom projektu „Modernizácia Platformy pre rozvoj a riešenie prioritných životných situácií“.

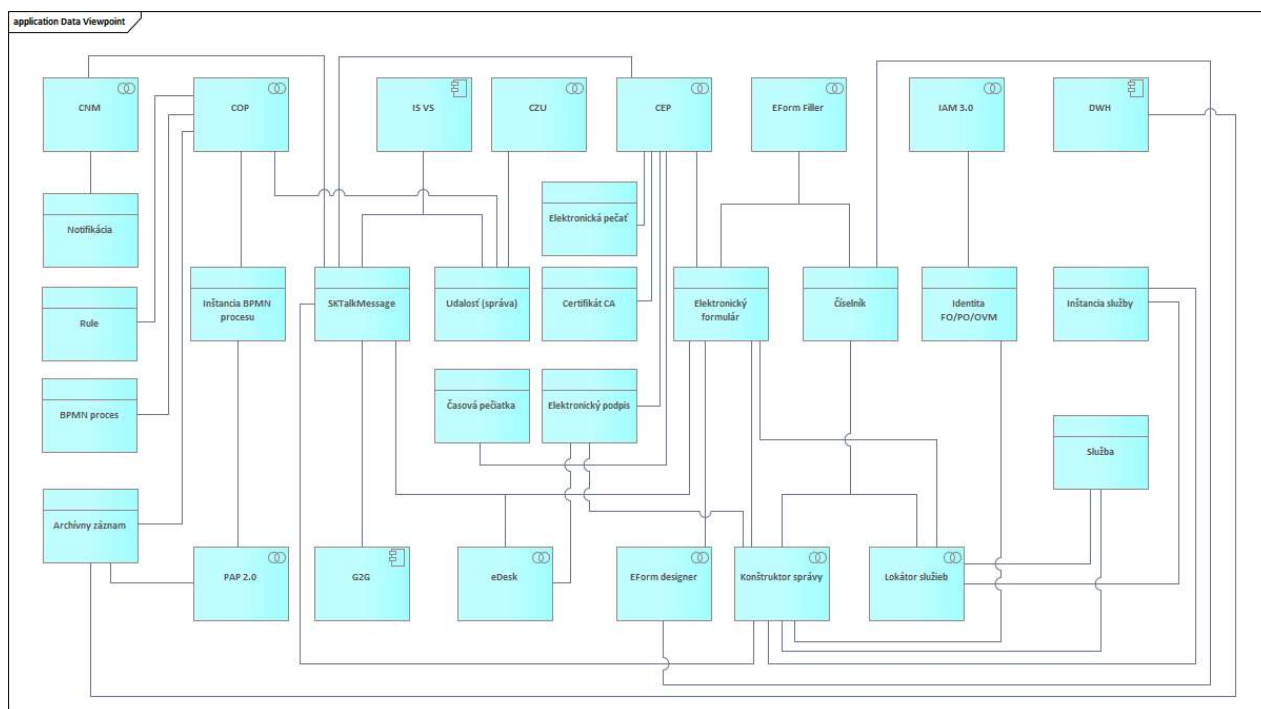
#### 5.1. Dátový rozsah projektu - Prehľad objektov evidencie - TO BE



Realizovaný projekt bude evidovať a využívať v rámci jednotlivých modulov množinu dátových objektov. Medzi tieto objekty patria objekty zabezpečujúcu spätnú kompatibilitu so súčasne prevádzkovaným riešením a nevyhnutnosťou vzájomnej integrácie medzi prevádzkovaným a novým riešením, ako aj nové dátové objekty, ktoré vzniknú v rámci nových modulov. Jedná sa najmä typy dátových objektov uvedené v nasledovnej tabuľke:

Názov	Popis
Notifikácia	Notifikácia generovaná modulom CNM
Rule	Objekt popisujúci pravidlo v rámci rule engine a BPMN procesu
BPMN proces	Definícia procesu v COP
Archívny záznam	Dátový objekt, ktorý je z modulu zasielaný do DWH a je ďalej spracovávaný v rámci DWH
Inštancia BPMN procesu	Konkrétna inštancia procesu životnej situácie v rámci modulu COP
SKTalkMessage	Kontajner pre správy doručované prostredníctvom G2G modulu
Udalosť	Vzniknutá udalosť v rámci životnej situácie zasielaná zo systémov vstupujúcich do danej životnej situácie prostredníctvom modulu CZU. Na základe udalosti sa riadi proces v COP
Elektronická pečať	Elektronická pečať používaná na podpisovanie službami CEP
Certifikát CA	Dátový objekt certifikát ktorý je potrebný k overovaniu elektronického podpisu
Časová pečiatka	Časová pečiatka používaná v rámci podpisovania službami CEP
Elektronický podpis	Objekt Elektronický podpis je používaný službami CEP
Elektronický formulár	Elektronický formulár a jeho jednotlivé artefakty sú používané v rámci tvorby elektronických podaní a rozhodnutí a sú používané množinou agend a modulov
Číselník	Dátový objekt číselník bude obsahovať základné atribúty číselníka ako aj hodnoty číselníkov. Číselníky budú jednotlivé moduly využívať na zabezpečenie konzistentnosti dát
Identita FO/PO/OVM	Údaje o identite
Služba	Údaje o službe
Správa	eDesk správa (SKTalk) je elektronická správa umožňujúca bezpečnú a právne záväznú komunikáciu medzi štátnymi inštitúciami a občanmi prostredníctvom portálu Slovensko.sk alebo iných špecializovaných portálov SK talk štandard v zmysle výnosu o štandardoch
Inštancia služby	Údaje o inštancii služby

Využívanie týchto dátových objektov je znázornené na nasledovnom obrázku.



Obrázok 65 Dátová vrstva – Aplikačná architektúra jednotlivých modulov

## 5.2. Analytické údaje

V rámci projektu a jednotlivých jeho modulov budú vznikať dáta, ktoré budú mať povahu analytických dát a tieto budú posielané do DWH. Nad DWH budú následne vznikať rôzne analytické prehľady a zostavy.

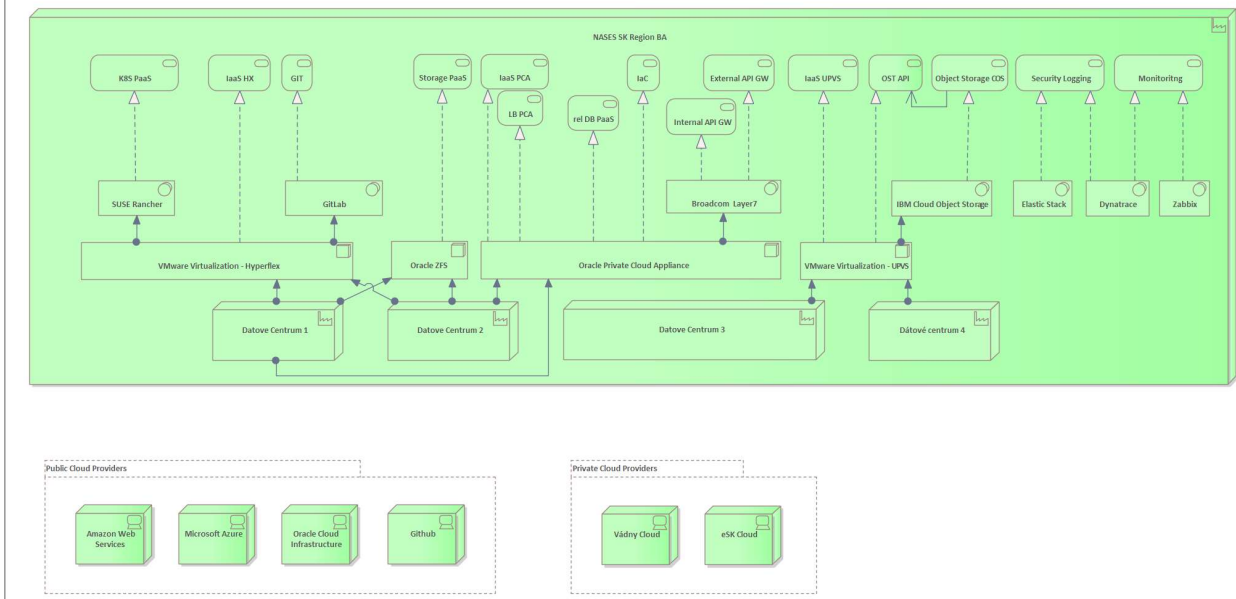
## 5.3. Referenčné údaje

V rámci projektu a jednotlivých jeho modulov nebudú vznikať referenčné dáta.

# 6. TECHNOLOGICKÁ VRSTVA

## 6.1. Prehľad technologického stavu - AS IS

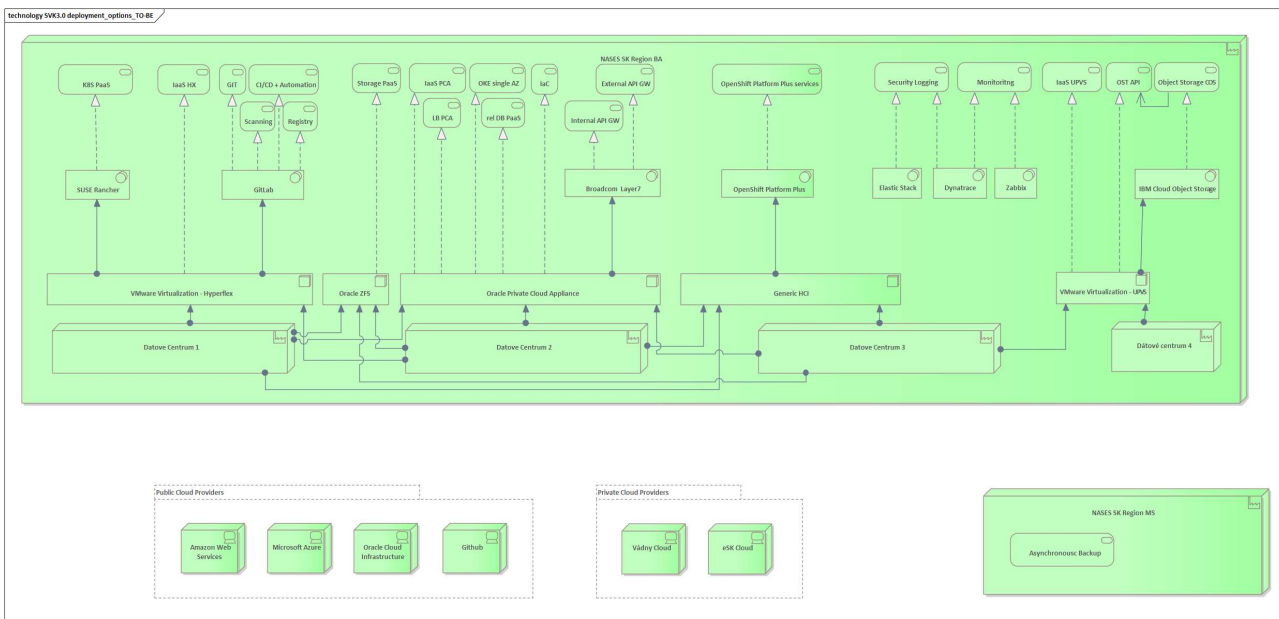
Kapitola popisuje model technologickej vrstvy AS IS stavu, používané výpočtové prostriedky, konfigurácie siete, problematické body, ktoré je potrebné projektom riešiť.



Obrázok 66 Technologické služby na nasadzovanie riešení AS IS (možnosti pre Release 1)

## 6.2. Návrh riešenia technologickej architektúry

Kapitola popisuje návrh a model architektúry technologickej vrstvy. NASES bude v rámci projektu využívať interné infraštruktúrne služby vlastných dátových centier.



Obrázok 67 Technologické služby na nasadzovanie riešení TO BE

### Opis technologických služieb

Súčasťou projektového zámeru je obnova a doplnenie robustnej, škálovateľnej a bezpečnej hybridnej cloudovej infraštruktúry, ktorá kombinuje privátny a verejný cloud s cieľom zabezpečiť širokú škálu technologických služieb. Cieľom je poskytovať výpočtové, úložné a orchestračné služby, spolu s monitoringom, bezpečnosťou a API správou, potrebné na podporu moderných aplikácií, ktoré využívajú kontajnerizáciu, automatizáciu a virtualizáciu. Tento návrh zohľadňuje nasadenie a správu Kubernetes klastrov, privátnych a verejných úložísk, CI/CD pipeline, a mnoho ďalších služieb.

Poradie kapitol jednotlivých služieb nie je definované preferenciou využitia, ale organizáciou modelov, tak aby bolo možné jednoduchšie sledovať opisy služieb vo vzťahu k ich poradiu na diagrame.

Voľba preferovaného scenára nasadenia konkrétneho riešenia bude súčasťou detailného návrhu riešenia, v ktorom z možností dostupných v danom čase vyberieme tú ktorá bude optimálna z pohľadu efektivity prevádzky, bezpečnosti a dlhodobej udržateľnosti riešenia.

#### 6.2.1. **K8S PaaS (Kubernetes Platform as a Service)**

Kubernetes PaaS poskytuje plnú podporu pre orchestráciu kontajnerizovaných aplikácií. Prostredníctvom platformy SUSE Rancher je umožnené nasadzovanie, škálovanie a správa Kubernetes klastrov. Táto služba poskytuje flexibilitu a škálovateľnosť pre aplikácie nasadzované v mikroservisnej architektúre.

#### 6.2.2. **IaaS HX**

Štandardné služby Infrastructure as a Service poskytované prostredím vCenter vo verzii 7. Tieto služby sú vo fáze postupného útlmu, preto je ich využitie podmienené schvaľovanou opodstatnenou výnimkou.

#### 6.2.3. **Gitlab – podpora DevSecOps procesov**

- **Verziónovanie kódu (Source Code Management - SCM)**  
Robustný systém na správu verziónovania kódu (Git), ktorý je základným stavebným prvkom DevOps procesov. Pomocou GitLabu môžu tímy spravovať zdrojový kód, sledovať zmeny a spolupracovať v reálnom čase.
- **CI/CD (Continuous Integration/Continuous Deployment)**  
Umožňuje automatizovať celý cyklus integrácie a nasadzovania aplikácií, od kompilácie a testovania až po nasadenie do produkčného prostredia. Všetky kroky sa vykonávajú automaticky pri každom „push“ kódu do repozitára, čo skracuje čas nasadenia a zvyšuje kvalitu.
- **Bezpečnostné kontroly (Security Scanning a DevSecOps Integrácia)**  
Integruje nástroje pre bezpečnostné kontroly v rámci CI/CD pipelines, čo znamená, že bezpečnosť je neoddeliteľnou súčasťou celého vývojového cyklu. Toto zahŕňa rôzne typy skenovania zamerané na detekciu bezpečnostných zraniteľností a compliance.
- **Automatizácia (GitLab Runners a Pipeline Orchestrácia)**  
Ponúka runnerov, ktoré umožňujú automatizovať úlohy definované v CI/CD pipelines, ako sú buildy, testovanie, nasadzovanie a ďalšie kroky. Tým sa eliminuje potreba manuálnych zásahov a zvyšuje efektivita tímov.
- **Kontajnerizácia a orchestrácia (Docker, Kubernetes Integrácia)**  
Je úzko integrovaný s kontajnerovými technológiami (napr. Docker) a platformami pre orchestráciu kontajnerov (Kubernetes), čo umožňuje efektívne nasadzovanie aplikácií vo forme kontajnerov v rôznych prostrediach.
- **Monitoring a sledovanie metrík (DevOps Analytics)**  
Poskytuje nástroje na sledovanie a monitorovanie výkonu aplikácií a samotného DevOps procesu. Tento monitoring zahŕňa analýzu výkonu pipeline, buildov, testov, a nasadení, čo poskytuje cenné dáta pre optimalizáciu vývojových a nasadzovacích procesov.
- **Spolupráca a sledovanie úloh (Issue Tracking a Collaboration Tools)**  
Umožňuje transparentnú spoluprácu medzi členmi tímu, manažérmi, a dodávateľmi pomocou nástrojov na sledovanie úloh a komentovanie kódu. Issue Tracking v GitLabe pomáha spravovať požiadavky, sledovať progres a zabezpečovať, aby boli problémy riešené včas. Táto funkčnosť je prepojená s celkovým riadením projektu v nástrojoch Jira s pluginom BigPicture a po prechode do prevádzky s manažmentom incidentov v Service Desk.

#### 6.2.4. **Storage PaaS (Storage as a Service)**

Storage PaaS umožňuje dynamické pridelovanie úložných kapacít na vyžiadanie, s dôrazom na vysokú dostupnosť a škálovateľnosť. Toto úložisko môže byť použité pre aplikácie bežiacie v cloude alebo pre zálohovacie účely.

#### 6.2.5. **IaaS PCA (Infrastructure as a Service - Private Cloud Appliance)**

Oracle Private Cloud Appliance (PCA) poskytuje robustnú infraštruktúru pre virtualizáciu a správu výpočtových zdrojov v privátnom cloude. Táto platforma je kľúčová pre správu kritických aplikácií a umožňuje vytváranie a správu kontajnerových a virtualizovaných prostredí.

- **LB PCA (Load Balancing pre PCA)**  
Služba vyrovnávania záťaže (Load Balancer) pre Oracle PCA zabezpečuje rozdelenie prevádzky medzi viacerými zdrojmi, čím zabezpečuje vysokú dostupnosť a odolnosť aplikácií voči výpadkom.
- **OKE Single AZ (Oracle Kubernetes Engine - Single Availability Zone)**  
OKE poskytuje Kubernetes služby na platforme Oracle Cloud Infrastructure (OCI). Nasadenie Kubernetes klastrov v jednej zóne dostupnosti umožňuje správu a škálovanie aplikácií v kontajneroch.
- **IaC (Infrastructure as Code)**  
Infrastructure as Code (IaC) umožňuje spravovať a nasadzovať infraštruktúru pomocou deklaratívnych nástrojov ako Terraform alebo Ansible. Automatizácia nasadzovania a správy infraštruktúry zvyšuje efektívnosť a znižuje riziko chýb.

#### 6.2.6. **Broadcom Layer7 API GW (API Gateway)**

API Gateway poskytuje centralizovanú správu a ochranu API rozhraní, vrátane autentifikácie, autorizácie a sledovania API volaní. Je kľúčovým komponentom pre správu interných a externých integrácií.

#### 6.2.7. **OpenShift Platform Plus**

OpenShift Platform Plus poskytuje komplexnú platformu pre správu Kubernetes kontajnerov, orchestráciu, automatizáciu a nasadzovanie aplikácií v kontajneroch a virtualizáciu.

- **Kontajnerizácia a orchestrácia aplikácií**  
Primárne postavený na Kubernetes a poskytuje rozsiahle nástroje na správu a orchestráciu kontajnerov, čo umožňuje vývojárom rýchlo nasadzovať a spravovať kontajnerizované aplikácie.  
Automatizovaná orchestrácia: Využíva Kubernetes na správu nasadených aplikácií, automatické pridávanie alebo odoberanie zdrojov podľa potrieb.  
Podpora pre multi-cluster: OpenShift umožňuje nasadzovanie aplikácií naprieč viacerými Kubernetes klastrami, čím zaisťuje vyššiu dostupnosť a škálovateľnosť.  
Deployment strategies: Podpora pre rôzne stratégie nasadenia aplikácií, ako sú Rolling updates, Blue/Green nasadenia, alebo Canary deployments, ktoré minimalizujú výpadky pri aktualizáciách aplikácií.
- **Virtualizácia (OpenShift Virtualization)**  
Aj keď je OpenShift primárne orientovaný na kontajnerizáciu, platforma podporuje plnohodnotnú virtualizáciu prostredníctvom OpenShift Virtualization, ktorá umožňuje nasadzovať a spravovať virtualizované pracovné záťažové jednotky (VMs) priamo vedľa kontajnerizovaných aplikácií.  
Správa virtuálnych strojov: Umožňuje nasadzovanie a správu tradičných virtuálnych strojov (VM) v rámci Kubernetes klastrov, čím poskytuje flexibilitu pri migrácii aplikácií z tradičnej VM infraštruktúry do kontajnerového prostredia.  
Kombinácia VM a kontajnerov: Možnosť spúšťať VM a kontajnerizované aplikácie vedľa seba, čo uľahčuje migráciu starších aplikácií bez potreby úplnej modernizácie.  
Centralizovaná správa: Administrátori môžu spravovať virtuálne stroje rovnako ako kontajnery, pomocou rovnakého nástroja a Kubernetes API, čím sa zjednodušuje správa infraštruktúry.

- **Integrovaná bezpečnosť (Security)**  
Obsahuje bezpečnostné nástroje, ktoré pomáhajú dodržiavať bezpečnostné normy a štandardy počas celého životného cyklu aplikácie. Jeho bezpečnostná architektúra je navrhnutá tak, aby poskytovala ochranu na úrovni kontajnerov aj virtuálnych strojov.  
Security Context Constraints (SCC): Nastavenie prístupových práv a izolácie na úrovni kontajnerov, aby sa zabezpečilo, že aplikácie bežia len s potrebnými oprávneniami.  
Image Vulnerability Scanning: Automatické skenovanie kontajnerových obrazov na prítomnosť zraniteľností pomocou integrovaných nástrojov.  
Podpora pre SELinux: OpenShift využíva SELinux na implementáciu prísnej bezpečnostnej politiky, ktorá zabezpečuje dodatočnú vrstvu ochrany nad aplikáciami.
- **Integrované nástroje pre CI/CD (Continuous Integration/Continuous Deployment)**  
Je integrovaný s rôznymi nástrojmi CI/CD, čo umožňuje rýchlejšie a efektívnejšie nasadzovanie aplikácií. Rovnako poskytuje nástroje na správu celého životného cyklu aplikácií od vývoja, cez testovanie až po produkčné nasadenie.  
BuildConfig: Umožňuje definovanie buildov priamo v rámci OpenShift, čo integruje build proces priamo do Kubernetes klastrov.  
Pipeline Integrácia: Podpora pre CI/CD pipeline pomocou nástrojov ako Jenkins alebo GitLab, čím sa zjednodušuje nepretržité testovanie a nasadzovanie aplikácií.  
GitOps: OpenShift podporuje model GitOps, ktorý umožňuje automatické nasadzovanie zmien v kóde do produkcie priamo z Git repozitára.
- **OpenShift Service Mesh**  
Je nástroj, ktorý umožňuje správu sieťovej komunikácie medzi mikroslužbami. Pomocou OpenShift Service Mesh môže dodávateľ riadiť, monitorovať a zabezpečovať internú komunikáciu medzi službami bez potreby zásahov do samotných aplikácií.  
Traffic Management: Umožňuje kontrolu nad tým, ako a kedy sa sieťová prevádzka distribuuje medzi rôznymi službami, vrátane podpory pre circuit-breaking a retries.  
Observability: Monitorovanie komunikácie medzi službami a sledovanie výkonnostných metrík, ktoré poskytujú prehľad o zdraví aplikácií.  
Security: Vstavaná podpora pre TLS šifrovanie medzi službami a autentifikáciu/autorizačné mechanizmy pre mikroslužby.
- **Monitoring a Logging**  
Ponúka integrované nástroje pre monitorovanie aplikácií, logovanie a správu metrík pomocou nástrojov ako Prometheus a Grafana. Tieto nástroje sú kľúčové pre udržiavanie vysokého výkonu a dostupnosti aplikácií.  
Prometheus a Grafana: Automatické zbieranie metrík z klastrov a aplikácií, ktoré sú následne vizualizované pomocou Grafana pre efektívne monitorovanie.  
Elasticsearch a Kibana: Podpora pre centralizované logovanie a vizualizáciu logov, ktoré zlepšujú sledovanie incidentov a identifikáciu problémov.  
Alerting: Vstavané upozornenia, ktoré automaticky informujú administrátorov o problémoch s aplikáciami alebo infraštruktúrou.
- **Škálovanie a vysoká dostupnosť**  
Poskytuje nástroje pre horizontálne a vertikálne škálovanie aplikácií na základe potrieb, vrátane automatického škálovania. Vysoká dostupnosť je zabezpečená podporou multi-cluster architektúry a automatickými mechanizmami pre obnovenie po výpadku.  
Horizontal Pod Autoscaling (HPA): Automatické pridávanie alebo odoberanie podov na základe aktuálneho zaťaženia aplikácie.  
Cluster Federation: Schopnosť nasadiť a spravovať aplikácie naprieč viacerými Kubernetes klastrami, čím sa zaisťuje ich dostupnosť a odolnosť voči výpadkom.  
Self-healing: Automatické reštartovanie zlyhaných kontajnerov a podov na základe health-checkov.

- Centralizovaná správa a governance

Poskytuje nástroje na správu a kontrolu nad infraštruktúrou, ktoré zjednodušujú životný cyklus aplikácií a zabezpečujú zhodu s predpismi. To zahŕňa nastavenia pre politiku prístupu, kontrolu zdrojov a auditovanie.

Role-Based Access Control (RBAC): Definovanie prístupových práv pre používateľov a služby v rámci OpenShift platformy.

Pod Quotas a Limits: Nastavenie obmedzení pre zdroje (CPU, pamäť) pre jednotlivé aplikácie a tímy, čo zabezpečuje rovnováhu medzi používateľmi a aplikáciami.

Audit Logging: Centralizované logovanie všetkých akcií na úrovni klastrov a aplikácií, čím sa zabezpečuje zodpovednosť a súlad s regulačnými požiadavkami.

#### 6.2.8. Security Logging

Služby pre bezpečnostné logovanie (Elastic Stack) umožňujú sledovanie a analýzu bezpečnostných udalostí, incidentov a anomálií v infraštruktúre. Bezpečnostné logy sú kľúčové pre audit a dodržiavanie predpisov.

#### 6.2.9. Monitoring

Monitoring aplikácií a infraštruktúry zahŕňa nástroje ako Dynatrace pre sledovanie výkonnosti aplikácií a Zabbix pre monitorovanie infraštruktúry. Tieto nástroje poskytujú alerty a metriky pre správu výkonu systémov.

#### 6.2.10. IaaS UPVS (Infrastructure as a Service - UPVS)

Infraštruktúra ako služba poskytovaná prostredníctvom UPVS (verejný sektor cloud) umožňuje škálovateľné poskytovanie výpočtových a úložných zdrojov. Tieto služby sú vo fáze postupného útlmu, preto je ich využitie podmienené schvaľovanou opodstatnenou výnimkou.

#### 6.2.11. Object Storage COS a OST API

Služba pre objektové úložisko (Cloud Object Storage) poskytuje bezpečné a škálovateľné ukladanie dát v cloude. OST API poskytuje rozhranie pre správu a prístup k uloženým objektom.

### 6.3. Využívanie služieb z katalógu služieb vládneho cloudu

NASES v rámci projektu bude využívať interné infraštruktúrne služby vlastných dátových centier.

#### Ďalšie privátne cloudy

##### 6.3.1. Vládny Cloud

Výpočtové a úložné služby, privátne Kubernetes klastre a ďalšie služby podľa aktuálnej dostupnosti zdrojov a potrieb projektu.

##### 6.3.2. eSK Cloud

Výpočtové zdroje, bezpečné úložiská, hybridné cloudové integrácie a ďalšie služby podľa aktuálnej dostupnosti zdrojov a potrieb projektu.

#### Verejné cloudy



### 6.3.3. Amazon Web Services (AWS)

EC2, S3, RDS, EKS a ďalšie služby podľa aktuálnej dostupnosti a potrieb projektu.

### 6.3.4. Microsoft Azure

Azure Virtual Machines, Blob Storage, SQL Database, AKS a ďalšie služby podľa aktuálnej dostupnosti a potrieb projektu.

### 6.3.5. Oracle Cloud Infrastructure (OCI)

Compute Instances, Object Storage, Autonomous Database, OKE a ďalšie služby podľa aktuálnej dostupnosti a potrieb projektu.

### 6.3.6. Github

Verziónovanie kódu, CI/CD integrácia, GitHub Actions a ďalšie služby podľa aktuálnej dostupnosti a potrieb projektu.

## 6.4. Bezpečnostná architektúra

Bezpečnostná architektúra systému bude navrhnutá s ohľadom na princípy Zero Trust a host-based security. Cieľom je vytvoriť prostredie, v ktorom je každý prístup overovaný a každý komponent chránený na úrovni hostov aj aplikácií. Architektúra bude podporovať proaktívnu detekciu a prevenciu bezpečnostných hrozieb, kontinuálne monitorovanie a zabezpečenie súladu s legislatívnymi a bezpečnostnými štandardmi.

### 6.4.1. Prístup Zero Trust

**Zásada minimálnej dôvery:** V rámci Zero Trust modelu bude prístup do systému riadený princípom minimálnej dôvery, kde každý pokus o prístup bude považovaný za potenciálne rizikový, a preto bude neustále overovaný.

**Overovanie identity a riadenie prístupu (IAM):** Každý prístup k službám, aplikáciám a dátam bude zabezpečený pomocou IAM (Identity and Access Management) systému. Budú využívané viacfaktorové overovanie (MFA) a princíp najmenej potrebných práv (least privilege).

**Segmentácia sietí a mikrosegmentácia:** Systém bude podporovať segmentáciu sietí a mikrosegmentáciu, ktorá umožní oddeliť citlivé zóny systému a minimalizovať riziko laterálneho pohybu útočníkov.

**Nepretržitá autentifikácia a autorizácia:** Prístupy budú priebežne overované a autorizované, a to nielen pri prihlásení, ale aj pri interakcii s jednotlivými aplikáciami a službami, čím sa zabezpečí, že každý prístup je vždy aktuálne overený.

### 6.4.2. Host-based Security

**Host-based Intrusion Detection and Prevention Systems (HIDS/HIPS):** Na všetkých hostoch (servery, koncové zariadenia) budú implementované HIDS alebo HIPS riešenia, ktoré budú monitorovať aktivitu a blokovat' podozrivé správanie priamo na úrovni hostov.

**Zabezpečenie konfigurácií a správna konfigurácia prístupov:** Každý host bude nastavený v súlade s bezpečnostnými štandardmi, čo zahŕňa nastavenie firewallov, riadenie prístupu, monitorovanie integrity súborov a konfigurácie, aby sa zabezpečila ich bezpečnosť a konzistentnosť.

**Skenovanie na malware a škodlivé aktivity:** Priebežné skenovanie hostov na prítomnosť škodlivých programov a aktivít pomôže identifikovať a blokovat' pokusy o kompromitáciu zariadení ešte predtým, ako môžu ovplyvniť zvyšok systému.

#### 6.4.3. DevSecOps – Integrácia bezpečnosti do vývojového a nasadzovacieho procesu

**Bezpečnosť ako súčasť CI/CD:** V rámci DevSecOps prístupu bude bezpečnosť integrovaná priamo do CI/CD pipeline, čo umožní priebežné skenovanie zdrojového kódu, detekciu bezpečnostných chýb a nasadenie bezpečnostných záplat v reálnom čase.

**Automatizované bezpečnostné testy a kontroly:** CI/CD pipeline bude podporovať automatizované bezpečnostné testy, vrátane statickej analýzy zdrojového kódu, dynamického testovania aplikácií a skenovania kontajnerov. Tieto testy budú zahŕňať kontroly na zraniteľnosti, šifrovanie údajov a dodržiavanie bezpečnostných štandardov.

**Shift Left – Posun bezpečnosti do skorých fáz vývoja:** Princíp "shift left" v DevSecOps znamená, že bezpečnostné kontroly sa budú vykonávať už počas vývojových fáz, čím sa minimalizujú riziká a náklady na opravy zraniteľností v neskorších fázach.

**Priebežné bezpečnostné školenia pre DevOps tím:** Pravidelné školenia pre DevOps tím zabezpečia aktuálnosť v oblasti najnovších bezpečnostných hrozieb a štandardov, čo umožní vývojárom identifikovať a riešiť bezpečnostné riziká už pri návrhu aplikácie.

#### 6.4.4. Cloud-native bezpečnostný dizajn a microservices architektúra

**Cloud-native prístup s princípom Zero Trust:** Všetky cloudové služby a aplikácie budú nasadené s princípmi Zero Trust, čo zahŕňa izoláciu jednotlivých služieb, šifrovanie dát a priebežné overovanie prístupov medzi mikroservismi.

**Service Mesh pre bezpečnú komunikáciu medzi mikroservismi:** Použitím service mesh v CNI Kubernetesového prostredia sa zabezpečí riadenie komunikácie medzi mikroservismi, čo umožní autentifikáciu a šifrovanie každej interakcie medzi jednotlivými komponentmi.

**Šifrovanie údajov v pokoji aj pri prenose:** Všetky údaje v cloude budú šifrované počas prenosu aj pri uchovávaní, čím sa dosiahne vysoká úroveň ochrany citlivých informácií.

#### 6.4.5. Monitorovanie aplikačnej bezpečnosti a integrácia s Dynatrace a SIEM

**Integrované monitorovanie aplikačnej bezpečnosti:** Systém bude napojený na Dynatrace pre pokročilé monitorovanie aplikačnej bezpečnosti, aby sa zabezpečila priebežná kontrola výkonu a detekcia anomálií v reálnom čase.

**SIEM pre centralizovanú správu logov a udalostí:** Všetky bezpečnostné logy a udalosti zo systému budú centralizovane zbierané a analyzované v SIEM riešení, čím sa zabezpečí detekcia podozrivých aktivít a umožní sa rýchla reakcia na bezpečnostné incidenty.

**Automatické reakcie a notifikácie na incidenty:** SIEM a Dynatrace budú nastavené na automatické generovanie notifikácií pri detekcii podozrivých aktivít alebo bezpečnostných incidentov, čo umožní okamžitú reakciu bezpečnostného tímu.

#### 6.4.6. Vulnerability manažment a patch management

**Priebežné skenovanie zraniteľností:** Systém bude podporovať priebežné skenovanie zraniteľností na všetkých vrstvách – od aplikácií až po jednotlivé hosty, aby sa zabezpečila ochrana pred aktuálnymi hrozbami.

**Rýchle aplikovanie bezpečnostných záplat:** Identifikované zraniteľnosti budú promptne riešené prostredníctvom patch management procesu, ktorý zabezpečí priebežnú aktualizáciu všetkých systémových komponentov a aplikácií.

**Reporting a prioritizácia zraniteľností:** Výsledky skenovania a nápravných opatrení budú priebežne reportované objednávateľovi s prioritizáciou podľa kritickosti zraniteľností, aby bola zabezpečená informovanosť a kontrola nad bezpečnostným stavom systému.

#### 6.4.7. Skenovanie zdrojových kódov a kontajnerov pre prevenciu rizík

**Automatizované skenovanie zdrojového kódu a kontajnerov:** V rámci CI/CD pipeline bude implementované automatizované skenovanie zdrojového kódu a binárnych obrazov kontajnerov, aby sa identifikovali bezpečnostné chyby už počas vývoja.

**Kontrola kontajnerových obrazov pred nasadením:** Pred každým nasadením do produkčného prostredia budú kontajnerové a VM obrazy skenované na zraniteľnosti, čím sa minimalizuje riziko nasadenia zraniteľného kódu.

**Vyhodnocovanie nálezov a nápravné opatrenia:** Výsledky skenovania budú pravidelne analyzované a nápravné opatrenia budú implementované podľa kritickosti jednotlivých zraniteľností, pričom sa budú dodržiavať SLA pre riešenie bezpečnostných problémov.

#### 6.4.8. Dodržiavanie štandardov OWASP a pravidelné penetračné testy

**OWASP štandardy pre bezpečný vývoj:** Vývoj aplikácií bude prebiehať podľa štandardov OWASP s cieľom minimalizovať riziko bezpečnostných zraniteľností už pri návrhu a implementácii.

**Testovanie na OWASP Top 10:** Testovanie aplikácií bude zahŕňať ochranu proti najvýznamnejším hrozbám podľa OWASP Top 10, vrátane ochrany proti SQL Injection, XSS a nesprávnej kontrole prístupu.

**Pravidelné penetračné testy:** Na overenie bezpečnosti aplikácií a infraštruktúry budú pravidelne vykonávané penetračné testy, ktorých výsledky budú analyzované a prijaté nápravné opatrenia na odstránenie zistených slabín.

#### 6.4.9. Integrácie s XDR, EDR a NDR systémami

**XDR na centralizované riadenie bezpečnostných udalostí:** Systém bude integrovaný s XDR riešením na centralizovanú analýzu a riadenie bezpečnostných udalostí, ktoré umožní celkový prehľad o bezpečnostných hrozbách.

**EDR pre koncové zariadenia:** EDR (Endpoint Detection and Response) zabezpečí ochranu koncových zariadení, čo umožní detekciu a prevenciu pokročilých hrozieb priamo na úrovni hostov.

**NDR pre monitorovanie sieťovej prevádzky:** Systém bude integrovaný s NDR (Network Detection and Response), ktorý umožní monitorovanie sieťového prostredia a detekciu podozrivých aktivít na úrovni sieťovej komunikácie.

### 7. ZÁVISLOSTI NA OSTATNÉ ISVS / PROJEKTY

Tento projekt rieši modernizáciu centrálnych komponentov a centrálnych blokov eGovernmentu v zmysle zákona č. 305/2013 Z.z.. Primárne sa zameriavať na znižovanie zastaranosti, optimalizáciu základných procesov a centrálnych komponentov ÚPVS. Výstupy tohto projektu budú slúžiť pre agendové systémy ostatných OVM (konzumentov centrálnych komponentov) pre rozvoj a zjednodušené riešenie životných situácií.

### 8. ZDROJOVÉ KÓDY

V rámci tohto projektu, realizovaného prostredníctvom verejného obstarávania, platia nasledovné podrobné požiadavky na dodanie zdrojového kódu a jeho integráciu do infraštruktúry objednávateľa. Tieto požiadavky zabezpečujú transparentnosť, konzistentnosť a kontrolu nad procesom vývoja, nasadzovania a údržby aplikácií.

#### 8.1. Kompletný zdrojový kód pre aplikácie vyvinuté na zákazku

**Zdrojový kód:** Dodávka bude obsahovať kompletný zdrojový kód každej aplikácie vytvorenej na zákazku. Táto dodávka zahŕňa všetky potrebné moduly, skripty, konfiguračné súbory, knižnice a iné závislosti potrebné pre správne zostavenie a nasadenie aplikácie.

**Závislosti a verzie:** Každá integrovaná externá knižnica alebo modul bude definovaný v kóde spolu s presnou verziou, aby sa zabezpečila konzistentnosť prostredia. Na tento účel bude pripravený súbor so závislosťami (napr. requirements.txt pre Python, package.json pre Node.js, pom.xml pre Maven a pod.), ktorý objednávateľovi uľahčí správu závislostí.

**Dokumentácia kódu:** Kód bude obsahovať internú dokumentáciu, ktorá vysvetľuje jednotlivé časti kódu, ich účel a spôsob interakcie. Pripojená bude aj technická dokumentácia popisujúca kľúčové architektonické komponenty a návrhové princípy, aby sa uľahčila údržba a rozšírenie riešenia.

## **8.2. Dodanie zdrojového kódu pre aplikácie postavené na open-source projektoch**

**Kompletný kód s modifikáciami:** V prípade aplikácií postavených na open-source projektoch bude dodaný celý kód vrátane všetkých úprav a prispôbení open-source komponentov. Tým sa zabezpečí konzistentnosť medzi prostrediami.

**Informácie o verziách a závislostiach:** Každý použitý open-source komponent bude explicitne uvedený s presnou verziou a informáciami o jeho kompatibilite. Na správu závislostí bude poskytnutý súbor s ich zoznamom.

**Licenčné informácie:** K dodanému kódu budú priložené licenčné informácie pre každý použitý open-source komponent. Dokumentácia bude zahŕňať informácie o prípadných obmedzeniach a súlade s licenčnými podmienkami.

## **8.3. Dodanie aplikácií založených na closed-source produktoch**

**Predpis na build kontajnera alebo VM image:** Pre aplikácie postavené na closed-source komponentoch bude dodaný presný predpis na vytvorenie (build) kontajnera alebo VM image. Tento predpis bude obsahovať všetky konfiguračné kroky a presné verzie použitých closed-source komponentov.

**Alternatíva - VM image:** Ak nie je možné použiť kontajnerizáciu, dodávateľ dodá obraz virtuálneho stroja (VM image) pripravený na integráciu do nasadzovacieho prostredia.

**Dokumentácia pre konfiguráciu closed-source komponentov:** Ak aplikácia využíva closed-source komponenty, dodávateľ poskytne detailné inštrukcie, ako ich integrovať a konfigurovať v rámci riešenia, vrátane krokov na ich aktualizáciu.

## **8.4. Automatizovaný CI/CD kód na nasadenie**

**Pipeline pre CI/CD:** Dodávateľ pripraví kód pre implementáciu CI/CD pipeline, ktorý umožní nasadzovanie aplikácie do vývojového, predprodukčného a produkčného prostredia. CI/CD pipeline bude navrhnutý podľa potrieb projektu a bude pokrývať všetky kroky, vrátane zostavenia, testovania a nasadenia.

**Podpora pre viacero cloudových prostredí:** Pipeline bude obsahovať mechanizmy na nasadenie do privátneho a verejného cloudového prostredia v súlade s bezpečnostnými a prevádzkovými štandardmi.

**Dokumentácia k CI/CD procesu:** Dokumentácia bude obsahovať kroky pre inicializáciu a konfiguráciu pipeline, postup riešenia chýb a podporu pri škálovaní CI/CD riešenia.

### 8.5. Integrácia zdrojového kódu do git repozitára objednávateľa

**Prístup do Git repozitára objednávateľa:** Git repozitár spravuje objednávateľ, ktorý dodávateľovi poskytne prístup s obmedzenými právami, určenými na zapisovanie do vývojových vetiev a na vytváranie pull requestov na implementáciu zmien. Dodávateľ bude dodržiavať predpísané postupy pre verzie a riadenie vetiev.

**Štruktúra dodaného kódu a organizácia v repozitári:** Dodávateľ dodrží dohodnutú štruktúru adresárov a súborov v repozitári, pričom budú dodržané interné štandardy objednávateľa na organizáciu zdrojových súborov a ich štruktúru. Tým sa uľahčí orientácia v kóde a efektívna údržba.

**Tagovanie verzií:** Dodávateľ označí jednotlivé verzie kódu (tagging), ktoré umožnia jednoznačnú identifikáciu verzií pre účely testovania a nasadenia. Verziovací systém bude dohodnutý na začiatku projektu (napr. Semantic Versioning).

### 8.6. Proces nasadenia a integrácie v git repozitári

**CI/CD integrácia s repozitárom:** CI/CD pipeline bude nakonfigurovaný tak, aby umožnil spúšťanie priamo z Git repozitára objednávateľa. Automatizované buildy a nasadzovanie sa budú spúšťať na základe zmien v určených vetvách (napr. staging a production), čím sa zabezpečí konzistentné nasadenie kódu.

**Automatizované buildy a nasadenia:** Zmeny v kóde budú spúšťať build a nasadzovacie procesy, čo zaručí, že do predprodukčných a produkčných prostredí budú vstupovať len plne testované verzie kódu.

### 8.7. Kontrola kvality kódu a zabezpečenie štandardov

**Code Review a schvaľovanie zmien:** Dodávateľ je povinný vytvárať pull requesty (PR) na každú zmenu, pričom tieto budú prechádzať schválením zo strany objednávateľa. Tento proces zabezpečí kontrolu nad kódom pred jeho nasadením.

**Štandardy kódu:** Dodávateľ bude dodržiavať štandardy kódu definované objednávateľom, vrátane formátovania, konvencií pomenovania a štruktúry komentárov.

### 8.8. Komunikácia a správa git repozitára

**Pravidelná synchronizácia:** Dodávateľ bude pravidelne synchronizovať svoj pracovný kód s Git repozitárom objednávateľa. Pravidelné zálohovanie kódu zabezpečí, že objednávateľ má priebežný prehľad o stave projektu.

**Dokumentácia k úpravám:** Každý commit bude obsahovať popis zmien. Pravidelná aktualizácia dokumentácie bude objednávateľovi poskytovať prehľad o všetkých zmenách a ich účele.

## 9. PREVÁDZKA A ÚDRŽBA

Pre zabezpečenie dlhodobej prevádzky, údržby a vysokej dostupnosti informačného systému sú medzi objednávateľom a dodávateľom dohodnuté pravidlá prevádzky, údržby a riadenia systému. Tieto pravidlá, vrátane úrovne podpory, monitorovania, bezpečnostných aktualizácií a súladu s ITIL procesmi, sú definované v dokumente Zmluva o poskytovaní služieb podpory a údržby informačného systému, ktorý je súčasťou podkladov jednotlivých verejných obstarávaní, aby bolo možné parametre zmluvy nastaviť

špecificky pre potreby obstarávaných riešení a komponentov. Tento dokument predstavuje záväzné rámce pre podporu a údržbu systému.

Jednotlivé parametre SLA služieb sú uvedené v rámci Prílohy 2 Katalóg požiadaviek. Popisy služieb prevádzky a údržby sú uvedené v Prílohe č.9 - Popis služieb vzor a procesy prevádzkové sú uvedené v prílohe č.10 - Manažment služieb Vzor.

## 10. POŽIADAVKY NA PERSONÁL

### Projektový manažér:

- zodpovedá za riadenie projektu počas celého životného cyklu projektu. Riadi projektové (ľudské a finančné) zdroje, zabezpečuje tvorbu obsahu, neustále odôvodňovanie projektu (aktualizuje BC/CBA) a predkladá vstupy na rokovanie Riadiaceho výboru. Zodpovedá za riadenie všetkých (ľudských a finančných) zdrojov, členov projektového tímu objednávateľa a za efektívnu komunikáciu s dodávateľom alebo stanovených zástupcom dodávateľa.
- zodpovedá za riadenie prideleného projektu - stanovenie cieľov, spracovanie harmonogramu prác, koordináciu členov projektového tímu, sledovanie dodržiavania harmonogramu prác a rozpočtu, hodnotenie a prezentáciu výsledkov a za riadenie s tým súvisiacich rizík. Projektový manažér vedie špecifikáciu a implementáciu projektov v súlade s firemnými štandardami, zásadami a princípmi projektového riadenia.
- zodpovedá za plnenie projektových/programových cieľov v rámci stanovených kvalitatívnych, časových a rozpočtových plánov a za riadenie s tým súvisiacich rizík. V prípade externých kontraktov sa vedúci projektu/ projektový manažér obvykle podieľa na ich plánovaní a vyjednávaní a je hlavnou kontaktnou osobou pre zákazníka.

### Kľúčový používateľ:

- zodpovedný za reprezentáciu záujmov budúcich používateľov projektových produktov alebo projektových výstupov a za overenie kvality produktu.
- zodpovedný za návrh a špecifikáciu funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu, požiadaviek koncových používateľov na prínos systému a požiadaviek na bezpečnosť.
- Kľúčový používateľ (end user) navrhuje a definuje akceptačné kritériá, je zodpovedný za akceptačné testovanie a návrh na akceptáciu projektových produktov alebo projektových výstupov a návrh na spustenie do produkčnej prevádzky. Predkladá požiadavky na zmenu funkcionality produktov a je súčasťou projektových tímov

### IT analytik:

- zodpovedá za zber a analyzovanie funkčných požiadaviek, analyzovanie a spracovanie dokumentácie z pohľadu procesov, metodiky, technických možností a inej dokumentácie. Podieľa sa na návrhu riešenia vrátane návrhu zmien procesov v oblasti biznis analýzy a analýzy softvérových riešení. Zodpovedá za výkon analýzy IS, koordináciu a dohľad nad činnosťou SW analytikov.
- analyzuje požiadavky na informačný systém/softvérový systém, formálnym spôsobom zaznamenáva činnosti/procesy, vytvára analytický model systému, okrem analýzy realizuje aj návrh systému, ten vyjadruje návrhovým modelom.
- Analytik informačných technológií pripravuje špecifikáciu cieľového systému od procesnej až po technickú rovinu. Mapuje a analyzuje existujúce podnikateľské a procesné prostredie, analyzuje biznis požiadavky na informačný systém, špecifikuje požiadavky na informačnú podporu procesov, navrhuje koncept riešenia a pripravuje podklady pre architektov a vývojárov riešenia, participuje na realizácii zmien, dohliada na realizáciu požiadaviek v cieľovom riešení, spolupracuje pri ich preberaní (akceptácie) používateľom.
- Pri návrhu IT systémov využíva odbornú špecializáciu IT architektov a projektantov. Študuje a analyzuje dokumentáciu, požiadavky klientov, legislatívne a technické podmienky a možnosti zvyšovania efektívnosti a výkonnosti riadiacich a informačných procesov. Navrhuje a prerokúva koncepcie riešenia informačných systémov a analyzuje ich efekty a dopady. Zabezpečuje spracovanie analyticko-projektovej špecifikácie s návrhom dátových a objektových štruktúr a ich väzieb, užívateľského rozhrania a ostatných podkladov pre projektovanie nových riešení.

- Spolupracuje na projektovaní a implementácii návrhov. Môže tiež poskytovať poradenstvo v oblasti svojej špecializácie. Zodpovedá za návrhovú (design) časť IT - pôsobí ako medzičlánok medzi používateľmi informačných systémov (biznis pohľad) a ich realizátormi (technologický pohľad).

#### **IT architekt:**

- zodpovedá za návrh architektúry riešenia IS a implementáciu technológií predovšetkým z pohľadu udržateľnosti, kvality a nákladov, za riešenie architektonických cieľov projektu dizajnu IS a súlad s architektonickými princípmi.
- vykonáva, prípadne riadi vysoko odborné tvorivé činnosti v oblasti návrhu IT. Študuje a stanovuje smery technického rozvoja informačných technológií, navrhuje riešenia na optimalizáciu a zvýšenie efektívnosti prostriedkov výpočtovej techniky. Navrhuje základnú architektúru informačných systémov, ich komponentov a vzájomných väzieb. Zabezpečuje projektovanie dizajnu, architektúry IT štruktúry, špecifikácie jej prvkov a parametrov, vhodnej softvérovej a hardvérovej infraštruktúry podľa základnej špecifikácie riešenia.
- zodpovedá za spracovanie a správu projektovej dokumentácie a za kontrolu súladu implementácie s dokumentáciou. Môže tiež poskytovať konzultácie, poradenstvo a vzdelávanie v oblasti svojej špecializácie. IT architekt, projektant analyzuje, vytvára a konzultuje so zákazníkom riešenia na úrovni komplexných IT systémov a IT architektúr, najmä na úrovni aplikačného vybavenia, infraštruktúrnych systémov, sietí a pod. Zaručuje, že návrh architektúry a/alebo riešenia zodpovedá zmluvne dohodnutým požiadavkám zákazníka v zmysle rozsahu, kvality a ceny celej služby/riešenia.

#### **Manažér kvality:**

- zodpovedá za priebežné vyžadovanie, hodnotenie a kontrolu kvality (vecnej aj formálnej) počas celého projektu. Je zodpovedný za úvodné nastavenie pravidiel riadenia kvality a za následné dodržiavanie a kontrolu kvality jednotlivých projektových výstupov. Sleduje a hodnotí kvalitatívne ukazovatele projektových výstupov a o zisteniach informuje projektového manažéra objednávateľa formou pravidelných alebo nepravidelných správ/záznamov.
- plánuje, koordinuje, riadi a kontroluje systém manažérstva kvality, monitoruje a meria procesy a identifikuje príležitosti na trvalé zlepšovanie systému manažérstva kvality v organizácii v súlade s platnými normami. Zabezpečuje tvorbu cieľov a koncepcie kvality, vrátane kontroly ich plnenia a vykonáva interné a externé audity kvality v súlade s plánom.
- Počas celej doby realizácie projektu zabezpečuje zhodu kvality projektových výstupov s požiadavkami. Realizuje postupy riadenia kvality tak, aby výsledkom boli projektové výstupy spĺňajúce požiadavky objednávateľa. Kontroluje, či sa riadenie a proces zabezpečenia kvality vykonáva správnym spôsobom, v správnom čase a správnymi osobami.

#### **Vlastník procesov:**

- zodpovedá za proces - jeho výstupy i celkový priebeh poskytnutia služby alebo produktu konečnému užívateľovi. Kľúčová rola na strane zákazníka (verejného obstarávateľa), ktorá schvaľuje biznis požiadavky a zodpovedá za výsledné riešenie, prínos požadovanú hodnotu a naplnenie merateľných ukazovateľov. Úlohou tejto roly je definovať na užívateľa orientované položky (user-stories), ktoré budú zaradzované a prioritizované v produktovom zásobníku. Zodpovedá za priebežné posudzovanie vecných výstupov dodávateľa v rámci analýzy, návrhu riešenia vrátane DNR z pohľadu analýzy a návrhu riešenia aplikácii IS.
- zodpovedný za schválenie funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu. Definuje očakávania na kvalitu projektu, kvalitu projektových produktov, prínosy pre koncových používateľov a požiadavky na bezpečnosť. Definuje merateľné výkonnostné ukazovatele projektov a prvkov. Vlastník procesov schvaľuje akceptačné kritériá, rozsah a kvalitu dodávaných projektových výstupov pri dosiahnutí platobných míľnikov, odsúhlasuje spustenie výstupov projektu do produkčnej prevádzky a dostupnosť ľudských zdrojov alokovaných na realizáciu projektu.

#### **Manažér kybernetickej a informačnej bezpečnosti:**

- zodpovedá za dodržanie princípov a štandardov na kybernetickú a IT bezpečnosť, za kontrolu a audit správnosti riešenia v oblasti bezpečnosti.
- *koordinuje a riadi činnosť v oblasti bezpečnosti prevádzky IT, spolupracuje na projektoch, na rozvoji nástrojov a postupov k optimalizácii bezpečnostných systémov a opatrení. Stanovuje základné požiadavky, podmienky a štandardy pre oblasť bezpečnosti programov, systémov, databázy či sietí.*



*Spracováva a kontroluje príslušné interné predpisy a dohliada nad plnením týchto štandardov a predpisov. Kontroluje a riadi činnosť nad bezpečnostnými testami, bezpečnostnými incidentmi v prevádzke IT. Poskytuje inštrukcie a poradenstvo používateľom počítačov a informačných systémov pre oblasť bezpečnosti*

#### **DevSecOps inžinier:**

- Zodpovedá za integráciu bezpečnostných postupov do všetkých fáz životného cyklu vývoja aplikácií v prostredí DevOps. Spolupracuje s vývojármi a prevádzkovými tímami na implementácii bezpečnostných opatrení a štandardov. Rieši zraniteľnosti, monitoruje bezpečnosť v prostredí CI/CD a vykonáva pravidelné testovanie bezpečnostných kontrol.
- Implementuje automatizované bezpečnostné kontroly a dohliada na ich neustále aktualizovanie podľa najnovších hrozieb. Zodpovedá za zabezpečenie infraštruktúry, vrátane správy práv a prístupov, ochrany dát, bezpečnosti sietí a nástrojov.

#### **Test manažér:**

- Zodpovedá za vytvorenie a riadenie testovacej stratégie, koordináciu testovacích aktivít a zdrojov, vrátane manuálneho a automatizovaného testovania. Vytvára testovacie plány a metodiky, definuje testovacie prípady a zodpovedá za sledovanie kvality výstupov.
- Dohliada na priebeh akceptačných testov a vykonáva kontrolu kvality výstupov v súlade s dohodnutými kritériami. Spolupracuje s kľúčovými používateľmi na definovaní akceptačných kritérií a dohliada na riešenie zistených chýb pred nasadením do produkcie.

#### **Cloud architekt**

- Zodpovedá za návrh, implementáciu a optimalizáciu cloudovej infraštruktúry, vrátane výberu vhodných cloudových technológií a služieb pre zabezpečenie dostupnosti, škálovateľnosti a bezpečnosti IS. Navrhne cloudové riešenia v súlade s požiadavkami na bezpečnosť a compliance.
- Zabezpečuje integráciu cloudových služieb s existujúcou IT infraštruktúrou a dohliada na správu, optimalizáciu a nákladovú efektívnosť cloudového prostredia. Poskytuje konzultácie v oblasti cloudových technológií a služieb.

#### **Data inžinier**

- Zodpovedá za návrh a implementáciu riešení pre zber, spracovanie, transformáciu a ukladanie dát. Vyvíja a optimalizuje dátové pipeline procesy, zodpovedá za bezpečnosť a kvalitu dát, ktoré sú potrebné pre analytické a prevádzkové účely.
- Navrhne riešenia pre spracovanie a distribúciu veľkého objemu dát (big data), pracuje s dátovými skladmi a ETL nástrojmi. Poskytuje podporu analytikom a ďalším členom tímu pri prístupe k relevantným dátovým zdrojom.

#### **Scrum Master (alebo Agile Coach)**

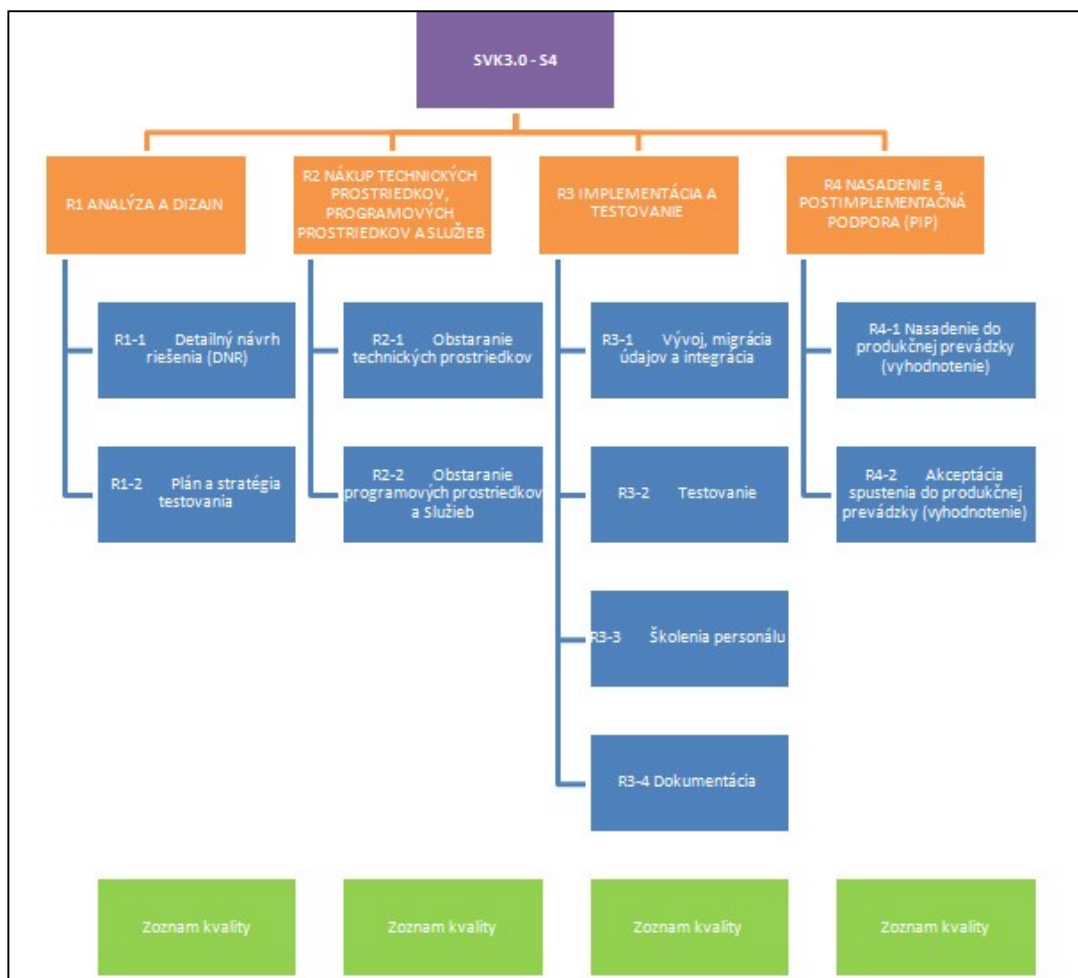
- Riadi agilné procesy projektu a zodpovedá za efektívne využitie agile metodológie v projektovom tíme. Facilitátor pre projektové tímy v rámci pravidelných agilných meetingov, zaisťuje plynulý priebeh agile procesov a pomáha riešiť prekážky.
- Zodpovedá za zvyšovanie produktivity tímu, zlepšovanie procesov a zvyšovanie transparentnosti práce prostredníctvom vizualizácie progresu a pravidelného hodnotenia prác (retrospektíva).

## **11. IMPLEMENTÁCIA A PREBERANIE VÝSTUPOV PROJEKTU**

Všetky výstupy projektu sú v zmysle Vyhlášky MIRRI č. 401/2023 Z.z. o riadení projektov.

Forma a štruktúra výstupu z hlavných etáp projektu je v zmysle Vyhlášky 401/2023 o riadení projektov a zmenových požiadaviek a príručky riadenie kvality, administrovanej zo strany útvaru Riadenia kvality MIRRI.

Dekompozícia hlavného produktu:



Obrázok 68 Výstupy projektu

Jednotlivé produkty / výstupy v zmysle dekompozície hlavného produktu rozdelené do dvoch základných skupín:

- Manažérske produkty a
- Špecializované (technické) produkty.

ID	Prehľad výstupov projektového riadenia	Manažérske	Špecializované
<b>PRÍPRAVNÁ A INICIAČNÁ FÁZA</b>			
I-01	Ideový zámer	áno	
<b>PRODUKTY VYTVARANÉ PRED VEREJNÝM OBSTARÁVANÍM</b>			
I-02	Projektový zámer Príloha: Zoznam rizík a závislostí Príloha: Analýza nákladov a prínosov (BC/CBA)	áno	
I-03	Prístup k projektu	áno	
I-04	Katalóg požiadaviek	áno	
<b>PRODUKTY VYTVARANÉ PO VEREJNOM OBSTARÁVANÍ</b>			
<b>REALIZAČNÁ FÁZA</b>			
R-01	Projektový iniciálny dokument (PID) Príloha 1.: Akceptačné kritériá	áno	
<b>R1 ANALÝZA A DIZAJN</b>			
R1-1	Detailný návrh riešenia (DNR)	áno	
R1-2	Plán a stratégia testovania Príloha 1: Testovacie prípady (TC) Príloha 2: Sumárny protokol	áno	

ID	Prehľad výstupov projektového riadenia	Manažérske	Špecializované
<b>R2</b>	<b>NÁKUP TECHNICKÝCH PROSTRIEDKOV, PROGRAMOVÝCH PROSTRIEDKOV A SLUŽIEB</b>		
R2-1	Obstaranie technických prostriedkov	áno	
R2-2	Obstaranie programových prostriedkov a Služieb	áno	
<b>R3</b>	<b>IMPLEMENTÁCIA A TESTOVANIE</b>		
R3-1	Vývoj, migrácia údajov a integrácia	áno	
R3-2	Testovanie:		
	(1) Funkčné testovanie (FAT)		áno
	(2) Systémové a integračné testovanie (SIT)		áno
	(3) Závažové a výkonnostné testovanie		áno
	(4) Bezpečnostné testovanie (SW/HW a kybernetická bezpečnosť)		áno
	(5) Používateľské testy funkčného používateľského rozhrania (UX)		áno
	(6) Užívateľské akceptačné testovanie (UAT)		áno
R3-3	Školenia personálu		áno
R3-4	Dokumentácia:		
	(1) Aplikačná príručka		áno
	(2) Používateľská príručka		áno
	(3) Inšalačná príručka a pokyny na inštaláciu (úvodnú/opakovanú)		áno
	(4) Konfiguračná príručka a pokyny pre diagnostiku		áno
	(5) Integračná príručka		áno
	(6) Prevádzkový opis a pokyny pre servis a údržbu		áno
	(7) Pokyny pre obnovu v prípade výpadku alebo havárie (Havarijný plán)		áno
	(8) Bezpečnostný projekt		áno
<b>R4</b>	<b>NASADENIE a POSTIMPLEMENTAČNÁ PODPORA (PIP)</b>		
R4-1	Nasadenie do produkčnej prevádzky (vyhodnotenie)		áno
R4-2	Akceptácia spustenia do produkčnej prevádzky (vyhodnotenie)		áno
<b>DOKONČOVACIA FÁZA</b>			
D-01	Manažérske správy, plány a odporúčania:		
	(1) Správa o dokončení projektu	áno	
	(2) Správa o získaných poznatkoch	áno	
	(3) Plán kontroly po odovzdaní projektu	áno	
	(4) Odporúčanie nadväzných krokov	áno	
<b>Produkty vytvárané PRIEBEŽNE počas celého projektu</b>			
M-01	Plán etapy/Plán fázy	áno	
M-02	Manažérske správy, reporty, zoznamy a požiadavky:		
	(1) Zoznam otvorených otázok	áno	
	(2) Zoznam funkčných zdrojových kódov	áno	
	(3) Zoznam licencií	áno	
	(4) Správa o stave projektu	áno	
	(5) Požiadavka na zmenu v projekte (CR)	áno	
	(6) Zoznam ponaučení	áno	
	(7) Zoznam rizík a závislostí	áno	
	(8) Zoznam kvality	áno	
	(9) Správa o ukončení fázy / etapy	áno	

ID	Prehľad výstupov projektového riadenia	Manažérske	Špecializované
M-03	Akceptačný protokol	áno	
M-04	Audit kvality projektu na mieste:		
	(1) audit kvality zameraný na výstupy Iniciačnej fázy	áno	
	(2) audit kvality zameraný na výstupy Realizačnej fázy	áno	
M-05	Analýza nákladov a prínosov (BC/CBA)	áno	
M-06	Evidencia e-Government komponentov v MetalS, vrátane architektonických modelov	áno	

Tabuľka 1 Zoznam produktov

Výstupy z podpornej aktivity Publicita a informovanosť v zmysle Zmluvy o PPM a aktuálneho Manuálu pre informovanosť a publicitu pre POO a Dizajnového manuálu komunikačných materiálov pre POO sú:

- Elektronická obrazovka
- Odporúčaná veľkosť formát A4 najneskôr 3 mesiace od ukončenia projektu (osadenie na 5 rokov po ukončení projektu).
- Koordinácia a tvorba obsahu publicity a informovanosti a jeho prezentovanie na konferenciách/workshopoch.
- Príprava tlačových správ a publikovanie informácií na Webovej stránke NASES.

## 12. PRÍLOHY

**Príloha č.1 Zoznam skratiek a pojmov**

**Príloha č.2 Katalóg požiadaviek**

**Príloha č.4 Zoznam KS a AS služieb**

**Príloha č.5 Zoznam IS v AS IS a TO BE**

**Príloha č.8 Závislosti na úrovni dopadov na externé systémy a ŽS**

**Príloha č.9 Popis služieb vzor**

**Príloha č.10 Manažment služieb Vzor**