**Dodávka a implementace informačního systému digitální technické mapy Jihomoravského kraje**

**PROVÁDĚCÍ DOKUMENTACE**

Verze: 1.3

Veřejná zakázka: Dodávka a implementace informačního systému digitální technické mapy Jihomoravského kraje.



# Obsah

[Obsah 2](#_Toc207203135)

[Seznam obrázků 6](#_Toc207203136)

[Seznam tabulek 6](#_Toc207203137)

[Historie verzí 7](#_Toc207203138)

[Seznam zkratek 7](#_Toc207203139)

[1. Úvod 11](#_Toc207203140)

[1.1. Cíl prováděcí dokumentace 11](#_Toc207203141)

[1.2. Předmět a cíle projektu 11](#_Toc207203142)

[2. Architektura technického řešení 12](#_Toc207203143)

[2.1. Návrh architektury DTM JMK 12](#_Toc207203144)

[2.1.1. Infrastrukturní vrstva 12](#_Toc207203145)

[2.1.2. Datová vrstva 17](#_Toc207203146)

[2.1.3. Aplikační vrstva 17](#_Toc207203147)

[2.1.4. Prezentační vrstva 17](#_Toc207203148)

[2.1.5. Obecné požadavky na systém 17](#_Toc207203149)

[2.2. Popis použitých technologií DTM JMK 18](#_Toc207203150)

[2.2.1. Windows 2019 (WIN 2019) 18](#_Toc207203151)

[2.2.2. Windows 11 (WIN 11) 19](#_Toc207203152)

[2.2.3. Rocky Linux 19](#_Toc207203153)

[2.2.4. Internet Information System (IIS) 19](#_Toc207203154)

[2.2.5. Docker 19](#_Toc207203155)

[2.2.6. .NET Framework 4.8 19](#_Toc207203156)

[2.2.7. DirectX 19](#_Toc207203157)

[2.2.8. Python 3 20](#_Toc207203158)

[2.2.9. Mapserver 20](#_Toc207203159)

[2.2.10. GDAL 20](#_Toc207203160)

[2.2.11. Orchard Core 20](#_Toc207203161)

[2.2.12. Create React App 20](#_Toc207203162)

[2.2.13. TypeScript 20](#_Toc207203163)

[2.2.14. React 20](#_Toc207203164)

[2.2.15. Redux 21](#_Toc207203165)

[2.2.16. REST 21](#_Toc207203166)

[2.2.17. Apollo client 21](#_Toc207203167)

[2.2.18. PostgreSQL 21](#_Toc207203168)

[2.2.19. Keycloak 21](#_Toc207203169)

[2.2.20. Zabbix 22](#_Toc207203170)

[2.2.21. Technologie pro statistiku a monitoring 22](#_Toc207203171)

[2.2.22. Drawings SDK 23](#_Toc207203172)

[2.2.23. Apache Tomcat 23](#_Toc207203173)

[2.2.24. PgAdmin (alternativně DBeaver) 23](#_Toc207203174)

[2.2.25. Tripwire 23](#_Toc207203175)

[2.3. Datový sklad – Produkční prostorové databáze 23](#_Toc207203176)

[3. Popis nastavení jednotlivých oblastí 26](#_Toc207203177)

[3.1. Popis instalace systému 26](#_Toc207203178)

[3.2. Šifrování, kryptografie a bezpečnostní nastavení webového serveru 27](#_Toc207203179)

[3.3. Konfigurace a parametrizace systému 28](#_Toc207203180)

[3.4. Zálohování systému 28](#_Toc207203181)

[4. Popis integračních vazeb 29](#_Toc207203182)

[4.1. Integrace na IS DMVS 29](#_Toc207203183)

[4.2. Rozhraní pro komunikaci s aplikacemi třetích stran 29](#_Toc207203184)

[4.3. IDM 30](#_Toc207203185)

[4.3.1. Funkční specifikace 30](#_Toc207203186)

[4.3.1.1. Autentizační server 30](#_Toc207203187)

[4.3.1.2. Rozhraní pro autentizaci k serverům 30](#_Toc207203188)

[4.3.1.3. Integrace s lokálními zdroji identit 30](#_Toc207203189)

[4.3.2. Propojení s JIP/KAAS 30](#_Toc207203190)

[4.3.3. Propojení s NIA 31](#_Toc207203191)

[4.3.3.1. Správa rolí 32](#_Toc207203192)

[4.3.4. Propojení s AD 34](#_Toc207203193)

[4.3.5. Sdílení informace o přihlášení klienta mezi komponentami 35](#_Toc207203194)

[4.4. Integrace na IS základních registrů a na Egon Service Bus 35](#_Toc207203195)

[4.5. Integrace na Portál stavebníka a Národní geoportál územního plánování 36](#_Toc207203196)

[4.6. Integrace na IS ÚAP 36](#_Toc207203197)

[4.7. Integrace na ISSI 36](#_Toc207203198)

[5. Návrh řešení postupu a pořadí při nasazování DTM JMK 37](#_Toc207203199)

[5.1. Příprava prostředí Objednatele 37](#_Toc207203200)

[5.2. Příprava prostředí Poskytovatele 37](#_Toc207203201)

[5.3. Instalace a nasazení datového skladu 37](#_Toc207203202)

[5.4. Import dat do datového skladu 37](#_Toc207203203)

[5.5. Způsob přeshraniční aktualizace dat ZPS 39](#_Toc207203204)

[5.6. Implementace portálu pro DTM JMK 40](#_Toc207203205)

[6. Popis komponent 41](#_Toc207203206)

[6.1. Popis komponent DMK JMK 41](#_Toc207203207)

[6.1.1. Portál DTM Kraje 41](#_Toc207203208)

[6.1.2. Redakční systém 41](#_Toc207203209)

[6.1.3. Klient pro výdej dat 42](#_Toc207203210)

[6.1.4. Komponenta pro poskytování exportu dat (výdejní modul) 43](#_Toc207203211)

[6.1.5. Komponenta pro správu aktualizačních dat 43](#_Toc207203212)

[6.1.5.1. Předběžné kontroly aktualizačních dat 44](#_Toc207203213)

[6.1.5.2. Příjem aktualizačních dat 44](#_Toc207203214)

[6.1.5.2.1. Příjem aktualizačních dat přes systém IS DMVS 46](#_Toc207203215)

[6.1.5.2.2. Příjem aktualizačních dat pomocí systému IS DTM 47](#_Toc207203216)

[6.1.5.2.3. Prvotní import do datového skladu DTM 47](#_Toc207203217)

[6.1.5.3. Řešení kolizí při souběžném zapracovávání dat 48](#_Toc207203218)

[6.1.6. Webová komponenta pro editaci ZPS 48](#_Toc207203219)

[6.1.7. Desktopová komponenta pro editaci ZPS/TI/DI 49](#_Toc207203220)

[6.1.8. Komponenty pro kontrolu (backend) 50](#_Toc207203221)

[6.1.8.1. Věcné kontroly vstupních aktualizačních dat JVF DTM 51](#_Toc207203222)

[6.1.8.2. Řízení prováděných kontrol 51](#_Toc207203223)

[6.1.9. Komponenta – Georeporty 51](#_Toc207203224)

[6.1.10. Komponenta – Metadatový klient 53](#_Toc207203225)

[6.1.11. Komponenta – Metadata 54](#_Toc207203226)

[6.1.12. Mapový klient DTM kraje pro veřejnost 56](#_Toc207203227)

[6.1.13. Komponenta pro správu mapových komponent 57](#_Toc207203228)

[6.1.14. Komponenta pro poskytování mapových služeb 57](#_Toc207203229)

[6.1.15. Statistika – klient 59](#_Toc207203230)

[6.1.16. Existence sítí 61](#_Toc207203231)

[6.1.17. Komponenta pro podporu reklamací datového obsahu a funkčnosti IS DTM 64](#_Toc207203232)

[6.1.18. Klient pro administraci 64](#_Toc207203233)

[6.1.18.1. Komponenta pro administraci datového skladu 64](#_Toc207203234)

[6.1.19. Komponenta zajišťující autentizaci a autorizaci všech přístupů a vstupů do IS DTM a jeho komponent včetně jeho služeb 65](#_Toc207203235)

[6.1.19.1. RolesManager 65](#_Toc207203236)

[6.1.20. Monitoring 65](#_Toc207203237)

[6.1.21. Logování 66](#_Toc207203238)

[6.1.22. Archivace 69](#_Toc207203239)

[6.1.23. Nápověda 70](#_Toc207203240)

[7. Návrh řešení migrace dat 71](#_Toc207203241)

[7.1. Referenční databáze RUIAN 71](#_Toc207203242)

[7.2. Číselníky DMVS, referenční údaje správců TI, DI, Editorů ZPS 71](#_Toc207203243)

[8. Požadavky na součinnost Objednatele 72](#_Toc207203244)

[8.1. Rozsah součinnosti ze strany Objednatele 72](#_Toc207203245)

[8.1.1. Fáze 1 – Dílčí fáze 1 72](#_Toc207203246)

[8.1.2. Fáze 1 – Dílčí fáze 2 72](#_Toc207203247)

[8.1.3. Fáze 1 – Dílčí fáze 3 74](#_Toc207203248)

[8.1.4. Fáze 1 – Dílčí fáze 4 74](#_Toc207203249)

[8.1.5. Fáze 1 – Dílčí fáze 5 75](#_Toc207203250)

[8.1.6. Fáze 1 – Dílčí fáze 6 75](#_Toc207203251)

## Seznam obrázků

[Obrázek 1 Schéma architektury komunikační síťové infrastruktury 14](#_Toc207203252)

[Obrázek 2 Schéma architektury technologické IT infrastruktury 15](#_Toc207203253)

[Obrázek 3 Ukázka uživatelského rozhraní deployment systému 27](#_Toc207203254)

[Obrázek 4 Přihlášení JIP/KAAS 31](#_Toc207203255)

[Obrázek 5 Přihlášení NIA 32](#_Toc207203256)

[Obrázek 6 Žádost o oprávnění 33](#_Toc207203257)

[Obrázek 7 Správa žádosti o oprávnění 34](#_Toc207203258)

[Obrázek 8 Přihlášení AD 35](#_Toc207203259)

[Obrázek 9 Datové toky při aktualizacích dat ZPS/TI/DI 46](#_Toc207203260)

[Obrázek 10 Workflow editace ZPS/TI/DI Desktopovou komponentou 50](#_Toc207203261)

[Obrázek 11 Komponenta Existence sítí 63](#_Toc207203262)

## Seznam tabulek

[Tabulka 1 Historie verzí 7](#_Toc207203263)

[Tabulka 2 Seznam zkratek 10](#_Toc207203264)

[Tabulka 3 Zabbix vč. jeho účelu 22](#_Toc207203265)

[Tabulka 4 Technologie pro statistiku a monitoring vč. jejich účelů 23](#_Toc207203266)

[Tabulka 5 Doplňující systémové databáze 25](#_Toc207203267)

[Tabulka 6 Tabulka s rozsahem a členěním statistických údajů 61](#_Toc207203268)

[Tabulka 7 Požadavky na součinnost Fáze 1 - Dílčí fáze 1 72](#_Toc207203269)

[Tabulka 8 Požadavky na součinnost Fáze 1 - Dílčí fáze 2 74](#_Toc207203270)

[Tabulka 9 Požadavky na součinnost Fáze 1 - Dílčí fáze 3 74](#_Toc207203271)

[Tabulka 10 Požadavky na součinnost Fáze 1 - Dílčí fáze 4 75](#_Toc207203272)

[Tabulka 11 Požadavky na součinnost Fáze 1 - Dílčí fáze 5 75](#_Toc207203273)

[Tabulka 12 Požadavky na součinnost Fáze 1 - Dílčí fáze 6 76](#_Toc207203274)

## Historie verzí

|  |  |  |  |
| --- | --- | --- | --- |
| **Verze** | **Datum** | **Autor** | **Popis** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Tabulka 1 Historie verzí

## Seznam zkratek

| **Zkratka** | **Definice** |
| --- | --- |
| ACID | Atomicita (Atomicity), konzistence (Consistency), izolovanost (Isolation), trvalost (Durability) |
| AD | Active Directory |
| API | Application Programming Interface |
| AT | AccessToken |
| AVETI | Automatizované Vyjádření k Existenci Technické a dopravní Infrastruktury |
| CAD/GIS | Computer-aided design/Geografický informační systém – rodiny SW pro práci s geografickými daty |
| CEPH | Objektové úložiště (technologie ukládání CESNET) |
| CMS | Content Management system (systém pro správu obsahu) |
| CMS2 | Centrální místo služeb (verze 2.1.2) |
| CPU | Central processing unit |
| CSV | Comma-separated values (hodnoty oddělené čárkami) |
| CS-W | OGC Catalogue Service for Web |
| CVSS | Common Vulnerability Scoring System (systém pro vyhodnocení penetračních testů) |
| ČÚZK | Český úřad zeměměřický a katastrální |
| DB | Databáze |
| DGN | Design (formát geoprostorových vektorových dat) |
| DI | Dopravní infrastruktura |
| DM ÚAP | Datový model Územně analytických podkladů |
| DMP | Digitální model povrchu |
| DMT | Digitální model terénu |
| DMVS | Digitální mapa veřejné správy |
| DNS | Domain Name Systém (systém doménových jmen) |
| DRP | Disaster Recovery Plan (Plán pro obnovu v případě závažného selhání) |
| DSŘ | Digitalizace stavebního řízení |
| DTM | Digitální technická mapa |
| DWG | Nativní formát souborů (výkresů) programu AutoCAD |
| eGSB | eGovernment Service Bus |
| FAQ | Frequently Asked Questions (často kladené dotazy) |
| GAD | Geodetická aktualizační dokumentace |
| GDAL | Geospatial Data Abstraction Library |
| GEMET | GEneral Multilingual Environmental Thesaurus |
| GeoJSON | Otevřený formát geoprostorových dat |
| GIS | Geografický informační systém |
| GISA | Produkt společnosti ISAX |
| GPKG | GeoPackage |
| HDD | Hard Disk Drive |
| HSM | Hierarchical Storage Management (technologie ukládání CESNET) |
| HTML | Hypertext Markup Language (hypertextový značkovací jazyk) |
| HTTP | Hypertext Transfer Protocol (protokol pro komunikaci v počítačových sítích) |
| HTTPS | Hypertext Transfer Protocol Secure (protokol pro komunikaci v počítačových sítích) |
| HW | Hardware |
| I/O | Input/Output (vstup/výstup) |
| ICMP | Internet Control Message Protocol |
| IČS | Identifikační číslo stavby |
| IIS | Internet Information Service (aplikace Microsoft) |
| IPMI | Intelligent Platform Management Interface |
| IS | Informační systém |
| IS DMVS | Informační systém Digitální mapy veřejné správy |
| IS DTM | Informační systém Digitální technické mapy |
| ISKN | Informační systém katastru nemovitostí |
| ISUI | Informační systém územní identifikace |
| ISVS | Informační systémy veřejné správy |
| ISZR | Informační systém základních registrů |
| JIP | Jednotný identitní prostor, který je součástí systému Czech POINT |
| JMK | Jihomoravský kraj |
| JVF DTM (JVF) | Jednotný výměnný formát Digitální technické mapy |
| JWT | SON Web Tokens |
| KAAS | Katalog autentizačních a autorizačních služeb |
| KC | Keycloak |
| KN | Katastr nemovitostí |
| KRS | Koordinační rada správců DMVS a DTM |
| KÚ | Krajský úřad |
| LAS, LAZ | LASer, LASzip (formáty geoprostorových dat) |
| LDAP | Lightweight Directory Access Protocol |
| LIDAR | Light Detection And Ranging (metoda dálkového měření vzdálenosti) |
| LMS | Letecké měřické snímky |
| LPIS | Land Parcel Identification System – Geografický informační systém MZ, který je tvořen primárně evidencí využití zemědělské půdy. |
| LV | List vlastnictví |
| MMR | Ministerstvo pro místní rozvoj |
| MZ | Ministerstvo zemědělství |
| NIA | Národní identitní autorita |
| NSESSS | Národním standardem pro elektronické systémy spisové služby (zveřejněný ve věstníku MV č. 57/2017) |
| NT | NT – označení řady operačního systému Microsoft Windows |
| NTP | Network Time Protocol |
| OAIS | Open Archival Information System |
| OGC | Open Geospatial Consortium (mezinárodní standardizační organizace) |
| OGR | Sada knihoven poskytující nástroje pro práci s vektorovými daty |
| OIDC | OpenID Connect |
| ORP | Obec s rozšířenou působností |
| OS | Operační systém |
| OVM | Orgán veřejné moci |
| OWASP | Open Web Application Security Project |
| PC | Personal Computer – osobní počítač |
| PDB | Prostorová databáze |
| PHP | Hypertext Preprocessor (hypertextový preprocesor) |
| PSK | Pre-shared key (Zabbix) |
| RAM | Random Access Memory |
| RDP | Remote Desktop Protocol |
| RDBMS | Relational Database Management System (Relační systém správy databáze) |
| REST | Representational State Transfer |
| RM | RolesManager |
| RSS | Rich Site Summary – XML formát určených pro čtení novinek |
| RUIAN | Registr územní identifikace, adres a nemovitostí |
| SDK | Software development kit – sada vývojářských nástrojů |
| SeP | Service Provider |
| SHP | Shapefile (formát geoprostorových vektorových dat) |
| S-JTSK | Systém jednotné trigonometrické sítě katastrální |
| SMTP | Simple Mail Transfer Protocol – protokol k přenosu e-mailů |
| SNMP | Simple Network Management Protocol |
| SQL | Structured Query Language (standardizovaný strukturovaný dotazovací jazyk) |
| SSH | Secure Shell |
| SVO | Správce vymezené oblasti |
| TA ČR | Technologická agentura České republiky |
| TI | Technická infrastruktura |
| TC | Technologické centrum |
| TCP | Transmitssion Cotrol Protocol |
| TP | Testovací případ |
| TPS | Technická pracovní skupina |
| ÚAP | Územně analytické podklady |
| UDP | User Datagram Protocol (Uživatelský protokol pro přenos datagramů v sítích) |
| URL | Uniform Resource Locator („jednotný lokátor zdroje“) - webová adresa |
| UUID | Universally unique identifier |
| vCPU | Virtual CPU |
| VFR | Výměnný formát registrů (RUIAN) |
| VLAN | Virtual Local Area Network (virtuální LAN) |
| VoKB | Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti |
| VPN | Virtual Private Network (virtuální privátní síť) |
| vRAM | Virtual RAM |
| VSP DTI | Vlastník/Správce/Provozovatel dopravní a technické infrastruktury |
| WAF | Web Application Firewall (firewall webové aplikace) |
| WFS | Web Feature Service |
| WMS | Web Map Service |
| WMTS | Web Map Tile Service |
| WYSIWYG | What you see is what you get |
| X/MIT | Licenční model pro open-source software |
| XML | Extensible Markup Language (rozšiřitelný značkovací jazyk) |
| ZD | Zadávací dokumentace |
| ZPS | Základní prostorová situace |

Tabulka 2 Seznam zkratek

# Úvod

## Cíl prováděcí dokumentace

Prováděcí studie předkládá komplexní a detailní návrh způsobu realizace předmětu plnění, a to ve vazbě na požadavky uvedené ve smlouvě o dílo a jejích přílohách. Cílem je zpracování dokumentu v takové míře detailu jednotlivých postupů a prací, zasazení do prostředí a jeho nastavení, která umožní implementaci systému do rutinního provozu řízenou formou.

Obsahem dokumentace jsou zejména tyto oblasti:

* Návrh řešení instalace aplikační a databázové části systému (architektura IS DTM JMK).
* Návrh řešení postupu a pořadí při nasazování jednotlivých oblastí.
* Upřesnění časového harmonogramu projektu – součástí harmonogramu dodávky budou i předpokládané termíny pro dodávku a nasazení dílčích řešení a technologií.
* Detailní popis nastavení, konfigurace a parametrizace jednotlivých částí systému.
* Návrh řešení importu a migrace dat.
* Popis případných organizačních opatření nutných pro implementaci (např. pracovní schůzky, využití komunikační platformy pro sdílení dokumentace, zápisů atd.).
* Popis rozsahu součinnosti ze strany Objednatele.
* Návrh průběhu testovacího provozu a akceptačního řízení.

## Předmět a cíle projektu

Cílem projektu je naplnění zákonné povinnosti kraje zřídit a spravovat Digitální technické mapy kraje a zlepšit podmínky pro práci s daty Digitální technické mapy. Účelem Digitální technické mapy je zajistit úplné a spolehlivé informace o existenci, prostorovém umístění a vlastnostech stavebních a technických objektů a zařízení, které jsou nezbytné pro přípravu a realizaci staveb, stavebních řízení, dále pro územní plánování, správu a rozvoj systémů dopravní a technické infrastruktury a pro další agendy a činnosti veřejné správy.

Předmětem projektu je dodávka a zavedení informačního systému Digitální technické mapy Jihomoravského kraje (IS DTM JMK) do určeného technického prostředí Objednatele, a to včetně nedílně souvisejících požadavků typu provedení integračních prací, migrací dat, zaškolení, dodání licencí a zpracování dokumentace. Předmětem plnění jsou dále i služby k zajištění celkového životního cyklu informačního systému v prostředí Objednatele v podobě služeb technické podpory a rozvoje informačního systému.

# Architektura technického řešení

Aplikační architektura je navržena s ohledem na požadavky byznys architektury, tedy z účelu definování Digitální technické mapy v legislativě, při zohlednění stanovených kompetencí zúčastněných subjektů, závazného procesního modelu a rozsahu zajišťovaných služeb. Architektura řešení zohledňuje požadavky Objednatele stanovené v zadávací dokumentaci a zároveň respektuje požadavky definované zákonem o ISVS a jeho prováděcích právních předpisech a Informační koncepcí České republiky, včetně architektonických principů eGovernmentu.

IS DTM je agendový informační systém. Jako takovému mu bude/může být umožněn přístup ke službám základních registrů, Informačnímu systému Digitální mapy veřejné správy IS DMVS, Národnímu bodu pro identifikaci a autentizaci (NIA), jednotnému identitnímu prostoru JIP/KAAS, budoucímu portálu stavebníka a případně dalším systémům v rámci propojeného datového fondu.

## Návrh architektury DTM JMK

### Infrastrukturní vrstva

Technologická infrastruktura je reprezentována virtuálními servery Windows a Linux, které jsou provozovány ve virtualizačním prostředí datových center. Datová centra budou v režimu active/passive s replikací virtuálních strojů aplikačních serverů do druhého datového centra pomocí technologie VMware vMotion. Ostatní servery jedná se hlavně o databáze a File server budou provozovány v redundantním režimu, replikace dat bude řešena aplikační cestou IS DTM. Důvodem je zachování integrity dat, kdy není zaručeno, že má virtuální server během přesunu do druhé lokality ukončeny všechny transakce. V případě výpadku datového centra dojde k nastartování kopie virtuálních strojů aplikačních serverů v druhém datovém centru. Obnova aplikace bude sice časově náročnější, ale nebude potřeba alokovat tolik HW zdrojů pro provoz standby instancí aplikace. Pomocí virtualizačních technologií bude zajištěna podpora pro poskytnutí dostatečných virtualizovaných HW zdrojů, dosažení požadované úrovně vysoké dostupnosti a také servisovatelnost infrastruktury za chodu. Kontejnerizace bude realizována v rozsahu komponent umístěných na WEB serveru 3 a na serveru Úložiště zdrojových dat (jedná se o komponenty Georeporty, Existence sítí a Úložiště zdrojových dat).

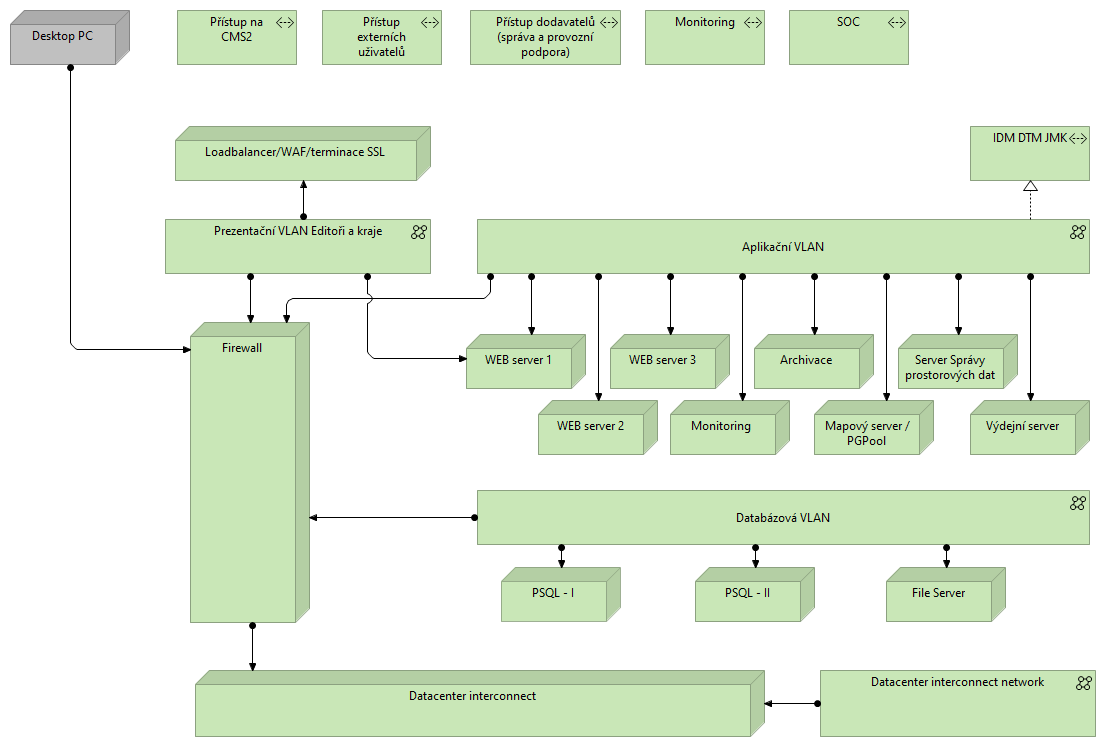
Návrh zasazení IS DTM do síťové infrastruktury využívá následující principy:

* Ochrana informačního systému před externími hrozbami bude realizována bezpečnostním perimetrem CMS2 a vlastních datových center pomocí firewallu na perimetru a segmentací sítě IS DTM na prezentační, aplikační a datová VLANy. Z důvodu vyšší bezpečnosti je doporučeno použití Web application firewall (WAF), WAF není předmětem plnění Poskytovatele.
* Aplikační a databázová vrstva informačního systému využívají oddělené VLAN. Komunikace mezi těmito VLAN bude řízena na firewallu. V rámci jedné VLAN není komunikace omezena.
* Virtualizační servery budou připojeny k diskovému poli tak, aby byla umožněna vysoká dostupnost virtuálních serverů v rámci virtualizační platformy.
* Přístup Poskytovatelů, správců a administrátorů pro správu a zajištění provozní podpory bude řešen pomocí VPN přístupu. Na firewallu bude povolena komunikace z VPN sítě do jednotlivých VLAN informačního systému. Jedná se o protokoly RDP, SSH a HTTP/HTTPS.

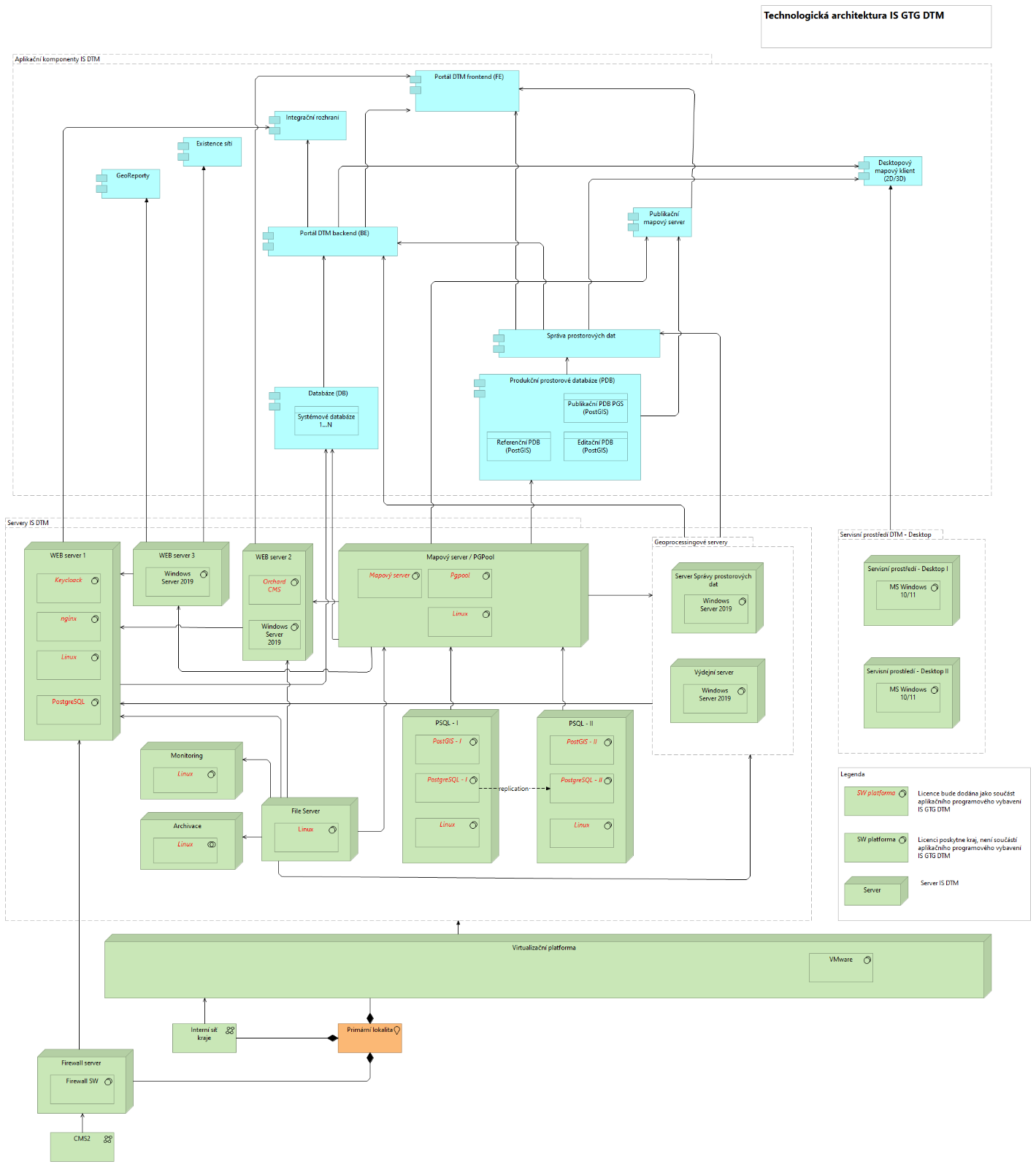
Požadovaná dostupnost a výkonnost bude zajištěna Objednatelem v následujících oblastech:

* Dostatečná výkonnost a redundance síťových spojení eliminující nedostatečnost propustnosti a výpadek jednotlivého spojení a směrování.
* Monitorování dostupnosti a spolehlivosti a provozních charakteristik jednotlivých komponent technologické architektury systému.
* Bezpečnostní monitoring a ochrana v rámci síťové infrastruktury.
* Sběr a vyhodnocování auditních logů.
* Virtualizace VMware vSphere využívá pro zajištění vysoké dostupnosti aplikací vlastnosti High Availability, vMotion, Resource Pool a Distributed Resource Scheduler. V případě výpadku nebo odstávky jednoho z fyzických virtualizačních serverů z něj bude převeden provoz na zbývající fyzické virtualizační servery s využitím afinitních pravidel pro alokaci virtuálních serverů na fyzické virtualizační servery a prioritizace plánovače zdrojů (vCPU, vRAM, I/O). V případě potřeby bude pro některé virtuální servery využit overcommit vCPU až do poměru 1:3.
* Provádění zálohování databází, obrazů virtuálních serverů a testování DRP scénářů.

Infrastruktura Objednatele poskytuje pro provoz informačního systému nejen datové zdroje, síťovou komunikační infrastrukturu, služby virtualizační platformy, ale i síťové infrastrukturní služby (NTP, SMTP, DNS) a zálohování.



Obrázek 1 Schéma architektury komunikační síťové infrastruktury



Obrázek 2 Schéma architektury technologické IT infrastruktury

Specifikace známých datových toků mezi jednotlivými částmi systému. Aktuálně neznámé datové toky budou specifikovány v dokumentaci skutečného provedení:

* Komunikace mezi webovým aplikačním firewallem a prezenčním webovým serverem (Web server 1) pomocí protokolu HTTPS na TCP portu 443.
* Komunikace mezi prezentačním webovým serverem a aplikačními servery pomocí protokolu HTTPS na TCP portu 443.
* Komunikace mezi aplikačními servery a prezentačním webovým serverem na TCP portu 443.
* Komunikace mezi aplikačními servery a databázovými servery na TCP portech 5432, 5433, 5434, 5435, 445, 139, 22 na UDP portech 137, 138.
* Komunikace mezi databázovými servery pro zajištění synchronizace dat mezi datovými centry na TCP portech 5432, 5433, 5434, 5435, 445, 139, 22, na UDP portech 137, 138.
* Komunikace ze servisního prostředí na aplikační servery na TCP portech 445, 139, 22, na UDP portech 137, 138.
* Všechny servery využívají DNS servery, UDP port 53.
* Všechny servery si synchronizují čas s NTP servery, UDP port 123.
* Aplikační servery využívají SMTP servery, TCP port 25.
* Monitorovací server komunikuje na všechny aplikační a databázové porty a také TCP port 10050 zabbix agenta.
* Aplikační a databázové servery komunikují na monitorovací server přes TCP port 10051.
* Aplikační a databázové servery komunikují syslog protokolem na monitorovací server TCP a UDP 514 pak na TCP 5044 logstach protokolem.

Specifikace datových toků na externí části systému:

Příchozí:

* Pro administraci všech serverů s operačním systémem Rocky Linux bude povolena příchozí komunikace z VPN na TCP port 22.
* Pro administraci všech serverů s operačním systémem Windows Server bude povolena příchozí komunikace z VPN na TCP port 3389.
* Na všechny aplikační severy bude povolena z příchozí komunikace z VPN na TCP porty 80 a 443.

Odchozí:

* Komunikace s úložištěm primárních dat na TCP portech 445, 139, na UDP portech 137, 138.
* Odchozí komunikace z aplikační VLAN na port 10051 centrálního monitoringu ICZ, kde budou předávány vzniklé alerty pro hlášení incidentů HelpDesku ICZ. Odchozí komunikace z aplikační VLAN na port 10051 zabbix proxy pro potřeby monitoringu dostupnosti externích části aplikace. Odchozí komunikace z aplikační VLAN na port 25 (SNMP) pro zasílání notifikačních e-mailů. Odchozí komunikace z aplikační VLAN pomocí protokolu ICMP na vybrané síťové prvky v CMS2, pro potřeby monitoringu infrastruktury.
* Z linux serverů zajistit komunikaci na server meduza-hk.tmapy.cz pro porty 873, 878 pro zajištění automatizace deploymentu.
* Z webserveru1 a mapových serverů přístup na [cz-services.tmapserver.cz](https://cz-services.tmapserver.cz/) a [services7.tmapserver.cz](https://services7.tmapserver.cz/) port 443 pro zajištění aktualizace RUIAN v lokálním datovém skladu.
* Z Webserveru 3 a Úložiště zdrojových dat na servery swd1.geovap.cz, swd2.geovap.cz, install.geovap.cz , devopsgallerystorage.blob.core.windows.net, \*.powershellgallery.com, go.microsoft.com porty 443 pro potřebu deploymentu aplikací.
* Z webserveru 4 doplnit přístup na katastr.cuzk.cz pro práci s anonymizovanými daty a na IP 5.59.97.126, download.docker.com:443, registry.dev.gmtech.cz:443, app.gmtech.cz:443, nv.cuzk.cz:443, wwwinfo.mfcr.cz:443 pro potřeby deploymentu aplikací majetkoprávy.

### Datová vrstva

Mezi aplikační VLAN a databázovou VLAN je umístěn L3 firewall, na kterém jsou definována pravidla povolující síťovou komunikaci mezi aplikačním VLAN a datovým VLAN.

Database cluster VLAN slouží pro interní komunikaci databázového clusteru. Tento VLAN musí být síťově, na třetí vrstvě, propojen mezi datovými centry tak, aby byla umožněna synchronizace databází, která bude prováděna databázovou platformou.

### Aplikační vrstva

Mezi prezentační VLAN a aplikační VLAN je umístěn L3 firewall, na kterém jsou definována pravidla povolující síťovou komunikaci mezi prezentační VLAN a aplikační VLAN.

Jednotlivé aplikační komponenty a API jsou publikovány do prezentační VLAN na příslušných URL na protokolu HTTP/HTTPS.

Jednotlivé komponenty jsou popsány v dalších kapitolách prováděcí dokumentace. Jedinou níže neuvedenou komponentou je JobScheduler. Jedná se o nástroj, který optimalizuje a škáluje provádění geoprocessingových procesů. Přijímá požadavky na provádění od komponent Komponenta pro správu aktualizačních dat a Komponenta pro poskytování exportu dat (výdejní modul) a prostřednictvím nástrojů Správy prostorových dat zajišťuje jejich vyřízení.

### Prezentační vrstva

Příchozí komunikace je na úrovni CMS2 směrována do aktivního datového centra, Vysoká dostupnost na úrovni síťového připojení do CMS2 bude zajišťována datovými centry.

Firewall pak zajistí bezpečnostní kontroly a následné směrování komunikace na virtuální servery. Publikační komponenty rozhraní poté směrují komunikaci na příslušná rozhraní nebo aplikační komponenty podle příchozí URL.

Portálová část IS DTM Jihomoravského kraje určená pro veřejnost bude přístupná prostřednictvím aktuálních verzí webových prohlížečů Microsoft Edge, Google Chrome, Mozilla Firefox a Safari. V případě použití nepodporovaného prohlížeče bude uživatel na tuto skutečnost upozorněn včetně seznamu podporovaných prohlížečů.

### Obecné požadavky na systém

Při vývoji systému budou zohledněny obecné požadavky a architektonické principy eGovernmentu:

* Bezpečnost je součástí návrhu systému, požadované bezpečnostní mechanismy a stupeň ochrany zpracovávaných údajů jsou v systému zabudovány již od jeho návrhu, tvorba systému splňuje definované bezpečnostní požadavky.
* Modulární architektura systému a jeho dekompozice na logické části umožní modifikovat části systému, rozšiřovat nebo měnit funkčnost částí systému bez dopadu na ostatní části systému nebo systém jako celek.
* Pro integraci IS DTM s ostatními informačními systémy a aplikacemi bude využito webových služeb s jasně definovaným a dokumentovaným API. Jakákoliv změna API bude řízená a bude dbáno na zpětnou kompatibilitu tak, aby v případě požadavku na nasazení nové verze webové služby zůstalo předcházející rozhraní funkční.
* Aplikační vrstva architektury je členěna na prezentační, business logickou a datovou. Jednotlivé vrstvy komunikují pomocí interního API systému. To například umožňuje provedení změn v byznys logice bez nutnosti změn v prezentační vrstvě systému.
* Dostupnost a přenositelnost, architektura systému je navržena tak, aby systém efektivně podporoval škálování, zejména na klíčových místech systému. Jsou využívány technologie, které umožní efektivně a rychle reagovat na zvyšování i snižování počtu zpracovávaných požadavků systémem za jeho chodu, architektura systému je koncipována jako vysoce dostupná. Pro realizaci jsou zvoleny technologie, které vycházejí z dlouhodobých zkušeností s realizacemi a provozem systémů DTM. Zvolené technologie mají schopnosti optimálního využití systémových prostředků pro danou úlohu a poskytují nejlepší možnosti pro provoz systému i z pohledu definovaných systémových prostředků pro jednotlivé instance systému.
* Všechny uživatelské části produkčního systému budou s uživatelem komunikovat v českém jazyce, a to včetně chybových hlášení, produkčních exportů a importů dat. Vybrané části systému určené pro tvorbu individuálních výstupů administrátorů, export a import dat a další funkcionality vyhrazené administrátorům systému (např. logy) budou komunikovat v anglickém jazyce.

Modulární, servisně orientovaná architektura řešení, jejíž implementace je postavena na využití otevřených standardů, umožňuje zajistit potřebnou udržitelnost projektu, kdy bude možné realizovat průběžnou provozní podporu a rozvoj i případné modernizace systému efektivně na úrovni souvisejících logických celků architektury řešení.

Pro zajištění požadované doby odezvy dle ZD je systém dekomponován do samostatných modulů, kterým je vyčleněna samostatná výpočetní kapacita. Tedy požadavky na jednotlivé komponenty nebudou navzájem ovlivňovány. V databázi PostgreSQL bude založeno několik oddělených instancí tak, aby geoprocesingové operace a čtení geografických dat nemělo vliv na plynulost provozu dalších komponent systému IS. Zároveň je čtení v PostgreSQL posíleno LoadBalancerem v podobě PGPool technologie.

Realizace geoprocessingových úloh je založena na průběžném odbavovaní fronty požadavků. Požadavky do fronty zapisují komponenty IS DTM a uživatele průběžně informují o průběhu jejich zpracování. Jednotlivé požadavky na processy jsou pomocí JobScheduleru distribuovány (paralelně i sekvenčně) na geoprocessingové servery (dle konfigurace). Jejich počet může být při zjištění nedostatečné kapacity a odezvy za chodu navyšován, a to buď přidáním procesních vláken na existujících serverech, nebo i doplněním dalšího geoprocessingového serveru. Požadavek je možné do fronty (pokud to dává smysl) vložit i opakovaně (například opětovné spuštění kontrol se stejnými parametry).

## Popis použitých technologií DTM JMK

### Windows 2019 (WIN 2019)

Jedná se o serverovou verzi operačního systému Windows (řady NT) od společnosti Microsoft. První vydání produktu proběhlo 13.11.2018. U zvolené verze operačního systému bude zajištěna dostupnost uživatelské podpory po celou dobu trvání projektu. Tento operační systém bude nasazen na všech serverech platformy Windows.

### Windows 11 (WIN 11)

Jedná se o 64bitovou verzi operačního systému Windows (řady NT) pro osobní počítače od společnosti Microsoft. První vydání produktu proběhlo 5.10.2021. Tento operační systém bude nasazen v servisním desktopovém prostředí a bude mimo jiné sloužit pro zajištění běhu Desktopové komponenty pro editaci ZPS. Místo operačního systému verze Windows 11 bude možno alternativně využít verzi Windows 10.

### Rocky Linux

Rocky Linux je open-source distribuce operačního systému. Jeho výhodou je, že se jedná o systém s binární kompatibilitou s Red Hat Enterprise Linux®. Nepřímo navazuje na původní OS CentOS, jehož vývoj byl v roce 2020 ukončen. V rámci projektu IS DTM bude instalován ve verzi Rocky Linux 8, která zajišťuje security support do května 2029. Průběžné aktualizace OS zajišťuje Poskytovatel vždy nejprve instalací do testovacího prostředí a po provedení testů i do prostředí produkčního. V případě ukončení projektu Rocky Linux jde na vrub Poskytovatele jeho výměna za jinou alternativní distribuci OS.

### Internet Information System (IIS)

IIS je softwarový webový server pro operační systém Windows s možností instalace rozšiřujících modulů od společnosti Microsoft. Jedná se o jeden z nejpoužívanějších webových serverů. IIS bude nasazen na všech aplikačních serverech platformy Windows, kde bude nutné zajistit provoz webových aplikací.

### Docker

Docker je otevřený software (open-source), který poskytuje jednotné rozhraní pro distribuci aplikací pomocí kontejnerů v prostředí Windows, Linux a macOS. Jedná se o efektivní tzv. odlehčenou formu virtualizace, kdy kontejner obsahuje pouze aplikace (bez operačního systému). V systému IS DTM bude Docker využit k zajištění efektivnější správy určitých vybraných částí systému (vybraných komponent).

### .NET Framework 4.8

Microsoft .NET Framework je základní komponentou platformy .NET. Jedná se o prostředí pro běh aplikací, nabízející spouštěcí rozhraní i potřebné knihovny. Vybrané části systému IS DTM budou založeny na technologii .NET. Instalace .NET Framework 4.8 bude vyžadována v servisním desktopovém prostředí, kde tuto technologii bude využívat Desktopová komponenta pro editaci ZPS.

### DirectX

Microsoft DirectX je sada knihoven, poskytující aplikační rozhraní pro umožnění přímého ovládání hardwarových prostředků. V rámci IS DTM bude vyžadováno nasazení aktuální verze knihovny DirectX. Využita bude zejména část DirectX Graphics. Nasazení se předpokládá v Servisním desktopovém prostředí, kde budou knihovny DirectX využívány Desktopovou komponentou pro editaci ZPS. Bude se jednat především o práci s 3D daty, kdy knihovny umožní maximální využití funkčnosti a výkonu dostupných hardwarových prostředků.

### Python 3

Je programovací jazyk, který umožní běh knihoven Django, Django Rest Framework a Strawberry. Tyto knihovny se v rámci systému IS DTM použijí pro tvorbu rozhraní, pomocí kterého budou klientské aplikace nebo geoprocesní nástroje konzumovat data uložená v databázích nebo externích službách. Instalace Python3 se očekává v serverovém prostředí, kde ji využije backend aplikačních komponent.

### Mapserver

MapServer je open-source vývoj prostředí pro vytváření prostorově aktivovaných internetových aplikací. Více na <https://mapserver.org/>

### GDAL

GDAL (Geospatial Data Abstraction Library) je knihovna určená pro čtení a zápis rastrových GIS formátů. Knihovna je vyvíjena pod hlavičkou Open Source Geospatial Foundation a vydávána pod licencí X/MIT. Součástí knihoven GDAL jsou i knihovny OGR poskytující nástroje pro práci s vektorovými daty. Více na https://gdal.org/

### Orchard Core

Orchard Core obsahuje dvě části – Orchard Core Framework a Orchard Core CMS. Orchard Core Framework je modulární, open-source, aplikační framework vytvořený pomocí ASP.NET Core. Orchard Core CMS (systém správy obsahu) je postavený na Orchard Core Framework a je využíván zejména ke správě webových aplikací. Všechny komponenty v Orchard Core lze měnit nebo rozšířit dle vlastních požadavků (modulární systém). Obsah lze přeložit do libovolného jazyka a poskytuje českou lokalizaci. Orchard Core disponuje otevřeným zdrojovým kódem (open-source).

### Create React App

"Create React App" je javascriptový dev stack integrující webpack, typescript a sass pro podporu vývoje a sestavení aplikace. Více na <https://create-react-app.dev/>.

### TypeScript

TypeScript je JavaScript s podporou statických typů. Více na <https://www.typescriptlang.org/>.

### React

React (také známý jako React.js nebo ReactJS) je bezplatná a otevřená front-end JavaScriptová knihovna umožňující vykreslování uživatelského rozhraní pomocí komponent. Více na <https://reactjs.org/>.

### Redux

Redux je javascriptová knihovna vycházející z Flux architektury, která unifikuje v aplikaci práci se stavem a daty. Více na <https://redux.js.org/>.

### REST

REST (REpresentational State Transfer) popisuje způsob předávání dat mezi klientem (webovým prohlížečem) a serverem. Pro popis rozhraní používáme specifikaci OpenAPI. Více na <https://swagger.io/specification/>.

### Apollo client

Apollo client je javascriptová knihovna pro dotazování serveru přes GraphQL. GraphQL je jazyk pro dotazování serveru. Apollo client bude využit na úrovni FrontEnd aplikací, které přistupují ke GraphQL rozhraní BackEdu jednotlivých komponent. Více na [https://graphql.org/.](https://graphql.org/)

### PostgreSQL

PostgreSQL (často se používá název Postgres) je svobodný a otevřený objektově-relační databázový systém. Funkce PostgreSQL zahrnují databázové transakce s atomicitou, konzistencí, izolovaností a trvalostí (ACID), automaticky aktualizovatelné pohledy, materializované pohledy, triggery, cizí klíče a uložené procedury. Systém je navržen pro zpracování celé řady vytížení, od jednotlivých strojů po datové sklady nebo webové služby s mnoha souběžnými uživateli. Pro podporu geografických objektů je využito rozšíření PostGIS. PostGIS umožňuje v databázi ukládat prostorové objekty, resp. jejich prostorové vyjádření (polohu). PostGIS implementuje specifikaci „Simple Features for SQL“ konsorcia Open Geospatial Consortium. PostGIS zahrnuje:

* Geometrické typy, jako jsou body, lomené čáry, polygony a další.
* Prostorové funkce průniku geoprvků.
* Prostorové funkce pro určení vzdálenosti, délky linií, výměry a obvodu ploch. Prostorové funkce obalové zóny, analýzy překryvu.
* Prostorový index R-tree používaný při prostorových dotazech.
* Výběr indexu při spojení prostorových a atributových dotazů.

### Keycloak

Keycloak je softwarový produkt s otevřeným zdrojovým kódem, který umožňuje jednotné přihlášení pomocí správy identit a přístupu zaměřené na moderní aplikace a služby. Pro většinu funkcí nabízí webové rozhraní, REST rozhraní a také rozšířitelné API. KeyCloak poskytuje přizpůsobitelné uživatelské rozhraní pro přihlášení, registraci, administraci a správu účtů. Bude použit ve verzi 18.0.0 a vyšší.

### Zabbix

Zabbix je open-source dohledový nástroj pro monitoring síťových prvků, serverů, operačních systémů a aplikací. Podporuje distribuovaný monitoring pomocí komponenty zabbix proxy, kdy je proxy server umístěn do jiné sítě a zabbix server s ní komunikuje přes jeden vyčleněný port.

Pro monitoring operačních systémů používá komponentu zabbix agent, ta sbírá z operačního systému základní výkonnostní metriky. Zabbix nativně pro monitoring používá různé protokoly, např. ICMP, SNMP, IPMI, HTTP, SSH. Nasbíraná data ukládá do databáze, kde probíhá automatická agregace dat pro práci s trendy. Data jsou vizualizována ve webovém frontendu, který nabízí pro zobrazení různé grafy, přehledy a další widgety. Na nasbírané metriky dovede zabbix reagovat upozorněním, pokud nějaká hodnota překročí určenou hranici. Upozornění může být zasláno formou e-mailu, sms, případně lze rozšířit o další IM technologie.

Nástroj bude sloužit pro monitoring kompletní aplikace DTM.

| **Název komponenty** | **Verze** | **Účel** |
| --- | --- | --- |
| Zabbix server | 6.0 LTS | Základní komponenta, která provádí měření a sbírá naměřené metriky, které dál předává do databáze. |
| Zabbix frontend | 6.0 LTS | Webový frontend napsaný v jazyce PHP sloužící pro zobrazení naměřených hodnot a také k administraci systému. |
| Zabbix proxy | 6.0 LTS | Proxy server sloužící pro monitoring distribuovaných sítí, také se používá pro offload Zabbix serveru. |
| Zabbix agent | 6.0 LTS | Agent instalovaný do operačních systémů pro sbírání základních výkonnostních metrik. |
| Nginx | 1.23 | Webový server. |
| PHP | 7.4 | Interpretr programovacího jazyka PHP. |
| PostgreSQL | 14 | Databázový server sloužící pro uchování dat. |

Tabulka 3 Zabbix vč. jeho účelu

### Technologie pro statistiku a monitoring

Jedná se o sadu open-source komponent OpenSearch, Logstash, Beats a OpenSearch Dashboards, které slouží pro sbírání, ukládání, analýzu (automatizované vyhodnocování vybraných auditních událostí) a zobrazení dat nasbíraných z logů a dalších zdrojů.

Nástroj bude sloužit pro modul statistika a monitoring. Pro statistiku zde budou vizualizována statistická data v grafech a tabulkách. V případě monitoringu bude prováděna analýza auditních záznamů.

| **Název komponenty** | **Verze** | **Účel** |
| --- | --- | --- |
| OpenSearch | 2.1 | Fulltextový vyhledávací nástroj podporující RESTfull rozhraní pro práci s daty. Data jsou uchovávána v indexech, ty pak slouží pro rychlé vyhledávání. |
| Logstash | 8.3 | Poskytuje vstupní a výstupní modul OpenSearch pro čtení a zápis dat do OpenSearch. Na vstupu přijímá data, např. textové logy, kde může provádět rozpad textového záznamu do jednotlivých atributů, takto předzpracovaná data ukládá do indexu OpenSearch. |
| OpenSearch DashBoards | 2.1. | Webový frontend pro vyhledávání a vizualizaci indexovaných dat v OpenSearch. Funguje také jako uživatelské rozhraní pro monitorování, správu a zabezpečení. |
| Filebeat | 8.3 | Kolektor dat, který je nainstalován na serverech jako agent sloužící k předání textových dat do OpenSearch buď přímo, nebo prostřednictvím Logstash. |
| Winlogbeat | 8.3 | Kolektor dat, který je nainstalován na serverech jako agent sloužící k předání logu Windows do OpenSearch buď přímo, nebo prostřednictvím Logstash. |
| Flexmonster | 2.8 | Flexmonster je reportovací nástroj (pivot table) pro vizualizaci dat. |

Tabulka 4 Technologie pro statistiku a monitoring vč. jejich účelů

### Drawings SDK

Drawings SDK je sada nástrojů pro vývoj, která poskytuje přístup ke všem datům ve formátu DWG a DGN prostřednictvím objektově orientovaného rozhraní API. Pomocí API je možné vytvářet a upravovat jakýkoli výkresový soubor typu DWG nebo DGN.

### Apache Tomcat

Apache Tomcat je open-source webový server založený na jazyce Java.

### PgAdmin (alternativně DBeaver)

Open source grafické administrační rozhraní pro správu a administraci RDBMS PostgreSQL.

### Tripwire

Tripwire je bezplatný systém detekce narušení s otevřeným zdrojovým kódem. Je to bezpečnostní nástroj pro sledování a upozorňování na změny souborů v systému. Tripwire je výkonný nástroj, který chrání systém před nežádoucími změnami. Pokud tedy dojde k nežádoucí změně v některém ze sledovaných souborů, tak pomocí reportu upozorní na zjištěné změny.

## Datový sklad – Produkční prostorové databáze

Produkční prostorové databáze slouží pro ukládání a správu prostorových dat ZPS, TI, DI a dalších datových sad nutných pro jejich správu a vedení (hranice SVO, obvody odvozovaných dat...).

Základní parametry prostorových databází:

* RDBMS PostgreSQL.
* Pro ukládání geometrických dat bude použita nadstavba PostGIS.
* Fyzický datový model obsahující údaje (atributy) pro dosažení kompatibility s aktuálně platným JVF DTM (splnění legislativních požadavků podle vyhlášky o DTM kraje).
* Administraci RDBMS provádějí uživatelé v roli „Administrátor datového skladu DTM“.
* Správa dat bude prováděna uživateli v roli „Správce dat ZPS“ a „Správce dat TI/DI“.
* Pro správu dat a zajištění integrity dat obsahují databáze triggery a úložné procedury.
* Pro potřeby zálohování databází bude pravidelně vytvářen backup, zálohování a recovery plán bude podrobně rozepsán v bezpečnostní dokumentaci.
* V rámci údržby budou pravidelně prováděny operace přepočítávání indexů a prostorové indexace (bude možné konfigurovat).
* Historizace dat bude řešena formou samostatných historizačních tabulek provázaných na tabulky s platnými daty (tzv. base tabulky).

Schéma datových skladů a datové toky mezi sklady jsou uvedeny v kap. [Příjem aktualizačních dat](#_Příjem_aktualizačních_dat). Oprávnění pro práci s daty jsou uveden v kap. [Popis práv a rolí](#_Popis_práv_a).

**Referenční PDB**

Množina prostorových databází systému DTM, které slouží pro evidenci a ukládání dat ZPS, TI a DI. Data budou vedena bezešvým způsobem a topologicky čistá. Ze systémového pohledu představují data obsažená v databázích Referenční PDB platná a referenční data DTM. Data budou v prostorových databázích historizována. Výdeje dat DTM budou prováděny z této Referenční PDB tak, aby byla zajištěna aktuálnost vydávaných dat.

Další funkcionalita datového skladu:

* Evidence systémových atributů.
* Evidence odvozených objektů "přesnosti hranic".
* Automatické odvození pomocných kartografických objektů ZPS.

**Publikační PDB**

Množina prostorových databází systému DTM, které slouží pro publikaci dat DTM. Databáze budou systematicky aktualizovány daty z Referenční PDB. Poskytují datový zdroj pro webové mapové služby provozované systémem DTM. Intervaly pro aktualizace databází budou konfigurovatelné a ve standardním nastavení budou prováděny denně. Publikační PDB bude konfigurována a optimalizována z hlediska výkonnosti pro dosažení max. odezvy a rychlosti při poskytování dat formou webových mapových služeb DTM.

**Editační PDB**

Databáze pro zpracovávání vstupních aktualizačních dat ZPS, TI a DI, které jsou předávány formou:

* Změnových dat v JVF DTM.
* Stavových dat v JVF DTM.

Mezi aktualizační data budou patřit data z GAD nebo data od VSP.

Pro zpracování aktualizačních dat bude vždy vytvořen samostatný pracovní prostor ve formě aktualizační verze. Jednotlivé verze pak slouží pro aktualizaci referenčních dat v Referenční PDB.

Funkcionalita datového skladu:

* Kontroly vstupních aktualizačních dat.
* Zpracovávání vstupních aktualizačních dat.
* Automatické generování odvozovaných objektů ZPS ze specifických typů objektů (Konstrukčních linií a definičních bodů).
* Editace dat.
* Odvozování objektů
* Doplnění systémových atributů, včetně identifikátoru objektu v rámci DTM ČR.

**Primární PDB TI/DI**

Prostorová databáze systému DTM, která slouží pro evidenci dat TI a DI vedená jako data vlastníka, správce nebo provozovatele (VSP). Data jsou vedena po jednotlivých VSP (např. obcích a městech), pro které bude kraj službu poskytovat. Ze systémového pohledu se jedná o data, která bude dále kraj jako VSP, resp. jako editor DTI, předávat do IS DMVS. Data budou historizována.

**Doplňující systémové databáze:**

| **Název** | **Popis** |
| --- | --- |
| Systémová DB DS DTM | Systémová databáze datového skladu DTM s konfiguračními tabulkami, které definují   * Zařazení objektů DTM do tříd prvků (tabulek). * Topologické kontroly dat. * Vztahy objektů reprezentovaných v DGN a v datovém skladu (využívá se při exportu dat do DGN). |
| Systémová DB JVF DTM | Systémová databáze JVF DTM s konfiguračními tabulkami, které definují:   * Vztahy objektů reprezentovanými v JVF DTM (aktuální verze) a v datovém skladu (využívá se při importu/exportu dat z/do JVF XML). Součástí definice jsou i typy objektů, které tvoří doplněk oproti standardu aktuální platné verze JVF DTM a vztahy mezi typy objektů ve výměnném formátu a typy objektů vyhlášky o DTM krajů. * Atributové kontroly dat JVF DTM. |
| Lokální data RUIAN | Pro potřeby realizace vybraných úloh bude vytvořena lokální databáze RUIAN s obsahem dat ISKN a ISUI. Obě tato schémata budou periodicky aktualizovaná. |

Tabulka 5 Doplňující systémové databáze

# Popis nastavení jednotlivých oblastí

Tato kapitola se zabývá detailním popisem nastavení, konfigurací a parametrizací jednotlivých oblastí (společné registry, role a přístupová oprávnění, číselníky, reporty).

## Popis instalace systému

**Instalace linuxových serverů**

Instalace linuxových serverů bude provedena pomocí kick start balíčků. Poskytovatel po schválení sizingu (sizing obsahuje kompletní informace o IP adresách instalovaných serverů) jednotlivých serverů připraví KICKSTART balíčky, které vystaví na ftp servery.

Postup instalace z kickstart balíčku:

* Stáhnout bootovací iso image pro síťovou instalaci.
* Nabootovat ze staženého ISO image.
* V menu vyplnit adresu kick startu.

Dále už instalace probíhá automaticky, po dokončení instalace se provede reboot.

Po dokončení základní instalace systému provede Poskytovatel dokončení instalace prostředí prostřednictvím ssh přístupu a začlení server do automatizovaného deployment systému.

Komunikace směrem do internetu bude omezena prostřednictví whitelistingu.

**Instalace windows serverů**

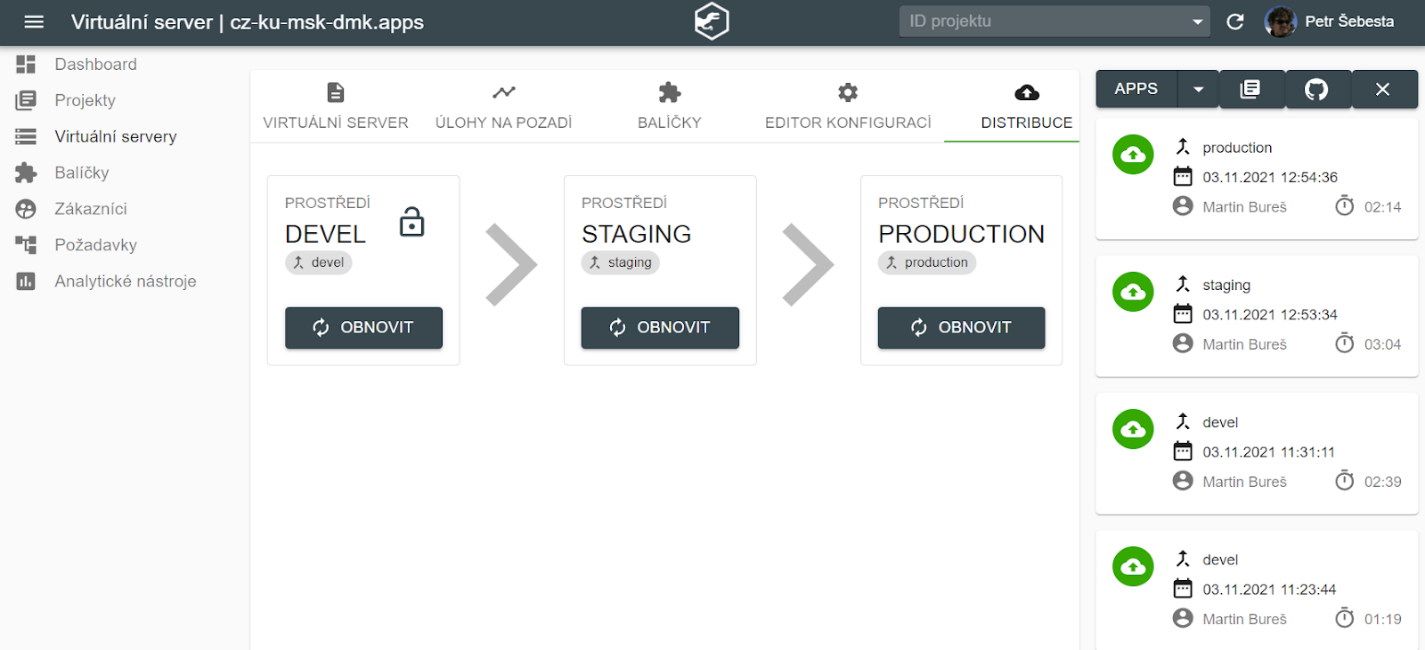
Základní instalaci operačního systému provádí Objednatel, který dle připraveného sizingu provede instalaci operačního systému s lokálním uživatelem Administrátor a předá přístup k serveru přes RDP Poskytovateli.

Po dokončení základní instalace systému provede Poskytovatel dokončení instalace prostředí a začlení server do automatizovaného deployment systému.

Komunikace směrem do internetu bude omezena prostřednictví whitelistingu.

**Instalace aplikací**

Aplikace budou na servery Objednatele instalovány prostřednictvím automatizovaného deployment systému, který prostřednictvím deployment serverů Poskytovatele (viz požadované prostupy) provádí aktualizace systému a aplikačních komponent na serverech. Průběh aktualizací bude ukládán do aktualizačních logů. Distribuční servery distribuují balíčky jak na testovací, tak i na produkční servery, a zajišťují tak instalaci totožných balíčků v obou lokalitách na testovacím i provozním prostředí. V rámci deploymentu bude na cílových serverech ukládáno posledních pět verzí příslušného aplikačního modulu. Vývoj probíhá ve vývojovém prostředí Poskytovatele. Distribuce aktualizací probíhá nejprve na testovací prostředí a po automatických i ručních kontrolách bude potvrzeno a provedeno nasazení do produkčního prostředí. Těmito nástroji bude provedena jak prvotní instalace, tak i následující aktualizace.



Obrázek 3 Ukázka uživatelského rozhraní deployment systému

**Nastavení a zprovoznění aplikačních databází**

Po instalaci HW PSQL serverů bude provedeno rozdělení systémových prostředků serverů pro jednotlivé instance DB (editační, referenční, publikační, systémové). Následně bude provedena konfigurace PgPool pro přístup k jednotlivým instancím. K datům PSQL přistupují koncové aplikace již pouze prostřednictvím PgPool, který zajišťuje load balancing nad datovým skladem.

**Založení geodatového skladu**

V jednotlivých instancích bude založena struktura geodatového skladu prostřednictvím zakládacích SQL skriptů. Zakládací skripty budou součástí implementační dokumentace a budou průběžně verzovány.

**Zakládání aplikačních databází**

Koncové aplikace jsou vybaveny aplikační komponentou, která při první instalaci provede založení struktury aplikační databáze a zajišťuje průběžnou aktualizaci databáze ve vazbě na verzi aplikačního modulu.

## Šifrování, kryptografie a bezpečnostní nastavení webového serveru

Bezpečnostní principy šifrování a kryptografie budou respektovat požadavky specifikované v zadávací dokumentaci včetně doporučení NÚKIB. Popis přesné specifikace a použitých parametrů kryptografických funkcí a algoritmů bude specifikován v bezpečnostní dokumentaci. Detailní popis použití konkrétních kryptografických funkcí a algoritmů (typ funkce, délka klíče, mód šifrování, použitý certifikát, bezpečnostní nastavení webového serveru, použité HTTP hlavičky) na úrovni jednotlivých prvků IS DTM, bude vznikat v průběhu implementace a stane se součástí dokumentace skutečného provedení.

## Konfigurace a parametrizace systému

Konfigurace a parametrizace jednotlivých prvků systému bude provedena v souladu s požadavky objednatele dané zadávací dokumentací, které jsou v odsouhlasené podobě detailně uvedeny v popisu jednotlivých komponent a funkcionalit v rámci této prováděcí dokumentace. Základní konfigurace systému, společné registry a číselníky budou vycházet z obecné definice s tím, že v průběhu postupného vývoje systému budou zohledněna specifika a požadavky Objednatele. Architektura řešení umožňuje pružně reagovat na případné změny legislativy, obecných principů a preferencí Objednatele, přičemž dílčí požadavky na změnu budou realizovány prostřednictvím změny konfigurace a parametrizace systému.

Detailní popis možností konfigurace a parametrizace systému do úrovně jeho jednotlivých částí, včetně registrů a číselníků, bude součástí samostatných dokumentů v rámci dokumentace skutečného provedení.

## Zálohování systému

Zálohování dat na úrovni serverové virtualizace bude realizováno nástrojem objednatele. Zálohování dat klíčových pro oživení systému nebo pro přenos na jinou lokalitu, které jsou součástí souborových úložišť a databází bude realizováno prostřednictvím standardních zálohovacích prostředků (systémů) objednatele, přičemž pro zálohování databáze bude použita kombinace plných a inkrementálních záloh transakčních logů (WAL) standardními prostředky databáze PostgeSQL.

Součástí dokumentace skutečného plnění bude detailní popis plánu a strategie zálohování systému, který bude obsahovat navržené formy zálohování včetně volby, jaké části informačního systému a databáze mají být navrženou (zvolenou) formou zálohovány.

Disaster recovery plán a strategie zálohování, popis procesu zálohování včetně kontrol stavu zálohování a proces obnovy systému budou tvořit nedílnou součást bezpečnostní a administrátorské dokumentace.

# Popis integračních vazeb

Kapitola se zaměřuje na návrh technického řešení integračních vazeb.

## Integrace na IS DMVS

Integraci se systémem IS DMVS zajišťuje komponenta IS DMVS WebAPI. Komponenta bude poskytovat sadu jednotlivých rozhraní (webových služeb), které budou zajišťovat komunikaci s konkrétními rozhraními (R1 – R28 dle aktuální dokumentace) IS DMVS prostřednictvím CMS2.

Komponenta zajistí plné komunikační workflow definované pro jednotlivé služby IS DMVS dle platného dokumentu – Popis a technické parametry služeb IS DMVS (https://cuzk.cz/DMVS/Popis-rozhrani/Popis-a-technicke-parametry-sluzeb-IS-DMVS\_-v1-5\_e.aspx).

Prostřednictvím tohoto rozhraní bude realizováno i přebírání dat lokálních správců DTM, jejichž povinností je provádět aktualizace prostřednictvím systému IS DMVS.

## Rozhraní pro komunikaci s aplikacemi třetích stran

Pro potřeby integrace na systémy třetích stran bude systém vybaven API, které bude poskytovat informace jednotlivých komponent IS DTM. API pracuje s aplikační databází jednotlivých komponent IS DTM a pomocí konfigurace umožňuje přístup k definovaným datovým sadám. Pro prvotní spuštění systému je plánováno zprovoznění API pro níže uvedené komponenty systému.

Na doménové adrese IS DTM JMK bude publikováno GraphQL rozhraní podporující aktivní práci s atributy aplikačních komponent. Ověření přístupu k API rozhraní bude probíhat prostřednictvím ověření JWT tokenu generovaného systémem Keycloak.

Součástí komunikace se systémy 3 stran jsou i mapové služby WMS a WFS, které jsou podrobněji popsány v kapitole [Komponenta pro poskytování mapových služeb](#_Komponenta_pro_poskytování).

Součástí dodávky bude dokumentace rozhraní, kterou bude Objednatel oprávněn předat neomezenému okruhu dalších subjektů, za účelem možnosti napojení na dodávaný informační systém. Dokumentace rozhraní bude natolik podrobná, aby umožnila napojení systému třetí strany administrátorem Objednatele a programovými úpravami výhradně v informačním systému třetí strany bez jakékoliv potřeby součinnosti Poskytovatele tohoto informačního systému. Popis jednotlivých rozhraní bude zpracován tak, aby umožňoval Objednateli jeho předání třetí straně, která na základě popisu bude schopna vytvořit bez jakékoliv součinnosti Poskytovatele odpovídající protikus rozhraní v plném rozsahu, a jeho spuštění bude odvislé pouze na povolení komunikace ze strany informačního systému.

Popis rozhraní bude obsahovat minimálně:

* Technologii, kterou je rozhraní realizováno.
* Popis jednotlivých datových typů a struktur, se kterými rozhraní pracuje.
* Způsob, kterým má být prostřednictvím rozhraní komunikováno.

V rámci technické podpory bude dokumentace udržována v aktuální podobě a bude reflektovat všechny případné změny. Dokumentaci rozhraní bude povinen Poskytovatel udržovat aktuální a v rámci ní udržovat platný popis veškerých rozhraní informačního systému a databází, se kterými je provázán. Taková dokumentace bude vedena až na úroveň popisu konkrétního způsobu práce rozhraní s daty a uvedení všech jednotlivých datových typů a jednotlivých položek, se kterými pracuje.

## IDM

Jako IDM server bude použit open-source nástroj KeyCloak (RedHat SSO). KeyCloak nabízí pro většinu funkcí webové rozhraní, REST rozhraní a také rozšířitelné API, přičemž administrátorské rozhraní bude členěno dle jednotlivých krajů a bude dostupné z adres CMS2. KeyCloak poskytuje přizpůsobitelné uživatelské rozhraní pro přihlášení, registraci, administraci a správu účtů. KeyCloak podporuje jednotné přihlašování a single sign-on (SSO) včetně podpory vícefaktorové autentizace (tzv. MFA, multifactor authentication). KeyCloak je možné také použít jako integrační platformu pro připojení ke stávajícím serverům LDAP a Active Directory. Ověřování je delegované na poskytovatele identity třetích stran. Jmenovitě Active Directory, případně JIP/KAAS pro zaměstnance krajského úřadu a NIA pro veřejnost.

### Funkční specifikace

#### Autentizační server

Bude použit open-source nástroj KeyCloak (RedHat SSO). KeyCloak nabízí pro většinu funkcí webové rozhraní, REST rozhraní a také rozšířitelné API. Nabízí také využití šablon pro webové stránky a notifikační e-maily.

#### Rozhraní pro autentizaci k serverům

Mezi KeyCloak a aplikačními servery bude využito standardizované rozhraní Open ID Connect (OIDC).

#### Integrace s lokálními zdroji identit

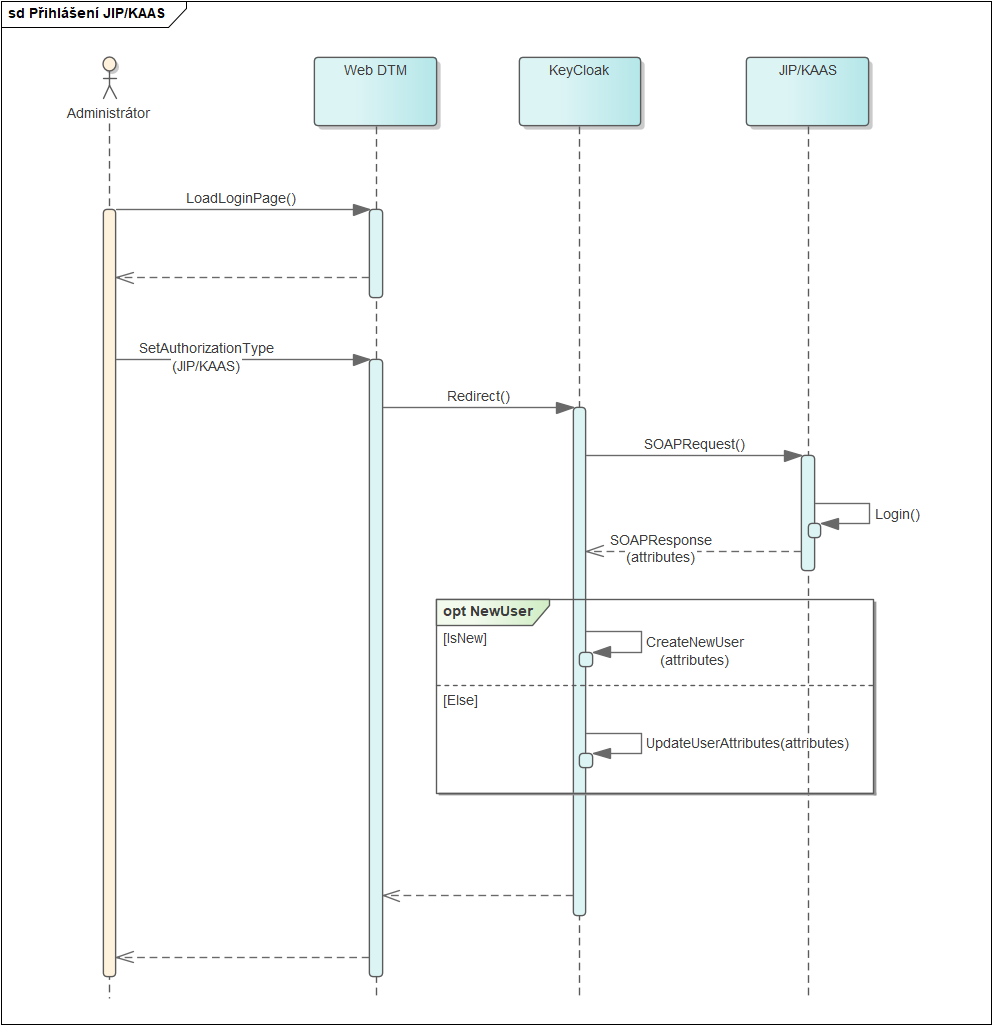
V rámci řešení bude realizována integrace s Active Directory jako lokálním zdrojem identit. Veškeré identity pro potřeby IS DTM se mohou čerpat i z JIP/KAAS nebo NIA.

Definované speciální účty budou mít vytvořenou lokální identitu v IDM KeyCloak.

### Propojení s JIP/KAAS

Přihlášení uživatele do systému DTM začíná volbou typu autentizace. Po výběru možnosti JIP/KAAS bude přesměrován na stránku CzechPointu, kde se přihlásí. Po úspěšném přihlášení dojde k přesměrování na DTM. Uživatel má přístupné funkce podle přiděleného oprávnění. Nový uživatel bude zaveden s oprávněním získaným z JIP/KAAS. Oprávnění pro IS DTM vkládá do JIP/KAAS správce Objednatele.

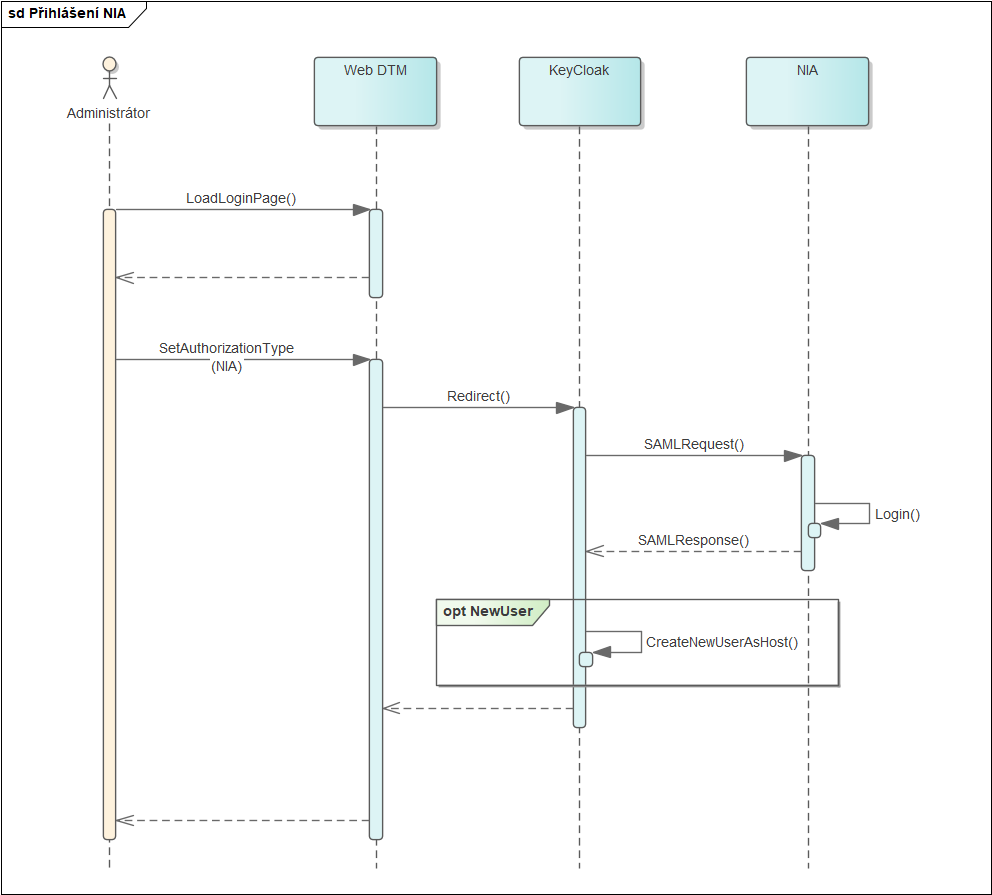
Přístupové role jsou vždy zapisovány do databáze nástroje KeyCloak. V případě nedostupnosti JIP/KAAS se musí použít jiný způsob přihlášení prostřednictvím NIA, případně lokálních účtů vytvořených správcem IS DTM.



Obrázek 4 Přihlášení JIP/KAAS

### Propojení s NIA

Přihlášení uživatelů může probíhat přes NIA. IS DTM bude registrován jako NIA Service Provider (SeP). Systém NIA neumožňuje poskytovat aplikační role. Proto bude pro uživatele autentizované prostřednictvím NIA vytvořena sada lokálních rolí.

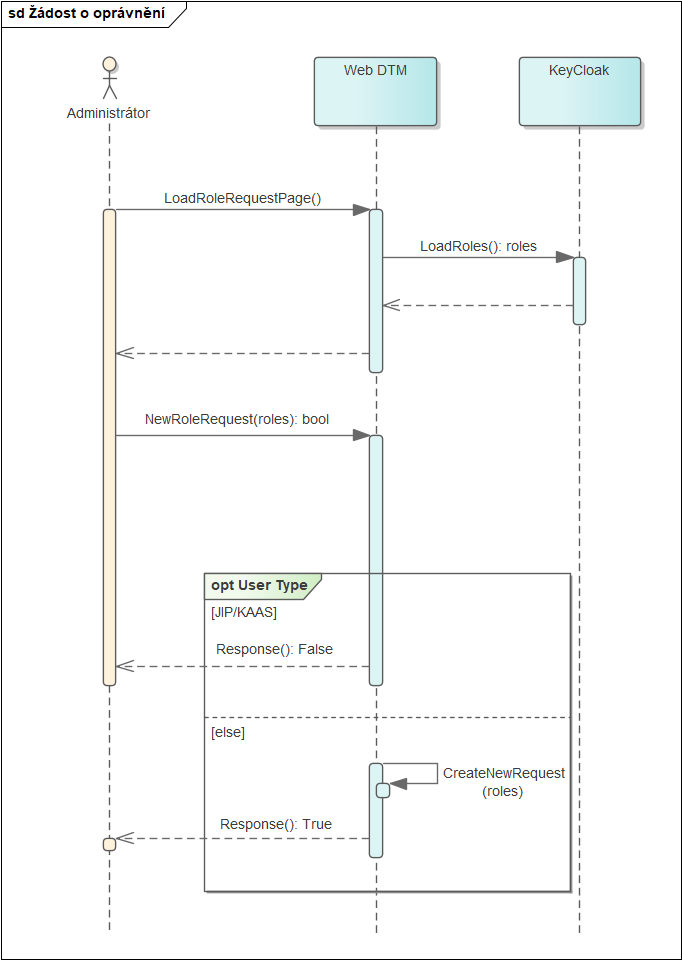


Obrázek 5 Přihlášení NIA

#### Správa rolí

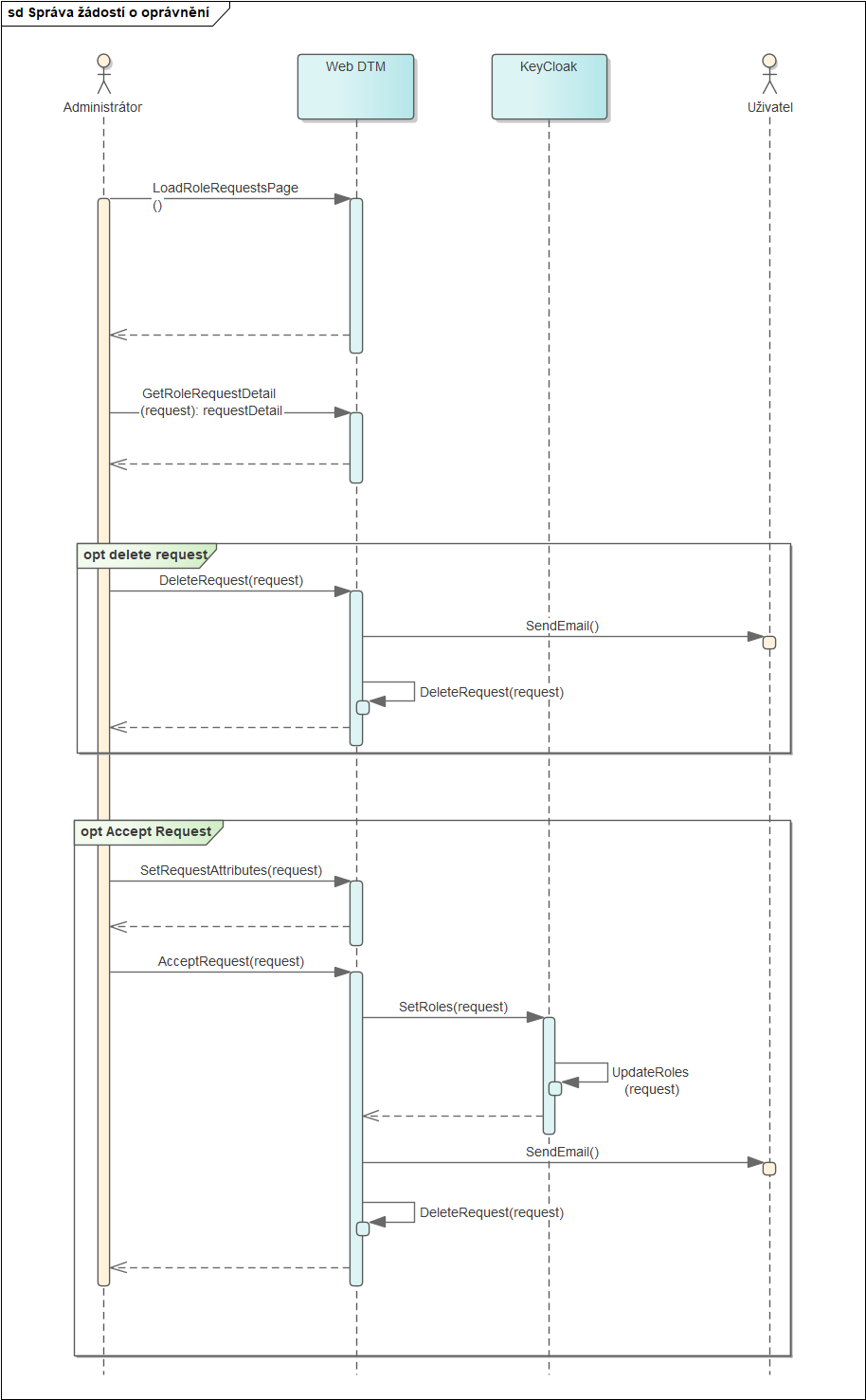
Po přihlášení bude moci uživatel prostřednictvím k tomu určenému modulu RolesManager (bližší popis modulu je uveden v kapitole [Komponenta zajišťující autentizaci a autorizaci všech přístupů a vstupů do IS DTM a jeho komponent včetně jeho služeb](#_Komponenta_zajišťující_autentizaci)) podat žádost o zařazení nebo odebrání aplikační role v IS DTM. Součástí žádosti bude kromě identifikace role a činnosti i poskytnutí informací pro následnou komunikaci o provedení (schválení či zamítnutí) operace (e-mailová adresa, telefonní číslo).

Toto je z principu věci povoleno pouze uživatelům autorizovaným přes NIA a AD. Uživatelé přihlašující se přes JIP/KAAS nebudou mít tuto možnost a musí si změnu oprávnění vždy řešit přímo se svým správcem JIP/KAAS.



Obrázek 6 Žádost o oprávnění

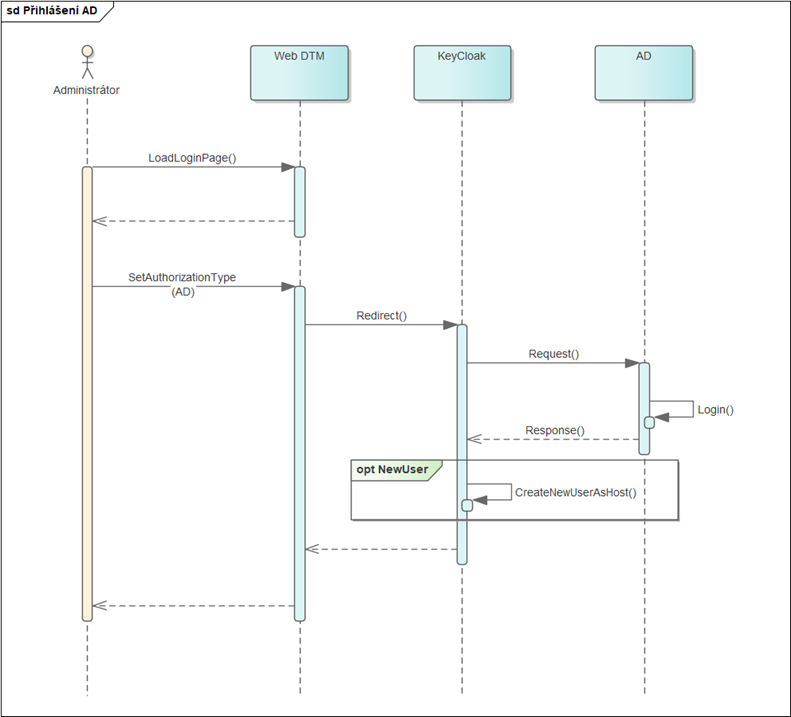
Rozhraní modulu umožní uživateli s rolí Security Admin prohlížet, schvalovat a zamítat tyto žádosti. Po potvrzení volby uživatelem s rolí Security Admin systém provede notifikaci – odeslání informace žadateli standardně elektronickou poštou.



Obrázek 7 Správa žádosti o oprávnění

### Propojení s AD

V rámci řešení bude realizována integrace s Active Directory jako lokálním zdrojem identit. Správa rolí pro AD je totožná, jako je u kapitoly [Správa rolí](#_Správa_rolí) pro NIA.



Obrázek 8 Přihlášení AD

### Sdílení informace o přihlášení klienta mezi komponentami

Keycloak poskytuje standard OIDC. Uživatel získá AccessToken (AT), kterým se prokazuje při komunikaci na klienta (resource), a to tak, že AT je obsahem http hlavičky.

## Integrace na IS základních registrů a na Egon Service Bus

V IS DTM není vedena lokální autoritativní evidence fyzických nebo právnických osob, není tedy realizováno přímé napojení na ISZR s tím, že využití referenčních údajů z ISZR je zprostředkováno prostřednictvím IS DMVS.

Pokud bude v průběhu realizace identifikována potřeba využití přímé komunikace s ISZR, nebo případné využití eGSB pro komunikaci s ostatními agendovými systémy (např. Portál stavebníka, IS IČS), bude na tyto nové skutečnosti reagováno a příslušná komunikační rozhraní budou do systému integrována.

## Integrace na Portál stavebníka a Národní geoportál územního plánování

Není součástí dodávky, je předmětem krácení projektu. Integrace na Portál stavebníka bude nahrazena integrací na UtilityReport.

## Integrace na IS ÚAP

Pro integraci se systémem ÚAP bude vytvořena speciální výdejová sada obsahující prvky jevů evidovaných v DM ÚAP (tento seznam v současné době připravuje MMR) a publikována přes příslušné rozhraní k dispozici dalším subjektům. Zároveň bude umožněno pracovat aktivně se službami WMS IS DTM.

## Integrace na ISSI

Není součástí dodávky, je předmětem krácení projektu.

# Návrh řešení postupu a pořadí při nasazování DTM JMK

V této kapitole je zpracován rámcový postup nasazení dodávaného systému. Jednotlivé kroky budou následovat za sebou ve stejném pořadí, v jakém jsou popsány v následujících kapitolách. Detailní časový harmonogram postupu nasazení jednotlivých částí je uveden v kapitole [Harmonogram projektu](#_Harmonogram_projektu).

## Příprava prostředí Objednatele

V prostředí Objednatele bude realizováno testovací a produkční prostředí. Prostředí a jejich jednotlivé části, včetně externí konektivity budou realizovány podle definovaného harmonogramu a požadovaných součinností uvedených v kapitole [Požadavky na součinnost Objednatele](#_Požadavky_na_součinnost). Detailní popis testovacího a provozního prostředí, jejich jednotlivých částí a externí konektivity, včetně konfigurací je uveden v samostatných dokumentech a bude tvořit součást dokumentace skutečného provedení.

## Příprava prostředí Poskytovatele

Vývojové prostředí bude sloužit programátorům k implementaci a konfiguraci daného řešení. Nebude se jednat o komplexní prostředí, tedy jednotlivé části celkového řešení spolu nemusí být integrovány. V tomto prostředí se také nemusí vyskytovat reálná data. Po otestování na testovacím prostředí bude systém nainstalován na produkčním prostředí Objednatele, kde proběhne finální testování. Způsob instalace a průběžných aktualizací systému bude podrobně popsán v provozní dokumentaci.

## Instalace a nasazení datového skladu

Po instalaci HW PSQL serverů bude provedeno rozdělení systémových prostředků serverů pro jednotlivé instance DB (editační, referenční, publikační, systémové). Následně bude provedena konfigurace PgPool pro přístup k jednotlivým instancím. K datům PSQL přistupují koncové aplikace již pouze prostřednictvím PGPool, který zajišťuje load balancing nad geodatovým skladem. V jednotlivých instancích bude založena struktura DB prostřednictvím zakládacích SQL skriptů. Zakládací scripty budou součástí Dokumentace skutečného provedení a budou průběžně verzovány.

## Import dat do datového skladu

Pro prvotní import dat do datového skladu bude využita Komponenta pro správu aktualizačních dat (potažmo její část pro příjem dat). Procesně bude prvotní import dat do datového skladu DTM proveden analogicky, jako v případě aktualizace dat ZPS z GAD. Import dat proto bude prováděn v následujících krocích:

* Základní kontroly syntaxe JVF DTM – kontrola validní struktury XML vstupních konsolidovaných nebo mapovaných dat ve formátu JVF DTM, v případě chyb v datech dojde k ukončení importu dat a předání chybových výstupů
* Kontrola předání doplňujících údajů a objektů nutných pro importy dat
  + Polygon oblasti aktualizace (formát SHP).
  + Polygon oblasti s plnými daty ZPS (území pro odvozování objektů – plochy a obvody, formát SHP).
  + Metadata k předaným datům (formát XML).
* Převod dat z JVF DTM do Editační PDB do části ZPS GAD (převod dat do struktury datového modelu datového skladu DTM).
* Věcné kontroly vstupních aktualizačních dat JVF DTM – kontrola převedených dat v Editační PDB, v případě chyb v datech dojde k ukončení importu dat a předání chybových výstupů.
* Topologické kontroly – kontrola převedených dat v Editační PDB, v případě chyb v datech dojde k ukončení importu dat a předání chybových výstupů.
* Import dat do Referenční PDB.
* Import/aktualizace metadat.
* Potvrzení importu dat.

Kontroly budou prováděny v souladu s kontrolami v kap. [Komponenty\_pro\_kontrolu.](#_Komponenty_pro_kontrolu)

Při prvotním importu konsolidovaných nebo mapovaných dat do DTM budou data od dodavatelů/kraje přebírána topologicky čistá. Data pro import musí být rozdělena (segmentována) na menší lokality (ORP, obce, katastrální území) a budou na sebe navazovat. Importy dat budou prováděny sekvenčně tak, aby na sebe jednotlivé importované lokality navazovaly, tj. byly zajištěny návaznosti v datech na hranicích lokalit. Kontroly konsolidovaných nebo mapovaných dat proto budou prováděny vždy po jednotlivých lokalitách. Dodavatelé dat budou mít zřízený přístup do kontrolních nástrojů IS DTM. Ze strany kraje bude zajištěna součinnost od pořizovatele dat podle následujících podmínek.

* Při nalezení chyb v datech vyzve zhotovitel pořizovatele dat k opravě dat a předá mu soubor s nalezenými chybami v datech ve formátu TXT případně ve formátu DGN.
* Reakce na opravy bude ze strany pořizovatel dat poskytnuta max. do 2 pracovních dnů od zaslané výzvy k opravě na kontaktní e-mail zhotovitele.
* Opravy chyb a nesouladů, tj. opravená nová data odešle pořizovatel dat zhotoviteli max. do 5 pracovních dnů od zaslání výzvy k opravě.

Dále bude v rámci importu dat ZPS provedeno jednorázové generování odvozených prvků ZPS (2D ploch a 3D hranice). Současně budou v datovém skladu nastaveny vazby mezi odpovídajícími konstrukčními a odvozenými prvky.

Metadata budou předána ve formátu XML v profilu ČR v4.2.

Aktualizaci dat importovaných lokalit bude zajišťovat do 21. 4. 2023 kraj přes svého dodavatele dat. Finální import aktualizovaných dat před ostrým spuštěním DTM bude proveden v průběhu měsíce května - června roku 2023. Validní data jsou taková data, která v předchozím období byla importována do DTM, tj. validně prošla kontrolami a byla nahrána do datového skladu.

Zhotovitel bude dále poskytovat objednateli součinnost při importech dat JVF DTM do datového skladu IS DTM JMK do 31. 12. 2023 (od 1. 1. 2024 nastává podle harmonogramu spuštění IS DMVS Pilotní provoz IS DMVS, tj. do této doby je vhodné nejpozději importovat data do IS DMT kraje).

Finální historizaci prvků v datovém skladu doporučujeme spustit dne 1. 1. 2024 (termín zahájení procesu historizace dat v datovém skladu IS DTM). Předchozí data v historizaci budou k tomuto datu smazána.

Popis způsobu importu dat je uveden v dokumentu Návod pro zavedení dat do IS DTM, který je k dispozici zde: <https://docs.google.com/document/d/1feHcW2iyLM326jTOyw8cQDESINqfiEKE/edit?usp=sharing&ouid=110469949795911157063&rtpof=true&sd=true>

## Způsob přeshraniční aktualizace dat ZPS

Přeshraniční aktualizace dat ZPS nastává pouze v provozní části projektu DTM kraje, tj. nesouvisí s pořizovací částí projektu.

Přeshraniční editace dat ZPS bude implementována podle pravidel a principů vycházejících z dokumentu Přeshraniční editace verze 0.6 schváleného KRS a zadávací dokumentace. Přeshraniční editace nastává na hranicích krajů nebo hranicích svěřených do editace jinému správci vybrané oblasti (SVO), na kterých se liší zejména v následujících bodech.

* Na hranici kraje se ukládají do datového skladu DTM kraje pouze objekty ZPS, které se nacházejí celé uvnitř území kraje (vymezeného hranicí kraje) nebo svou částí do tohoto území zasahují (kříží hranici kraje).
* Na hranicích SVO se ukládají do datového skladu DTM objekty ZPS v celém rozsahu vymezených oblastí svěřených do editace jinému SVO (data ZPS se vedou jak v systému DTM kraje, tak v systému jiného SVO).

Současně platí, že v rámci DTM bude provozováno 14 samostatných krajských datových skladů, ve kterých se data DTM vedou a spravují odděleně. V případě využívání dat je pak doporučeno s daty DTM jednotlivých krajů pracovat odděleně.

S ohledem na výše uvedený dokument a požadavky Objednatele jsou relevantní a validní následující vlastnosti dat ZPS.

* Data ZPS v datovém skladu kraje nemusí být topologicky validní s daty ZPS v datovém skladu sousedního kraje, tj. v datech se mohou vyskytovat překryvy, duplicitní geometrie apod.
* Historizace identických prvků ZPS vedených v datových skladech DTM různých krajů si nemusejí odpovídat, tj. mohou být rozdílné.
* S ohledem na předchozí bod výše související s historizací platí, že vydaná změnová nebo stavová data ZPS ze dvou datových skladů DTM krajů nemusejí být ve vzájemné integritě, tj. stavy změnových dat ZPS se ve vydaných změnových datech mohou na hranicích kraje lišit. Výsledná stavová data ZPS musejí být po aplikaci aktualizačních souborů ve všech spolu hraničících krajích shodné.
* Pro odvozené prvky ZPS (2D plochy a 3D hranice) v datovém skladu DTM kraje nebudou na hranici kraje vedeny kompletní odpovídající konstrukční prvky, ze kterých byl odvozený prvek vytvořen, tj. konstrukční hranice a definiční bod odvozeného prvku.
* S ohledem na předchozí bod související s odvozenými prvky platí, že datový sklad DTM kraje nemusí obsahovat databázové vazby mezi konstrukčními a odvozovanými objekty ZPS.
* Metody aktualizace dat ZPS v datovém skladu DTM (update, delete, insert) nemusejí odpovídat metodám aktualizace dat uvedeným ve změnových datech JVF DTM v podkladu pro vedení digitální technické mapy (GAD nebo v podklad zpracovaný jiným editorem ZPS).

Veškeré případné změny výše uvedených principů, pravidel nebo vlastností dat ZPS budou řešeny v rámci jednání Poskytovatele a Objednatele IS DTM, kde budou, na základě provedených analýz, stanoveny a odsouhlaseny podmínky pro realizaci takových změn.

## Implementace portálu pro DTM JMK

Implementace systému Orchard Core CMS se provede nasazením do softwarového prostředí webového serveru IIS. Bude založen příslušný Orchard adresář v MS IIS a spuštěna WEB Aplikace, která bude mít nastaven hostname a prostřednictvím nginx na Webserveru 1 bude vypublikována do CMS2 a internetu.

V rámci implementace bude provedeno nastavení databáze pro ukládání systémových údajů, kde bude využita RDBMS PostgreSQL. Současně bude provedena integrace (napojení) Orchard Core CMS s KeyCloak, ze kterého budou sdíleny uživatelské role, a to včetně rolí pro administraci. Integrační modul pro propojení s KeyCloak bude součástí instalace. Administrace bude prováděna pomocí uživatelského rozhraní Dashboard.

# Popis komponent

## Popis komponent DMK JMK

### Portál DTM Kraje

Portál DTM kraje bude vstupní aplikací pro webovou část řešení IS DTM. Jako Portál DTM kraje je označena webová část řešení IS DTM. Portál DTM kraje bude realizován dle příslušného grafického manuálu Jihomoravského kraje. Bude se jednat o soubor webových stránek včetně nástrojů na jejich správu, webových aplikací a webových mapových aplikací. Jednotlivé nástroje a uživatelská rozhraní budou sloužit nejen pro prohlížení evidovaných dat DTM, ale také pro jejich správu (evidence aktualizací, výdej dat DTM a další webové aplikace IS DTM) a pro komunikaci správce dat DTM s IS DMVS a s uživateli DTM uvnitř i vně úřadu. Portál bude splňovat veškeré požadavky na přístupnost webových stránek dané legislativou a metodickými doporučeními v dané oblasti včetně responsivního designu. Portál a veškeré jeho komponenty budou dostupné v české jazykové mutaci.

Obsah a funkcionalita:

* Informace o projektu (úvodní stránka, mapa stránek, kontaktní údaje).
* Aktuality (registrace k odběru novinek, RSS).
* Odkazy (IS DMVS, IS DTM sousedních krajů...).
* Nápověda (často kladené otázky).
* Dokumenty (možnost publikace libovolných dokumentů, metodik...).
* Hledání (fulltextové vyhledávání) v obsahu portálu.
* Odkazy do jednotlivých webových komponent IS DTM (rozcestník IS DTM).

### Redakční systém

Redakční systém představuje systém správy obsahu portálu DTM, který bude postaven na řešení Orchard CMS. Součástí komponenty bude možnost tvorby, modifikace a publikace textu webových stránek prostřednictvím jednoduchého WYSIWYG editoru, řízení přístupu k webovým stránkám, správa souborů, správa obrázků nebo galerií, kalendář.

Komponenta bude umožňovat konfiguraci a publikaci webových aplikací IS DTM na Portálu DTM kraje a potřebných webových stránek včetně připojování příloh v podobě dokumentů, obrázků atd. Přístup do redakčního systému bude umožněn pouze přihlášeným uživatelům s dostatečným oprávněním (s rolí Administrátor IS DTM nebo Security Admin). Obsah a funkcionalita je popsána níže:

* Systém pro správu obsahu portálu (CMS):
  + Tvorba webových stránek pomocí uživatelského rozhraní.
  + Strukturování obsahu, možnost využití datového obsahu.
  + Správa souborů, správa obrázků nebo galerií, správa kalendáře.
  + Workflows při schvalování obsahu.
  + Modul pro diskuzní fórum včetně jeho správy.
* Správa uživatelských práv – uživatelské role budou přebírány z Keycloak, dále bude umožněno nastavování oprávnění přístupu k určité části obsahu.
* Přizpůsobení grafické podoby portálu grafickému manuálu kraje nebo jiným předpisům definujícím vzhled a logiku uživatelského rozhraní kraje.

### Klient pro výdej dat

Klient pro výdej dat bude představovat prostředí pro zadávání požadavků na poskytnutí dat z datového skladu DTM a jejich vystavení. Požadavek na výdej dat bude podmíněn autorizací s výjimkou předpřipravených exportů a Opendat (které budou řešeny zejména pomocí předpřipravených balíčků dat). Veškeré žádosti o výdej neveřejných dat budou probíhat přes systém IS DMVS, kde bude prováděna i autentizace žadatele včetně ověření oprávněnosti na výdej dat (jedná se o informaci k 8. 3. 2023, která se může ještě měnit – případné změny budou reflektovány v dalších verzích této dokumentace). Veřejná data DTM budou dostupná ve formě Opendat. Komponenta bude umožňovat:

* Přebírání žádostí z IS DMVS a předávání informací o stavech a vyhotovení zpět do IS DMVS (vazba na rozhraní pro stahovací služby IS DMVS).
  + Služba pro poskytnutí obsahu DTM v definovaném území.
  + Služba pro získání veřejné části obsahu DTM.
  + Služba pro získání neveřejné části obsahu DTM.
  + Po přijetí požadavku na výdej z IS DMVS je workflow shodné s body níže.
* Výběr výdejní sady (sady ZPS, TI, DI) a požadovaného formátu (JVF DTM, SHP, DGN V8, GPKG, případně jejich kombinace).
* Výběr rozsahu výdeje:
  + Pomocí mapového zobrazení, prostřednictvím kterého bude možné graficky určit lokalizaci požadavku. Součástí bude prostředí pro zadání zájmového území – nakreslením výřezu (n-úhelník) v mapovém okně klienta.
  + Pomocí číselníků s oblastmi daného kraje (ORP, obce, katastrální území).
  + Součástí mapové části komponenty bude možnost vyhledání adresy nebo parcely v mapové aplikaci.
* Možnost zadání doplňujících údajů (Účel, poznámka, nahrání přílohy).
* Zadání platnosti dat (stavová data, změnová data od/do).
* Komponenta bude obsahovat workflow pro schválení žádosti.
  + Možnost přijetí/zamítnutí žádosti.
  + Odeslání notifikací (v podobě e-mailu) informující dané uživatele o schválení/zamítnutí žádosti.
    - Notifikace schvalovateli v případě žádosti o data podléhající schválení.
    - Notifikace žadateli o data v případě zamítnutí žádosti.
  + Odeslání notifikace (výzvy) ke stažení dat.
* Možnost konfigurace výdejů.
  + Nastavení výdejních sad (datová náplň).
  + Nastavení formy poskytnutí (datový balíček, standardní export dle vybrané oblasti).
  + Nastavení intervalů pro automatické vytváření datových balíčků.
  + Nastavení formátů pro výdejní sadu.
  + Nastavení schvalování pro výdejní sadu.
* Přehledy výdejů.
  + Zobrazení informace o stavu výdeje, id, informace o uživateli, rozsahu a obsahu výdeje.
* Filtrování ve výdejích.
  + Uživatel vidí jen své žádosti a stavy jejich vyřizování (správce/admin vidí vše).
* Možnost zrušení nebo pozastavení procesu výdeje dat
* Možnost nastavení období, po které je možné předávaná data archivovat.
* Nástroj pro transformaci dat DI a TI do datového modelu ÚAP.
  + Možnost konfigurace automatických transformací (v určitý čas, na základě nějaké události, např. při aktualizaci zdrojových dat DI/TI v datovém skladu DTM).
  + Možnost konfigurace vstupních a výstupních dat, jejich výběr (např. na základě sestaveného SQL dotazu, šablon pravidel atd.), transformace do jiné datové struktury či automatické vyplňování atributů dle zadávaných vstupních parametrů.
  + Logování prováděných operací.

Výdejní komponenta bude dostupná z portálu DTM pro přihlášeného i nepřihlášeného uživatele (v případě Opendat).

### Komponenta pro poskytování exportu dat (výdejní modul)

Komponenta pro poskytování služeb exportu je backend komponentou pro komponentu Klient pro výdej dat a poskytuje služby výdeje dat. Na základě požadavku se automatizovaně provede příprava výdeje ve formě datového balíčku ke stažení.

Komponenta bude umožňovat export zvolených dat DTM do zvoleného formátu. Balíčky vydaných dat budou ve formátu ZIP. Výdej dat bude realizován formou webové služby. Komponenta bude poskytovat následující funkcionalitu:

* Získání obsahu DTM v definovaném území.
* Získání veřejného obsahu DTM.
* Získání úplného obsahu DTM (včetně neveřejných údajů).
* Výdej dat DTM ZPS/TI/DI ve zvoleném formátu.
  + Stavová data – kompletní obsah dat v datovém skladu.
  + Změnová data – data za konkrétní období (od – do).
* Výdej dat bude umožněn do formátů: JVF DTM, SHP, DGN V8, GPKG.
* Vytvoření balíčku vydaných dat ve formátu ZIP.

Vytvoření exportů pro portály územního plánování

### Komponenta pro správu aktualizačních dat

Komponenta slouží k příjmu geodetických aktualizačních dokumentací ZPS, TI a DI, k jejich kontrolám a ke správě těchto dokumentací. Komponenta bude integrována do webového portálu IS DTM kraje. Autentizace do komponenty bude prováděna pomocí komponenty zajišťující autentizaci a autorizaci všech přístupů a vstupů do IS DTM a jeho komponent (přes portál IS DTM). Komponenta umožňuje kontroly aktualizačních dokumentací (ty jsou dále popsané v komponentě pro kontrolu), příjem aktualizačních dokumentací a součástí komponenty bude také kompletní workflow související se správou aktualizačních dokumentací. Komponenta pro správu aktualizačních dat bude propojena s komponentou IS DMVS WebAPI, která zajišťuje integraci se systémem IS DMVS (napojení na jednotlivé služby). Postup editace dat ZPS se proto bude řídit podle schémat:

* schéma procesu předání a kontroly aktualizačních dokumentací,
* schéma postupu editace – základní workflow zpracování změny,
* schéma postupu editace – workflow vlastní editace,
* schématy z dokumentu přeshraniční editace,
* workflow aktualizace TI a DI,

uvedených v zadávací dokumentaci nebo v dokumentu Přeshraniční editace verze 0.6 schváleného KRS.

#### Předběžné kontroly aktualizačních dat

Nástroj pro předběžnou kontrolu aktualizačních dat ZPS bude sloužit pro předběžnou kontrolu aktualizačních dat po formální stránce a popř. též pro účely testování výstupů geodetických SW třetích stran. Služba bude sloužit ke snížení chybovosti aktualizačních dokumentací, které budou geodeti předávat. Nástroj bude řešen jako součást komponenty pro správu aktualizačních dat (která bude řešena formou webové stránky), přičemž bude umožňovat funkčnost a procesy zajišťující:

* Nástroj pro výběr změnových aktualizační dat z disku uživatele ve formátu JVF DTM (výkres ve formátu JVF DTM).
* Možnost výběru typu kontroly – ZPS/TI/DI.
* Nástroj pro spuštění kontroly.
* Po spuštění kontroly uživatelem jsou systémem kontroly provedeny asynchronně.
* Provedení základních a topologických kontrol.
* Uživatel je informován o předpokládaném čase dokončení dané kontroly.
* Zobrazení výsledků kontrol.
  + Logovací soubor (soubor i log jako součást stránky).
  + Soubor (výkres) s lokalizacemi chyb ve formátu PDF/GML/XML.
  + Možnost stažení výsledků kontrol.
* Uživateli se zobrazí přehled jeho kontrol (historie kontrol k dané aktualizační dokumentaci).

Prováděny budou kontroly na validní strukturu XML dat JVF DTM a dále věcné a topologické kontroly dat, které jsou řešeny v kapitole [Komponenty pro kontrolu (backend)](#_Komponenty_pro_kontrolu) v této dokumentaci.

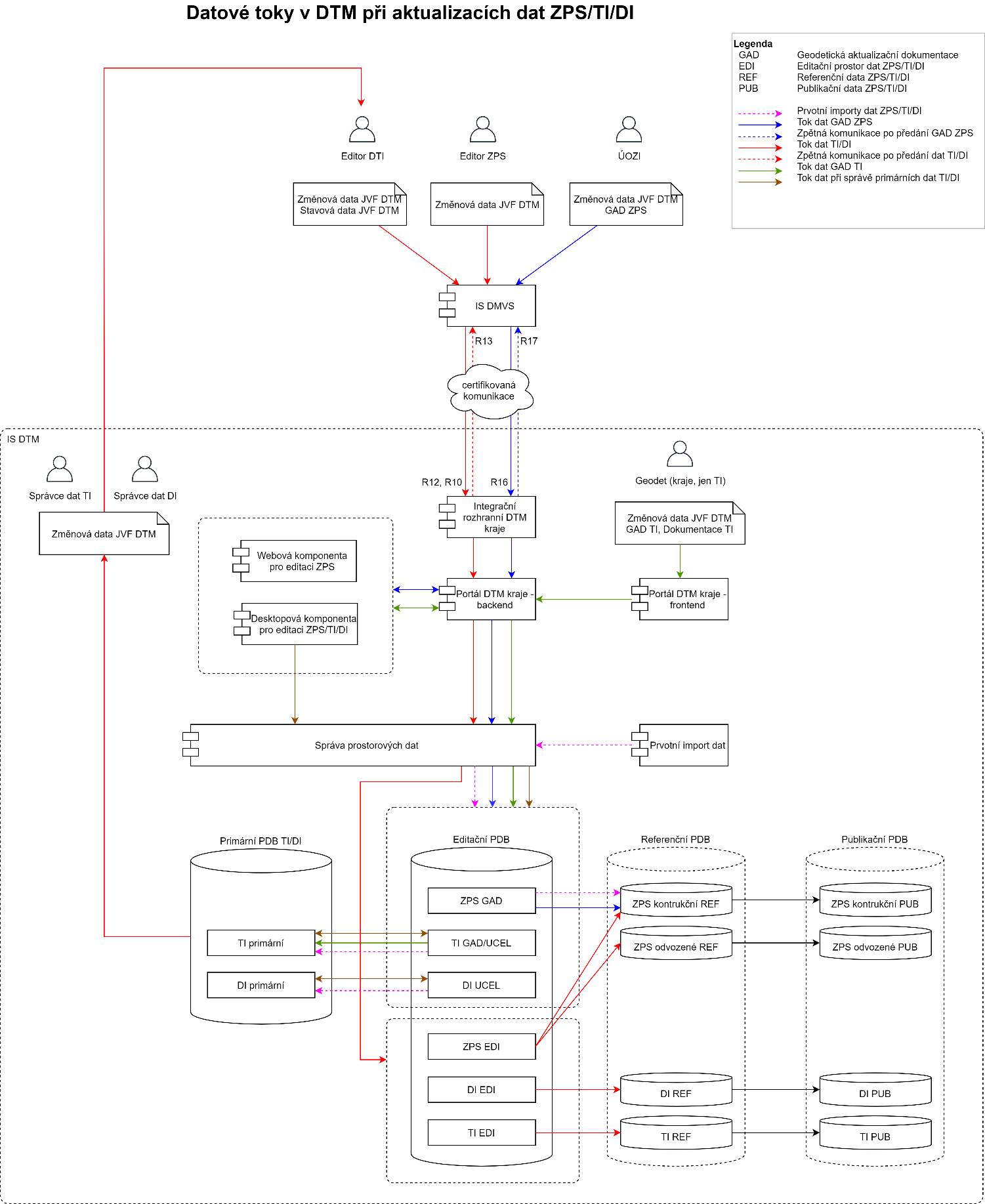
#### Příjem aktualizačních dat

Součástí komponenty pro správu aktualizačních dat budou nástroje pro přebírání aktualizační dokumentace. Součástí implementace těchto nástrojů bude i vytvoření vazeb na služby IS DMVS. Komponenta bude obsahovat nástroje, společné pro všechny případy příjmu dat, které jsou popsány níže v této kapitole:

* Nástroj pro spuštění importu do editační databáze.
  + Indikace probíhajícího importu.
* Možnost vyhledávání a zobrazení seznamu aktualizačních dokumentací podle nastaveného filtru (ID, název, stav, organizace).
  + Bude možné rozlišit dokumentace přijímané přes IS DMVS, IS DTM a prvotní importy.
* Možnost zobrazení přehledných informací o dané aktualizační dokumentaci (detail dokumentace).
* Vedení údajů o průběhu zpracovávání aktualizace, včetně importu (stavy životního cyklu).
* Možnost zrušení aktualizace.
* Možnost uzavření aktualizace.
* Možnost informování IS DMVS o ukončení aktualizace.
* Nástroj pro přiřazení editora aktualizačních dat.
* Nástroj pro spuštění webového editačního klienta z detailu dokumentace.
* Vazba na Rozhraní a pro správu údajů o vlastnících, správcích a provozovatelích sítí dopravní a technické infrastruktury IS DMVS.

Mimo to bude komponenta obsahovat obecné rozhraní API, které bude mimo jiné sloužit pro komponentu Statistika s možností konfigurace zadávaných parametrů a obsahu zobrazení výsledků (časové intervaly od-do, subjekt, typ, stav) s možností exportů a práce se statistikami (řazení, dodatečné filtrování atd.).

Dále jsou popsány jednotlivé možnosti příjmu dat (vstupy). K zobrazení postupů slouží obrázek č. 9 – Diagram datových toků v DTM při aktualizacích dat ZPS/TI/DI. Jedná se o příjem aktualizačních dat přes systém IS DMVS, příjem aktualizačních dat přes IS DTM a součástí komponenty je také prvotní import dat do datového skladu DTM



Obrázek 9 Datové toky při aktualizacích dat ZPS/TI/DI

#### Příjem aktualizačních dat přes systém IS DMVS

Pro změnová data přijímaná přes IS DMVS budou vytvořeny nástroje popsané níže:

* Ověření uživatele zasílajícího geodetickou aktualizační dokumentaci DTM vůči roli Geodet.
* Možnost převzetí aktualizačních dat vložených do IS DMVS do evidence k zapracování do DTM.
  + Přiřazení unikátního ID.
  + Převzetí informací o aktualizační dokumentaci z IS DMVS včetně přiložených souborů.
  + Možnost doplnění metadat včetně typu aktualizační dokumentace
  + Možnost kontroly aktualizačních dat.
  + Možnost zamítnutí/přijetí aktualizační dokumentace včetně předání informace do IS DMVS.
    - * Kategorizace a popis reklamace při zamítnutí.
      * Notifikování uživatelů při zamítnutí dokumentace.
      * Evidence údajů o geodetech a správcích za účelem možnosti mimoreklamační komunikace.
* Možnost uzavření aktualizace po zapracování aktualizačních dat do DTM.
  + Informování IS DMVS o ukončení aktualizace.

#### Příjem aktualizačních dat pomocí systému IS DTM

Mimo příjem přes IS DMVS bude systém umožňovat také provádění příjmu čistě přes IS DTM kraje, a to GAD s daty TI, DI nebo dokumentaci TI, DI. Pro tento příjem budou sloužit funkcionality popsané níže.

* Nástroj pro přebírání aktualizační dokumentace z bezchybné předběžné kontroly.
* Nástroj pro založení geodetické aktualizační dokumentace.
  + Možnost zadání informací (metadat) k aktualizační dokumentaci.
  + Možnost nahrání aktualizační dokumentace.
  + Přidělení unikátního ID dokumentaci.
  + Možnost odeslání dokumentace ke kontrole ze strany správce DTM.
* Nástroj pro odeslání dat do IS DMVS a následné převzetí zpět do IS DTM.
* Možnost kontroly aktualizačních dat přijímaných přes IS DTM.
* Možnost zamítnutí/přijetí aktualizační dokumentace.
* Notifikace uživatelů při zamítnutí aktualizační dokumentace.
* Zobrazení protokolu k importu dat, případně chybové výstupy kontrol.
* Vizualizace importovaných dat bude prováděna pomocí mapových služeb (WMS).

#### Prvotní import do datového skladu DTM

Tato komponenta bude využita pro prvotní import dat do datového skladu DTM, při kterém budou zpracovávány velké objemy vstupních dat ve formátu JVF DTM. Data do datového skladu DTM budou importována postupně (sekvenčně) po lokalitách. Data importovaných lokalit budou odpovídat charakteristikám popsaným níže. Kontroly a workflow příjmu dat budou prováděny stejným způsobem, jako je to u standardního příjmu aktualizačních dat.

Charakteristiky importovaných lokalit:

* Data lokality budou limitována max. rozsahem nebo max. počtem prvků.
* Segmentace dat bude odpovídat specifikovaným pravidlům (pravidla definují způsob uzavírání ploch apod.); pravidla definuje Poskytovatel v součinnosti s krajem a budou sloužit zpracovatelům dat pro validní segmentaci dat; pravidla budou zpracována v rámci realizace projektu (nejsou součástí prováděcí dokumentace) s předpokládaným termínem do poloviny září 2022.

Segmentace dat ŘSD a SŽ bude provedena na základě dohody s ŘSD a SŽ.

#### Řešení kolizí při souběžném zapracovávání dat

Uvedený popis se nevztahuje na případ přeshraniční editace dat.

Při zapracovávání dat z GAD jsou souběhy řešeny na úrovni Editační PDB, tj. pomocí editačních prostorů jednotlivých GAD, které jsou v databázi vytvářeny. Pro každou rozpracovanou GAD je vytvářena oblast změny. Všechny oblasti změn zpracovávaných GAD jsou vedeny v jednotné třídě prvků, včetně informací o jejich stavu zpracování. V případě finálního zapracování jakékoliv změny GAD do referenčních dat systém provede kontrolu kolizí se všemi rozpracovanými změnami GAD. V případě kolize zapíše do všech identifikovaných změn GAD (do editačních prostorů GAD v Editační PDB) údaje o kolizi. Na základě zapsaných údajů o kolizi následně systém informuje odpovídající správce změn GAD. Systém následně provede aktualizaci referenčních dat v editačním prostoru identifikované kolizní změny GAD.

### Webová komponenta pro editaci ZPS

Základním požadavkem na komponentu je zajištění maximální přehlednosti, intuitivnosti a ergonomie z hlediska workflow. V komponentě bude minimalizováno množství nutných viditelných ovládacích prvků na ploše aplikace a maximalizován efektivní rozsah uživatelského rozhraní pro podporu provádění klíčových úkonů uživatele. Maximální důraz bude kladen na využití vhodných editačních nástrojů. Uživatelské prostředí nástroje bude obsahovat grafické editační rozhraní pro práci ve 2D. Editační prostředí v rámci webové komponenty bude podporovat:

* Základní nástroje pro navigaci ve scéně (změnu měřítka, posun mapy, přechod na výchozí rozsah, přiblížení mapy na vybrané objekty, rozsah mapy na všechny objekty).
  + Možnost zvolení mapového měřítka (zoomu mapy).
  + Přiblížení, oddálení, posun v mapě.
  + Možnost zobrazení výchozího rozsahu mapy.
  + Možnost přiblížení na vybrané objekty.
  + Možnost zobrazení rozsahu všech objektů.
* Zobrazení stromové struktury tříd objektů.
* Zobrazení a přepínání tříd objektů (vrstev).
* Zobrazení vektorových tříd objektů z centrálních datových zdrojů IS DTM a IS DMVS.
* Zobrazení rastrových tříd z centrálních datových zdrojů IS DTM a IS DMVS.
* Zobrazení webových prohlížecích služeb dle standardu OGC (WMS, WMTS).
* Možnost výběru objektu/objektů a zobrazení jejich detailu.
* Vyhledání objektu na základě jeho atributu.
* Měření délek, ploch a odečítání souřadnic.
* Možnost exportu mapy.
* Možnost zobrazení lokalizovaných chyb.
* Nástroj pro provádění průběžných kontrol v průběhu editace.
* Nástroje pro podporu editace (nástroje pro zapracování dat).
* Možnost pro porovnání aktualizačních a referenčních dat.
* Nástroj pro upozornění uživatele, že proběhla změna referenčních dat.
* Nástroje pro podporu práce a ověřování LEVELS, tj. možnost samostatného zobrazení jednotlivých LEVELS pro pohledovou i aplikační kontrolu topologické návaznosti konstrukčních prvků a existenci příslušných definičních bodů v jednotlivých úrovních API rozhraní.

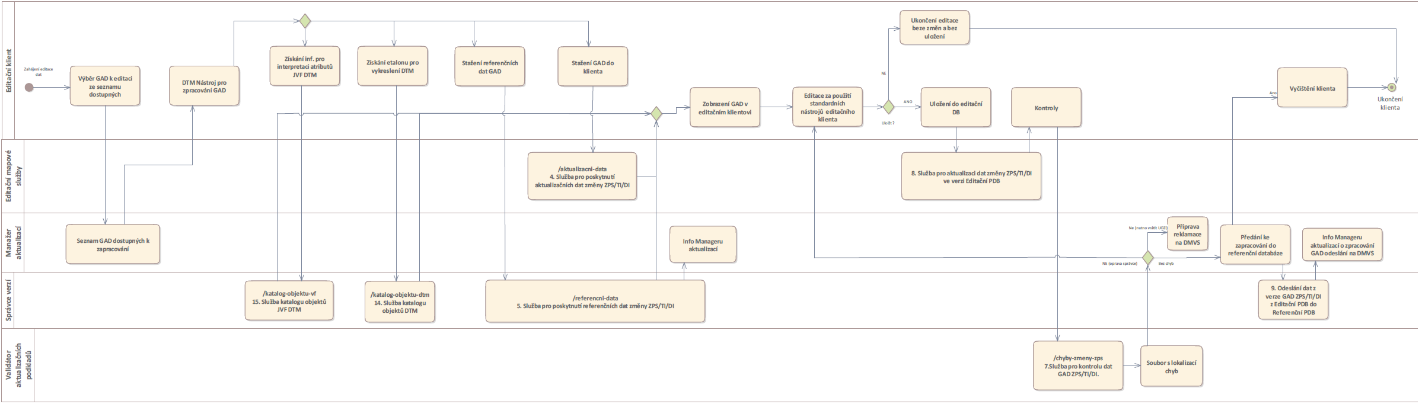
### Desktopová komponenta pro editaci ZPS/TI/DI

Komponenta bude sloužit ke kontrole a editaci GAD – ZPS/TI/DI a primárně bude určena pro správce/editora datového skladu. Jedná se o alternativu komponenty “Webová komponenta pro editaci ZPS”, kdy úkolem desktopového editoru ZPS bude zejména provádění složitějších a specifických úkonů s daty. Proto bude klient sloužit zejména pro zpracovávání aktualizačních dat (GAD) v provozní fázi DTM, které budou většího rozsahu nebo budou obsahovat větší chybovost dat GAD. Pomocí nástrojů klienta pak bude možné ze strany správce/editora datového skladu např. připravovat účelové podklady pro zpracovatele chybných GAD (geodety) tak, aby jejich opravy prováděli efektivně.

Provedení zobrazení historických dat k určitému datu bude realizováno prostřednictvím výdeje dat v souborovém formátu JVF, který následně správce/editor otevře v komponentě.

Nástroj bude realizován formou desktopové aplikace pro operační systém MS Windows a bude lokálně nainstalován na PC správce/editora. Základním konceptem technologie bude využití jednotného jádra GSFrameWork, vyvíjeného na komponentním objektovém principu. Bude se jednat o produkt Poskytovatele (není třeba zajišťovat licence komponent třetích stran).

Základní činnosti v rámci správy DTM, související se zobrazováním, kontrolami a zpětnou propagací prvků ZPS do datového skladu, budou realizovány formou webových služeb (REST API). Díky tomu bude zaručena bezpečnost a zejména konzistentnost procesů prováděných při manipulaci s prvky ZPS v různých klientech (ve webové editační komponentě a v desktopové editační komponentě). Samotný import aktualizačních dat ZPS ve formátu JVF DTM do datového skladu a vyplnění základních metadatových údajů zajistí [Komponenta pro příjem a kontrolu aktualizačních dat](#_Příjem_aktualizačních_dat). Takto přejatá a základním způsobem zkontrolovaná data může následně desktopový editační klient prostřednictvím webových služeb převzít k dalším kontrolám, editaci a zpracování.



Obrázek 10 Workflow editace ZPS/TI/DI Desktopovou komponentou

Mimo požadovanou funkcionalitu bude disponovat i další vybranou funkcionalitou běžnou pro CAD/GIS desktopové produkty. Nástroj bude koncipován modulově. Uživatel tedy bude mít možnost zapínat a vypínat jednotlivé panely nástrojů a pracovní okna a volit jejich uspořádání a velikost v rámci pracovní plochy za účelem přehlednosti, intuitivnosti, ergonomie, konkrétního workflow a osobních preferencí a zvyklostí. Uživatelské rozložení nástrojů a oken bude uloženo za účelem načtení při příštím spuštění. Součástí aplikace bude běžné 2D mapové okno a dále 3D mapové okno se středovou projekcí zobrazených prvků. K dispozici bude mimo jiné funkcionalita, která zajistí synchronizaci pohledů 2D a 3D oken a nástroje a zobrazení pro podporu vizualizace a kontroly editace.

Součástí 2D mapového okna bude ovládací panel pro základní práci se scénou, případně bude možné vybranou funkcionalitu aktivovat příslušnou klávesovou zkratkou. K dispozici budou nástroje pro změnu měřítka, posun mapy, přechod na výchozí rozsah, přiblížení mapy na vybrané objekty, rozsah mapy na všechny objekty. Aplikace umožní zobrazení a přepínání jednotlivých rastrových a vektorových vrstev (tříd) z různých zdrojů, včetně IS DTM a IS DMVS (formáty WMS, WMTS, JVF DTM, GeoJSON, DGN, SHP, bodová mračna). Dále bude umožněn grafický a atributový výběr prvků, měření délek a ploch, odečítání souřadnic, pokročilé nastavení symbologie tříd prvků, měřítkově závislé nastavení tříd prvků, zobrazení mapy v zadaném měřítku, identifikace prvku a zobrazení jeho vlastností. Součástí nástroje budou nástroje pro podporu editace a kontrol a nástroje pro podporu práce a ověřování LEVELS.

Mimo zobrazení prvků v klasickém mapovém okně bude k dispozici i 3D mapové okno. Součástí funkcionality bude identifikace objektů a zobrazení jejich vlastností, nástroje pro navigaci ve 3D scéně, přepnutí do standardních pohledů, návrat do výchozího zobrazení scény, výběr objektů, zobrazení stavu DTM k zadanému datu/času. V rámci 2D a 3D okna bude možné zobrazovat i další podkladová data (např. bodová mračna, DMT).

### Komponenty pro kontrolu (backend)

Komponenta poskytuje backend služby pro validaci (kontrolu) aktualizačních podkladů pro zpracování kontrol dat ZPS, TI, DI, které využívají komponenty zajišťující kontrolu dat. Mezi vstupní data patří aktualizační data, která budou sloužit pro aktualizaci dat v provozní fázi projektu a dále konsolidovaná nebo mapovaná data (importovaná data při prvotních importech), která budou zavedena do systému v realizační fázi projektu. Komponenty provádí kontrolu dat ZPS, TI, DI vůči referenčním datům. V následujících podkapitolách jsou uvedeny jednotlivé komponenty pro kontrolu aktualizačních dat.

Komponenta poskytuje kontroly pro data:

* ZPS, TI, DI přijatých z IS DMVS.
* Předběžné kontroly aktualizačních dat prováděných geodety (viz kap. [Předběžné kontroly aktualizačních dat](#_Předběžné_kontroly_aktualizačních)).
* TI, DI GAD přijatých na Portálu DTM kraje.

Služba bude umožňovat konfiguraci rozsahu prováděných kontrol v závislosti na způsobu volání služby ze strany klientů nebo rozhraních systému. Proto bude možné provádět kontroly v následujícím rozsahu:

* Základní kontroly syntaxe JVF DTM.
* Věcné kontroly vstupních aktualizačních dat JVF DTM.
* Topologické kontroly.

Kontroly budou prováděny pro následující verze JVF DTM.

* Pro data ZPS pro verze JVF DTM 1.4.2 a JVF DTM 1.4.2.1
* Pro data TI a DI pro verzi JVF DTM 1.4.2.1

Kontroly budou vracet následující výstupy.

* Soubor logu procesu kontroly.
* Výpis identifikovaných chyb (možnost exportu do logu).
* Soubor s lokalizacemi chyb ve formátu JVF DTM.
* Soubor (výkres) s lokalizacemi chyb ve formátu PDF/GML/XML (pouze pro předběžné kontroly aktualizačních dat).

#### Věcné kontroly vstupních aktualizačních dat JVF DTM

Provádí se kontroly údajů JVF DTM, které nelze zajistit základními kontrolami syntaxe JVF DTM, a které jsou v rámci JVF DTM vyžadovány.

#### Řízení prováděných kontrol

Kontroly jsou v systému prováděny pomocí samostatných řízených procesů. Spouštění kontrol může provádět Komponenta pro správu aktualizačních dat nebo komponenta Editační mapové služby. Při vytvoření požadavku na kontrolu je nastavena každé kontrole priorita, na základě které systém spouští procesy jednotlivých kontrol z hlediska jejich důležitosti. Systém na základě priorit spouští jednotlivé kontroly v různých časech s ohledem na optimální využívání prostředků (balancování zátěže).

### Komponenta – Georeporty

Komponenta umožňuje uživatelskou tvorbu georeportů z datového fondu DTM. Ke generování georeportů a k administraci této funkcionality bude sloužit webová aplikace. Aplikace bude přístupná přes webový prohlížeč ze zařízení připojeného do sítě Internet. Aplikace umožní zadání parametrů a vygenerování georeportu pro přihlášené uživatele. Nepřihlášený anonymní uživatel bude moci po zadání e-mailové adresy provést vygenerování vybraných georeportů bez možnosti uložení zadaných parametrů a opakování generování. Zároveň aplikace umožní přihlášenému administrátorovi provádět konfiguraci systému. Budou tedy využívány následující role:

* Host
  + role oprávněná ke generování základních georeportů.
* Správce IS DTM (administrátor).
  + role určená pro administraci komponenty georeporty.
* Případně dle potřeby další role IS DTM.
  + dle případných specifických požadavků je možné jednotlivým rolím konfigurovat určitou sadu georeportů.

Jednotlivé uživatelské role mohou mít dle konfigurace k dispozici různé typy georeportů. Zadání vstupních parametrů georeportu proběhne přes webový formulář. Zakreslení zájmového území provede uživatel polygonem v mapové aplikaci, která bude součástí modulu. U všech přihlášených uživatelů bude mimo vygenerování georeportu provedeno uložení zadaných vstupních parametrů. Následně budou v aplikaci uživateli k dispozici informace o vygenerovaných georeportech. Uživateli bude umožněno využít v minulosti zadané vstupní parametry pro načtení do formuláře, kde provede dle potřeby jejich případnou úpravu a spustí generování nového georeportu. Generování georeportu se předpokládá asynchronně následujícím způsobem (popsaný postup může být upraven):

* Zadání požadavku na georeport:
  + Volba typu georeportu.
  + Zadání vstupních parametrů georeportu.
  + Případně načtení a úprava parametrů dříve realizovaného georeportu.
* Odeslání požadavku:
  + Odeslání požadavku na georeport ke zpracování.
  + Uložení požadavku a vstupních parametrů do provozní DB.
* Zpracování požadavku:
  + Spuštění procesu zpracování požadavků.
  + Vyzvednutí relevantních požadavků z DB fronty.
  + Zpracování požadavků – vygenerování georeportu (dle šablony a vstupních parametrů).
* Předání vygenerovaného georeportu:
  + Odeslání vygenerovaného georeportu (předpoklad je formát PDF) na e-mailovou adresu uživatele.

Ke zvážení a konzultaci s Objednatelem je definice omezujících podmínek vstupních parametrů (např. maximální velikost vstupního polygonu) za účelem omezení extrémní zátěže HW a SW prostředků při zpracování náročných požadavků. Konkrétní hodnoty bude možné stanovit v rámci testovacího provozu. Případně bude možné hodnoty měnit i v rámci provozu systému.

Součástí aplikace bude návrhář georeportů (grafické uživatelské rozhraní), kde administrátor může provádět úpravu šablon georeportů nebo vytvářet nové šablony. Další související nastavení aplikace (např. dostupnost daného georeportu pro jednotlivé role) provede administrátor pomocí dalších nástrojů dostupných ve webové aplikaci. Pro zajištění komplexní správy systému georeportů – zejména vytváření nových georeportů musí administrátor znát datovou strukturu IS DTM, orientovat se v jazyce SQL, orientovat se v URL řetězci a umět pracovat v grafickém uživatelském prostředí návrháře georeportů. Případné generování mapových příloh georeportů zajistí mapový server, který bude součástí komponenty. Případnou konfiguraci podoby mapové přílohy provede administrátor pomocí desktop administračního nástroje mapového serveru. Spuštění generování mapové přílohy bude voláno prostřednictvím HTTPS požadavku s parametry uvedenými v URL řetězci. Jako výsledek bude mapovým serverem vrácen rastrový obrázek, který bude umístěn do georeportu.

Veškerá provozní data budou uložena v relační databázi (PostgreSQL) na serveru. DB struktura objektů a jejich hierarchie bude definována pomocí metamodelu uloženého v databázi.

Přístup do aplikace bude umožněn autorizovaným uživatelům. Autorizaci uživatelů bude na centrální úrovni zajišťovat “Komponenta zajišťující autentizaci a autorizaci všech přístupů a vstupů do IS DTM a jeho komponent včetně jeho služeb”.

V rámci dodávky komponenty, pokud budou dostupná příslušná data, budou nakonfigurovány šablony pro následující georeporty:

* Výpis informací ke zvolenému místu – obec.
* Výpis informací ke zvolenému místu – pozemek.
* Výpis informací ke zvolenému místu – adresa.
* Výpis informací ke zvolenému místu – n-úhelník.
* Výpis prvků ZPS – seznam.
* Výpis prvků ZPS – zobrazení v mapě.
* Výpis prvků sítí a jejich ochranných pásem (nenahrazuje vyjádření).
* Výpis provedených aktualizací v daném místě (včetně stavu jejich zapracování).
* Výpis editorů DTM v daném místě.

Všechny připravené georeporty budou v úvodní konfiguraci dostupné pro přihlášené uživatele (alespoň role Host). Nepřihlášení uživatelé budou mít k dispozici následující georeporty:

* Výpis informací ke zvolenému místu – obec.
* Výpis informací ke zvolenému místu – pozemek.
* Výpis informací ke zvolenému místu – adresa.
* Výpis informací ke zvolenému místu – n-úhelník.
* Výpis prvků ZPS – seznam.
* Výpis prvků ZPS – zobrazení v mapě.

### Komponenta – Metadatový klient

Metadatový klient bude umožňovat plnohodnotnou tvorbu a editaci metadat k datovým sadám a službám dle Národního metadatového profilu pro autentizované a autorizované uživatele odpovědné za své datové sady a služby. Pro veřejnost bude k dispozici vyhledávání a filtrace v metadatovém katalogu. Metadatový katalog bude sdílet metadata pomocí standardizovaných webových služeb dle OGC CS-W a bude umožňovat harvestování dat externími aplikacemi jako je například Národní portál INSPIRE.

Metadatový klient bude jako součást IS DTM k dispozici na Portálu DTM ve formě webové aplikace. Vzhledem ke způsobu správy DTM jako výkonu přenesené státní správy bude kraj schopen deklarovat metadata o všech datech, která budou součástí DTM. Součástí IS DTM bude podpora správy a publikace kompletního datového modelu jevů DTM (ZPS/TI/DI), které bude realizováno samostatným modulem, viz kap. [Komponenta pro administraci datového skladu](#_Komponenta_pro_administraci).

Obsah a funkcionalita:

* Ruční tvorba metadat oprávněným uživatelem.
* Vyhledání metadat (volba kritérií).
* Tvorba a správa metadatových profilů (šablon).
* Zobrazení strukturovaných metadat (formulář), včetně zobrazení rozsahu v mapovém okně.
* Export (XML, XLS, PDF) či tisk metadat.
* Publikace URL adres jednotlivých záznamů pro potřeby mapového klienta.
* Publikace služeb pro harvestování metadat.
* Publikace obsahu datového modelu jevů DTM (ZPS/TI/DI, bude řešeno pomocí Komponenty pro administraci datového skladu).

### Komponenta – Metadata

Komponenta bude umožňovat poloautomatickou či ruční tvorbu metadat o datových sadách a vrstvách v datovém skladu DTM a tím zajišťovat požadovanou správu metadat. Bude vytvářet backend pro Metadatového klienta. Komponenta bude poskytovat služby metadatového katalogu pro poskytování metadat pomocí standardizovaných webových služeb dle OGC CS-W a bude umožňovat harvestování dat externími aplikacemi. Metadaty budou popsány i výdejní balíčky OpenDat. Komponenta bude realizována jako webová aplikace s vlastní databází s vazbou na komponenty zajišťující správu datového skladu DTM, která bude zajišťovat aktualizaci metadat v rámci aktualizace dat v datovém skladu. Tvorba metadat bude umožněna při tvorbě dat nebo aktualizaci datového skladu. Základní funkcí bude správa metadatového katalogu a publikace katalogové služby.

Metadatový katalog bude možné plnit:

* Dávkově prostřednictvím harvestingu jiného katalogu, pokud je lokální katalog k dispozici.
* Importem XML(HTML) souborů v požadovaném profilu.
* Prostřednictvím editace metadat v prostředí webové aplikace Metadatový klient.

Editace v aplikaci je řízena konfiguračním profilem, kterých může být v rámci organizace využíváno hned několik. Konfiguračním profilem je myšlena sada šablon pro vytváření, editaci a validaci metadat. Aplikace pro editaci metadat bude obsahovat validační funkce, a to v takovém rozsahu, aby bylo možné provést validace vůči národnímu profilu, ISO normám, vůči INSPIRE požadavkům, ale také vůči vlastním pravidlům nadefinovaným přímo pro účely daného kraje. Komponenta bude umožňovat editaci metadat podle různých profilů (zejména v návaznosti na požadavky vyplývající z prováděcích pravidel – datových specifikací INSPIRE), podporovat vytváření multijazyčných metadatových záznamů, podporovat vyplňování klíčových slov INSPIRE Data Themes a také podporovat vyplňování klíčových slov prostřednictvím on-line napojení na řízený slovník GEMET.

Bude k dispozici funkcionalita pro zobrazení obsahu datového modelu jevů DTM (ZPS/TI/DI), viz Komponenta pro administraci datového skladu.

Obsah a funkcionalita:

* Tvorba a editace metadat s využitím informací z dat či jiných komponent IS DTM.
* Správa práv na editaci metadat bude řešena podle uživatelských rolí.
* Webové služby pro harvestování metadat.
* Konfigurace metadatových profilů – podpora metadatových profilů a standardů, včetně standardů ISO 19139/19115, 19139/19119 a profilu INSPIRE i národního profilu INSPIRE, včetně možnosti rozšíření o další vlastní metadatové profily.
* Katalogové služby dle OGC CS-W 2.0.2.
* Vazba na Národní Geoportál INSPIRE bude realizována prostřednictvím katalogové služby dle OGC CS-W.
* Správa datových modelů jevů DTM (ZPS/TI/DI) je řešena v samostatné komponentě, viz Komponenta pro administraci datového skladu.

Metadata budou v DTM předdefinovaná (strukturována) podle následujících úrovní.

* Pro datové sady DTM budou předdefinovaná metadata pro:
  + ZPS.
  + TI.
  + TI – Sdílená stavba technické infrastruktury.
  + TI – Elektrické vedení.
  + TI – Elektronické komunikace.
  + TI – Plynovod.
  + TI – Vodovod.
  + TI – Přivaděče vody.
  + TI – Kanalizace.
  + TI – Produktovod.
  + TI – Teplovod.
  + TI – Potrubní pošta.
  + TI – Zařízení staveb technické infrastruktury.
  + ZPS.TI – Domovní přípojky.
  + DI.
  + DI – Silniční doprava.
  + DI –Drážní doprava.
  + DI – Vodní doprava.
  + DI – Letecká doprava.
  + DI – Společná dopravní stavba.
* Pro mapové služby DTM budou předdefinovaná metadata pro:
  + WMS ZPS.
  + WMS TI.
  + WMS TI – Sdílená stavba technické infrastruktury.
  + WMS TI – Elektrické vedení.
  + WMS TI – Elektronické komunikace.
  + WMS TI – Plynovod.
  + WMS TI – Vodovod.
  + WMS TI – Přivaděče vody.
  + WMS TI – Kanalizace.
  + WMS TI – Produktovod.
  + WMS TI – Teplovod.
  + WMS TI – Potrubní pošta.
  + WMS TI – Zařízení staveb technické infrastruktury.
  + WMS ZPS.TI – Domovní přípojky.
  + WMS DI.
  + WMS DI – Silniční doprava.
  + WMS DI – Drážní doprava.
  + WMS DI – Vodní doprava.
  + WMS DI – Letecká doprava.
  + WMS DI – Společná dopravní stavba.
  + WFS ZPS.

### Mapový klient DTM kraje pro veřejnost

Webový mapový klient bude sloužit pro zpřístupnění příslušných mapových kompozic DTM. Klient bude umožňovat propojení dostupných nástrojů a datových zdrojů DTM. Mapový klient bude využíván pro základní prohlížení obsahu DTM a DMVS. Nástroje mapového klienta bude možné konfigurovat podle zvoleného tématu a obsahu mapové kompozice a flexibilně přizpůsobovat a rozšiřovat podle budoucích požadavků kraje. Používání mapového klienta nebude vyžadovat instalaci žádného dodatečného pluginu do webového prohlížeče uživatele.

Klienta bude možné spouštět ve všech obvyklých desktopových a mobilních prohlížečích. Rozložení nástrojů klienta se bude přizpůsobovat podle rozlišení zařízení (responzibilita). Mapový klient pro veřejnost bude zpřístupňovat 2D zobrazení. Jedná se o veřejnou komponentu.

Obsah a funkcionalita:

* Zobrazení datových vrstev DTM.
* Nástroj pro uživatelské přidání vrstev (WMS/WMTS).
* Možnost identifikace zvolené vrstvy.
* Nástroj pro vyhledávání ve vrstvách.
* Nástroje mapového okna.
  + Možnost zvolení mapového měřítka (zoomu mapy).
  + Přiblížení, oddálení, posun v mapě.
  + Lokalizace uživatele.
  + Zobrazení legendy.
  + Měření délek, ploch a odečítání souřadnic.
  + Nástroj pro kreslení (vkládání vlastní grafiky).
  + Možnost vygenerování odkazu s konkrétním nastavením mapy.
* Nástroje pro export mapy.
  + Volba měřítka.
  + Tisk do velikostí A3 a A4, na výšku a na šířku.
  + Nástroj bude automaticky využívat vhodné rozlišení pro tisk v požadovaném měřítku
  + Zobrazení copyrightu.
* Zobrazení seznamu vrstev.
  + Zapnutí/vypnutí vrstev.
  + Nastavení transparentnosti.
  + Možnost zobrazení metadat (odkazů na zdroje) dané vrstvy.
* Identifikace prvků v mapě (informace o prvku).
* Možnost uložení mapového výřezu do schránky.
* Možnost vyhledávání nad daty RÚIAN (fulltextové vyhledávání s našeptávačem).
  + Vyhledání obce, adresy, KÚ, parcely, budovy.
* Nástroj pro nahlášení reklamace:
  + Pro přihlášené i nepřihlášené uživatele.
  + Nástroj je napojený na komponentu pro správu reklamací.
* Nástroj pro možnost přechodu do komponenty Georeporty.
* Možnost zobrazení mapového klienta v mobilní aplikaci (plná responzivita).

Konfigurace některých funkcí, jako je například měřítkové omezení či konfigurace řazení vrstev je řešena v komponentě pro správu mapových komponent.

### Komponenta pro správu mapových komponent

Komponenta bude sloužit k možnosti konfigurace mapových komponent. Jmenovitě jde o komponenty:

* Mapový klient DTM kraje pro veřejnost.
* Webová komponenta pro editaci ZPS.
* Klient pro výdej dat.

Součástí komponenty budou funkce popsány níže:

* Nástroj pro vybrání komponenty (výběr komponenty, u které bude provedena změna konfigurace).
* Zobrazení přehledu vrstev.
* Nástroj pro otevření detailu vrstvy.
* Nástroje pro konfiguraci vrstev.
  + Možnost nastavení měřítkového omezení.
  + Nastavení skupin vrstev.
  + Nastavení pořadí vrstev a skupin.
* Nástroje pro vkládání WMS vrstev.

### Komponenta pro poskytování mapových služeb

Komponenta bude realizována pomocí aplikačního modulu postaveném na open-source mapovém serveru MapServer Minesotské University (<https://mapserver.org/>).

Data pro publikaci dat veřejnosti a uživatelům DTM budou načítána z publikační databáze. Data pro služby sloužící editačním klientům z referenční a editační databáze.

Obsah, nastavení služeb a podpora metod bude v souladu se závěry projektu “TA ČR TITBMV021 – Zavedení Digitální technické mapy ČR”. Dokumentace ke stažení na portálu JVF DTM <https://jvfdtm.ogibeta2.gov.cz/Portal/dokumenty>.

Mapové služby budou publikovány na adrese vyplývající z domluvy KRS. Tedy:

* /mapservice/v1/wms
* /mapservice/v1/wmts
* /mapservice/v1/wfs

Seznam mapových služeb je uveden v následující tabulce:

|  |  |
| --- | --- |
| **WMS služby DTM** | **Varianta a ID WMS služby** |
| ZPS linie a body (včetně shora neviditelných, všechny level) | dtm\_zps\_linie\_body |
| ZPS plochy (všechny level) - pohled ze shora | dtm\_zps\_plochy |
| DI | dtm\_di |
| TI | dtm\_ti |
| Záměry DI, TI | dtm\_zamery |
| Ochranná pásma DI, TI | dtm\_op\_bp\_di\_ti |
| Geodet. kartogr. prvky (body) | dtm\_geod\_kart\_prvky |
| Oblasti | dtm\_oblasti |
| Zóny nejistoty pro ZPS | dtm\_zony\_nejist\_zps |
| Zóny nejistoty pro DI | dtm\_zony\_nejist\_di |
| Zóny nejistoty pro TI | dtm\_zony\_nejist\_ti |
|  |  |
| **WMTS služby DTM** | **ID WMTS služby** |
| ZPS - barevná | dtm\_zps\_bar |
| ZPS - šedotónová | dtm\_zps\_seda |
| DI (bez OP) | dtm\_di |
| TI (bez OP a BP) | dtm\_ti |
| OP TI DI | dtm\_op\_bp\_di\_ti |

Mapové služby budou publikovány prostřednictvím:

* Reverzní proxy na WEB Serveru 1.
* Zobrazovaný obsah prohlížecích a stahovacích služeb bude odpovídat aktuálnímu stavu dat DTM se zpožděním max. 1 den.

**Detailní popis WMS**

* WMS služby budou zpracovány dle standardu OGS ve verzi 1.3.0.
* WMS služby budou podporovat metody GetMap, GetFeatureInfo a GetCapabilities.
* WMS služba bude nastavena jako 3úrovňová s tím, že poslední (4. úroveň) bude sloužit k měřítkových mutacím symbolů konkrétního jevu DTM.
  + 1. úroveň – tematický okruh (Budovy, Dopravní stavby, Vodní díla apod.).
  + 2. úroveň – objekty dle datového modelu (typy objektů).
  + 3. úroveň – hodnoty atributů.
* Názvy jednotlivých vrstev budou alfanumerické a formou zkratek budou popisovat zobrazované jevy.
* V rámci WMS služeb bude publikována queryvrstva pro každý objekt bez měřítkových omezení, která bude sloužit pro metodu GetFeatureInfo.
* WMS služby budou publikovány s podporou pro souřadnicové systémy:
  + EPSG:5514 (S-JTSK / Krovak East North).
  + EPSG:3857 (WGS 84 – Web Mercator).
  + EPSG:4326 (WGS 84).
  + EPSG:3045 (ETRS89 / TM33).
  + EPSG:3046 (ETRS89 / TM34).

**Detailní popis WMTS**

* WMTS služby budou zpracovány dle standardu OGS ve verzi 1.0.0.
* WMTS služby budou publikovány s podporou pro souřadnicové systémy:
  + EPSG:5514 (S-JTSK / Krovak East North).
  + EPSG:3857 (WGS 84 – Web Mercator).
* Měřítkové sady budou odpovídat společným domluveným setům dle projektu “TA ČR TITBMV021 – Zavedení Digitální technické mapy ČR” (nutné pro možnost sjednocení v rámci mapových služeb IS DMVS).
* Mapová cache nad měřítkem 1:500 nebude automaticky předgenerovávána, ale cache bude vytvářena (on the fly), tedy až při prvním požadavku na danou oblast.
* Komponenta umožní generovat a přegenerovat (smazat) mapovou cache pro vybrané území pro zajištění úloh:
  + Přegenerovat mapovou cache dle aktualizovaných oblastí DTM.
  + Přegenerovat mapovou cache při nahrání aktuálních referenčních dat mimo vektorový obsah DTM např. ortofoto.

**Společná specifikace WMS a WMTS**

* Služby budou vytvořeny jako prohlížecí služby pro vizualizaci jednotlivých objektů v definovaných měřítkových úrovních (Viz tabulky projektu TA ČR). Tedy symbologie bude vždy odpovídat pouze vztažnému měřítku a v rámci daného rozsahu se budou symboly zvětšovat (zmenšovat).
* Symbologie vrstev bude uložena v adresářích na mapovém serveru, a to vždy jako kompletní balík pro příslušnou verzi JVF DTM, včetně podverze symbologie tak, aby administrátor mohl jedním zásahem zajistit povýšení verze vizualizace DTM.
* Symbologie je zpracována pomocí svg files a popisu zveřejněném na portálu DMVS. <https://cuzk.cz/DMVS/Znackovy-klic.aspx>

**Detailní popis WFS**

* Stahovací služba WFS bude poskytována podle standardu OGC ve verzi schválené KRS.
* Podrobná specifikace stahovacích služeb ve formátu WFS bude specifikována na Portále IS DMVS. Specifikace bude obsahovat také rozčlenění do tříd objektů a jejich atributů a další požadavky. Každý objekt DTM publikovaný prostřednictvím WFS bude obsahovat také údaj o čase poslední aktualizace záznamu v IS DTM. Poskytovatel počítá se specifikací WFS, která bude publikována na Portálu JVF DTM jako výstup z Technologické agentury ČR a odsouhlasena KRS.

### Statistika – klient

Součástí komponenty Portál DTM bude modul pro zobrazení statistik. Přípravu statistických údajů a jejich podobu zobrazení zajišťuje backend komponenta, která pomocí sady technologií pro statistiku (viz kapitola [Popis použitých technologií IS DTM](#_Popis_použitých_technologií)) zajištuje sběr, indexaci a formátování relevantních události z jednotlivých aplikačních komponent. Bude se jednat o podpůrné nástroje zajišťující tvorbu statistických reportů o používání IS DTM z pohledu vnitřní správy a z pohledu externího využívání systému, konkrétní rozsah informací, včetně rozdělení na veřejnou (vnější portál DTM určený pro veřejnost) a neveřejnou část, je uveden v tabulce níže. Nad touto definovanou skupinou statistických údajů (sloupec Portál DTM v tabulce níže) bude komponenta umožňovat uživatelskou tvorbu přehledů a statistik, včetně konfigurace jejich podoby a publikace (grafy, tabulky atd.). Komponenta bude zpřístupňovat jednotlivé statistiky na základě přidělených uživatelských rolí. Další detailní statistické údaje budou dostupné oprávněným uživatelům v rámci jednotlivých komponent IS DTM.

Prezentace základních neveřejných statistických údajů bude řešena sadou předpřipravených dashboardů dle jednotlivých tematických oblastí. Veřejná část bude obsahovat dashboard, který bude přehledným způsoben zobrazovat základní sadu volně dostupných statistik a přehledů sloužících zejména pro sledování vývoje aktualizace obsahu DTM a procesu její správy (sloupec Portál DTM – Veřejnost v tabulce níže). Komponenta bude zobrazovat statistické údaje platné k předchozímu dni, přičemž aktualizace údajů bude realizována jednou za den v nočních hodinách. Ve statistikách bude zohledněn import a aktualizace dat v rámci prvotního naplnění tak, aby nedocházelo ke zkreslení vybraných statistických údajů.

Na veškeré přehledy a statistiky veřejné části DTM bude nahlíženo jako na OpenData (sloupec OpenData v tabulce níže). Statistické údaje budou prostřednictvím pomocného modulu komponenty Statistika automatizovaně předávány v rámci datové sady do Národního katalogu otevřených dat. Rozsah a definice datové sady bude projednána s koordinátorem otevřených dat kraje. Datové sady včetně metadat budou v souladu se závaznými pravidly pro zveřejnění v Národním katalogu otevřených dat (např. Otevřená formální norma) obsahovat hlavičku a odkazy na jednotlivé distribuce datových sad, které budou generované ve formátu .csv a .json.

Tabulka s rozsahem a členěním statistických údajů:

| **Popis statistiky** | **Portál DTM** | **Portál DTM - Veřejnost** | **OpenData** |
| --- | --- | --- | --- |
| Počet aktualizací ZPS za určité období (dle typu) | ANO | ANO | ANO |
| Počty externích uživatelů (dle období a typu přihlášení) | ANO | ANO | ANO |
| Využití poskytovaných služeb – výdej dat (dle druhu – ZPS/TI/DI) | ANO | ANO | ANO |
| Využití poskytovaných služeb – mapové služby | ANO | ANO | ANO |
| Četnost využití poskytovaných služeb (dle typu) | ANO | ANO | ANO |
| Statistiky obsahu DTM – počty geografických prvků | ANO | ANO | ANO |
| Statistiky obsahu DTM – plochy či délky prováděného plošného mapování | ANO | ANO | ANO |
| Seznam geodetů a organizací provádějících geodetické činnosti | ANO |  |  |
| Seznam aktualizací – podle stavu aktualizace | ANO |  |  |
| Seznam aktualizací – podle termínu realizace (od – do) | ANO |  |  |
| Statistika výdejů neveřejných dat DI a TI podle vlastníka/správce/provozovatele | ANO |  |  |

Tabulka 6 Tabulka s rozsahem a členěním statistických údajů

### Existence sítí

Komponenta Existence sítí se bude skládat z veřejné části pro příjem žádostí o vyjádření k existenci infrastruktury a z části neveřejné pro zpracování žádosti a sestavení vyjádření. Komponenta bude kraji pokrývat jeho zákonnou povinnost jako vlastníka/správce/provozovatele technické a dopravní infrastruktury poskytovat informace o existenci této infrastruktury. Současně bude komponenta nabízet zajištění této funkcionality dalším subjektům, kterým to kraj umožní (typicky svým zřizovaným organizacím, obcím nebo malým správcům na svém území). Jako informační systém správce technické a dopravní infrastruktury pro vyřizování vyjádření bude sloužit neveřejná aplikace komponenty Existence sítí. Správce, kterému bude krajem umožněno komponentu využívat, se bude k žádostem vyjadřovat v rámci této aplikace. Způsob podání žádosti pro všechny žadatelem zvolené subjekty (subjekty DI nebo TI infrastruktury) bude shodný. Pokud se bude vyjadřovat subjekt TI, tak bude workflow sestavení vyjádření ve výchozím nastavení stejné jako v případě subjektu DI. Aplikace bude nabízet stejné stavy pro objekt žádost. Konfigurace schvalovacího workflow bude umožněna každému zapojenému subjektu.

**Aplikace pro příjem žádostí**

Dle Dodatku č. 1 ke smlouvě na Dodávku a implementaci informačního systému digitální technické mapy Jihomoravského kraje nebude realizován příjem žádostí podaných přes Portál stavebníka, namísto toho bude komponenta pomocí svého modulu umožňovat příjem žádostí podaných na portálu Utility Report pro subjekt Jihomoravský kraj. Modul komponenty bude kontrolovat obsahovou a formální správnost podaných žádostí. V případě nedostupnosti portálu Utility Report bude komponenta disponovat vlastním řešením pro příjem žádostí. Tímto řešením bude samostatná responzivní webová aplikace přístupná přes webový prohlížeč ze sítě Internet. Zadání údajů žádosti o vyjádření provede žadatel v aplikaci prostřednictvím webového formuláře, který se bude skládat z několika tematických záložek (na sebe navazujících kroků). Před každým krokem vpřed bude aplikace validovat obsah, takže při konečné rekapitulaci bude mít žadatel jistotu, že jeho sestavená žádost je validní a obsahuje všechny potřebné informace pro vybrané subjekty (vlastník/správce/provozovatel) k řádnému sestavení vyjádření. Prostorový dotaz prováděný prostřednictvím zakreslování zájmového území bude očekávat ve výchozí konfiguraci validní polygon nebo multipolygon dle definice OGC standardu s maximálním počtem 50 lomových bodů v součtu všech uživatelských polygonů. Uvedená konfigurace prostorového dotazu bude provedena v rámci instalace aplikační instance. Maximální počet lomových bodů a určení, zda subjekt dovoluje zakreslit polygon nebo multipolygon, bude možné konfigurovat prostřednictvím administrační role z prostředí aplikace. Prostorová analýza nad zakresleným zájmovým územím bude využívat datové zdroje RUIAN, kdy v rámci prostorových kontrol žadatele upozorní na překročení počtu lomových bodů, nevaliditu uživatelského polygonu nebo na způsob řešení prostorového konfliktu mezi správním obvodem kraje a uživatelským polygonem. V takovém případě, kdy uživatelský polygon bude ležet mimo správní obvod kraje, vyzve aplikace žadatele k novému zákresu zájmového území a lokalizuje mapu nad oblastí správního obvodu. Konfigurace prostorových analýz v případě řešení prostorových konfliktů, nastavení tolerance [m] pro průnik grafických prvků a stanovení textů výstražné notifikace pro žadatele v případě zákresu mimo správní obvod kraje nebo na hranici kraje bude možné realizovat prostřednictvím administrační role z prostředí aplikace. Uvedená konfigurace prostorových analýz bude provedena v rámci instalace aplikační instance. Komponenta bude integrovat službu pro získávání seznamu subjektů DTI z IS DMVS a žadateli zobrazovat do aplikačního prostředí pouze relevantní seznam dotčených subjektů DTI působících v průniku katastrálních území a uživatelského polygonu, kteří jsou zároveň zapojeni do komponenty Existence sítí, takže jejich žádost bude evidována a vyřizována prostřednictvím neveřejné aplikace komponenty Existence sítí. Komponenta Existence sítí bude těžit data o subjektech DTI z datového skladu, do kterého budou plněny prostřednictvím konzumace webové služby IS DMVS. Službu konzumace bude zajišťovat komponenta IS DMVS webAPI, prostřednictvím které bude umožněno službu konfigurovat. Konfigurace z pohledu komponenty Existence sítí bude spočívat v možnosti zapojit nebo odpojit vybraný subjekt DTI do/z komponenty Existence sítí. Pokud dotčený subjekt bude umožňovat napojení k infrastruktuře, potom bude v rámci podání žádosti uživateli umožněno o napojení požádat. Možnosti a podmínky způsobu napojení nebo podmínky dotčených ochranných a bezpečnostních pásem bude definovat vyjadřovatel TI/DI v samostatné neveřejné aplikaci pro vyřizování vyjádření v procesu zpracování vyjádření. V rámci instalační konfigurace bude definován číselník důvodů žádostí shodný pro všechny zapojené subjekty a bude určena povinnost nebo volitelnost přiložení souboru (přílohy) k vybraným důvodům žádosti.

Uživatel v roli Správce IS DTM bude mít oprávnění spravovat aplikaci za všechny zapojené subjekty z pozice správce území (kraj). Této roli bude umožněna konfigurace podoby žádosti prostřednictvím správy vlastností aplikace a řízení povinnosti vybraných atributů nebo zpřístupnění vybraných záložek formuláře pro podání žádosti. V rámci nastavení veřejné části komponenty bude umožněno definování informativních textů včetně FAQ.

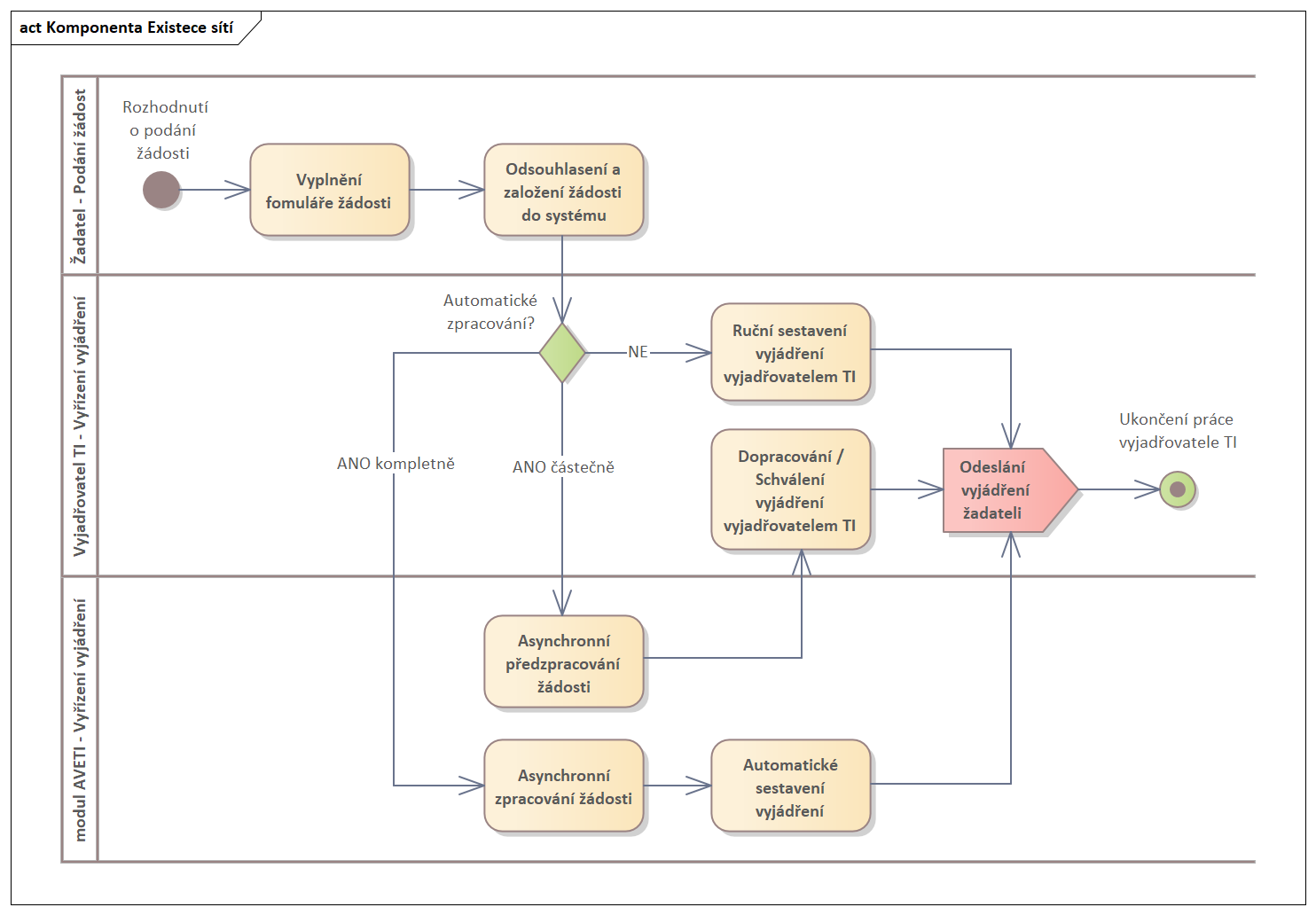
Veřejnost bude za účelem podání žádosti o vyjádření vstupovat do aplikace v roli Anonymního uživatele bez nutnosti předchozí registrace v systému IS DTM. Po založení žádosti odešle aplikace žadateli e-mail s potvrzením o založení a se zestručněnou rekapitulací žádosti.

**Aplikace pro vyřizování vyjádření**

Neveřejná část komponenty Existence sítí bude samostatná responzivní webová aplikace. Aplikace bude zajišťovat plnou podporu celého procesu vypořádání žádosti. Pokud žádost vyhoví vstupní podmínce bude zpracována modulem komponenty pro „Automatizované Vyjádření k Existenci Technické a dopravní Infrastruktury“ (AVETI). Modul AVETI bude možné z prostředí aplikace aktivovat nebo deaktivovat pro každý zapojený subjekt zvlášť a konfigurovat hloubku zpracování žádosti nastavením jeho konečného stavu workflow. Modul buď zpracuje žádost a sestaví pro ni vyjádření, které odešle e-mailem žadateli spolu s relevantními přílohami, nebo ukončí zpracovávání žádosti v definovaném stavu workflow pro kontrolu, případně pro doplnění údajů předtím, než vyjadřovatel TI/DI vyjádření odešle žadateli. Žádosti, které nevyhoví vstupní podmínce AVETI, budou od podání žádosti po vydání vyjádření zpracovány vyjadřovatelem TI/DI, který bude mít dostupné operace aplikační logiky poplatné jednotlivým stavům workflow v procesu vyjadřování. Dle Dodatku č. 1 ke smlouvě na Dodávku a implementaci informačního systému digitální technické mapy Jihomoravského kraje nebude realizována zpětná propagace vyjádření na Portál stavebníka. Operace, která vygeneruje textový soubor PDF s vyjádřením sestaví také PDF se situačním náhledem uživatelského polygonu nad pokladovými daty s technickou infrastrukturou subjektu. Uložením těchto dat v databázi Existence sítí bude dosažena archivace stavu dat v době vydání vyjádření pro jejich budoucí dokladování.

Aplikace bude umožňovat konfiguraci jejích vlastností pro každý zapojený subjekt. V rámci konfigurace bude možné nastavovat e-mailové notifikace pro různé situace a nad různými stavy zpracovávaných žádostí, bude možné zapnout / vypnout funkcionalitu schvalovacího workflow, přednastavit texty odpovědí v závislosti na důvodu žádosti v podobě textové šablony vyjádření, doplňujících textů oznámení a varování. Dále přednastavit automatické přikládání libovolných souborových příloh v libovolném množství k textové části vyjádření pro různé situace (na základě důvodu žádosti nebo pro všechny žádosti). Limitem počtu a velikosti příloh je nastavení na straně SMTP serveru a webového serveru, který bude ve výchozí konfiguraci nastaven na limit 25 MB pro upload.

Uživatel v roli Vyjadřovatel TI/DI bude zpracovávat žádosti a sestavovat vyjádření za subjekt, za který bude do aplikace vstupovat. V aplikačním pracovním prostředí uvidí vyjadřovatel TI/DI žádosti přidělené jemu ke zpracování a všechny další žádosti tříděné podle stavu od podaných, přes rozpracované, čekající na interní stanovisko, nebo případně na schválení, až po schválené, vygenerované a odeslané. Kontroly nad prováděnými editačními operacemi a jejich zpřístupnění na základě pevně definovaného stavového workflow budou zajišťovat vyjadřovateli TI/DI oporu pro bezchybný, jednoznačný a intuitivní postup při zpracovávání žádosti a sestavování vyjádření.



Obrázek 11 Komponenta Existence sítí

### Komponenta pro podporu reklamací datového obsahu a funkčnosti IS DTM

Komponenta bude sloužit ke správě reklamací včetně vyřízení jejich workflow (přebrání reklamace z veřejného mapového klienta, možnost vyřízení, uzavření apod.). Komponenta slouží pro přihlášené i nepřihlášené uživatele a vstupem do ní je veřejný mapový klient a webová editační komponenta. Funkcionality komponenty jsou popsány níže:

* Možnost zobrazení reklamace:
  + Nástroje pro vyřízení workflow reklamace (přijetí, zamítnutí, znovuotevření, uzavření).
  + Zobrazení detailu reklamace včetně jejích metadat.
* Notifikační služby pro informování uživatelů o stavu reklamace.
* Přehled a evidence reklamací s možností filtrování.
* API rozhraní pro možnosti využití v komponentě Statistika.
* Odeslání validních připomínek k funkčnosti IS DTM formou e-mailové notifikace do aplikace ServiceDesk JMK

### Klient pro administraci

Administrace komponent systému bude prováděna pomocí specifických uživatelských rozhraní, která budou poskytovat nástroje pro jejich konfiguraci a správu. Řešení bude poskytovat zejména následující administrační rozhraní.

* Dashboard Orchard Core CMS
  + Administrační rozhraní umožňující správu redakčního systému v běžném webovém prohlížeči.
  + Administrace obsahu Portálu DTM, přístupů, aplikačních modulů redakčního systému, widgetů, integračních rozhraní apod.
* Admin klient komponenty IDM
  + Administrace klienta komponenty IDM umožňující administraci, správu účtů a rolí, bude realizována prostřednictvím aplikace KeyCloak, resp. nadstavby RolesManager, v které bude řešen proces podání žádosti o zařazení, odebrání nebo změnu aplikační role v IS DTM pro uživatele přihlašující se přes NIA. Administrátorské prostředí umožnuje uživateli s rolí Security Admin prohlížet, zamítat a schvalovat žádosti. V případě schválení je v KeyCloaku založeno příslušné oprávnění a žadateli je přiřazeno požadované oprávnění pro přístup do IS DTM, včetně jeho komponent a služeb.

#### Komponenta pro administraci datového skladu

Jedná se o sadu dvou komponent, které slouží pro administraci datového skladu DTM.

První komponentou je webová aplikace (Katalog datového skladu DTM), která bude poskytovat následující funkcionalitu.

* Zobrazování pravidel pro zpracovávání dat (editační pravidla).
  + Základní kontroly syntaxe JVF DTM.
  + Věcné kontroly vstupních aktualizačních dat JVF DTM.
  + Topologické kontroly.
* Zobrazování pravidel pro převody dat.
  + Převodníku dat mezi datovým modelem datového skladu DTM a vektorovými GIS formáty - JVF DTM, SHP a GPKG.
  + Převodníku dat mezi datovým modelem datového skladu DTM a vektorovým CAD formátem DGN.

Druhou komponentou pro správu datového skladu (datového modelu, odvozování dat, historizace, editačních pravidel, převodníků apod.) je software pgAdmin (alternativně DBeaver). Software bude poskytovat rozhraní pro definici příkazu ve standardizovaném jazyku SQL včetně GUI a bude pomocí něho možné provádět veškeré administrátorské činnosti v databázích datového skladu, a to včetně možnosti exportu všech databází (tabulek).

### Komponenta zajišťující autentizaci a autorizaci všech přístupů a vstupů do IS DTM a jeho komponent včetně jeho služeb

Jako IDM server bude použit open-source nástroj KeyCloak (RedHat SSO). KeyCloak nabízí pro většinu funkcí webové rozhraní, REST rozhraní a také rozšířitelné API. KeyCloak poskytuje přizpůsobitelné uživatelské rozhraní pro přihlášení, registraci, administraci a správu účtů. Ověřování je delegované na poskytovatele identity třetích stran. Jmenovitě Active directory, JIP/KAAS a NIA.

KC bude mít zabudován provider pro JIP/KAAS a bude čerpat přístupové role. KC bude logovat do souborů a dále do Syslogu na localhostu, tyto údaje budou využity pro monitoring a statistiku.

#### RolesManager

Aplikací přidruženou ke KeyCloak bude RolesManager (RM). Jedná se o jednoduchou serverovou webovou aplikaci (bez Javascriptu), což umožní, aby v KeyCloak byl zaveden jako confidential client pro zvýšenou bezpečnost.

Úloha RM bude následující:

* Uživatel (např. geodet), který se hlásí přes NIA, bude mít pouze roli guest, protože NIA potřebné informace (uživatel je geodetem) neposkytuje. Pokud uživatel bude chtít další role, navštíví web RolesManager, kde se přihlásí přes KC, a následně bude moci ve formuláři určit, které role požaduje. RM pak uvědomí takového žadatele e-mailem.
* Uživatel s oprávněným Security admin se přihlásí do RolesManager přes KC, zobrazí si stránku se žádostmi z předchozího bodu, provede potřebnou činnost, a dané žádosti buď vyhoví, nebo ji smaže. RolesManager pak v kladném případě přes REST API Keycloaku nastaví žadateli požadovanou roli a v každém případě uvědomí žadatele e-mailem.

### Monitoring

Aplikační a systémový monitoring bude zajištěn službami Zabbix. Ten poskytuje ke sledování provozních charakteristik virtuálních serverů sledování dostupnosti aplikačních komponent.

Na každém virtuálním serveru bude nainstalován Zabbix agent. Na serveru monitoring v datovém centru bude nainstalován Zabbix server a lokální instance databázového serveru PostgreSQL, která je dedikovaná pro potřeby Zabbixu. Zabbix server bude předávat informace o monitorovaných stavech a událostech na centrální Zabbix server ICZ, a to prostřednictvím internetu. Komunikace mezi Zabbix Serverem a centrálním Zabbix serverem je šifrována na úrovni Zabbix protokolu pomocí PSK klíče. Komunikace mezi Zabbix Agenty a Zabbix serverem šifrovaná není.

Monitorování bude prováděno na následujících úrovních:

* Základní výkonnostní charakteristiky virtuálních serverů.
  + Vytížení CPU.
  + Využití RAM.
  + Zaplnění pevných disků.
  + Využití síťových rozhraní.
* Dostupnost virtuálních serverů.
  + ICMP check.
* Dostupnost aplikačních komponent.
  + Stav běžících procesů.
  + Kontrola dostupnosti komunikačních portů (TCP check).
  + Kontrola funkčnosti komponent voláním služeb *probe* a jejich nativních protokolů.
* Dostupnost aplikace z internetu.
  + Bude realizováno testem komunikace přes Zabbix proxy, která bude umístěna mimo datové centrum v internetu.
  + Po komunikaci s proxy bude využit pasivní režim, směrem ze Zabbix serveru na Zabbix proxy.
  + Stav dostupnosti komunikace bude k dispozici na Zabbix serveru.
* Alerty.
  + Budou stanoveny prahové hodnoty čítačů, při jejich překročení budou generovány e-mailové notifikace. Pro zasílání těchto notifikací bude využit SMTP server datového centra.
  + Alerty s vysokou prioritou budou zpracovány centrálním Zabbix serverem a řešeny v rámci procesů Service Desku Poskytovatele.

Na Zabbix serveru budou prezentovány výstupy monitoringu v jeho grafickém rozhraní ve formě tabulek a grafů, které budou součástí dashboardů. Do webového rozhraní Zabbixu bude zřízen přístup Administrátorům IS DTM a pracovníkům provozní podpory Poskytovatele.

Předpřipravené dashboardy budou respektovat členění IS na jednotlivé servery nebo služby.

### Logování

Logování bude provádět informační aktivum do lokálního logu nebo databáze.

**Logované informace**

Události, které jsou uvedeny v prvním sloupci následující tabulky, jsou požadovány vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti (VoKB), zároveň jsou doplněny další, které je potřeba zaznamenávat vzhledem k charakteru IS. Záznamy, které jsou vyžadovány VoKB, by měly být předávány do SIEM.

Níže je uvedena tabulka mapování logovaných událostí vyžadovaných VoKB na umístění a typ logů:

| **Logovaná událost** | **Uložení, kam se události ukládají** | **Způsob realizace** |
| --- | --- | --- |
| Přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů | Keycloak logovací adresář  syslog  Windows EventLog | Přes Keycloak, administrátoři na servery – OS |
| Činnosti provedené administrátory | syslog  Windows EventLog  log DB (logovací adresář clusteru) | Logováno na úrovni OS, DB |
| Úspěšné i neúspěšné manipulace s účty, oprávněními a právy | syslog  log DB (logovací adresář clusteru)  Windows EventLog  Keycloak logovací adresář | Keycloak, OS, DB |
| Neprovedení činností v důsledku nedostatku přístupových práv a oprávnění | syslog  Windows EventLog | Aplikace, neautorizovaný přístup |
| Činnosti uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému | syslog  Windows EventLog | Nastavení vybraných pracovních stanic (Servisní prostředí – Desktop) |
| Zahájení a ukončení činností technických aktiv | syslog  Windows EventLog  log DB (logovací adresář clusteru)  Keycloak logovací adresář | Keycloak, OS, DB, start aplikace |
| Kritická a chybová hlášení technických aktiv | syslog  Windows EventLog  log DB (logovací adresář clusteru)  Keycloak logovací adresář | Keycloak, OS, DB, start kontejneru |
| Přístupy k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí | syslog | Nastavení oprávnění, oddělit admin syslog od admin aplikací  Hardening OS |
| Změna konfigurace nebo parametrů komponenty (toto již není požadavek VoKB) | syslog | Konfigurace aplikace správy systému – Provozní deník.  Auditovat přístup ke konfiguračním souborům – potřeba dodat seznam konfiguračních souborů.  Nastavení přístupů OS, hardening OS |

*Tabulka 7 Mapování logovaných událostí na umístění a typ logů*

**Struktura auditního záznamu**

Auditní záznamy budou obsahovat tyto parametry a metadata:

* Identifikátor události.
* Identifikátor zdroje událostí.
* Přesné datum vzniku události.
* Přesný čas vzniku události.
* Typ/název události.
* Případně popis události (pokud není zřejmé z typu/názvu).
* Jednoznačnou identifikaci účtu, pod kterým byla událost provedena.
* Jednoznačnou síťovou identifikaci zařízení původce.
* Úspěšnost nebo neúspěšnost události.

Všechny relevantní logy budou centralizovány na monitoring serveru v datovém centru. Logy budou ukládány ve struktuře do lokálního souborového systému. Dostupné místo bude monitorováno, logy starší než jeden den budou automaticky komprimovány. Logy budou ukládány 2 roky s využitím jejich záloh.

Logy budou ukládány ve formátech:

* Syslog (RFC 5424) + syslog over TLS.
* MS Windows Event Log (vlastní umístění XPath pro informační aktivum).
* W3C (pro MS IIS Web server).
* Standardní nginx logy.
* Plain-text line-oriented logy.

K centralizaci logů z jednotlivých serverů budou události předávány pomocí:

* syslog protokol,
* filebeat a winlogbeat,
* překopírování

na monitorovací server.

Rotace logů na monitorovacím serveru bude nastavena na jeden den, odrotované logy budou automaticky komprimovány a budou mít koncovku složenou z data a času rotace souboru pro zajištění časové souslednosti a lepší orientaci při vyhledávání. Integrita dat souborů bude kontrolována pomocí linuxového nástroje Tripwire, který bude spouštěn na denní bázi na kořenovém adresáři, kde budou logy uchovávány. Pokud dojde k chybě integrity dat, tak bude odreportována v monitorovacím nástroji Zabbix.

Relevantní události (např. kompletní audit pohybu uživatele po systému, uživatelské logy, bezpečnostní události/incidenty) budou pro potřeby vyhodnocování podezřelých událostí importovány do noSQL databáze na monitorovacím serveru. Z důvodu kapacity monitorovacího serveru bude doba uložení těchto událostí omezena. Pro vyhodnocování takto uložených událostí bude k dispozici technologie OpenSearch DashBoards, která umožní prohlížení a vyhledávání včetně exportu do csv. Kompletní výčet relevantních událostí bude uveden v Dokumentaci skutečného provedení.

Pro prohlížení a vyhledávání ostatních událostí v lozích budou správci využívat standardní nástroje operačního systému Linux monitorovacího serveru. Tyto nástroje budou umožňovat export vybraných nebo vyhledaných událostí do textového souboru s danou strukturou. Pro tuto činnost bude Poskytovatel poskytovat součinnost.

Relevantní události budou pro potřeby vyhodnocování podezřelých událostí importovány do noSQL databáze na monitorovacím serveru. Z důvodu kapacity monitorovacího serveru bude doba uložení těchto událostí omezena. Pro vyhodnocování takto uložených událostí bude k dispozici technologie OpenSearch DashBoards.

Integrace na nástroje pro sběr a analýzu logů a auditních záznamů bude realizována pomocí nástrojů rsyslog a logstash, pomocí kterých bude umožněno předávání událostí do SIEM kraje.

### Archivace

Obsahy vybraných předávaných zpráv, vydaná data a vybrané protokoly (provozní logy) budou ukládány do systému ICZ DESA, zajišťující střednědobé a dlouhodobé důvěryhodné uložení elektronických dokumentů. Architektura systému vychází z mezinárodně uznávaného standardu OAIS (ISO 14721:2003 - Open Archival Information System), který vymezuje základní koncepci archivu pro uložení elektronických dokumentů. Standard definuje hlavní funkce, které má archiv zajišťovat. Jedná se o příjem dokumentů, správu dat, archivní uložení, přístup, administraci a plánování uchovávání. Použitá technologie dlouhodobé archivace, kromě ochrany před ztrátou dat, zachovává čitelnost dokumentů, jejich autenticitu a nezměnitelnost. Dále je zajištěno, že budou prováděny pouze kontrolovatelné a autorizované zásahy a ty budou prokazatelně dokladované. ICZ DESA dále splňuje požadavky kladené archivní legislativou a národním standardem pro elektronické systémy spisové služby (NSESSS) na elektronickou spisovnu. Architektura zvoleného řešení umožnuje variabilní přístup ke správě dokumentů v závislosti na skutečnosti, zda dokumenty vzniklé z činnosti DTM budou považovány za dokumenty dle zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů (dále jen „zákon o archivnictví“), či nikoliv. Zvolené řešení umožnuje zabezpečit uložení a správu elektronických dokumentů v rámci celého životního cyklu v souladu s požadavky zákona o archivnictví, včetně skartačního řízení s příslušným oblastním archivem. Pokud bude vyhodnoceno, že dokumenty vzniklé v rámci správy DTM nejsou považovány za dokumenty dle zákona o archivnictví, bude zničení elektronických dokumentů provedeno v souladu s požadavky na bezpečnou likvidaci digitálních dokumentů bez skartačního řízení.

Do systému ICZ DESA ke střednědobému (dlouhodobému) důvěryhodnému uložení budou ukládány vybrané informace z provozní části IS DTM, které mají statut důkazního prostředku a mají přímo dopad na autenticitu, nezpochybnitelnost, důvěryhodnost a kvalitu digitální technické mapy spravované v IS DTM. Pokud v IS DTM bude provedena událost přímo ovlivňující základní informace digitální technické mapy (garantovaná data), případně bude realizován výdej dat, bude tato událost zaznamenána formou elektronického dokumentu (JVF DTM, PDF), který bude doplněn nezbytnými metadaty (např. retenční politika) a uložen jakožto archivní balíček v archivním úložišti. V uloženém dokumentu budou zaznamenána celá předávaná data, případně bude umožněno uložit pouze popisná metadata v rozsahu zajišťujícím průkaznou identifikaci a autenticitu předávaných dat. Pro komunikaci a předávání dokumentů k uložení bude využito univerzální komunikační rozhraní (REST API), které budou využívat dotčené komponenty IS DTM. Komunikační rozhraní bude vycházet ze struktury METS definovaná národním standardem (NSESSS verze 3), přičemž bude upraveno pro potřeby a specifika ukládání a archivaci geodetických dokumentací. Všechny operace předání a převzetí a jejich čas, včetně vybraných události z provozního logu budou zaznamenány do transakčního protokolu. Transakční protokol umožňuje dohledat, identifikovat, popřípadě rekonstruovat činnost IS DTM, jednotlivých uživatelů v systému a stav entit v minulosti.

Systém archivace ukládá objekty (elektronické dokumenty) minimálně do dvou na sobě nezávislých úložišť, přičemž mohou být jako fyzická úložiště použita běžná disková pole, úložiště v DC nebo může být pro ukládání objektů využita infrastruktura datových úložišť CESNET s využitím souborových (HSM) nebo objektových (CEPH) úložišť. Architektura systému umožňuje zvolit vhodnou kombinaci úložišť dle možností a požadavků Objednatele. Při výběru vhodné kombinace fyzických úložišť je potřeba zohlednit, že bude ukládán relativně velký objem dat, ale protože jde o archiv se specifickým použitím (asynchronní ukládání, správa malého počtu uživatelů, nižší nároky na odezvy aplikace) nemusí být kladen velký důraz na rychlost příslušných úložišť.

Návrh:

* Pro uložení bude využita kapacita uložišť v datových centrech (TC “Žerotínovo” a “Cejl”). Poznámka: V rámci návrhu požadavků na HW byl na příslušných serverech kvalifikovaným odhadem alokován prostor pro základní rozsah archivace dat.

Návrh dalšího rozvoje:

* ICZ DESA muže sloužit pro důvěryhodné uložení primárních dat (zdrojových souborů), jejichž uložení na externích HDD může představovat riziko ztráty cenných dat.

Detailní popis úložišť bude uveden v Dokumentaci skutečného provedení a bude vycházet z analýzy potřeb a možností Objednatele.

### Nápověda

Nápověda informačního systému bude obsažena v rámci aplikace, jako nápověda kontextová. Tedy tak, že uživateli bude vždy přímo dostupná a bude se nacházet vždy v části odpovídající pozici uživatele, ve které se v informačním systému nalézá.

Systém bude obsahovat rozsáhlou on-line dostupnou podporu ve formě návodu pro všechny uživatele systému (uživatel i administrátor). Obsah nápovědy bude vždy odpovídat funkcionalitám aktuální verze systému.

# Návrh řešení migrace dat

V rámci prvotního spuštění aplikací a následného provozu bude třeba naplnit sadu provozních a referenčních databází a zajistit jejich pravidelnou aktualizaci. Jedná se o následující databáze:

* Referenční databáze RUIAN.
* Číselníky DMVS – referenční údaje správců TI, DI, Editorů ZPS, dokumentace JVF DTM.

## Referenční databáze RUIAN

Databáze RUIAN bude založena pomocí zakládacích SQL scriptů ve struktuře odpovídající výměnnému formátu VFR RUIAN. Následně bude provedeno prvotní naplnění pomocí synchronizace s distribučním serverem cz-services.tmapserver.cz. Pomocí synchronizačních služeb bude tato databáze udržována v aktuálním stavu. Databáze každého kraje bude obsahovat pouze data na území příslušného kraje.

## Číselníky DMVS, referenční údaje správců TI, DI, Editorů ZPS

Údaje přebírané z informačního systému IS DMVS budou importovány prostřednictvím komponenty IS DMVS WebAPI, kterou využívají jednotlivé aplikační moduly IS DTM. Obsah takto migrovaných dat bude součástí aplikační databáze aplikačních modulů IS DTM, které tato data využívají. Příslušné aplikační moduly budou zajišťovat i průběžnou aktualizaci.

# Požadavky na součinnost Objednatele

## Rozsah součinnosti ze strany Objednatele

Rozsah součinností je definován pro jednotlivé fáze separátně. V součinnostech jsou uvedeny pouze aktuálně známé součinnosti, které je Poskytovatel schopen identifikovat ve fázi tvorby prováděcí dokumentace. Součinnosti vycházejí z harmonogramu uvedeného v kap. 9. V závislosti na stavu dodávky HW se termíny dílčích součinností mohou posouvat v čase. Tabulky pro jednotlivé fáze se skládají z:

* Oblast součinnosti – v tomto sloupci je definováno, pro jakou oblast je součinnost vyžadována. Může se jednat např. o projektové součinnosti, součinnost v rámci testování, či pro konkrétní modul apod.
* Popis součinnosti – v tomto sloupci je co nejvíce konkretizován popis součinnosti, která je v rámci dané oblasti požadována. V některých případech (pokud je poskytovatel součinnosti totožný) je v řádku, resp. buňce uvedeno více součinností najednou.
* Poskytovatel součinnosti – zde je definována role, která bude pro součinnost vyžadována. Pokud není známa role, je uvedeno pouze jako “Objednatel”.

### Fáze 1 – Dílčí fáze 1

Součinnost je vyžadována v rámci Dílčí fáze 1 realizované v termínu 20. 7. 2022 – 1. 9. 2022.

| **Oblast součinnosti** | **Popis součinnosti** | **Poskytovatel součinnosti** |
| --- | --- | --- |
| Obecné | * Definování komunikační matice. * Průběžné připomínkování prováděcí dokumentace. | Objednatel |

Tabulka 7 Požadavky na součinnost Fáze 1 - Dílčí fáze 1

### Fáze 1 – Dílčí fáze 2

Součinnost je vyžadována v rámci Dílčí fáze 2 realizované v termínu 2. 9. 2022 – 11. 1. 2023.

| **Oblast součinnosti** | **Popis součinnosti** | **Poskytovatel součinnosti** |
| --- | --- | --- |
| Testování | * Definování garanta pro dílčí akceptační řízení (pro dílčí fázi 2) za příslušné kategorie testů. | PM kraje |
| Testování | * Odsouhlasení akceptačních scénářů pro dílčí fázi 2. * Účast garanta na online schůzkách při provádění akceptačních scénářů pro jednotlivé kategorie testů. | Garanti pro dílčí akceptační řízení pro dílčí fázi 2 |
| Certifikáty | * Zajištění služeb interní certifikační autority pro vydání serverových certifikátů pro zabezpečení interní komunikace informačního systému. * Zajištění potřebných certifikátů pro zabezpečení komunikace a autentizace systému k službám eGovernmentu. * Zajištění potřebných certifikátů pro zabezpečení komunikace na webové servery z CMS2 a internetu. * Pro komunikaci HTTPS na Keycloak je třeba rovněž Poskytovateli dodat privKey&cert. Platí pro testovací i produkční prostředí. * Zajistit certifikát a dodat Poskytovateli privKey&cert pro komunikaci do JIP/KAAS webovou službou SOAP, kde KC figuruje jako TLS-klient s klientským certifikátem. * Zajistit certifikát a dodat Poskytovateli privKey&cert, kterým má NIA šifrovat odpovědi. | Objednatel |
| Technologická infrastruktura | * Zajištění technologické infrastruktury Objednatele, poskytnutí výpočetního výkonu a zajištění jeho dostupnosti, zálohování virtuálních serverů a datových úložišť. * Prvotní instalace linux serverů přes KICKSTARTY * Prvotní instalace WIN serverů * Poskytnutí služeb SMTP brány. * Poskytnutí síťových infrastrukturních služeb (NTP, DNS). | Objednatel |
| Komunikační infrastruktura | * Zajištění síťové komunikační infrastruktury Objednatele pro vzájemnou komunikaci mezi vlastními komponentami informačního systému. * Zajištění přístupu k AD pro možnosti ověření lokálních uživatelů. * Zajištění služeb CMS2 pro:   + Přístup do Internetu.   + Přístup z Internetu ke službám IS DTM. * Součinnost při zajištění integrace se systémem IS DMVS. * Zajištění síťového propojení systému v rámci DC i mezi datovými centry. * Zřízení VPN přístupů pro pracovníky Poskytovatele k implementaci a k následné správě systému. * Definování procesu řízení přístupů pro pracovníky Poskytovatele. * Zřízení SSH a RDP přístupů pro pracovníky Poskytovatele ke správě systému. | Objednatel |
| Bezpečnost komunikační infrastruktury | * Zajištění síťové a bezpečnostní infrastruktury datových center pro příchozí a odchozí komunikaci z/do CMS2. | Objednatel |
| Bezpečnostní dokumentace | * Zajištění osob, které se zúčastní interview, kde bude zjišťována hodnota aktiva a úroveň hrozeb pro analýzu rizik. * Připomínkování zprávy z analýzy rizik. * Poskytování odpovědí na otázky související s návrhem bezpečnostních opatření a tvorbou bezpečnostní dokumentace. * Připomínkování návrhů bezpečnostní dokumentace. | Objednatel |
| Import dat | * Poskytnutí a průběžná aktualizace harmonogramu datového projektu. * Poskytnutí kontaktů na Poskytovatele dat pro import. * Součinnost při vyřizování všech situací vzniklých při koordinování datového projektu s projektem IS DTM. * Předání pravidel pro segmentaci dat Poskytovatelům datových projektů a zajištění přípravy importovaných dat podle těchto pravidel. | Objednatel |
| Registrace | * Zaregistrovat AIS do JIP/KAAS.   + Nastavení redirect URL pro návrat z KAAS a do ICZ dodat ATS\_ID. * Zaregistrovat IS DTM jako kvalifikovaného poskytovatele do NIA. | Objednatel |
| Konfigurace | * Dodat IP adresu a port Active Directory. * Dodat login a heslo do Active Directory. * Dodat strukturu LDAP, aby bylo jasné, kde přesně role pro daného uživatele hledat. | Objednatel |

Tabulka 8 Požadavky na součinnost Fáze 1 - Dílčí fáze 2

### Fáze 1 – Dílčí fáze 3

Součinnost je vyžadována v rámci Dílčí fáze 3 realizované v termínu 11. 1. 2023 – 19. 5. 2023.

| **Oblast součinnosti** | **Popis součinnosti** | **Poskytovatel součinnosti** |
| --- | --- | --- |
| Testování | * Definování garanta pro dílčí akceptační řízení (pro dílčí fázi 3) za příslušné kategorie testů. | PM kraje |
| Testování | * Odsouhlasení akceptačních scénářů pro dílčí fázi 3. * Účast garanta na online schůzkách při provádění akceptačních scénářů pro jednotlivé kategorie testů. | Garanti pro dílčí akceptační řízení pro dílčí fázi 3 |
|  |  |  |
| Obecné | * Součinnost při tvorbě a akceptaci všech dokumentací. | Objednatel |
| Import dat | * Zajištění dat JVF DTM pro prvotní importy do IS DTM kraje. * Zajištění oprav identifikovaných chyb v datech zjištěných při prvotních importech (potřeba pro opakované importy a odladění chyb v datech). | Objednatel |
| Konfigurace | * Definice rolí a úložišť pro archivaci v systému ICZ DESA. | Objednatel |
| OpenData | * + Definování datových sad statistických údajů DTM a jejich registrace v Národním katalogu otevřených dat. | Objednatel |

Tabulka 9 Požadavky na součinnost Fáze 1 - Dílčí fáze 3

### Fáze 1 – Dílčí fáze 4

Součinnost je vyžadována v rámci Dílčí fáze 4 realizované v termínu 19. 5. 2023 – 2. 6. 2023.

| **Oblast součinnosti** | **Popis součinnosti** | **Poskytovatel součinnosti** |
| --- | --- | --- |
| Školení | * Definování administrátorů a klíčových uživatelů jako účastníků školení. * Zajištění prostor vybavení pro účely školení (notebooky nebo PC sestavy, prezentační technika, konektivita na prostředí IS DTM...), případně zřízení online schůzek pro školení. | Objednatel |
| Školení | * Účast definovaných osob na školeních. | Administrátoři a klíčoví uživatelé Objednatele |
| Testování | * Definování testerů v rámci testovacího provozu. | Objednatel |

Tabulka 10 Požadavky na součinnost Fáze 1 - Dílčí fáze 4

### Fáze 1 – Dílčí fáze 5

Součinnost je vyžadována v rámci Dílčí fáze 5 realizované v termínu 10. 1. 2023 – 2. 6. 2023.

| **Oblast součinnosti** | **Popis součinnosti** | **Poskytovatel součinnosti** |
| --- | --- | --- |
| Import dat | * Zajištění validních dat JVF DTM z datových projektů, které respektují požadavky IS DTM, pro jejich finální ostré importy do IS DTM kraje do požadovaného termínu definovaného Poskytovatelem. 50 % dat bude zajištěno do 12. 5. 2023. Zbývající část dat bude zajištěna do 19. 5. 2023, případný posun s dodáním zbývajích dat bude mít vliv na dokončení dílčí fáze 5. * Koordinace předávání dat mezi datovým projektem a projektem IS DTM. * Součinnost při vyřizování všech situací vzniklých při koordinování datového projektu s projektem IS DTM. | Objednatel |
| Testování | * Definování garanta pro dílčí akceptační řízení (pro dílčí fázi 5) za příslušné kategorie testů | PM kraje |
| Testování | * Odsouhlasení akceptačních scénářů pro dílčí fázi 5.Účast garanta na online schůzkách při provádění akceptačních scénářů pro jednotlivé kategorie testů. | Garanti pro dílčí akceptační řízení pro dílčí fázi 5 |

Tabulka 11 Požadavky na součinnost Fáze 1 - Dílčí fáze 5

### Fáze 1 – Dílčí fáze 6

Součinnost je vyžadována v rámci Dílčí fáze 6 realizované v termínu 2. 6. 2023 – 16. 6. 2023.

| **Oblast součinnosti** | **Popis součinnosti** | **Poskytovatel součinnosti** |
| --- | --- | --- |
| Testování | * Účast garanta na online schůzkách při provádění akceptačních scénářů pro jednotlivé kategorie testů. (Pokud se bude realizovat 2. kolo akceptačního testování pro dílčí fázi 5) | Garanti pro dílčí akceptační řízení pro dílčí fázi 5 |
| Testování | * Souhrnné provedení akceptačních testovacích scénářů | Testeři objednatele |

Tabulka 12 Požadavky na součinnost Fáze 1 - Dílčí fáze 6