Technická specifikace IS WEB MV

1 Obsah

2 Základní údaje

2.1 Cíl dokumentu

Cílem dokumentu je popis technických požadavků na předmět veřejné zakázky, jímž je dodávka IS WEBy MV, v rámci dokumentu dále veden pod zkratkou „WEB MV“. Popis by měl uchazečům veřejné zakázky předat základní informace o požadavcích na požadovaný nový systém WEB MV a měl by umožnit odpovídající vytvoření nabídek uchazeči s odpovídající cenovou nabídkou a popisem nabízeného IS a souvisejících služeb.

Dokument popisuje projekt v jeho intencích a vztahu k WEB MV, dále stanovuje architektonické požadavky, které budou dodavatelem dále rozpracovány v rámci dodávky, popisuje požadavky na jednotlivé funkcionality pro WEB MV, systémové vlastnosti WEB MV, bezpečnost, shodu s legislativou, požadované testy v rámci dodání, požadované licence k WEB MV, vyžadované školení a dodání dokumentace, vše v souladu s platnou legislativou.

Dále dokument uvádí požadavky na řízení projektu dodavatelem vč. fázování, které bude dále dodavatelem rozpracováno v rámci dodávky, respektive projektového řízení dodání WEB MV a předimplementační analýzy zpracované Dodavatelem, která bude podléhat akceptaci ze strany Odběratele.

2.2 Související dokumenty

Souvisejícími dokumenty jsou dokumenty této veřejné zakázky, především Studie proveditelnosti a podpůrné dokumenty, které uchazeč je povinen vyplnit formou odpovědi na zadanou otázku (excel soubory). Dále pak Návrh smlouvy.

Tento dokument je v rámci veřejné zakázky přílohou Zadávací dokumentace, po ukončení veřejné zakázky bude přílohou smlouvy, uzavřené s vítězným uchazečem.

2.3 Použité pojmy

Pro účel dokumentu je označován zadavatel veřejné zakázky i jako Odběratel. Vítězný Uchazeč veřejné zakázky, pro nějž bude tato technická specifikace závazná, je veden jako „Dodavatel“.

3 Popis projektu – stávající stav a představení požadavků

3.1 Důvod realizace – Výchozí stav

Internetový portál MV, PČR a HZSČR (dále jen Portál MV) byl klasifikován jako Významný informační systém. Portál MV slouží jako hlavní komunikační kanál ministerstva vnitra (dále též "MV") a v nedávné době se potýkal s problémy s nedostatečným výkonem, například výpadky v době vyhlášení restrikcí pro cestování mezi okresy v rámci boje proti pandemii covid-19. Současný Portál MV není dostatečně HW a SW nadimenzován, ani infrastrukturní prvky, co se výkonnosti týká, aby zvládl nelegální zátěž (hackerské DDoS útoky). Stávající Portál má velké výkonnostní problémy, pokud má zvládnout zvýšenou legitimní zátěž (Přihlášení a práce současně pracujících čtenářů a redaktorů). Současně Odběratel upozorňuje, že stávající infrastruktura WEB MV nenaplňuje v řadě ohledů platnou legislativu (zákony, vyhlášky, nařízení a resortní předpisy) a v některých ohledech je v provizorním stavu (zejména proxy server). Proto s ní není možno počítat se zařazením ani do dočasně využívaného systému. Tento fakt byl dalším podnětem proč vytvořit nový IS WEB MV. Nicméně obsah veřejné zakázky se bude týkat pouze vytvoření aplikačních komponent, včetně instalace a konfigurace vrstvy Kubernetes.

Aby nedošlo k problémům při souběhu projektu dodávky této veřejné zakázky s dodávkou nového on-premise prostředí, tak Odběratel zajistí po vysoutěžení dočasné prostředí na veřejném Cloudu. V současné době je hlavním problémem závislost na dodavateli při jakýchkoliv požadavcích na změnu. Dnes jakoukoliv změnu musí provést stávající dodavatel, což způsobilo fakticky závislost na dodávkách dodavatele, a to jak kapacitně, tak i finančně.

Jednou z částí, kterou je potřeba prověřit po stránce funkční a bezpečnostní, je stávající stav služeb zdrojových aplikací. Některé činnosti jsou manuální a bude potřeba je automatizovat bez zásahu aplikačních administrátorů. Popis současného stavu zdrojových aplikací je evidován a je přiložen v samostatné Příloze Technické specifikace IS WEB MV č. 6 – Checklisty k aplikacím. Návrh na případnou změnu řešení funkční architektury (API aplikační) pro všechny požadované služby a procesy předloží Dodavatel Odběrateli k oponentuře (posouzení). Celý návrh budoucího řešení bude podléhat akceptaci v rámci dodávky analytické části realizačního projektu.

3.2 Popis požadovaných změn – proti stávajícímu stavu

Hlavní rozdíly proti stávajícímu stavu:

- Nový internetový portál WEB MV, bude lépe zajištěn z hlediska naplnění legislativních požadavků, které vychází z požadavků na zajištění kybernetické bezpečnosti. Odběratelem požadovaný soulad s platnou legislativou je mířen na zajištění všech požadavků spojených s IS typu VIS (významný informační systém).
- Jednotlivá prostředí budou provozována na dostatečně výkonné infrastruktuře na on-premise prostředí (dále i privátní cloud MV nebo UPAAS).
- Bude zavedeno prostředí (vrstva) Kubernetes, která umožní větší flexibilitu při rozvoji a provozu systému.
- Pro provoz a další rozvoj se bude preferovat využití takového SW vybavení, které má jasně definovaný „Life cycle" min. s 5letou periodou.

- Aplikační komponenty budou využívat moderní responsivní design v rámci definovaných pravidel Design Systému gov.cz a budou splňovat požadavky na přístupnost.

Při vývoji nového IS bude kladen velký důraz na zajištění nezávislosti Odběratele z hlediska možného budoucího vývoje a rozvoje aplikační vrstvy. Z tohoto důvodu byla navržena architektura nového IS WEB MV modulárně a součástí dodávek bude i požadavek na dodávku licencí, zdrojů a dokumentace.

V neposlední řadě je nový IS WEB MV definován v souladu s platnou legislativou. Jde o následující zákony, vyhlášky a interní předpisy:

- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím.
- Zákon č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací.
- Zákon č. 500/2004 Sb., Správní řád.
- Zákon č. 141/1961 Sb., Trestní řád.
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.
- Zákon č. 240/2000 Sb. Krizový zákon.
- Zákon č. 365/2000 Sb. o informačních systémech veřejné správy.
- Zákon č. 110/2019 Sb. o zpracování osobních údajů.
- Zákon č.12/2020 Sb. o právu na digitální služby a o změně některých zákonů.
- Vyhláška č. 82/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).
- Vyhláška č. 529/2006 Sb. o dlouhodobém řízení informačních systémů veřejné správy (od 1.7.2024 nahrazena vyhl. č.360/2023 Sb.).
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.
- Zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci (tzv. DEPO).
- Nařízení EP a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
- Agendy uvedené v Registru práv a povinností:
  - Poskytování informací (A1261),
  - Policie České republiky (A418),
  - Požární ochrana (A341),
  - Služební poměr příslušníků bezpečnostních sborů (A876),
  - Obecní policie (A420),
  - Správa státních hranic (A409).

3.3 Popis stávajícího stavu RS a trendy v oblasti RS

Popis stávajícího stavu redakčního systému (dále také “RS”), aktuální trendy v této oblasti, příklady RS podobných aktuálně používanému či přídavné funkce RS jsou uvedeny v samostatné Příloze Technická specifikace IS WEB MV č. 1 – Základní popis RS.

3.4 Pravidla a stanovení odpovědnosti Dodavatele při projektových dodávkách

V samostatné Příloze Technické specifikace IS WEB MV č. 7 je uložen dokument, který popisuje rozdělení odpovědnosti za vývoj integrace. V tabulce jsou uvedeny body, které jsou

uloženy ve schématech Byznys architektury. V těchto bodech (služby, procesy, komponenty) je definována odpovědnost za vývoj integrační činnosti. V tabulce je označen Garant (zeleně podbarvená buňka) a Odběratel (žlutě podbarvená buňka). Garant a Odběratel spolu tvoří Technický tým. Technický tým zajišťuje nutnou součinnost při analýze a vývoji jednotlivých částí dodávky.

Postup a odpovědnost při vývoji integrace je stanovena následně:

- Odběratel předá dokumentaci, potřebné informace a požadavky Garantovi.
- Garant na základě těchto informací vyvine integrační prvek (např. soubor v definovaném formátu, datovou větu, a další) a provede otestování integračního prvku v součinnosti Odběratele.
- Odběratel po úspěšném testu akceptuje provedení úspěšného funkčního testu na integraci.

Popis rolí jednotlivých subjektů:

- Odběratel – Zadavatel VZ, pracovníci projektu zadavatele, řídicí výbor nebo techničtí pracovníci.
- Dodavatel – jde o vysoutěženého Dodavatele nebo více Dodavatelů.
- Projektový tým - jde o pracovníky obou stran, kteří koordinují svoje týmy.
- Technický tým – jde o pracovníky Dodavatelů, kde je nutné zajištění odpovědnosti ale i součinnosti při dodávce společného úkolu (například Integrace mezi komponentami – každý dodavatel bude předávat požadavky na zprovoznění integrovaného na cizí komponenty. Každý dodavatel musí předat v rámci týmu integrační analýzu s popisem vlastního API a požadavků na toto API).

3.5 Schémata a popis aplikační vrstvy požadovaného řešení

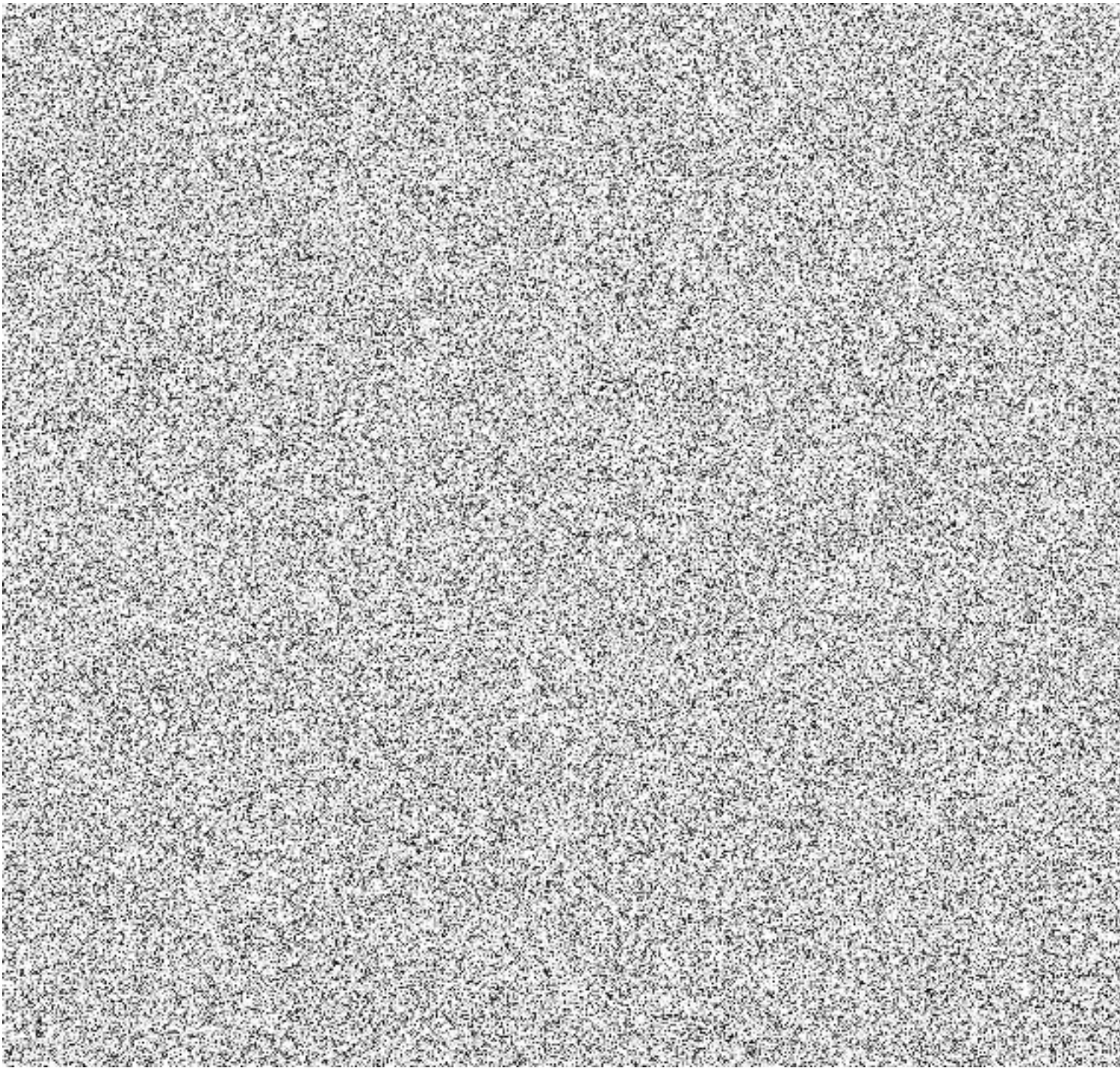
IS WEB MV je architektonicky navržen v souladu s požadavkem na vytvoření modulárního systému, jehož komponenty mohou pracovat nezávisle, a to včetně integrovaných systémů. Za nezávislost se považuje vlastnost systému, který umožní jednotlivým komponentám pracovat nezávisle na druhých komponentách.

Hlavními komponentami poptávaného systému jsou komponenty RS – redakční systém a IdM, PUB – Portál, který se dělí na WEB a Micro WEBy a v neposlední řadě je to komponenta API aplikační. Služby a funkce jednotlivých aktivit jsou popsány níže v tomto dokumentu. Na schématu níže jsou mimo tyto komponenty vyznačeny další integrované komponenty, které budou poskytnuty na zajištění hlavních služeb a činností IS WEB MV.

Pro ulehčení prezentace poptávaného řešení, jsou v dokumentu uložena schémata a tato schémata jsou popsána níže v jednotlivých článcích. Schémata po vytištění mohou být obtížně čitelná a z tohoto důvodu jsou uložena v Příloze č.2 tohoto dokumentu.

3.5.1 Vymezení poptávané dodávky aplikační vrstvy

Předmět dodávky je vytýčen šedým pozadím (Group – IS WEB MV) na Obrázek 1 - Schéma poptávaná dodávka (1 prostředí). Popis jednotlivých prostředí a jeho instancí je uveden níže v textu.



Obrázek 1 - Schéma poptávaná dodávka (1 prostředí)

3.5.1.2 Popis schématu poptávané dodávky

Cílem prezentace tohoto schématu je vysvětlení pojmu „poptávaná dodávka“ včetně vymezení integrovaných komponent, které podporují základní služby a funkce celého IS.

3.5.1.3 Poptávaná dodávka z pohledu Subjektů

IS WEB MV bude vytvořen pro tři subjekty, které jsou zodpovědné za prováděné aktivity v rámci resortu MV. Jmenovitě se jedná o subjekt Ministerstvo vnitra České republiky (dále

také “MVČR”). Druhým subjektem je Policie ČR (dále také “PČR”) a posledním subjektem je Hasičský záchranný sbor (dále také “HZS”). Všechny subjekty mají dnes vlastní doménu. V rámci WEBů jsou hojně využívané odkazy (redirekty) mezi jednotlivými WEBy těchto subjektů.

3.5.1.4 Poptávaná dodávka z pohledu počtu prostředí

IS WEB MV bude vytvořen na více prostředích a více lokalitách. Jejich použití bude velmi rozdílné jak z hlediska využití, tak i z hlediska doby trvání daného prostředí. Přehled budovaných a provozovaných prostředí projektu:

Tabulka 1 – Přehled prostředí

Typ prostředí	Prostředí	Instance	Hostingové centrum	Poznámka
Dočasné – Veřejný cloud	TEST	Resort	EU datová centra	Bez integrace
Dočasné – Veřejný cloud	VÝVOJ	Resort	EU datová centra	Bez integrace
On-premise	TEST	Resort	DC1 primární	Včetně integrace
On-premise	VÝVOJ	Resort	DC1 primární	Včetně integrace
On-premise	STAGE (PROD)	PČR, MVČR, HZS	DC1 primární	Včetně integrace
On-premise	PROD (PROD)	PČR, MVČR, HZS	DC1 primární	Včetně integrace
On-premise	STAGE (ZAL)	PČR, MVČR, HZS	DC2 sekundární	Včetně integrace
On-premise	PROD (ZAL)	PČR, MVČR, HZS	DC2 sekundární	Včetně integrace

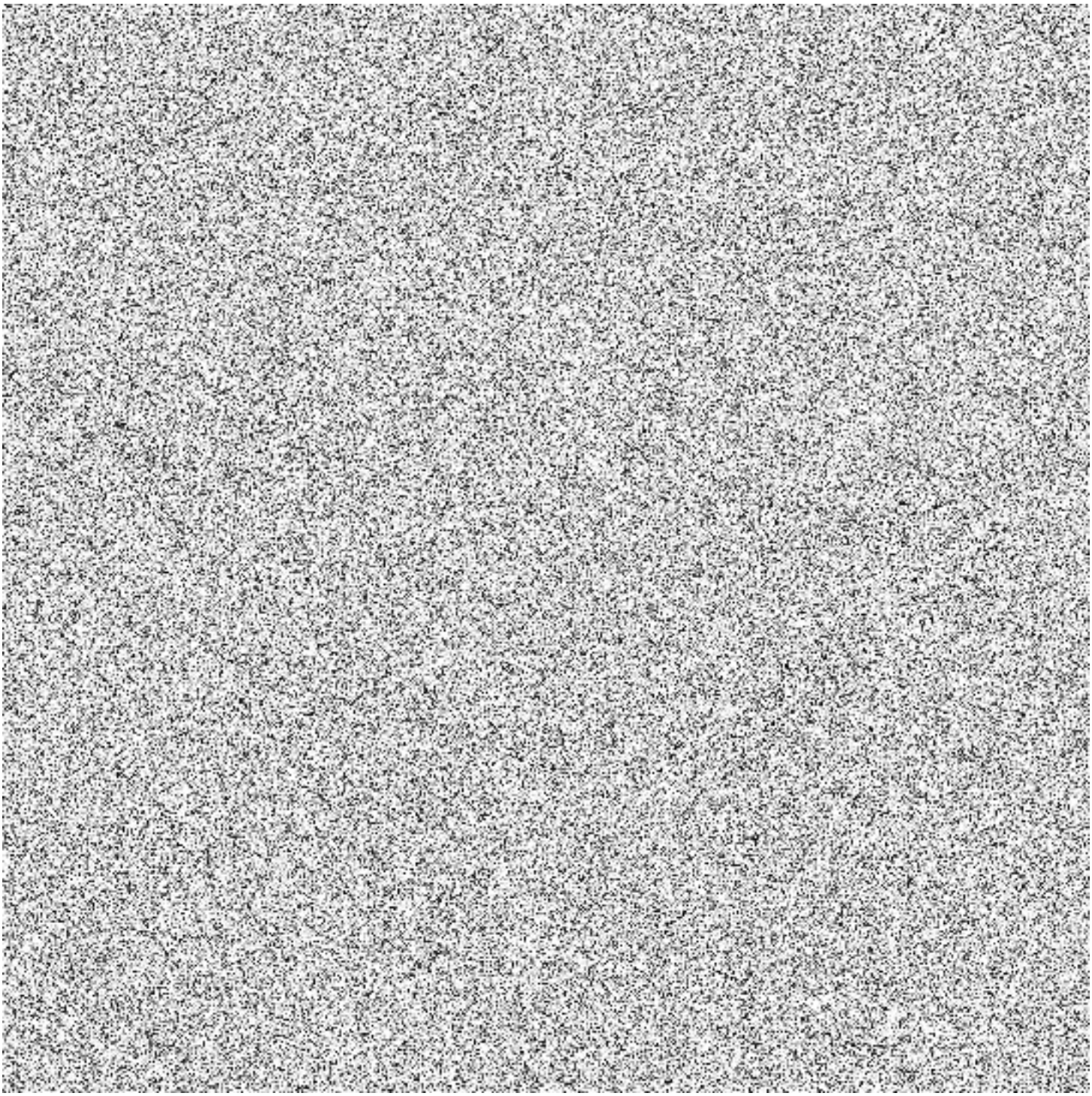
V rámci každého prostředí jsou na vrstvě Kubernetes vytvořeny instance, požadované jsou 4 druhy instancí, které se liší pouze v možnosti využití v rámci Prostředí. Z tabulky 1 výše je zřetelné, že Prostředí VÝVOJ v instanci Resort mohou být instalovány jednotlivé další instance Subjektů a hlavním úkolem pro tuto instanci je naprogramovat nebo nakonfigurovat nově vyvíjenou nebo upravenou funkcionalitu ve VÝVOJ prostředí. Prostředí se bude využívat pro provádění testů vývojovými pracovníky před předáním změny na TEST prostředí pro vyvíjenou instanci.

Prostředí TEST – v instanci Resort mohou být instalovány jednotlivé další instance Subjektů a hlavním úkolem pro tuto instanci je prověřit nově vyvíjenou nebo upravenou funkcionalitu v TEST prostředí. Autentizace do tohoto prostředí je prováděna přes IdM. Prostředí se bude využívat pro UAT.

Prostředí STAGE (PROD i ZAL) – prostředí je výkonově identické s prostředím PROD (PROD i ZAL) a nazývá se také předprodukční prostředí. Při prováděni změn akceptovaných na TEST prostředí je nutno STAGE prostředí výkonově a konfiguračně nastavit tak, aby bylo možno otestovat toto prostředí mimo jiné na soulad s provozními a servisními SLA parametry. Na tomto prostředí se dále provádějí výkonové testy a bezpečnostní testování, které je v souladu s legislativou. Prostředí je rozloženo do dvou lokalit a z tohoto důvodu je požadováno na tomto prostředí provádět DRP testování jednotlivých scénářů. Prostředí STAGE nese všechny instance jednotlivých Subjektů s výjimkou instance Resort.

Prostředí PROD (PROD i ZAL) – produkční prostředí na které se měří na provozní a servisní SLA parametry. Prostředí je rozloženo do dvou lokalit. Prostředí PROD (PROD i ZAL) nese všechny instance jednotlivých Subjektů s výjimkou instance Resort. Kromě provozních služeb se na tomto prostředí provádí pravidelné bezpečnostní testy.

3.5.1.5 Aplikační schéma – komponenty jedné instance včetně integrace



Obrázek 2 - Schéma aplikační vrstva instance včetně integrace

3.5.1.6 Popis aplikační vrstvy – komponenty jedné instance včetně integrace

3.5.1.6.1 Obecný přehled

Aplikační schéma (Obrázek 2 - Schéma aplikační vrstva instance včetně integrace) zobrazuje celý pohled na obsah instance pro jeden subjekt, a to včetně jeho integrace

s ostatními systémy. Ve schématu je znázorněna provázanost celého dodávaného systému. Hlavními vazbami se rozumí vazby mezi zdrojovými systémy a datovými uložišti dodávaného systému. Další významné vazby jsou mezi redakčním systémem a Portálem (statickými stránkami) a vazba mezi API aplikační a Portálem (dynamické stránky). V neposlední řadě je požadována dodávka IdM (AD – Active Directory), který zajišťuje centrální autentizaci a částečnou autorizaci do dodávaných základních komponent (redakční systém, API aplikační a Portál). IdM (AD) zprostředkovává propojení na zdrojová centrální IdM nebo AD, kde je nutno provádět kontrolu na aktualizace jednotlivých administrátorů. Při aktualizaci role ve zdrojovém systému je nutno řešit manuálně autentizaci v IdM (AD). O aktualizaci ID je vybraný aktér Red_Admin notifikován. Rozdíl je u subjektu PČR, kde dochází k provedení autentizace a autorizace ze zdrojového systému prostřednictvím protokolu OAUTH 2.0.

Dále je požadovaný systém integrován k provozně bezpečnostním nástrojům (monitoring, zálohování, logování celého systému s přenosem logů na definovaný prostor). V neposlední řadě je na schématu naznačena integrace s notifikačními systémy. Všechny integrace, které se budou provádět mimo požadovaný systém, se budou provádět v rámci součinnosti s Odběratelem.

3.5.1.6.2 Komponenta Portál (publikace) – základní požadavky na dodávku

- Webové Portály (weby a micro weby) – prázdné struktury s byznys logikou (služby) a procesy.
- Webové portály musí být schopny poskytovat službu publikace ve více světových jazycích společně s funkcí, která zajistí pro zápis využívání registrovaných kódovacích znaků vybraného jazyka.
- Vytvoření rozhraní pro vstup Občanů na publikační část.
- Administrátorské rozhraní (Pohled činnostních funkcí - WEBy MV) s GUI pro administraci.
- Vytvoření dynamických a statických stránek s našeptávači.
- Instalace a konfigurace Portálů.
- Vytvoření systému Logů a sestavy možných chybových hlášení pramenících z chyby v kódu. Bude sloužit pro nastavení monitoringu.
- Integrace Portálů (publikační části):
    - Integrace s API aplikační,
    - Integrace s redakčním systémem,
    - Integrace s IDM „Služba správa části AD pro MVČR“.
- Provoz v rámci projektu.
- Testování a akceptace.

3.5.1.6.3 Redakční systém a AD

- Dodávka redakčního systému podle požadavků.
- Instalace a konfigurace pro všechny subjekty.
- Zprovoznění všech procesů a vybraných funkcí.
- Redakční systém musí být schopen poskytovat službu generování stránek a jejich publikaci ve více světových jazycích společně s funkcí zajistit využívání pro zápis registrovanými kódovacími znaky vybraného jazyka.

- Exporty pro IS OpenData.
- Vytvoření systému Logů a sestavy možných chybových hlášení pramenících z chyby v kódu. Bude sloužit pro nastavení monitoringu.
- Integrace Redakčního systému:
    - Integrace s IDM „Služba správa části AD pro MVČR“,
    - Integrace s API aplikační (zdrojová data),
    - Integrace s Portály (publikační část).
- Provoz v rámci projektu.
- Testování a akceptace.

3.5.1.6.4 API aplikační

- Dodávka API aplikační podle požadavků.
- Instalace a konfigurace API aplikační pro všechny subjekty.
- Zprovoznění všech procesů a vybraných funkcí.
- API aplikační musí být schopen poskytovat službu převzetí vytvořených informací v registrovaných kódových znakových sadách předaných z WEBů (informace zapsané zadavatelem na dynamických stránkách ve zvoleném světovém jazyku a znakových kódech) a zpět předat sestavené informace ve stejných znakových kódech a jazyku na WEBy.
- Exporty pro IS OpenData.
- Zprovoznění SFTP a potřebných úložných DB tabulek a souborů.
- Vytvoření byznys logiky pro přebírání dat ze zdrojových systémů.
- Vytvoření byznys logiky pro výměnu dat zajišťovaných pomocí scheduleru (konfigurace ad-hoc a plánovaných jobů).
- Vytvoření a zprovoznění Administrátorské rozhraní s GUI pro administraci API aplikační.
- Vytvoření systému Logů a sestavy možných chybových hlášení pramenících z chyby v kódu. Bude sloužit pro nastavení monitoringu.
- Integrace API aplikační:
    - Integrace s Portály (publikační část),
    - Integrace se zdrojovými systémy.
- Provoz v rámci projektu.
- Testování a akceptace.

3.5.2 Vymezení architektury dodávky kontejnerové orchestrace

Pokud je dále v textu uveden pojem „Kubernetes“ je míněna jakákoliv kontejnerová orchestrace.

3.5.2.1 Schéma – architektonický model

Schéma je publikováno a popsáno v kapitole níže (2.6.1.1 Schéma – architektonický model).

3.5.2.2 Sledovat dostupnost jednotlivých částí webů

a:

- Dynamicky měnit počet alokovaných zdrojů tak, aby nebyla ohrožena uživatelské zkušenost (pomocí definovaných metrik),
- Preferovat dostupnost klíčových částí webu před ostatními částmi webu, a to především v případě krizových situací s cílem maximalizovat dostupnost webu.

3.5.2.3 Nasazování nových verzí

- Sledovat uživatelskou zkušenost (pomocí definovaných metrik) při nasazování nových verzí systému či aplikací,
- Umožnit postupné nasazování verzí pro definovaný počet uživatelů s cílem posoudit kvalitativní rozdíl jednotlivých verzí (pro definované metriky).

3.5.2.4 Navrhnout způsob využití existujících infrastrukturních prvků

- Využití load balanceru pro směřování zátěži či filtrování útoků,
- Využití uložiště pro uchování aplikací a jejich verzování.

3.5.2.5 Navrhnout způsob zálohování

Při návrhu zálohování vycházet z existujících systémů nebo služeb, které jsou na trhu dostupné. Cílem je zajistit vytváření záloh a obnov vrstvy Kubernetes.

Mezi základní požadavky patří:

- Nástroj nebo služba která zajišťuje zálohování pro Kubernetes vrstvy. Nástroj musí zabezpečovat metadata a data aplikace ukládáním záloh na nezávislém úložišti.
- Nástrojem nebo službou jsou možné úplné nebo přírůstkové zálohy clusteru a obnova je v případě ztráty dat.
- Nástroj nebo služba umožní migrovat z jednoho clusteru do druhého a spouštět pre- a post-hook pro operace zálohování a obnovy.
- Nástroj umožní plánovat zálohování a definovat zásady uchovávání pro vaše zálohy.
- Nástroj nebo služba umožnuje použít webovou konzolu pro správu k podrobné kontrole stavu operací zálohování a obnovy.
- Nástroj umožní provést obnovu Kubernetes vrstvy do záložní lokality.

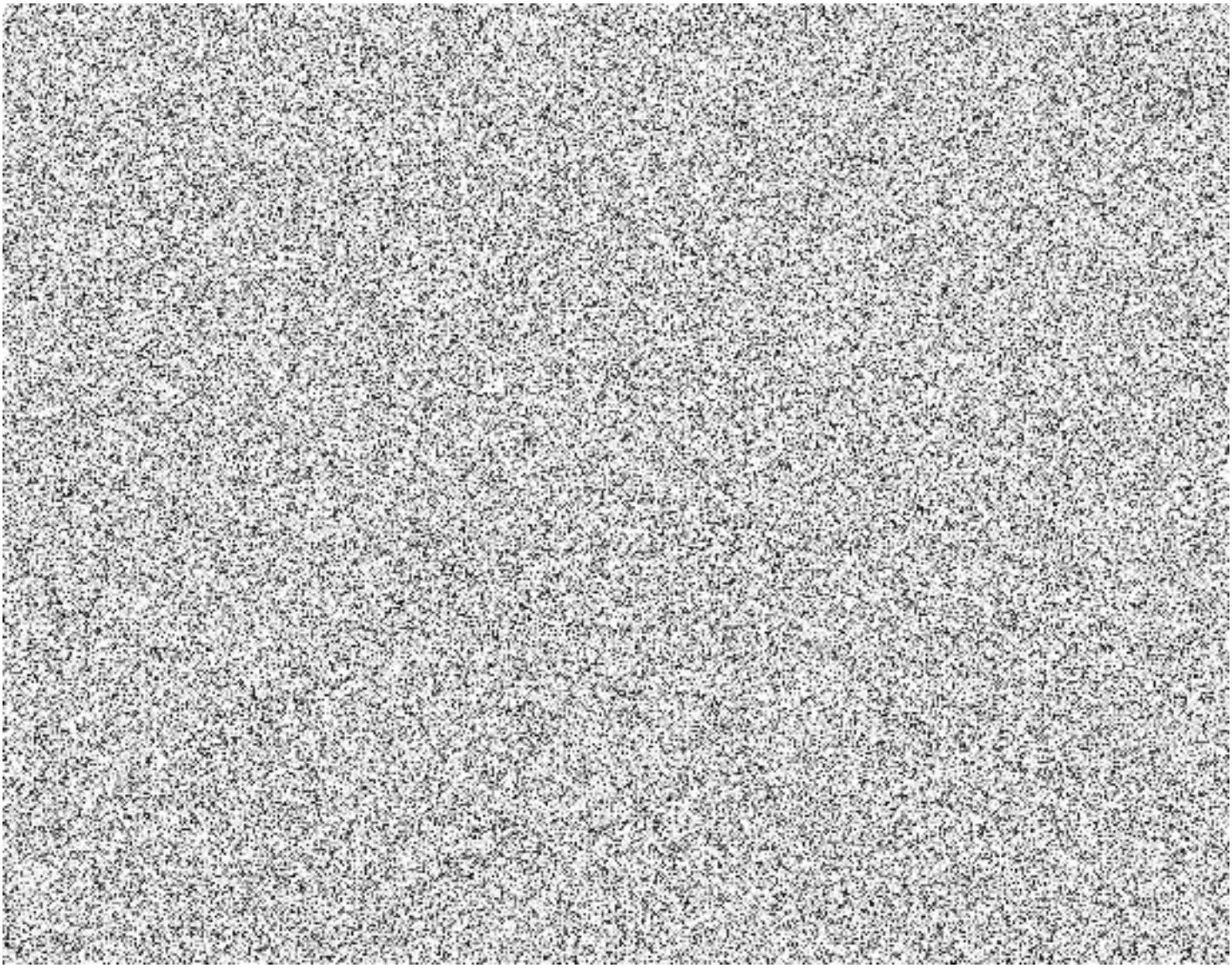
Přesný návrh využití architektury na aplikační a technologické vrstvě vrstvou Kubernetes předloží Dodavatel Odběrateli k oponentuře (posouzení). Celý návrh bude podléhat akceptaci v rámci dodávky analytické části realizačního projektu.

3.6 Schémata a popis technologické vrstvy (sítě a serverová část s hostingovými službami)

3.6.1 Prostředí a instance na UPAAS (Služby UPAAS včetně vrstvy Kubernetes)

3.6.1.1 Schéma – architektonický model

Zadavatel požaduje, aby Dodavatel využil minimálně následující možnosti, které nabízí architektura Kubernetes nebo Docker Swarm.



3.6.1.2 Popis a požadavků modelu

- Modulární a škálovatelná architektura: Systém musí být navržen jako soubor na sobě nezávislých modulů (mikroslužeb), které mohou být nasazovány, škálovány a rozvíjeny samostatně. Tento přístup umožňuje flexibilní přístup k budoucím rozšířením a aktualizacím systému.
- Platforma pro orchestraci a nasazení kontejnerů: Systém musí být provozován na platformě umožňující orchestraci kontejnerizovaných aplikací, která zajistí jejich dostupnost, škálovatelnost a jednoduchou správu. Tato platforma musí podporovat automatizované nasazování, škálování a správu aplikací, a to prostřednictvím API.
- Příklady platformy pro orchestraci jsou technologie Kubernetes či Docker Swarm.
- Kontejnerizované aplikace: Každá mikroslužba musí být zabalená jako kontejnerový obraz (image), který bude umístěn v repositáři kontejnerových obrazů. Tyto obrazy budou nasazovány na produkční prostředí pomocí vybrané platformy pro orchestraci kontejnerů.
- API-first přístup: Komunikace mezi jednotlivými moduly systému musí být realizována výhradně prostřednictvím definovaných API. Veškeré API musí být detailně

dokumentováno a vystaveno tak, aby umožňovalo integraci dalších systémů a aplikací třetích stran.

3.6.1.3 Dynamické škálování a dostupnost:

- Požadavek na flexibilitu systému: Systém musí být navržen tak, aby byl schopen dynamicky reagovat na kolísání návštěvnosti. Zejména v případech, kdy dojde k náhlému nárůstu návštěvnosti v důsledku mimořádných událostí, jako jsou přírodní katastrofy (např. povodně) nebo důležité zprávy, musí systém být schopen automaticky škálovat dostupné zdroje.
- Automatické přidělování zdrojů: Dodavatel musí navrhnout systém, který bude schopen automaticky přidělovat a škálovat zdroje na základě aktuální zátěže. To zahrnuje automatické nasazení dalších instancí kritických mikroslužeb a aplikací v závislosti na aktuální potřebě.

3.6.1.4 Kritické části webu a aplikací:

- Identifikace kritických komponent: Zadavatel musí mít možnost definovat, které části webu a aplikací jsou považovány za kritické a musí být vždy dostupné i za mimořádných okolností. Tyto komponenty mohou zahrnovat například informační stránky, krizové hlášení, kontaktní formuláře, API pro nouzové komunikace atd.
- Prioritizace zdrojů: Systém musí umožňovat prioritizaci zdrojů pro tyto kritické komponenty tak, aby byly vždy dostupné. V případě extrémní zátěže se méně kritické části systému mohou stát nedostupnými, aby byly klíčové funkce zachovány.

3.6.1.5 Požadavky na vývoj aplikací a jejich dokumentaci

- Mikroservisní architektura:
  - Mikroslužby: Aplikace musí být vyvíjeny jako samostatné mikroslužby, které budou komunikovat mezi sebou pomocí API. Každá mikroslužba musí být nezávislá, aby mohla být nasazována a škálována samostatně.
  - Nasazování a provoz: Každá mikroslužba musí být dodána jako kontejnerový obraz a uložena do určeného repozitáře. Nasazování mikroslužeb musí být plně automatizované a kompatibilní s běžně užívanými platformami pro orchestraci kontejnerů.

3.6.1.6 API a dokumentace:

- Definice API: Každá mikroslužba musí mít definované API, které bude sloužit k její komunikaci s ostatními službami a aplikacemi. API musí být navrženo tak, aby bylo snadno rozšiřitelné a umožňovalo integraci s dalšími systémy.
- Swagger / OpenAPI dokumentace: API každé mikroslužby musí být popsáno pomocí specifikace Swagger / OpenAPI (či obdobné), která bude součástí dodané dokumentace. Tato dokumentace musí být aktualizována při každé změně API.
- Verzování API: API musí být verzované, aby bylo možné udržovat kompatibilitu s různými verzemi klientů nebo jiných služeb, které na něm závisí.

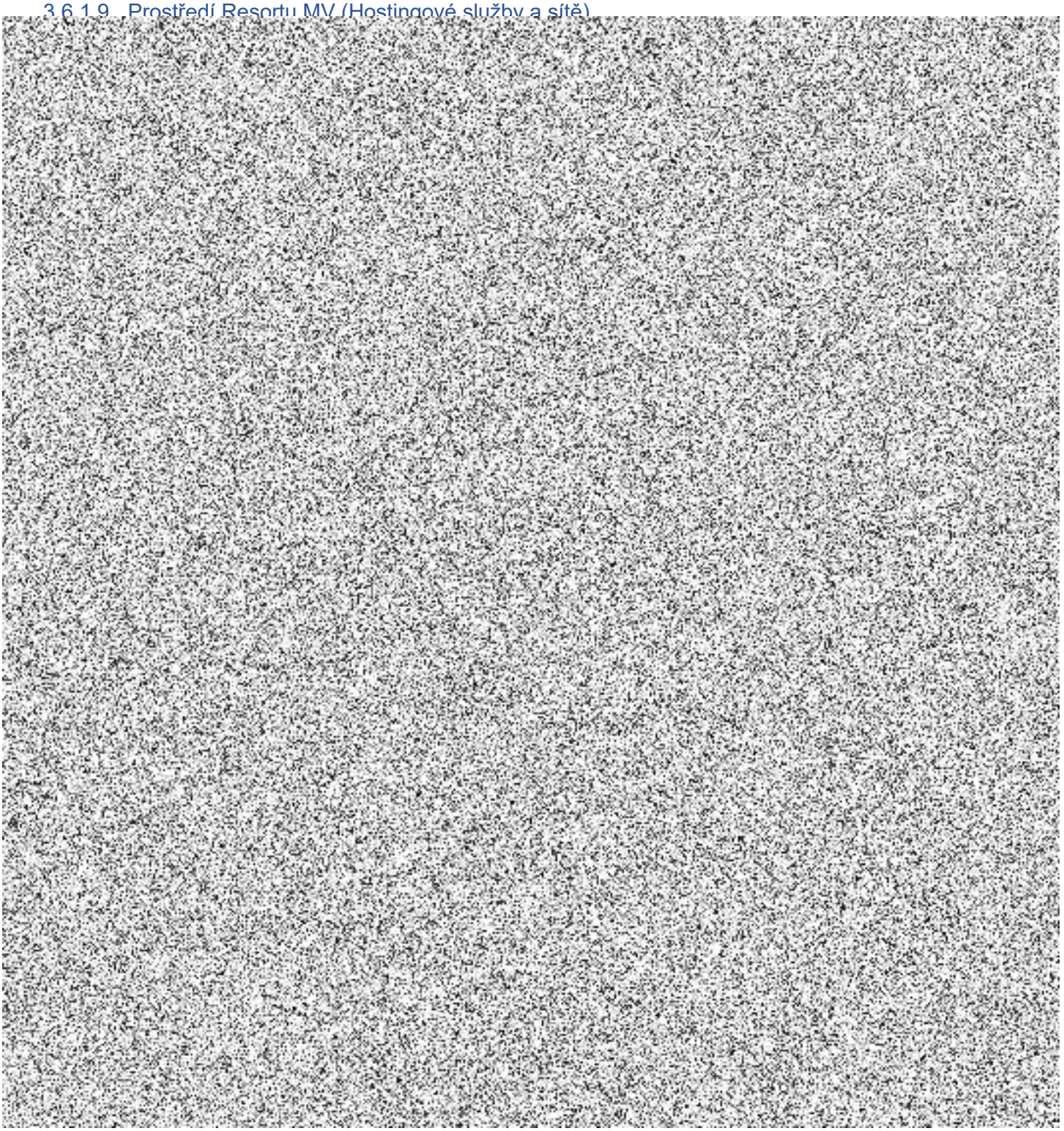
3.6.1.7 Kvalita kódu a bezpečnost:

- Unit testy: Každá mikroslužba musí být dodána s kompletní sadou unit testů, které ověřují funkčnost jednotlivých částí aplikace. Testy musí být součástí kontinuální integrace a musí být automaticky spouštěny při každé změně kódu.
- Bezpečnostní standardy: Vývoj musí dodržovat bezpečnostní standardy, včetně ověřování vstupů, ochrany proti útokům typu SQL injection, XSS, CSRF a dalších běžných bezpečnostních rizik. Veškeré bezpečnostní mechanismy musí být popsány v dokumentaci.

3.6.1.8 Dokumentace:

- Technická dokumentace: Každá mikroslužba musí být dodána s technickou dokumentací, která bude obsahovat:
- Popis architektury mikroslužby
- Detailní specifikaci API včetně příkladů použití
- Informace o nasazení a provozu mikroslužby
- Pokyny pro škálování a aktualizaci mikroslužby
- Bezpečnostní opatření a postupy pro zabezpečení aplikace
- Popis testů a jejich výsledky
- Provozní dokumentace: Dokumentace musí obsahovat pokyny pro administrátory a provozní týmy, včetně postupů pro monitorování, zálohování a obnovu, řešení problémů a škálování aplikací.

3.6.1.9 Prostředí Resortu MV (Hostingové služby a sítě)



3.6.2 Popis poptávaného řešení – popis schémat

3.6.2.1 Prostředí UPAAS (Služby UPAAS včetně vrstvy Kubernetes)

Schéma znázorňuje prvky, které obsahují vrstvu Kubernetes a orchestraci Control Plane, které jsou součástí dodávky dodavatele. Odběratel zajistí v rámci součinnosti všechny ostatní

prvky, které jsou umístěny na schématu, a to včetně síťových prostupů, VLAN, adresních prostorů potřebných pro jednotlivé architektonické vrstvy. Prvky budou vzájemně kontrolovány na úrovni certifikátů. Bezpečnostní sekce budou nastaveny prostřednictví VLAN. Do DMZ bude vystaven jen Portálová část IS WEBů MV. Všechny prvky budou monitorovány a budou vytvářeny logy, které budou přenášeny na určené místo.

Na schématu jsou prezentovány instance v jednotlivých prostředích. Každý subjekt má vlastní instanci (3 subjekty MV, PČR, HZS).

Dodavatel navrhne doporučené hodnoty (CPU, RAM, diskový prostor), které budou alokovány pro VM (virtualizační vrstvu) pro jednotlivá prostředí. S tím, že jednotlivá prostředí budou výkonnostně nastavena následovně:

- VÝVOJ – výkonnost 50% prostředí PROD (PROD)
- TEST – výkonnost 50% prostředí PROD (PROD)
- STAGE (PROD) – výkonnost 100% prostředí PROD (PROD)
- STAGE (ZAL) – výkonnost 100% prostředí PROD (ZAL)
- Produkční prostředí slouží jako metrika pro definici prostředí

3.6.2.2 Prostředí Resortu MV (Hostingové služby a sítě)

Schéma ve spodní části znázorňuje přístup jednotlivých aktérů k centrálnímu komunikačnímu bodu. Je zde znázorněno propojení na dočasné prostředí Cloudu prostřednictvím IPsec technologie. Na vyšší vrstvě jsou vyznačeny sítě a lokality, přes které je nutné nakonfigurovat, aby bylo možno pracovat s dodávaným systémem.

Jednotlivá prostředí budou umístěna do dvou lokalit. Obě centra budou balancovaná pro případ výpadku primárního centra.

Všechna prostředí budou umístěna v primárním centru Na Vápence (PROD produkční, STAGE předprodukční, Resort Vývoj a Resort TEST.

V záložním centru v Zelenči bude umístěno produkční záložní prostředí (PROD ZAL) a před produkční prostředí (STAGE) bude kopií produkčního prostředí v obou lokalitách (STAGE předprodukční a STAGE předprodukční záložní).

Tato prostředí budou v průběhu projektu provozována dodavatelem na aplikační úrovni.

3.6.3 Dodavatelské aktivity na aplikačních prostředích

Dodavatel zajistí provedení instalace, zprovoznění, provoz a odstranění na všech Cloudových prostředí. Prostředí Cloudu se budou využívat dočasně a budou zde vytvořená prostředí VÝVOJ a TEST.

Na prostředí UPAAS (on-premise) budou vytvořeny další dvě prostředí VÝVOJ a TEST s instancemi Resort a po dokončení, akceptaci a zprovoznění těchto prostředí se na tyto prostředí přimigrují data a aplikační část z prostředí z Cloudu. Po zprovoznění Resort prostředí budou Cloud prostředí odstraněna.

Následně budou vytvořena Produkční a předprodukční prostředí umístěné ve dvou lokalitách.

Produkční a předprodukční prostředí po jejich vytvoření budou akceptována a následně zprovozněna. Prostředí budou provozována na aplikační úrovni (včetně vrstvy Kubernetes) Dodavatelem.

Každé prostředí bude obsahovat 3 oddělené instance. Subjekty MV, PČR a HZS budou moci provádět změny ve svých instancích ve svých systémech nezávisle.

Všechny tyto aktivity budou součástí projektu.

3.6.4 Součinnost Odběratele

Odběratel zajistí infrastrukturní platformu v rámci veřejného cloudu (AZURE prostředí) na dočasnou dobu v souladu s nastaveným projektovým plánem realizačního projektu. Prostředí veřejného cloudu budou sloužit k úvodní instalaci a konfiguraci 3 základních komponent. Budou zde připravena 2 prostředí, a to vývojové a testovací. Následně bude zpřístupněna další infrastrukturní prostředí, které již budou nasazena na UPAAS (on-premise) prostředí. Zde budou vytvořena prostředí produkční a předprodukční (stage). Do prostředí „Resort“ budou přesunuta vytvořená prostředí na Cloudu. Po zprovoznění prostředí „Resort“ budou všechna prostředí na Cloudu uzavřena. Prostředí Resort bude využito pro další rozvoj a vývoj systému pro všechny subjekty. Releasové aktivity se budou provádět separátně pro jednotlivé subjekty, aby plánované výpadky (releasy) neovlivňovaly všechny subjekty naráz v průběhu projektu.

Součinnost Odběratele bude poskytnuta formou zajištění kapacit technické podpory Odběratele na provedení integrace s autentizačními a autorizačními existujícími systémy, dále pak bude poskytnuta součinnost na integraci s notifikačními systémy subjektů (eMail, SMS). Pro notifikační služby bude předán popis API rozhraní. Stejně tak bude poskytnuta součinnost při zasílání logů na určenou IP adresu.

3.6.5 Portál (publikace) – základní požadavky na dodávku

- Webové Portály (weby a micro weby) – prázdné struktury s byznys logikou (služby) a procesy.
- Vytvoření rozhraní pro vstup Občanů na publikační část.
- Vytvoření Webových portálů, které musí být schopny poskytovat službu publikace ve více světových jazycích společně s funkcí zajistit využívání pro zápis registrovaných kódovacích znaků vybraného jazyka.
- Administrátorské rozhraní (Pohled činnostních funkcí - WEBy MV) s GUI pro administraci.
- Vytvoření dynamických a statických stránek s našeptávači.
- Vytvoření samostatného webového rozhraní digitální úřední desky, optimalizovaného pro dotykové panely a provoz ve veřejném prostoru, s automatickou synchronizací obsahu s hlavními webovými portály prostřednictvím redakčního systému.
- Instalace a konfigurace Portálů.
- Vytvoření systému Logů a sestavy možných chybových hlášení pramenících z chyby v kódu. Bude sloužit pro nastavení monitoringu.
- Integrace Portálů (publikační části):
  - Integrace s API aplikační,
  - Integrace s redakčním systémem,
  - Integrace s IDM „Služba správa části AD pro MVČR“.

- Provoz v rámci projektu.
- Testování a akceptace.

3.6.6 Redakční systém a AD

- Dodávka redakčního systému podle požadavků.
- Instalace a konfigurace pro všechny subjekty.
- Zprovoznění všech procesů a vybraných funkcí.
- Redakční systém musí být schopen automatického generování překladu stránek a jejich publikaci ve více světových jazycích společně s funkcí zajištění využívání kódovacích znaků vybraných jazyků a redakční systém musí mít možnost jazykovou revizi generovaných stránek.
- Redakční systém musí umožňovat vytváření a správu úředních desek a centrální úřední desky, která slouží jako rozcestník pro digitální úřední desku.
- Integrační vrsta pro napojení na publikovaný obsah prostřednictvím rozhraní (API).
- Exporty pro IS OpenData.
- Vytvoření systému Logů a sestavy možných chybových hlášení pramenících z chyby v kódu. Bude sloužit pro nastavení monitoringu.
- Integrace Redakčního systému:
  - Integrace s IDM „Služba správa části AD pro MVČR“,
  - Integrace s API aplikační (zdrojová data),
  - Integrace s Portály (publikační část).
- Provoz v rámci projektu.
- Testování a akceptace.

3.6.7 API aplikační

- Dodávka API aplikační podle požadavků.
- Instalace a konfigurace API aplikační pro všechny subjekty.
- Zprovoznění všech procesů a vybraných funkcí.
- API aplikační musí být schopen poskytovat službu převzetí vytvořených informací v registrovaných kódových znakových sadách předaných z WEBů (informace zapsané zadavatelem na dynamických stránkách ve zvoleném světovém jazyku a znakových kódech) a zpět předat sestavené informace ve stejných znakových kódech a jazyku na WEBy.
- Exporty pro IS OpenData.
- Zprovoznění SFTP a potřebných úložných DB tabulek a souborů.
- Vytvoření byznys logiky pro přebírání dat ze zdrojových systémů.
- Vytvoření byznys logiky pro výměnu dat zajišťovaných pomocí scheduleru (konfigurace ad-hoc a plánovaných jobů).
- Vytvoření a zprovoznění Administrátorské rozhraní s GUI pro administraci API aplikační.
- Vytvoření systému Logů a sestavy možných chybových hlášení pramenících z chyby v kódu. Bude sloužit pro nastavení monitoringu.
- Integrace API aplikační:
  - Integrace s Portály (publikační část),
  - Integrace se zdrojovými systémy.
- Provoz v rámci projektu.

- Testování a akceptace.

3.6.8 Provozní požadavky IS WEB MV

Dodaný systém musí být provozovatelný s níže uvedenými parametry.

3.6.8.1 Požadovaná SLA pro IS

Režim provozu je 24x7 - služba je poskytována nepřetržitě 24 hodin denně 7 dní v týdnu, tzn. každý den v roce.

Tabulka 2 - Požadované parametry SLA

Dostupnost / měsíc	Max. doba výpadků v min/měsíc	Doba odezvy na Incident			Doba vyřešení Incidentu		
Kategorie		A	B	C	A	B	C
99,50 %	219,00	30minut	30 minut	30 minut	6 hodin	48 hodin	best effort

SLA pro Výkonnost:

Hodnota požadovaného SLA parametru pro výkonost (čas odezev měřené části aplikace) bude měřena na měsíční a roční bázi. Čas odezev měřené části aplikace musí dosahovat 100-150 ms max. + 20 % měřené odezvy transakce dosažené za zvolenou periodu.

3.6.8.2 Dostupnost

Dostupnost - Poměr mezi dobou, kdy je po Sledované období Služba dostupná k celkové provozní době Služby v rámci Sledovaného období, vyjádřený v %.

Služba je považována za plně dostupnou, pokud není zatížena incidentem kategorie A.

Nedostupná Služba je považována za opět dostupnou v okamžiku, kdy je incident kategorie A vyřešen.

Hodnota požadovaného SLA parametru pro dostupnost bude měřena na měsíční a roční bázi. Dostupnost musí dosahovat hodnoty min. 99,5% na PROD prostředí, OST prostředí se nebudou měřit ani vyhodnocovat.

3.6.8.3 Incident

Incident - Nestandardní provozní událost identifikovaná Odběratelem, Dodavatelem nebo automaticky dohledovým (monitorovacím) systémem, která působí nebo může způsobit výpadek, zhoršení kvality nebo nestandardní chování poskytovaných služeb.

Začátek incidentu - Incident začíná zaznamenáním nahlášeného incidentu (Monitoringem automaticky generovanou zprávou nebo Uživateli) v ticketovacím systému.

Doba odezvy na incident - Doba mezi začátkem incidentu a okamžikem, kdy Dodavatel potvrdí Odběrateli jeho převzetí.

Doba na vyřešení incidentu - Doba mezi začátkem incidentu a okamžikem, kdy je incident vyřešen.

3.6.8.4 Kategorie incidentů

A: Některé nebo všechny části Systému (případně i jen dílčí komponenta některé části) selhaly a jsou zcela nefunkční nebo je jejich funkčnost omezena tak, že je kritickým způsobem ovlivněna činnost Systému.

B: Činnost Systému je podstatně omezena, některé části selhaly a jsou zcela nefunkční nebo je jejich funkčnost omezena tak, že je zásadním způsobem ovlivněna činnost Systému

C: Ostatní stavy nespadající do kategorie incidentů A nebo B.

V případě vyhlášení krizového stavu MV může požadovat vyřešení incidentu kategorie B za podmínek incidentu kategorie A. V případě výpadku dílčího systému či dílčí části dílčího systému, který by ohrozil naplnění povinností uložených zákonem, zejména z hlediska lhůt, může se postupovat stejně jako při vyhlášení kritického stavu.

3.6.8.5 Provozní aplikační monitoring

Součástí řešení je i aplikační monitoring, který zajišťuje dohled všech komponent řešení IS včetně integrací.

Výstup monitoringu je dostupný přes Dashboard a formou notifikací. Dále umožňuje reporting monitorovaných provozních ukazatelů dostupnosti a výkonnosti IS za volitelná časová období.

Monitorovací nástroj obsahuje API, které umožní předávání dat do monitorovacího nástroje dodavatele.

Monitoring je konfigurovatelný a umožňuje upravovat nastavení monitorovaných provozních ukazatelů a přidávání nových nebo rušení stávajících.

3.6.8.6 Provozní Dokumentace a zdrojové kódy

- Popis architektury informačního systému (HLD, LLD, fyzický a logický model, síťová architektura…).
- Podrobný popis informačního systému, obsahuje alespoň:
  - výčet komponent a sdílených prvků technologické a komunikační infrastruktury, které jsou nutné pro provoz informačního systému,
  - popis programových rozhraní,
  - výčet komponent informačního systému, jejich vzájemných vazeb a vazeb na jiné informační systémy,
  - přehled dostupných funkcí a poskytovaných služeb informačního systému,
  - přehled evidovaných údajů a jejich strukturu.
- Dokumentace skutečného provedení.
- Dokumentace k monitoringu.
- Dokumentace a Instalační postupy pro použitý SW (včetně instalačních médií).
- Administrátorská dokumentace.
- Popis profylaktických činností.
- Popis logů a práce s nimi.
- Autorizační koncept.
- Testovací scénáře, detail bude vydefinován v rámci předimplementační analýzy dodavatelem.

- Popis integrací.
- Seznam všech certifikátů + popis instalace a obnovy.
- Všechny účty potřebné pro přístup a kompletní správu SW včetně Servisních a DB účtů.
- Soupis všech customizací SW a konfigurací řešení oproti výchozímu nastavení po instalaci s patřičnou dokumentací pro administrátory.
- Seznam všech DB instancí a DB schémat v nich (v případě, že se nejedná o součást krabicového produktu) s doložením platnosti pořízených licencí pro každou instanci (v případě, že jde o licencovaný DB systém) včetně DB modelu.
- Dokumentace zálohovacích a obnovovacích procedur FailOver a FailBack kroků s popisem analýzy chybových stavů pro vyhodnocení jejich úspěšného naplnění, včetně instalačních postupů pro zálohovací řešení.
- Předaná licenční čísla (klíče) a počet licencí, inventarizační seznam licencí, včetně platnosti maintenance.
- DR plány, detail bude vydefinován v rámci předimplementační analýzy dodavatelem.
- Exit plán, detail bude vydefinován v rámci předimplementační analýzy dodavatelem.
- Uživatelská dokumentace.
- Zdrojové kódy v aktuálním stavu, včetně popisu kompilace a nástrojů a knihoven nutných ke kompilaci a provozu v tomto rozsahu:
    - u každého rozhraní, třídy, metody a globální nebo veřejné proměnné,
    - u části kódu, kde se používají nestandardní postupy nebo kde je vhodné význam kódu vysvětlit,
    - napsány tak, aby z kódu mohla být vytvořena dokumentace pomocí generátoru dokumentace.

  Zadavatel musí mít práva zdrojové kódy zveřejnit ve formě open source.

Tabulka 3 - Požadavek na dokumentaci

Položka	Název	Krátký popis obsahu
Dokumentace	Chybář API aplikací	Vytvoření chybářů z API aplikační.
Dokumentace	Chybář portálu	Vytvoření chybářů z portálu (publikace).
Dokumentace	Provoz	Dodání provozní (administrátorská) a uživatelské dokumentace v souladu s vyhláškou č. 360/2023 Sb., Vyhláška o dlouhodobém řízení informačních systémů veřejné správy.
Dokumentace	Bezpečnost	Dodání bezpečnostní dokumentace v souladu s platnou legislativou pro významné informační systémy.
Dokumentace	Schéma	Dodání detailního designu finálního řešení.

3.6.8.7 Dodavatel navrhne strukturu předávané dokumentace, kterou Odběratel musí potvrdit v rámci předimplementační analýzy.Zálohování

Obsahem dodávky je zálohování, které odpovídá SLA parametrům. Dodavatel vytvoří detailní návrh zálohování celého informačního systému v minimální struktuře (Aktivní prvek, Co zálohovat, Interval, Kolik záloh uchovávat, Kolik dní uchovávat zálohy, Jak často provádět

rozdílové zálohy, Kdy probíhá zálohování, Předpokládaná doba obnovy). Z hlediska potřebných zálohovacích médií bude uplatněno pravidlo 3-2-1, - 0 0 tedy že jsou k dispozici tři kopie dat na dvou různých typech médií, přičemž jedno z nich se bude nacházet mimo lokalitu umístění informačního systému („offsite“).

3.6.8.8 Školení

Obsahem dodávky je školení pro IT provozní administrátory a hlavní uživatele IS Rozsah každého školení bude minimálně 5 pracovních dní.

Detailní rozsah školení bude navržen Dodavatelem v rámci předimplementační analýzy.

3.6.9 Bezpečnostní požadavky

Nové weby MV budou informačním systémem veřejné správy ve smyslu ustanovení zákona č.365/200 Sb., o informačních systémech veřejné správy, a tedy podléhají pravidlům stanovených prováděcí vyhláškou č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy, respektive od 1.7.2024 vyhláškou 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy.

Ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti bude významným informačním systémem. Zde nutno poznamenat, že schválením nového zákona o kybernetické bezpečnosti a jeho prováděcích vyhlášek, dojde k zásadním změnám v právní regulaci, které bude nutné v průběhu realizace projektu zohlednit a vypořádat.

3.6.9.1 Bezpečnostní opatření a zohlednění principu „Security by design“

Požadavky na bezpečnostní opatření jsou navrhovány v rozsahu a detailu odpovídajícímu zadání a z toho plynoucích informací potřebných pro stanovení bezpečnostních opatření. Pro vymezení základních bezpečnostních pravidel, v souladu s postupy OHA a požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti byly použity ustanovení bezpečnostních politik ISMS MVČR a Minimální bezpečnostní standard vydaný NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost.

3.6.9.2 Bezpečnostní opatření

3.6.9.2.1 Organizační opatření

- *Plán zavádění bezpečnostních opatření*

Odběratel má v rámci dokumentace ISMS MV a jeho bezpečnostních politik zpracovaný a schválený seznam bezpečnostních opatření, která musí být zavedena. Požadavky na zajištění kybernetické bezpečnosti jsou definovány v ISMS MV (politiky, šablony). Znalost ISMS MV je pro dodavatele nezbytná pro účely přípravy nabídky, resp. zpracování nabídkové ceny. Na vyžádání bude uchazečům o veřejnou zakázku ISMS MV předán, a to oproti podpisu dohody o mlčenlivosti (NDA – Non-disclosure agreement) o informacích, které dodavatel nebo jeho zástupce z dokumentů získá (dále jen „Dohoda o mlčenlivosti“). Závazný vzor Dohody o mlčenlivosti bude přílohou Smlouva o ochraně důvěrných informací (NDA) v rámci zadávací dokumentace.

- *Klasifikace a ochrana informací*

Odběratel v souladu s Politika řízení aktiv a rizik ISMS MV a její přílohou Metodika identifikace a hodnocení aktiv a rizik, stanovil pravidla a metriky pro hodnocení informačních aktiv z hlediska důvěrnosti, integrity a dostupnosti a případné ztráty dat. Dodavatel musí stanovit osoby odpovědné za dodržení stanovených pravidel při práci s informacemi.

- *Řízení dodavatelů*

Dodavatel při uzavírání nové subdodavatelské smlouvy je povinen zařadit do smlouvy relevantní požadavky na smluvní vztah v souladu s požadavky příl. č.7 vyhlášky č. 82/2014 Sb., o kybernetické bezpečnosti, implementovaných v příloze Požadavky na smluvní vztahy bezpečnostní Politiky pro řízení dodavatelů ISMS MV v rozsahu odpovídajícím předmětu dotčené smlouvy.

- *Řízení lidských zdrojů*

Dodavatel pravidelně teoreticky a prakticky školí své zaměstnance (uživatele, administrátory a osoby zastávající bezpečnostní role) v souladu s Politikou rozvoje bezpečnostního povědomí ISMS MV a pravidelně kontroluje dodržování stanovených bezpečnostních opatření.

- *Řízení změn*

Dodavatel v souladu s Politikou řízení změn ISMS MV eviduje všechny změny a zajišťuje testování a akceptaci změn před uvedením do produkčního provozu. Posuzuje a eviduje významné změny. Provádí analýzu rizik plynoucích ze zranitelností vyvolaných významnou změnou a provádí posouzení účinnosti přijatých opatření. O rizicích a přijatých opatřeních neprodleně informuje Odběratele.

- *Řízení kontinuity činností*

Dodavatel je povinen mít zpracovanou dokumentaci pro řízení kontinuity činností a zvládání KBU a KBI v souladu s Politikou řízení kontinuity činností a Politikou zvládání KBU a KBI ISMS MV. Dodavatel v případě narušení kontinuity činností a v případě detekce KBU a KBI provádí činnosti a zajišťuje předávání informací určenými náhradními kanály všem zainteresovaným rolím a stranám.

- *Audit kybernetické bezpečnosti*

Dodavatel je povinen umožnit Odběrateli provedení auditu dodržování stanovených bezpečnostních opatření, pověřeným pracovníkem Odběratele a, nebo nezávislým auditorem v souladu s dokumentem Politika auditu, kontroly a přezkoumání ISMS. Dodavatel je povinen zajistit audit kybernetické bezpečnosti v rámci své organizace nezávislým externím auditorem. Stejným způsobem postupuje u svých subdodavatelů dotčené zakázky.

- *Další opatření*

Dodavatel provádí v souladu s pravidly stanovenými v bezpečnostních politikách ISMS MV.

3.6.9.2.2 Technická opatření

Vzhledem k plánovanému využití infrastruktury Univerzální prostředí pro provoz aplikací a služeb (dále jen UPAAS) se technická opatření budou řídit bezpečnostními opatřeními stanovenými Bezpečnostní politikou IS UPAAS ISMS MV a vrcholovými politikami ISMS MV.

- *Fyzická bezpečnost*

Bezpečnostní opatření pro fyzickou bezpečnost Odběratel definoval v Politice fyzické bezpečnosti a její příloze Bezpečnost datových center. Provoz webů bude zajišťován částečně on-premis v NDC a částečně prostřednictvím cloudových služeb od komerčního poskytovatele dle nabídky katalogu cloudových služeb. Neveřejné prostory Odběratele, dodavatelů a NDC musí být zabezpečeny před vstupem neoprávněných osob.

- *Řízení přístupů*

Odběratel definuje pravidla a postupy pro omezení a kontrolu přístupu k HW a SW v politice řízení přístupu ISMS MV. Uživatelům nebude umožněn na přidělené ICT prostředky instalovat vlastní SW. Privilegovaní uživatelé budou mít oddělené uživatelské a administrátorské účty. V rámci Bezpečnostní politice IS budou stanovena bezpečnostní opatření pro nastavení oprávnění pro jednotlivé role tak, aby uživatelé mohli přistupovat pouze k údajům souvisejícím s jejich rolí či pracovním zařazením. Bude zavedena ochrana před škodlivým kódem na API Aplikační. Dodavatel je povinen v prostředích, která budou integrována se zdrojovými systémy implementovat nástroje pro ochranu před škodlivým kódem. Bude tak naplněn požadavek na soulad s požadavky VyKB a Politikou ochrany před škodlivým kódem ISMS MV.

- *Řešení kyberbezpečnostních událostí a incidentů v průběhu projektu*

Dodavatel je povinen Odběratele informovat o detekovaných bezpečnostních událostech a incidentech v souladu s požadavky ISMS MVČR.

- *Aplikační bezpečnost*

Pro zajištění realizace opatření bude minimálně vytvořeno oddělené vývojové, testovací a provozní prostředí systému, přičemž musí být zajištěna bezpečnost jednotlivých prostředí a ochrana používaných testovacích dat a produkčních dat.

Testování aplikací bude prováděno v odděleném prostředí v souladu s ustanoveními Politiky akvizice, vývoje a údržby ISMS MV, dále budou stanovena pravidla pro testovací data.

Pro zvýšení bezpečnosti vyvíjených aplikací bude dodavatelem provedena analýza zdrojového kódu a otestování zranitelností. Součástí akceptace bude prohlášení o provedení těchto testů a jejich výsledky. Dodavatel informačního systému poskytne prohlášení o provedení těchto testů, které bude obsahovat minimálně tyto položky: (datum provedení testu, použitá testovací metodika a metodika scoringu, název nástroje použitého pro testování, konfigurace profilu pro testování, výsledky testování, navržení opatření, shrnutí výsledku testování a závěrečná zpráva, osobní odpovědnost – jména odpovědných osob).

V rámci bezpečného vývoje je Dodavatel povinen dodržovat:

- Požadavky definované v OWASP/ASVS úrovně L1, L2.
- Předimplementací OWASP/ASVS je nutné upravit vývoj software tak, aby odpovídaly charakteru díla (tzn. lokalizovat, upravit vůči použitým technologiím atp.,
- Použít modelování hrozeb.
- Je zapotřebí splnit maturitu OWASP/SAMM minimálně maturity score 2 optimálně maturity score 3 a to ve všech oblastech.

- *Kryptografické prostředky dle doporučení NÚKIB*

Data a informace zpracovávaná v rámci informačního nebo komunikačního systému musí být chráněna proti zneužití vhodnými kryptografickými metodami, které zajistí pouze autorizovaný přístup k těmto datům a informacím. Odběratel v souladu s Politikou bezpečného používání kryptografické ochrany ISMS MV použije při šifrování přenosu dat, šifrování uložených dat na základě typu a charakteru dat, v souladu s aktuálním dobručením NUKIB v oblasti kryptografických prostředků v. 3.0, nebo vyšší.

- *Požadavky v oblasti cloudových služeb*

Odběratel musí pro dekomponované části IS, která budou provozovaná v cloudovém prostředí dodržet ustanovení vyhlášky č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu v rozsahu stanoveném v příloze vyhlášky pro bezpečnostní úroveň VYSOKÁ.

Dalšími podmínkami pro využívání cloudových služeb jsou:

- Doložená deklarace místa uložení zákaznických dat v rámci jurisdikce EU.
- Doložená deklarace úrovně bezpečnosti poskytovaných cloudových služeb.
- Certifikátu ČSN ISO/IEC 27001 nebo Auditní zprávu SOC 2 Type II (AT101), případně zajištění auditu na místě.
- Šifrovaná komunikace (TLS/VPN) přes internet s využitím kryptografických algoritmů publikovaných v doporučení NÚKIB v3 nebo pozdější.
- Smlouva s provozovatelem cloudových služeb obsahující vymezení provozních podmínek (SLA) a tzv. exit strategii (exit plán) včetně přádání dat.
- Smluvní podmínky s provozovatelem cloudových služeb, které jsou v souladu s požadavky na zpracovatele dle čl. 28 Obecného nařízení GDPR.
- Smlouva s provozovatelem cloudových služeb obsahující povinnost informovat o bezpečnostních incidentech týkajících se IS Odběratele, a spolupracovat při jejich zvládání.

- *Řízení výjimek běhu, chyb a hlášení*

Dodavatel je povinen zavést proces řízení výjimek, které musí vždy odsouhlasit oprávněný zástupce Odběratele. Dodavatel je povinen vést evidenci všech výjimek. Tyto výjimky musí být zaznamenány v LOGu, které průběžně vyhodnocuje. U zjištěných nedostatků, nebo závad IS, Dodavatel zajistí jejich neprodlené odstranění. Zjištěné nedostatky, závady neprodleně hlásí Odběrateli.

- *Ochrana webových aplikací*

Dodavatel se bude řídit doporučeními OWASP/ASVS a bude věnovat zvýšenou pozornost aktuálním zranitelnostem. Při vývoji aplikace musí dodavatel věnovat pozornost především následujícím známým zranitelnostem:

- Cross Site Scripting (XSS). XSS je metoda narušení webových stránek využitím bezpečnostních chyb ve skriptech (především neošetřené vstupy).
- Injection útoky. SQL injection je technika napadnutí databázové vrstvy programu vsunutím (injection) kódu přes neošetřený vstup a vykonání vlastního, pozměněného, SQL dotazu. Vedle SQL injection existují též další podobné scénáře s jiným cílem, např. shell command injection, LDAP injection atd.
- Vzdálené spuštění kódu. Buď vlivem zranitelnosti v samotném webovém serveru, použitém frameworku či logice ve webové aplikaci.
- Nezabezpečený přímý popis objektu. Zranitelnosti této kategorie umožňují útočníkovi získat informace o jednotlivých objektech cílové aplikace bez patřičné autentizace.
- Cross Site Request Forgery (CSRF). CSRF je technika, která umožňuje útočníkovi podvrhnout formulář na jiné stránce nebo pomocí některých HTTP metod přesměrovat prohlížeč oběti na skript zpracovávající legitimní formulář aplikace s daty, která můžou oběť poškodit.
- Únik informací nebo nedostatečné řízení chyb. Zranitelnosti tohoto typu útočníkovi zpřístupňují v případě chybového stavu aplikace informace, které lze později použít k lepšímu plánování útoku.
- Špatná autentizace a správa relace. Zranitelnosti tohoto typu umožňují útok na přihlašovací části aplikace či úplné obcházení přihlašovacího systému.
- Nezabezpečené kryptografické úložiště. Zranitelnosti tohoto typu můžou způsobit kompromitaci privátního šifrovacího klíče jedné či obou stran spojení.
- Nezabezpečená komunikace. Zranitelnosti tohoto typu umožňují útočníkům odchytávat komunikaci, která jim není určená, a provádět též aktivní útoky typu Man-in-the-Middle.
- Chybné zamezení URL přístupu. V případě, že aplikace umožňuje neautentizovaný přístup i ke stránkám, ke kterým by měl být přístup jen po příslušné autentizaci, je možnou zranitelností situace, kdy takto odkazovaná stránka zobrazí některé informace, které by měly být přístupné jen konkrétním autorizovaným uživatelům, či systémové informace citlivého charakteru.
- Zabezpečení komunikace s externími systémy
- Komunikace webů s interními a externími agendovými systémy probíhá uvnitř zabezpečené sítě CMS2.0. Komunikace s externími informačními nebo komunikačními systémy bude zabezpečena:
  - zabezpečenými kanály přenosu (šifrování dat) s povinnou úrovní zabezpečení koncových bodů informačního systému na úrovni infrastruktury,
  - šifrováním dat pro přenos a autorizací uživatelů v rámci informačního systému,
  - zajištěním šifrování nebo náhradu citlivých dat na úrovni poskytovatelských a konzumentských informačních nebo komunikačních systémů pomocí end to end metody při přenosu dat.

- *Další opatření*

Dodavatel provádí v souladu s pravidly stanovenými Odběratelem v ISMS MV.

3.6.10 Ochrana osobních údajů

Informační systém (dále jen IS) bude splňovat požadavky Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále jen GDPR), zákona č. 365/2000 Sb. o informačních systémech veřejné správy v platném znění a souvisejících právních předpisů. Bude v souladu s doporučeními Národního úřadu pro kybernetickou a informační bezpečnost, platným ISMS MV a stanovisky odboru kybernetické bezpečnosti MV.

IS nebude zpracovávat utajované informace dle zákona č. 412/2005 Sb. o ochraně utajovaných informací v platném znění.

Účel a právní základ pro zpracování bude určovat Odběratel. Zpracování osobních údajů bude probíhat na základě ust. čl. 6 odst. 1 písm. c) a e), tedy zpracování z důvodu plnění zákonné povinnosti a plnění úkolu ve veřejném zájmu a při výkonu veřejné moci a souvisejících činností dle níže uvedených zákonů.

- § 12 zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy v platném znění.
- Zákona č. 273/2008 Sb., o Policii České republiky pro osobní údaje u občanů v platném znění.
- Zákona č. 320/2015 Sb., o Hasičském záchranném sboru v platném znění.
- Zákona č. 133/1985 Sb., o požární ochraně, ve znění pozdějších předpisů.
- Souvisejících právních předpisů v oblasti vnitřní bezpečnosti státu.
- Plnění úkolů služebních povinností dle zákona č. 218/2002 Sb., o službě státních zaměstnanců ve správních úřadech a o odměňování těchto zaměstnanců a ostatních zaměstnanců ve správních úřadech (služební zákon) a zákona č. 361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů, dále v rámci pracovně právní agendy dle zákoníku práce u civilních zaměstnanců PČR, HZS.
- Zákona č. 106/1999 Sb., o svobodném přístupu k informacím v platném znění.

Doba zpracování osobních údajů bude určena Odběratelem.

Zpracovávané údaje: upřesní Odběratel v průběhu úvodní analytické fáze.

- Data uživatelů redakčního systému
- Zveřejněné osobní údaje
  - Zaměstnanců (vedoucí pracovníci, tiskoví mluvčí apod.)
  - Osoby pohřešované
  - Osoby v pátrání
  - apod.
- Logy, IP adresy

3.6.10.1 Cookies

Dodavatel je povinen plnit ustanovení zákona č. 374/2021 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, od jehož účinnosti nově platí, že cookies může provozovatel webu používat pouze se souhlasem návštěvníka (tzv. princip opt-in), až na některé výjimky – nutné technické cookies.

3.7 Realizační tým dodavatele

3.7.1 Předmět plnění – Redakční systém a publikační část

Dodavatel v rámci plnění předmětu veřejné zakázky zajistí níže uvedené role, které budou dodavatelem definovány v předložené nabídce. Požadavky Odběratele na kvalifikaci členů realizačního týmu jsou definovány v Zadávací dokumentaci.

- Projektový manažer senior
- Business analytik senior
- Business analytik
- IT architekt senior
- Databázový specialista
- Vývojář senior
- Vývojář
- Specialista datových sítí
- Copywriter
- UX researcher
- UX designer
- UI designer
- SEO specialista
- Tester senior
- Tester
- Bezpečnostní manažer
- Bezpečnostní architekt

3.7.2 Předmět plnění – API Aplikační

Dodavatel v rámci plnění předmětu veřejné zakázky zajistí níže uvedené role, které budou dodavatelem definovány v předložené nabídce. Požadavky Odběratele na kvalifikaci členů realizačního týmu jsou definovány v Zadávací dokumentaci.

- Projektový manažer senior
- Business analytik senior
- Business analytik
- IT architekt senior
- Databázový specialista
- Vývojář senior
- Vývojář
- Specialista datových sítí senior
- Copywriter
- UX researcher

- UX designer
- UI designer
- SEO specialista
- Tester senior
- Tester
- Bezpečnostní manažer
- Bezpečnostní architekt

3.7.3 Předmět plnění – Provoz a podpora

Dodavatel v rámci plnění předmětu veřejné zakázky zajistí níže uvedené role, které budou dodavatelem definovány v předložené nabídce. Požadavky Odběratele na kvalifikaci členů realizačního týmu jsou definovány v Zadávací dokumentaci.

- IT architekt
- Specialista provozu senior
- Specialista provozu
- SLM manažer
- Operátor dohledového centra - L1
- Specialista dohledového centra (bezpečnostní dohled) – L2
- Bezpečnostní manažer
- Bezpečnostní architekt
- Bezpečnostní administrátor
- Auditor kybernetické bezpečnosti
- Vývojář senior
- Tester senior
- Specialista datových sítí senior

3.7.4 Předmět plnění – Bezpečnostní testování

Dodavatel v rámci plnění předmětu veřejné zakázky zajistí níže uvedené role, které budou dodavatelem definovány v předložené nabídce. Požadavky Odběratele na kvalifikaci členů realizačního týmu jsou definovány v Zadávací dokumentaci.

- Vedoucí bezpečnostní tester
- Bezpečnostní tester

3.8 Fázování dodávky

Dílo bude dodáno ve třech fázích:

- Předimplementační analýza.
- Vývoj a Implementace.
- Odstranění vad plnění.

3.8.1 Předimplementační analýza

Dodavatel zpracuje předimplementační analýzu do 2 měsíců od účinnosti smlouvy.

Před implementační analýza podléhá akceptačnímu řízení Odběratele. Na základě dohody mezi Odběratelem a Dodavatelem může být předimplementační analýza akceptována po částech.

Obsah předimplementační analýzy:

- Mapování přístupů k funkcionalitám (oprávněním).
- Návrh UX a UI.
- Výstupy SOE analýzy a návrhy řešení.
- Návrh testovacích scénářů.
- Návrh DR plánů.
- Návrh Exit plánu.
- Detailní rozsah školení IT provozních administrátorů a hlavních uživatelů.
- Návrh migrace.
- Návrh zpracování osobních údajů.
- Struktura předávané dokumentace.
- Implementační plán, vč harmonogramu prací.
- Případné návrhy Dodavatele na optimalizaci definovaného řešení.

3.8.2 Vývoj a Implementace

Dodavatel vyvine a implementuje plnění max. do 6 měsíců od akceptace předimplementační analýzy, nebo její poslední části.

Předaný předmět plnění podléhá akceptačnímu řízení Odběratele. Doba trvání akceptačního řízení je stanovena na 1 měsíc. Součástí akceptačního řízení je ověření všech požadavků definovaných touto Technickou specifikací.

3.8.3 Odstranění vad plnění

V případě, že Odběratel v rámci akceptačního řízení definuje vady plnění, je Dodavatel povinen tyto vady odstranit do 10 pracovních dní, pokud nebude dohodnuto jinak.

4 Redakční systém a IdM (API na AD a AAD)

Součástí řešení je redakční systém vč. AD a napojení na UPAAS (vrstva Kubernetes)

4.1 Technická specifikace

Architekturní schémata jednotlivých vrstev jsou uvedena níže v textu.

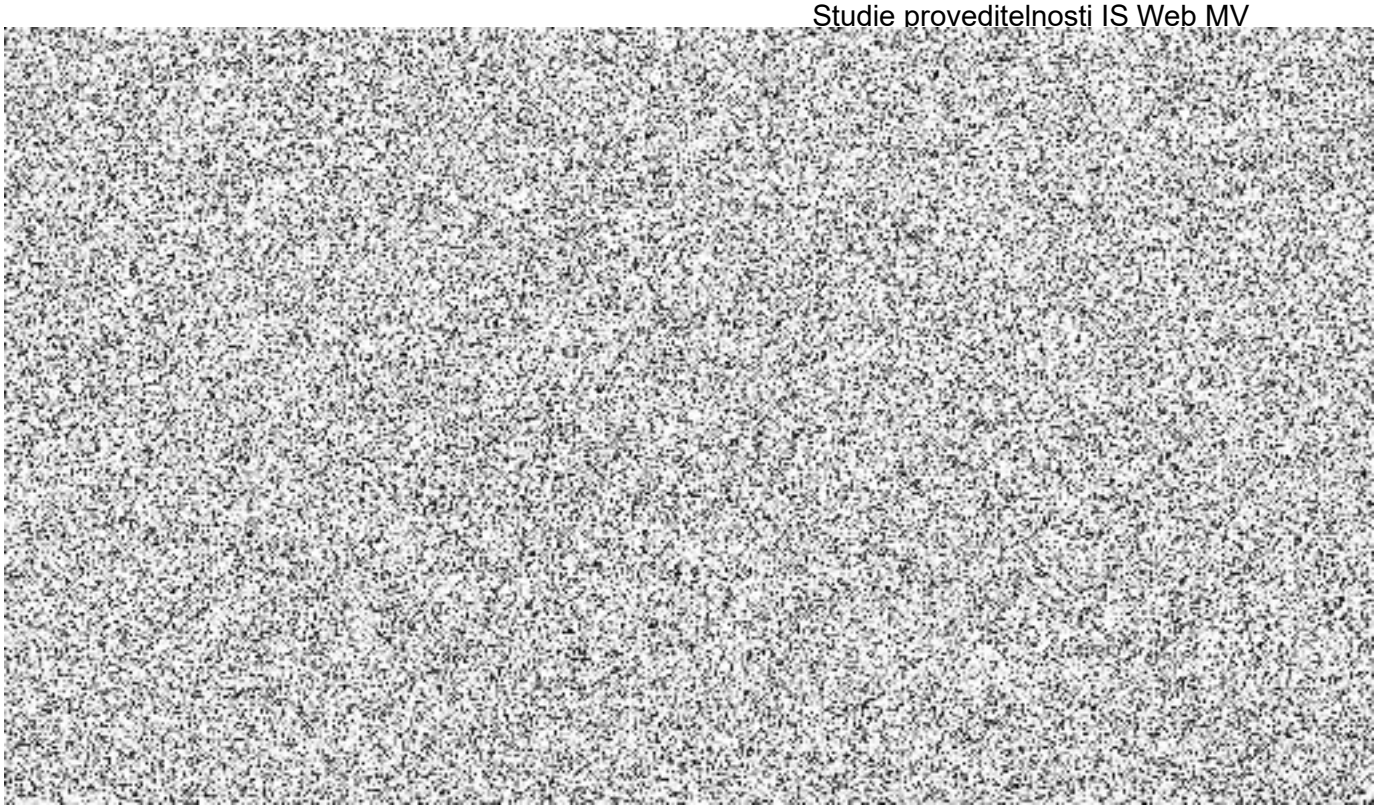


Schéma obsahuje jednotlivé procesy, které jsou nutné pro tvorbu, aktualizaci jednotlivých článků. Redakční systém se využívá po vytvoření stránek pro řízenou publikaci stránek na WEBech nebo MicroWEBech. IdM (AD), slouží pro udržování evidence aktérů (ID), rolí a parametrů ID, které se využívají k 2FA autentizaci a autorizaci pro práci s redakčním systémem. Pokud redakční systém má vlastní evidenci uživatelů pak je třeba zajistit pravidelnou kontrolu na aktuálnost evidence uživatelů v redakčním systému. Zdrojem dat pro autentizaci je vždy IdM (AD).

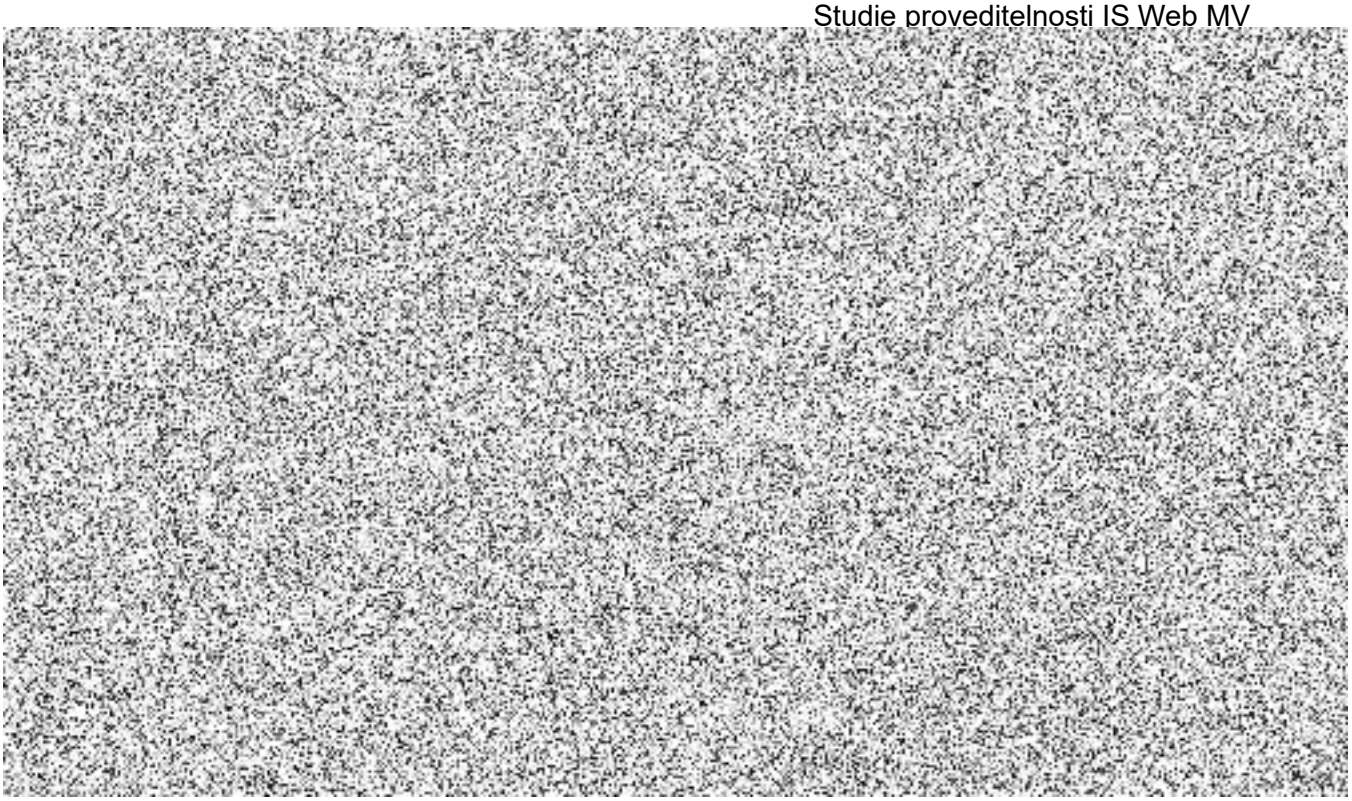


Schéma obsahuje jednotlivé procesy, které jsou nutné pro tvorbu, aktualizaci jednotlivých článků. Redakční systém se využívá po vytvoření stránek pro řízenou publikaci stránek na WEBech nebo MicroWEBech. IdM (AAD), slouží pro udržování evidence aktérů (ID), rolí a parametrů ID, které se využívají k 2FA autentizaci a autorizaci pro práci s redakčním systémem. Pro autentizaci se využívá standart protokol OAUTH 2.0 – vyznačeno modrou šipkou. Pokud redakční systém má vlastní evidenci uživatelů pak je třeba zajistit pravidelnou kontrolu na aktuálnost evidence uživatelů v redakčním systému. Zdrojem dat pro autentizaci je vždy IdM (AD).

Schéma obsahuje jednotlivé procesy, které jsou nutné pro tvorbu, aktualizaci jednotlivých článků. Redakční systém se využívá po vytvoření stránek pro řízenou publikaci stránek na WEBech nebo MicroWEBech. IdM (AD), slouží pro udržování evidence aktérů (ID), rolí a parametrů ID, které se využívají k 2FA autentizaci a autorizaci pro práci s redakčním systémem. Pokud redakční systém má vlastní evidenci uživatelů, pak je třeba zajistit pravidelnou kontrolu na aktuálnost evidence uživatelů v redakčním systému. Zdrojem dat pro autentizaci je vždy IdM (AD).

4.1.4 Role a oprávnění

Tabulka rolí a oprávnění je uvedena v samostatné Příloze Technické specifikace IS WEB MV č. 3 – Role a oprávnění. Tato tabulka představuje návrh mapování přístupů k funkcionalitám (oprávněním) vůči jednotlivým aktérům a rolím, se kterými je v rámci dodávaného systému počítáno. Role a oprávnění jsou primárně vydefinovány v AD (IDM), jehož dodání se předpokládá spolu s redakčním systémem, a budou předávány při autentizaci uživatele. Systém musí umět reagovat na obdržená data a zpřístupnit autentizovanému uživateli příslušné funkcionality. Jedná se o návrh mapování rolí na identifikovaná oprávnění (funkcionality), který může být na základě konzultací mezi Odběratelem a Dodavatelem s ohledem na dodané řešení v rámci předimplementační analýzy a implementace dále zpřesňován.

4.2 Požadavky na poptávané řešení

4.2.1 Technické požadavky

Technické požadavky na redakční systém a AD/IDM jsou uvedeny v samostatné Příloze Technické specifikace IS WEB MV č. 4 – Funkční a nefunkční požadavky na listu „Redakční systém + AD“. Tyto požadavky je nutno vypracovat a jednotlivé odpovědi jsou součástí celkového hodnocení navrhovaného řešení.

Popis stávajícího stavu redakčního systému, aktuální trendy v této oblasti, příklady RS podobných aktuálně používanému či přídavné funkce RS jsou uvedeny v samostatné Příloze Technické specifikace IS WEB MV č. 1 – Základní popis RS.

4.2.2 Funkční požadavky

Naplnění funkčních požadavků se bude hodnotit podle stavu vyplnění příloh Uchazečem k této Technické specifikaci IS WEB MV. Funkční požadavky popisují požadavky na chování systému a funkce nabízené jednotlivým aktérům. Přehled a popis funkčních požadavků pro část Díla **Redakční systém + IdM (API na AD a AAD)** je obsažen v samostatné Příloze Technické specifikace IS WEB MV č. 4 – Funkční a nefunkční požadavky na listu „Redakční systém + AD“. Tyto požadavky je nutno vypracovat a jednotlivé odpovědi jsou součástí celkového hodnocení navrhovaného řešení.

4.2.3 Nefunkční požadavky

Naplnění nefunkčních požadavků se bude hodnotit podle stavu vyplnění příloh Uchazečem k této Technické specifikaci IS WEB MV. Přehled a popis nefunkčních požadavků pro část Díla **Redakční systém a IdM (API na AD a AAD)** je obsažen v samostatné Příloze Technické specifikace IS WEB MV č. 4 – Funkční a nefunkční požadavky na listech:

- Redakční systém a AD – obsahuje funkční a nefunkční požadavky specifické pro tuto část Díla,
- Obecné nefunkční požadavky – obsahuje nefunkční požadavky platné pro celý systém,
- Ostatní – obsahuje další podpůrné požadavky na dodávku,
- Bezpečnost – obsahuje požadavky na soulad s legislativou a ISMS MV.

Tyto požadavky je nutno vypracovat a jednotlivé odpovědi jsou součástí celkového hodnocení navrhovaného řešení.

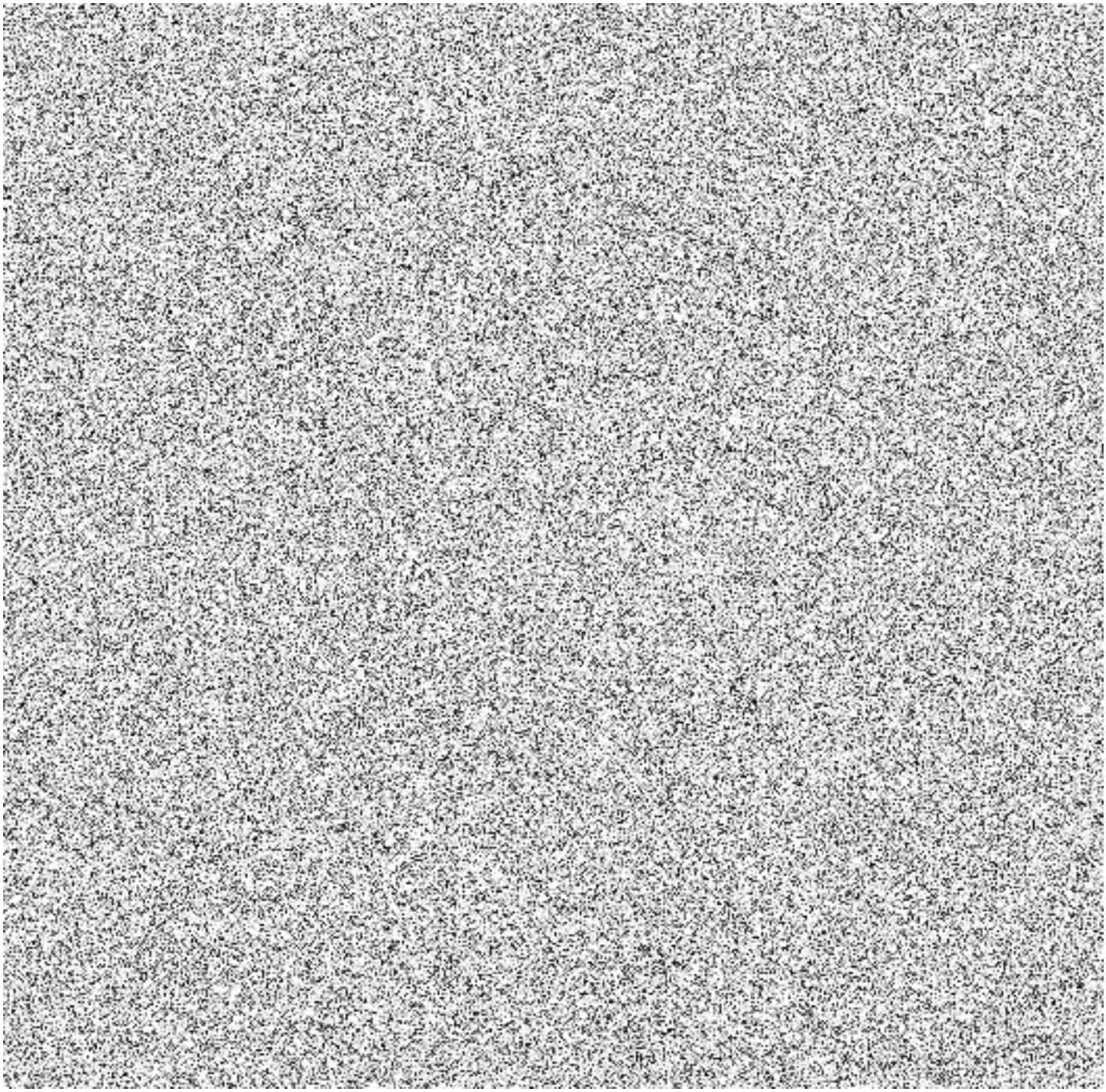
Větší detail vybraných požadavků je obsažen v jednotlivých kapitolách této Technické specifikace.

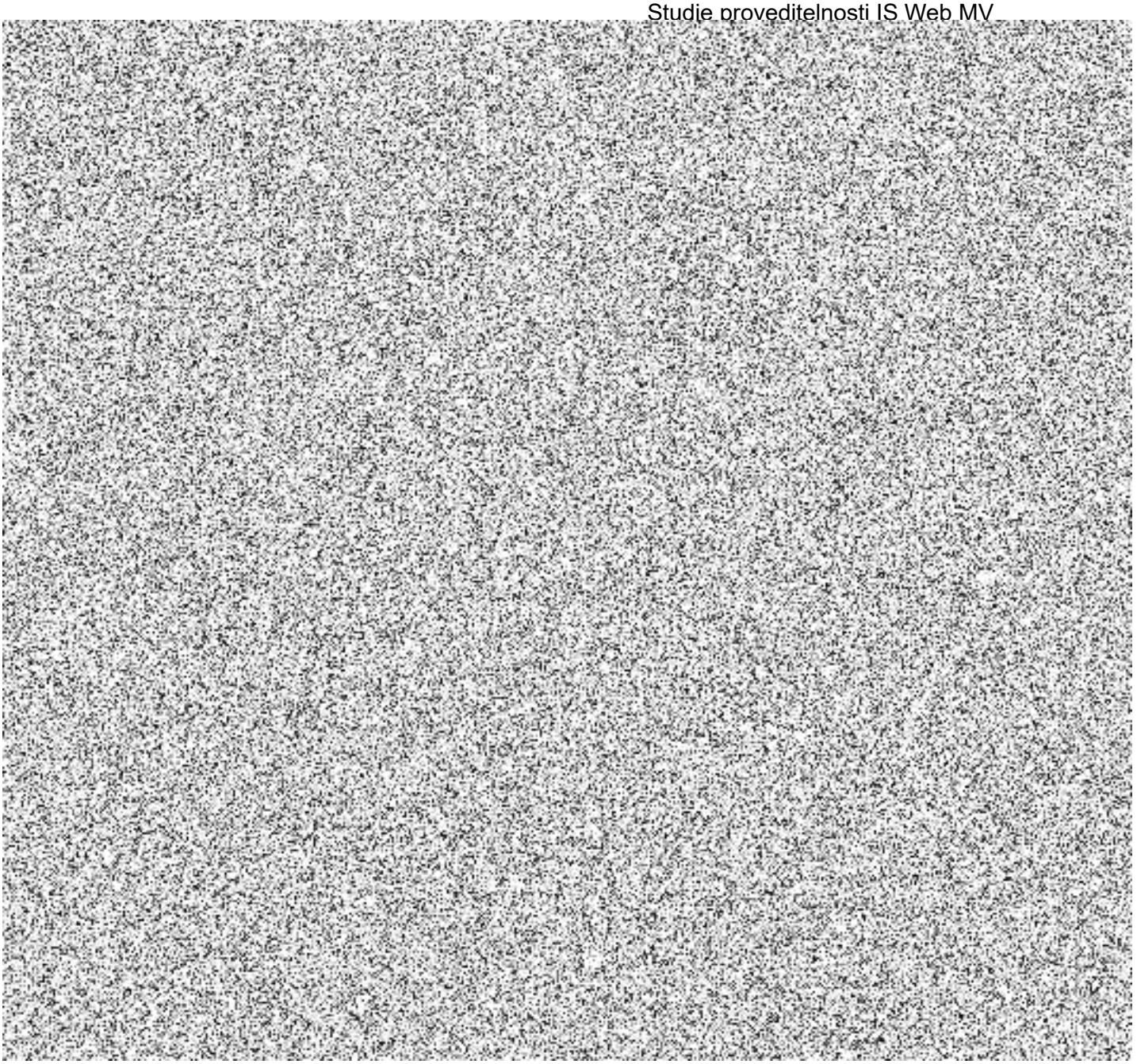
5 API aplikační (API App)

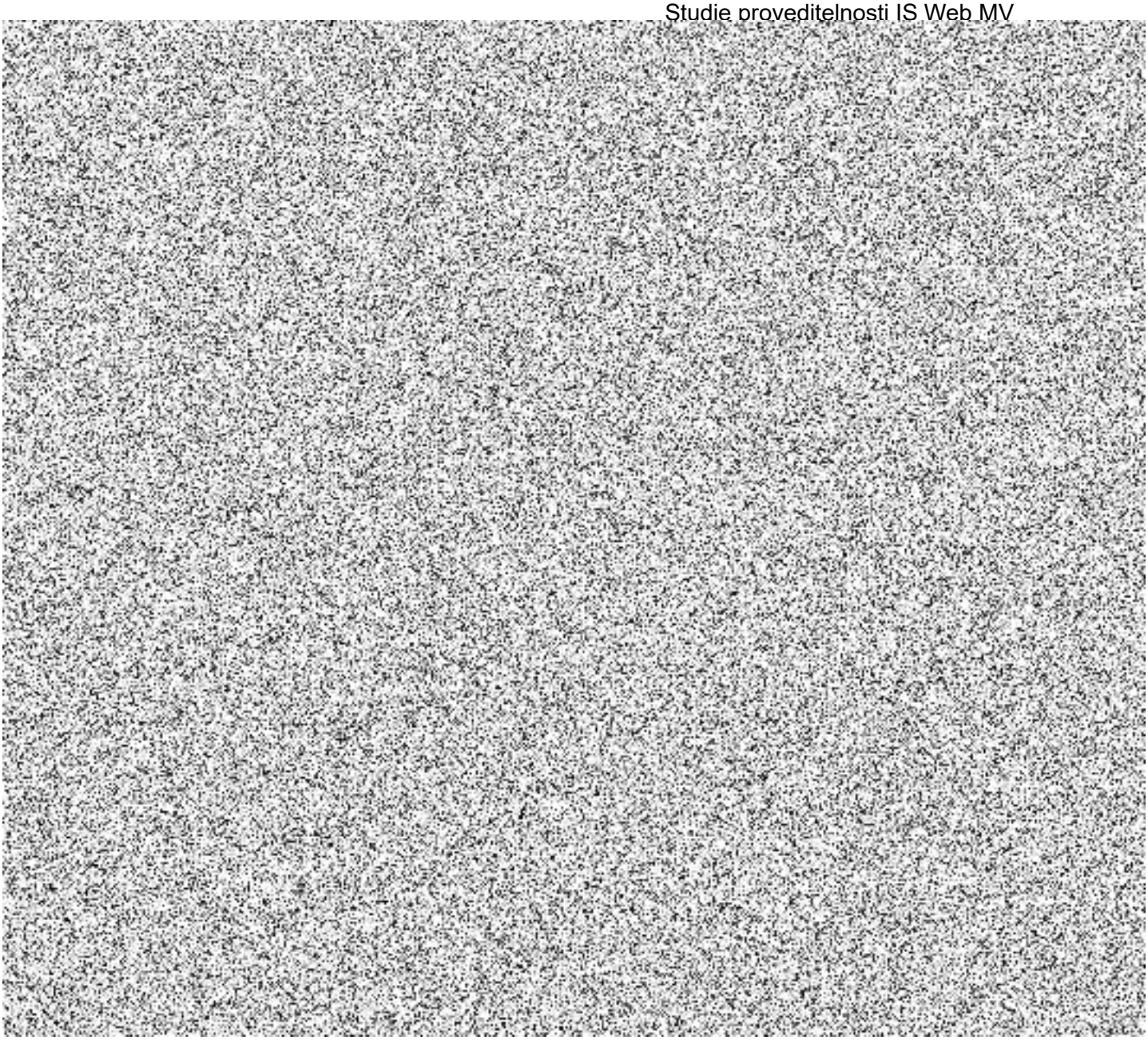
Součástí řešení je API aplikační a UX, vč. napojení na UPAAS (vrstva Kubernetes).

5.1 Technická specifikace

5.1.1 Byznys schéma API App MVČR







5.1.4 Popis schémat API App

Výše uvedená schémata představují základní pohled na jejich hlavní procesy a funkce. Dále pak prezentují vztah mezi zdrojovými systémy dat a dat, se kterými API App pracují. Vztah je nastaven tak, že zdrojové systémy jsou master nositeli dat, které předávají API App. Zodpovídají tak za kvalitu a obsah předaných dat. API App odpovídá za správné zpracování a umístění dat. Prvním úkolem API App je zde nastavit jasnou evidenci a organizaci dat, aby bylo možné kontrolovat a případně obnovit předávaná data ze zdrojových systémů. Platí to jak pro data, která jsou ukládána do DB tabulek, tak pro souborová data. Předání dat se může navrhnout jako předání dat metodou „Pushing“, kdy administrátor zdrojových dat pomocí vlastních nástrojů předá data na uložiště API App. Metoda „Pulling“ je rozdílná ve způsobu využití nástrojů. Při této metodě se Administrátor zdrojových dat přihlásí k nástrojům na straně API App a stáhne data na uložiště API App na určené místo.

Další aktivity se pak provádí v režii nástroje „Scheduleru“, který reaguje na příznaky, které byly provedeny při ukládání aktualizovaných nebo nových zdrojových dat. Předpokládá se, že aktualizovaná data budou přesunuta v rámci uložiště k dalšímu zpracování. Přesunutá data se ukládají do tabulek databáze, které slouží jako data pro zajištění procesů a funkcí poskytovaných API App do publikační části Portálu. Přesunutá souborová data se buď obsahově transformují do tabulek DB nebo jsou připravena jako soubory, které využívá Redakční systém pro prezentaci souborů na statických stránkách. K API App se přihlašují jen autorizovaní aktéři (2FA autentizace se provádí přes IdM (AD)) a je jim umožněno pomocí administrativního GUI administrovat celý systém. Jde hlavně o konfiguraci a vytváření nových příkazů (Jobů), které provádí Scheduler. Scheduler je nástroj, který pomáhá připravit vyžádaná data pro odpovědi na dynamické stránky umístěné v komponentě Portálu. Scheduler může podporovat procesy a funkce s předáváním dat do intranetů jednotlivých subjektů nebo zasílá notifikace na zdrojový systém (Exchange nebo SMS Gateway) s cílem odeslat notifikaci prostřednictvím těchto kanálů. K další části patří předávání open dat na systém OpenDat.

5.2 Požadavky na poptávané řešení

5.2.1 Technické požadavky

Technické požadavky na redakční systém a AD/IDM jsou uvedeny v samostatné Příloze Technické specifikace IS WEB MV č. 4 – Funkční a nefunkční požadavky na listu „API aplikační“. Tyto požadavky je nutno vypracovat a jednotlivé odpovědi jsou součástí celkového hodnocení navrhovaného řešení.

5.2.1.1 Klíčové procesy API aplikační

Mezi API aplikační a Portálem (tzv. dynamickou publikační částí) musí být realizována integrace pro zajištění níže uvedených procesů. Na základě vstupních parametrů, které obdrží API aplikační z Portálu, dochází k vyhledání dat (shody) v API aplikační a předání výsledku zpět na Portál. Z pohledu API aplikační se jedná o následující klíčové procesy, které budou dodávkou zajištěny:

- Vyhledání neplatného dokladu.
- Vyhledání ztraceného služebního průkazu.
- Vyhledání obsazovaného služebního místa.
- Registrace e-mailové adresy pro zasílání notifikací o novém služebním místě.
- Zaslání notifikace o novém služebním místě.
- Vygenerování hesla pro přístup do neveřejné části webu.
- Poskytnutí hesla zasláním do e-mailu či publikací na Intranet.
- Vyhledání politické strany či hnutí.
- Vyhledání veřejné sbírky.
- Vyhledání stanoviska ODK.
- Vyhledání odcizeného mobilního telefonu.
- Vyhledání dopravních informací.
- Vyhledání policejních služeben dle územní příslušnosti.
- Vyhledání osoby v pátrání.
- Registrace e-mailové adresy pro zasílání notifikací o osobě v ohrožení.
- Zaslání notifikace o osobě v ohrožení.
- Vyhledání vozidla či registrační značky v pátrání.

- Vyhledání statistiky dopravních nehod.
- Vyhledání revizního technika spalinových cest.

Dalšími procesy API aplikační (mimo integraci s Portálem) jsou procesy spojené s tzv. schedulerem, který zajišťuje konfiguraci pravidelných či jednorázových importů dat či souborů ze zdrojových aplikací vč. jejich následného zpracování a další potřebné pravidelné akce. Dále musí být dodán frontend pro administrátorskou správu vybraných dat API aplikační, kontrolu jejich příjmu, pro nastavování scheduleru, správu číselníků, správu e-mailových adres, ad-hoc generování a zasílání hesel atd.

5.2.1.2 Scheduler API aplikační

Scheduler spadající pod API aplikační zajišťuje řadu funkcí v rámci zpracování a poskytování dat. Níže jsou uvedeny jeho základní funkce.

Spouštění ad-hoc a plánovaných jobů na základě:

- Vyhodnocení dat v Číselníku ke službám.
- Na základě dotazu na službu obdrženého z Portálu.

Zajištění převzetí dat ze zdrojových systémů:

- Podporuje vybírání dat ze zdrojových systémů.
- Aktualizuje databáze na základě obdržených dat ze zdrojových aplikací.
- Zpracovává obdržená souborová data a provádí jejich transformaci do příslušných databází v API aplikační.
- Řídí přebírání dat od zdrojových systémů pomocí přesouvání přijatých dat ze zdrojových systémů do vlastních struktur ke zpracování.
- Při zpracování obdržených dat ze zdrojových systémů do příslušných databází API aplikační scheduler kontroluje příznak pro spuštění okamžitého jobu pro odeslání příslušné notifikace (např. notifikování v případě osoby v ohrožení).
- Při zpracování obdržených dat ze zdrojových systémů do příslušných databází API aplikační scheduler kontroluje příznak, na základě, kterého spustí plánovaný job pro odeslání příslušné notifikace (např. notifikování o novém obsazovaném služebním místě). Mezi přijatá data patří data, která obsahují informace, které jsou vyžadovány Odběratelem na WEBu. Data z Webů mohou být předána v různých znakových sadách (znacích). Zpracovaná data pro odpověď musí být předána zpět ve stejném formátu znaků aby se zajistila čitelnost obsahu (znaků) zadavatelem v souladu se zvoleným jazykem na WEBu (například zvolený jazyk Angličtina na WEBu zadavatelem => odpověď je v předána v Anglickém jazyce).
- Zdrojové systémy předávají data ve více jazycích a scheduler na základě zvoleného jazyka připraví (vytvoří) odpověď v daném jazyce z přijatých dat ze zdrojových systémů

Zajištění odpovědí pro Portál:

- Na základě dotazu na službu AG-00XX (či na základě vytvořeného příznaku) je spuštěný scheduler, který má nakonfigurované příkazy pro provedení dotazu a pomocí těchto příkazů vytvoří odpověď, která je následně publikována.

Předání dat:

- Pro OpenData,
- Pro Redakční systém,
- Pro Intranet,
- Pro notifikace.

Administrace API aplikační:

- Scheduler zajišťuje za pomoci frontendu administraci vybraných dat API aplikační, kontrolu jejich příjmu, nastavování scheduleru, správu číselníků, správu e-mailových adres, ad-hoc generování a zasílání hesel atd.
- Umožňuje nastavení přenosu (zasílání) logů na IP adresu.

Scheduler API aplikační dále vytváří bezpečnostní a aplikační logy.

Do API aplikační jsou předávána potřebná data ze zdrojových aplikací jednotlivých útvarů. Forma, struktura dat, způsob zpracování dat, intervaly předávání apod. budou vydefinovány na základě konzultace (součinnosti) mezi Dodavatelem a zástupci jednotlivých útvarů na straně Objednatele.

5.2.1.3 UX administrace

Pro správu všech API aplikačních navrhnout administrátorský přístup k číselníkům, správě e-mailů pro zasílání notifikací nebo ke správě scheduleru, případně dalším funkcionalitám. Administrátorské rozhraní zajistí pro příslušného uživatele správu a řízení těchto funkcionalit. Při návrhu obrazovek a samotné realizace této administrace vycházet z principů a zadání pro Portál (např. Design systém, responzivní design).

5.2.2 Funkční požadavky

Naplnění funkčních požadavků se bude hodnotit podle stavu vyplnění příloh Uchazečem k této Technické specifikaci IS WEB MV. Funkční požadavky popisují požadavky na chování systému a funkce nabízené jednotlivým aktérům. Přehled a popis funkčních požadavků pro část Díla **API aplikační** je obsažen v samostatné Příloze Technické specifikace IS WEB MV č. 4 – Funkční a nefunkční požadavky na listu „API aplikační“. Tyto požadavky je nutno vypracovat a jednotlivé odpovědi jsou součástí celkového hodnocení navrhovaného řešení.

5.2.3 Nefunkční požadavky

Naplnění nefunkčních požadavků se bude hodnotit podle stavu vyplnění příloh Uchazečem k této Technické specifikaci IS WEB MV. Přehled a popis nefunkčních požadavků pro část Díla **API aplikační** je obsažen v samostatné Příloze Technické specifikace IS WEB MV č. 4 – Funkční a nefunkční požadavky na listech:

- API aplikační – obsahuje funkční a nefunkční požadavky specifické pro tuto část Díla,
- Obecné nefunkční požadavky – obsahuje nefunkční požadavky platné pro celý systém,
- Ostatní – obsahuje další podpůrné požadavky na dodávku,
- Bezpečnost – obsahuje požadavky na soulad s legislativou.

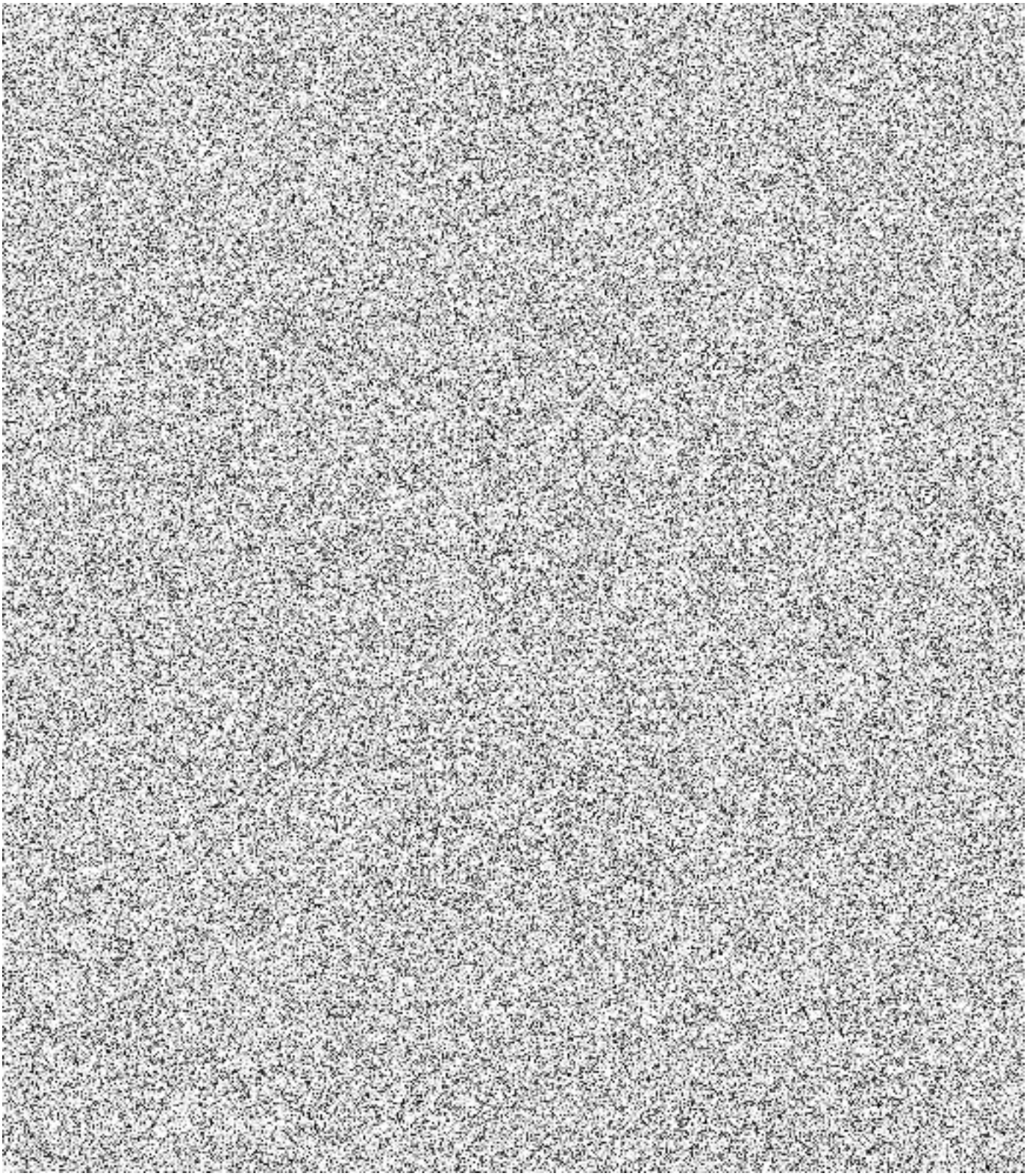
Tyto požadavky je nutno vypracovat a jednotlivé odpovědi jsou součástí celkového hodnocení navrhovaného řešení.

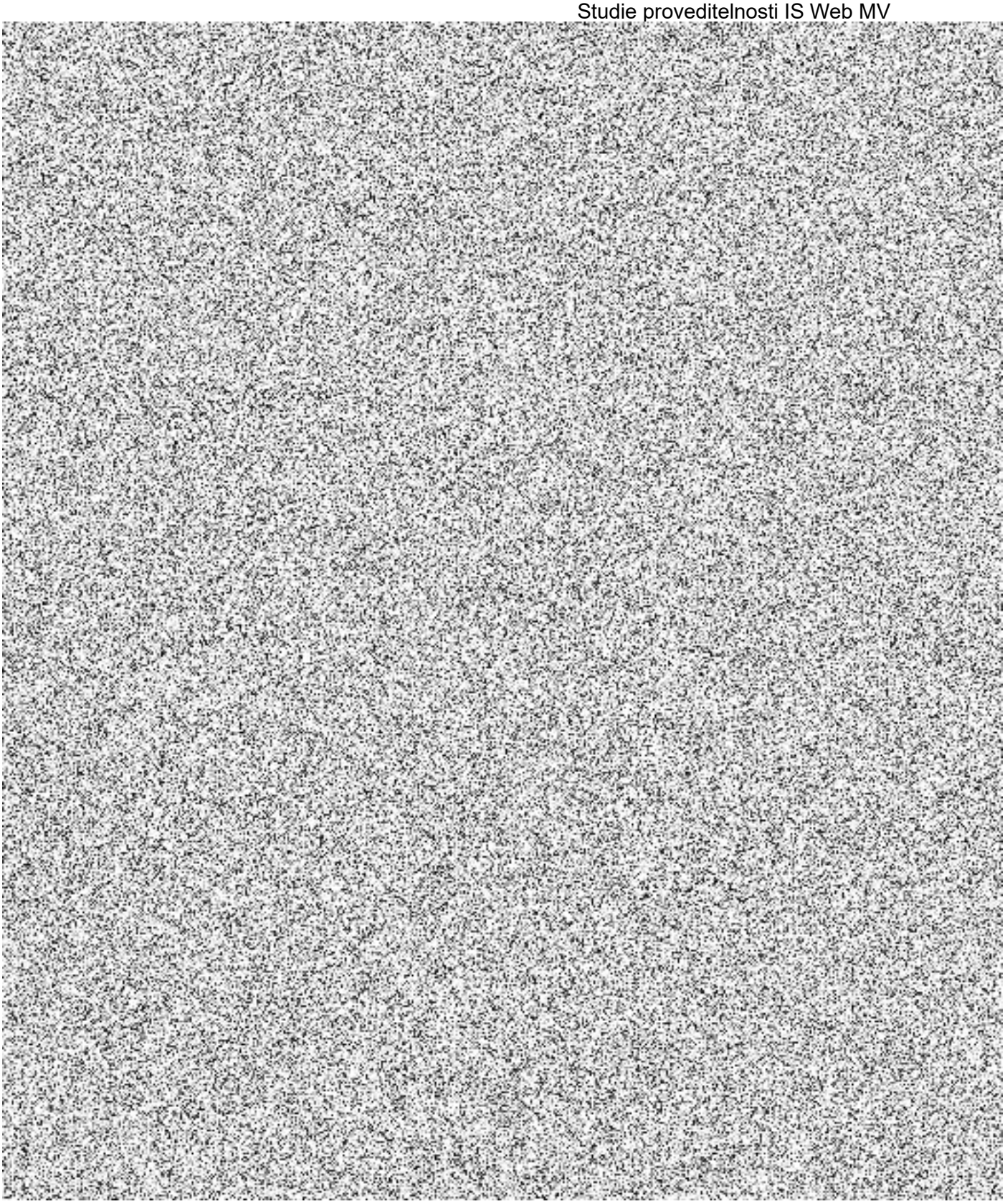
Větší detail vybraných požadavků je obsažen v jednotlivých kapitolách této Technické specifikace.

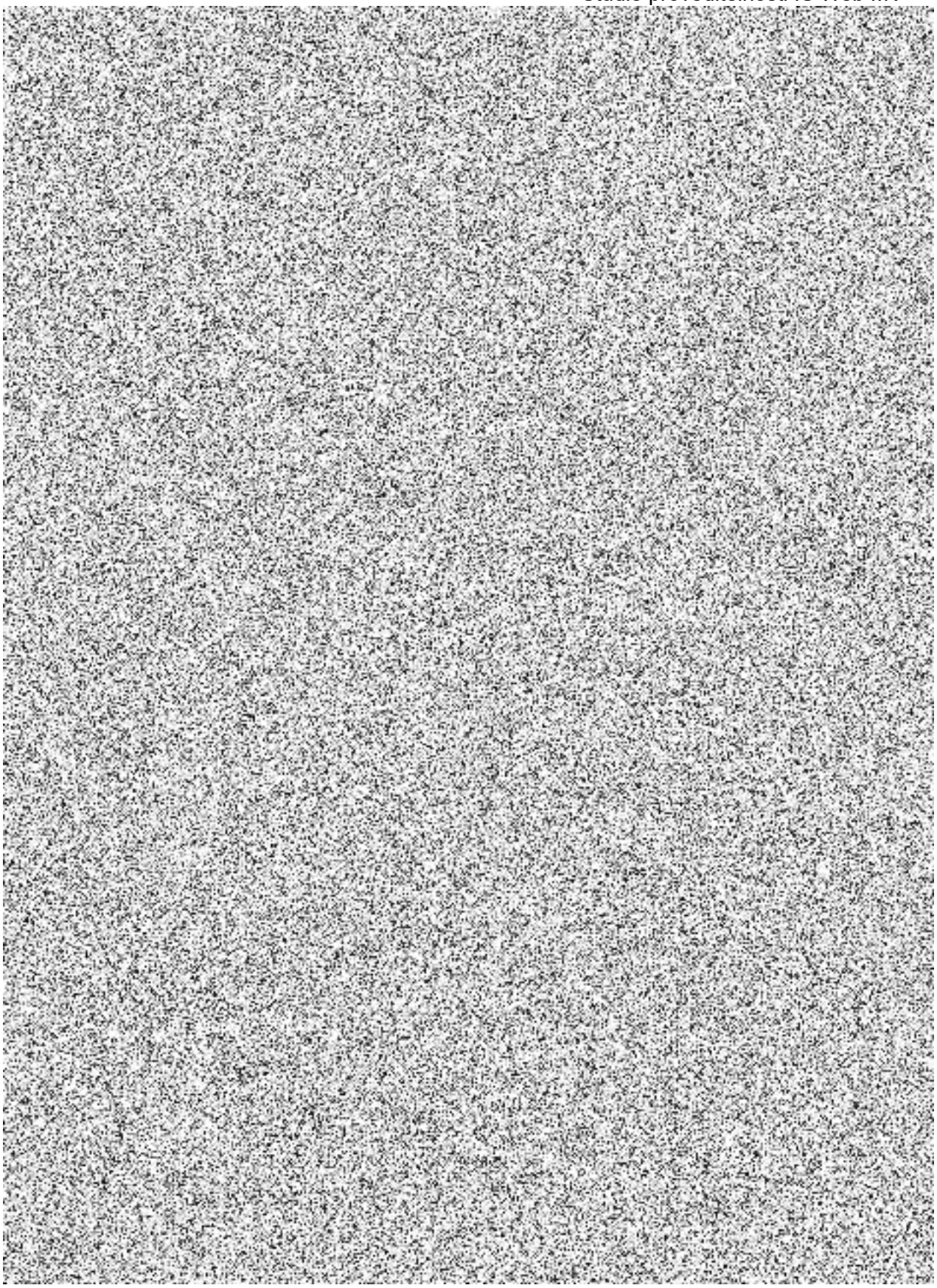
6 Portál publikační část (PUB)

Součástí řešení je publikační část a UX, vč. napojení na UPAAS (vrstva Kubernetes)

6.1 Technická specifikace







Obrázek 13 - Byznys schéma PUB HZS

6.1.4 Popis schémat PUB

Jednotlivé subjekty publikují WEBové stránky nezávisle. Stránky se generují do jednotlivých domén také nezávisle. Z hlediska domén má každý subjekt jednu hlavní doménu, která publikuje statické a dynamické stránky. Dále pak jsou pomocné domény (MicroWEBy), které se využívají pro předávání informací na statických stránkách. Většinou jde o doplňkové informace, které je lepší umístit na MikroWEB než na hlavní statické stránky. Portál na publikační části využívá administrátorského rozhraní pro zajištění služby „Správa WEBu“. Pro administraci funkcí Číselníky a archivace je nutno vytvořit administrátorské GUI. 2FA autorizace pro správu zajišťuje vstup na administraci jen oprávněným aktérům s požadovanou rolí. Archivace dat se provádí do určeného datového zdroje (historická data – stránky, které nejsou nebo byly zrušeny k publikaci). Číselníky nesou informace, které řídí provedení publikace jednotlivých stránek nebo informace, kde jsou uloženy data k „našeptávání“ pro vybrané stránky, které tuto funkci využívají.

6.2 Požadavky na poptávané řešení

6.2.1 Technické požadavky

Technické požadavky na redakční systém a AD/IDM jsou uvedeny v samostatné Příloze Technické specifikace IS WEB MV č. 4 – Funkční a nefunkční požadavky na listu „Portál (publikace)“. Tyto požadavky je nutno vypracovat a jednotlivé odpovědi jsou součástí celkového hodnocení navrhovaného řešení.

6.2.1.1 Klíčové procesy Portálu

Mezi Portálem (tzv. dynamickou publikační částí) a API aplikační musí být realizována integrace pro zajištění níže uvedených procesů. Standardně je na Portálu vydefinován požadavek uživatele (občana), kdy na základě těchto vstupních parametrů dochází k vyhledání dat (shody) v API aplikační a předání výsledku zpět na Portál. Portál následně daný výsledek uživateli zobrazí. Z pohledu Portálu se jedná o následující klíčové procesy, které budou dodávkou zajištěny:

- Vydefinování požadavku na vyhledání neplatného dokladu a zobrazení výsledku.
- Vydefinování požadavku na vyhledání ztraceného služebního průkazu a zobrazení výsledku.
- Vydefinování požadavku na vyhledání obsazovaného služebního místa a zobrazení výsledku.
- Požadavek na registraci e-mailové adresy pro zasílání notifikací o novém služebním místě.
- Vydefinování požadavku na vyhledání politické strany či hnutí a zobrazení výsledku.
- Vydefinování požadavku na vyhledání veřejné sbírky a zobrazení výsledku.
- Vydefinování požadavku na vyhledání stanoviska ODK a zobrazení výsledku.
- Vydefinování požadavku na vyhledání odcizeného mobilního telefonu a zobrazení výsledku.
- Vydefinování požadavku na vyhledání dopravních informací a zobrazení výsledku.
- Vydefinování požadavku na vyhledání policejních služeben dle územní příslušnosti a zobrazení výsledku.

- Vydefinování požadavku na vyhledání osoby v pátrání a zobrazení výsledku.
- Požadavek na registraci e-mailové adresy pro zasílání notifikací o osobě v ohrožení.
- Vydefinování požadavku na vyhledání vozidla či registrační značky v pátrání a zobrazení výsledku.
- Vydefinování požadavku na vyhledání statistiky dopravních nehod a zobrazení výsledku.
- Vydefinování požadavku na vyhledání revizního technika spalinových cest a zobrazení výsledku.
- Zajištění archivace uložených dat do struktury definované pro archivaci a jejich případná rearchivace.

6.2.2 Funkční požadavky

Naplnění funkčních požadavků se bude hodnotit podle stavu vyplnění příloh Uchazečem k této Technické specifikaci IS WEB MV. Funkční požadavky popisují požadavky na chování systému a funkce nabízené jednotlivým aktérům. Přehled a popis funkčních požadavků pro část Díla **Portál (publikační část)** je obsažen v samostatné Příloze Technické specifikace IS WEB MV č. 4 – Funkční a nefunkční požadavky na listu „Portál (publikace)“. Tyto požadavky je nutno vypracovat a jednotlivé odpovědi jsou součástí celkového hodnocení navrhovaného řešení.

6.2.3 Nefunkční požadavky

Naplnění nefunkčních požadavků se bude hodnotit podle stavu vyplnění příloh Uchazečem k této Technické specifikaci IS WEB MV. Přehled a popis nefunkčních požadavků pro část Díla **Portál (publikační část)** je obsažen v samostatné Příloze Technické specifikace IS WEB MV č. 4 – Funkční a nefunkční požadavky na listech:

- Portál (publikace) – obsahuje funkční a nefunkční požadavky specifické pro tuto část Díla.
- Obecné nefunkční požadavky – obsahuje nefunkční požadavky platné pro celý systém.
- Ostatní – obsahuje další podpůrné požadavky na dodávku.
- Bezpečnost – obsahuje požadavky na soulad s legislativou.

Tyto požadavky je nutno vypracovat a jednotlivé odpovědi jsou součástí celkového hodnocení navrhovaného řešení.

Větší detail vybraných požadavků je obsažen v jednotlivých kapitolách této Technické specifikace.

6.3 UX, grafika, SEO, přístupnost, Obsah

Cílem celé části je komplexní dodávka UX, UI/grafiky, SEO analýzy a doporučení, Testování (použitelnosti, přístupnosti) a obsahu. Vše pro web, aplikace a microsites.

U všech podčástí je požadována konzultace s Odběratelem, průběžné reportování výstupů (vše definováno níže). Odběratel v této části může zapojit externí subjekt jako UX konzultanta.

Dodavatel může u jednotlivých částí při zpracování předimplementační analýzy navrhnout změnu oproti níže uvedenému.

Dodavatel provede úvodní UX analýzu, která slouží zejm. ke zmapování současného webu a jeho informační architektury a k definování jeho uživatelů a jejich potřeb. Minimální rozsah činností, které dodavatel provede:

- Rozpracovat strukturu webů a aplikací, vytvořit schéma aktuální informační architektury, namapovat současný stav všech webů, aplikací a microsites.
- Identifikovat všechny typy publikovaného obsahu a používaných komponent webů.
- Identifikovat slabá a silná místa webů.
- Provést analýzu uživatelů, jejich potřeb a definovat uživatelské cesty.
- Sesbírat relevantní a potřebné podklady a informace.
- Rozpracovat celkový harmonogram všech prací včetně návazností, konzultací, workshopů s Odběratelem (včetně jejich formátu a odhadovaného termínu), průběžných výstupů a akceptace Odběratele.

Finální výstupy budou zpracovány v rámci předimplementační analýzy a předány k akceptaci Odběrateli.

6.3.1 SEO analýza a doporučení

Dodavatel dodá kompletní SEO analýzu současných webů včetně doporučení na implementaci konkrétních prvků a kroků v oblasti SEO. Analýza je rozdělena do několika částí podle oblastí. Účelem analýzy je lepší průchodnost webu pro vyhledávače, jeho lepší dohledatelnost a celkově větší přínos pro uživatele.

Výstupy z analýzy:

- Významné pozice konkrétních stránek ve vyhledávačích.
- Analýza klíčových slov a frází relevantních pro webovou prezentaci
- Aktuální umístění stránek ve vyhledávačích a srovnání s konkurencí (konkurencí se rozumí články s podobnou tématikou na jiných webových stránkách).
- Doporučení a návrhy pro zlepšení pozic klíčových stránek ve vyhledávačích a jejich zachování po zpracování návrhu nové webové prezentace
- Zpracování přehledu URL stránek celé současné webové prezentace.
- Doporučení pro strukturu URL i s ohledem na přesměrování staré verze na novou.

On-page faktory:

- Optimalizace meta prvků, včetně title tagů, meta popisů a dalších relevantních tagů.
- Správná struktura nadpisů.
- Optimalizace obrázků (alt atributy a formáty obrázků)
- Interní prolinkování mezi relevantními stránkami a články na webu.

Off-page faktory:

- Analýza odkazového profilu.
- Vyhodnocení kvality, relevance a autority domén odkazujících na web. Zjištění potenciálních odkazových příležitostí (zejména z portfolia webů státní správy).

Technické SEO faktory:

- Doporučení a direktivy pro vyhledávací roboty, včetně souborů sitemap.xml a robots.txt.
- Rychlost načítání stránky na desktopových i mobilních zařízeních.
- Optimalizace webu pro mobilní zařízení.
- Analýza a doporučení týkající se strukturovaných dat, implementace HTTPS a dalších technických aspektů, které mohou ovlivnit viditelnost stránky ve vyhledávačích.
- Indexovatelnost a přístupnost webu pro vyhledávače
- Doporučení ke zvolení vhodné technologie pro server side page rendering

Kromě výše uvedených bodů může vybraný dodavatel podle vlastního odborného posouzení začlenit i další relevantní informace a doporučení týkající se SEO.

Finální výstupy budou zpracovány v rámci předimplementační analýzy a předány k akceptaci Odběrateli.

6.3.2 Nová informační architektura

Po úvodní UX analýze a SEO analýze dodavatel zpracuje novou informační architekturu všech webů a aplikací.

- Při zpracování využít výstupy z předchozích analýz a aplikovat je do návrhu informační architektury a následně i do wireframů.
- Definovat menu všech úrovní, všechny kategorie a jejich další členění a obecně celou strukturu.
- Definovat cíl a rámcový obsah každé stránky, sekce a obecně každé části webu a aplikace.
- Ve spolupráci s Odběratelem definovat, které části a s jakým obsahem budou migrovány do nového webu (např. vizitky, strukturální data, některé články) a které zůstanou v “archivu” (archiv bude řešen jako původní web, který bude přístupný veřejnosti, bude označen příznakem archiv a Odběratel bude v průběhu času přenášet další obsah do nového webu).

Průběh prací a návrhy budou průběžně konzultovány formou workshopů a validovány s Odběratelem. Finální výstupy budou zpracovány v rámci předimplementační analýzy a předány k akceptaci Odběrateli.

.

6.3.3 Wireframy nových webů a aplikací

Po zpracování nové informační architektury a předchozích analýz je potřeba zpracovat a dodat wireframy všech nových webů, microsites a aplikací. Wireframy zahrnují zpracování všech typizovaných částí webu (jednotlivé použité komponenty, organismy i celé stránky). Wireframy zpracovat pro desktop (šířka 1366 px), tablet (šířka 768 px) a mobil (šířka 360 px) a zároveň definovat chování pro větší obrazovky (tj. nad 1366 px) i malé obrazovky (tj. pod 360 px), včetně definice breakpointů a případně dalších pravidel pro responzivní chování.

Zpracovat klikatelný prototyp hlavních částí/průchodů webu (zejm. části pro uživatelské testování). Klikatelný prototyp zpracovat primárně pro desktop a mobil.

Při tvorbě wireframů dodržovat pravidla Design systém Gov (dostupné na https://designsystem.gov.cz/) v jeho aktuální platné verzi. Design systém Gov je dostupný v nástroji Figma (k dispozici ke stažení na výše uvedeném webu Design systému). Pro tvorbu použít layouty/templates z Design systému Gov, pokud jsou v aktuálně platné verzi k dispozici.

Ve wireframech zpracovat všechny typové stránky, komponenty, organismy a obecně všechny prvky webu. Jejich přesný rozsah určí předchozí analýzy a informační architektura, půjde zejm. o následující (nejde o konečný výčet a jednotlivé prvky se mohou změnit):

- Vizualizace všech typů navigace (pro všechny varianty webu, hlavní navigace, doplňkové typy, drobečková navigace a případně sidebar navigace, pokud bude obsahem nového webu aj.).
- Microsites (minimálně 4 odlišné šablony pro microsites mimo web – viz. katalog požadavků), responzivní šablony zahrnující různé komponenty (např. hlavička, patička, formátovatelné obsahové části (články), tabulky, obrázky/galerie, formuláře, kalendář, cookies lišta, registrace newslettery a případně další – uvedené jako další komponenty samotných webů), s možností barevných schémat, vkládání loga, banneru a dalších.
- Domovské stránky (Homepages) pro všechny 3 weby.
- Subhomepages v rámci webů (standardní záhlaví, zápatí, hlavní rozcestník, ale ostatní rozložení a prvky lze do určité míry dělat individuálně a vybírat z dostupných komponent webu (např. aktuality, výpis článků, kategorie, bannery, související odkazy, X feed, apod.). Vytvořit min. 2 šablony subhomepage.
- Mikroweby v rámci webů (mikroweby mají stejný layout jako zbytek webu, ale lze nastavit individuálně: hlavní menu, hero banner (záhlaví), ostatní bannery, celkové rozložení obsahu stránky (lze vybírat z dostupných komponent webu (např. aktuality, výpis článků, kategorie, bannery, související odkazy, formuláře, X feed, apod.).
- Header (hlavička webů, vytvořit varianty defaultní, s černou stuhou (smutek), s trikolorou (oslava)).
- Cookies lišta včetně možnosti volby používaných cookies.
- Patička (cookies, důležité odkazy a informace, sociální sítě, prohlášení přístupnosti a ochrana osobních údajů, příp. další).
- Registrace do newsletteru/odběru novinek (zejm. pro pátrání o osobách a u služebních míst, případně v jiných částech webu).
- Zpracování různých variant článků, včetně variant pro různý typ obsahu (formátovatelný text, videa - vlastní přehrávač i YouTube video, audio - podcasty, obrázky – galerie i samostatně stojící obrázky, tabulky (v různých variantách), soubory ke stažení aj.), konkrétní počet variant bude vycházet z obsahové analýzy aktuálního obsahu a zjištění uživatelských preferencí.
- Komponenta pro stahování souborů, export tabulek do různých formátů.
- Zpracování kategorií pro články (i víceúrovňové).
- Zpracování sekce kariéra (seznam pozic, pokročilé filtrování, detail inzerátu, kontaktní formulář – ucházení se o pozici).
- Zpracování stránek pro vyhledávání (searchbox, výsledky vyhledávání, našeptávání (pokud bude), nejčastěji hledané (pokud bude), ostatní prvky vyhledávání)
- systémové stránky (404, 500, příp. další).

- Formuláře a jejich varianty (inputy, dropdowny, radiobuttony, checkboxy, upload souborů a případně další) včetně doprovodných věcí jako stavy, validace, chytové hlášky, potvrzení odeslání atd.).
- Tabulky (řazení sloupců, pokročilé filtrování, možnost většího počtu sloupců).
- Interaktivní mapa (jen ČR, s kombinací s filtrováním - např. u vyhledávání služeben).
- Kalendář akcí s možností zobrazení/prokliku na detail akce.
- Zpracování komponent pro filtrování (i více parametrů a jejich kombinace a vyloučení, zpracovat všechny stavy filtrů).
- Stránkování.
- Vizitky poboček (v různých variantách), kontakty.
- Časté dotazy.
- Bannery na web (různé pozice v různých částech webu).
- Sociální sítě (Instagram, YouTube, Facebook, X - různé formáty náhledů/feedů. sociálních sítí na různých místech webu).

Při zpracování komponent a wireframů řešit i jednotlivé stavy komponent.

Celou část zpracovat v softwaru na trhu běžně dostupném, mezi jehož základní funkcionality patří:

- Možnost výstupů ve formátu s možností další budoucí editace.
- Export do PDF/PNG.
- Možnost kolaborace Odběratele během tvorby (např. přidávání komentářů) (včetně zajištění případných licencí pro Odběratele a další osoby dle požadavků).
- Možnost použití ve webovém prohlížeči v operačním systému Windows a iOS.
- Možnost realizovat wireframy, grafické práce a klikatelné prototypy (lze použít odlišné nástroje pro každou část, preferovaný je však jeden nástroj).

Při tvorbě wireframů realizovat workshopy s Odběratelem, průběžně konzultovat výstupy, akceptovat jednotlivé části a prezentovat výstupy.

6.3.4 Uživatelské rozhovory / testování použitelnosti

Provést komplexní uživatelské testování použitelnosti návrhu webů (wireframů), resp. jeho vybraných částí (dle jejich důležitosti, která vzejde z předimplementační analýzy) na pro-klikatelném prototypu. Připravit scénář pro testování. Realizovat strukturované rozhovory s respondenty (ty vybrat dle definice cílových uživatelů z úvodní analýzy, výběr respondentů koordinovat s Odběratelem, zajistit celkovou administrativu spojenou s testováním).

Výstupy z testování zpracovat do prezentace (hlavní zjištění, návrhy na změny) a dodat Odběrateli. Výstupy následně zapracovat do wireframů a klikatelného prototypu.

6.3.5 Tvorba obsahu

Samotný obsah dodá primárně Odběratel. Pro konzultace a návrhy na doporučení je třeba zajistit roli copywritera.

6.3.6 Zpracování grafiky / UI

Zpracovat komplexní grafiku/UI nových webů, aplikací a microsites (tj. upgrade wireframů do grafiky) (finální verze pro vývoj). Zpracovat typové stránky, komponenty a prvky webu, ostatní grafické prvky (např ikony, ilustrační obrázky pro články a další). Specifikace pro vývoj a testing (např. popis chování všech komponent, vysvětlení všech stavů, breakpointy, specifikace a konzultace). Zpracování v softwaru na trhu běžně dostupném, v otevřeném formátu s možností budoucí editace, s možností exportu (PDF, PNG, SVG), s možností kolaborace Odběratele, vývoje a testingu během tvorby.

Zajistit, aby celkový výstup (tj. ve fázi před samotným vývojem) splňoval všechny pravidla a podmínky přístupnosti

Zpracovat favicon, og:image. V rámci grafiky dodat ilustrace, ilustrační obrázky, ikony pro web (pokud budou na webu obsaženy). Dodat bannery v různých formátech (pokud budou na webu obsaženy).

Využít grafický manuál a vizuální prvky MVČR, Policie a HZS (pokud bude k dispozici) (podklady dodá Odběratel). Využít Design systém Gov (verzi, která bude v době tvorby aktuální. Pokud budou k dispozici layouty/organismy z Design systém Gov, použít je).

6.3.7 Přístupnost a testování přístupnosti

Dodržení pravidel přístupnosti dle Design systému Gov (viz. https://designsystem.gov.cz/pravidla/pristupnost-webovych-stranek.html.) a aktuální legislativy.

Zejména dodržení požadavků, které jsou popsané v Metodickém pokynu k zákonu č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů (včetně požadavků normy EN 301 549 V2. 1.2). Harmonizovaná norma požaduje splnění povinností na úrovni A-AA definované dle WCAG 2.1.

Realizovat testování přístupnosti celého webu a všech jeho částí. Toto testování provést po dokončení vývoje na testovacím prostředí. Zpracovat výstupy z testování (a dodat je jako PDF dokument Odběrateli), zajistit opravu nalezených chyb a znovu je otestovat.

7 Migrace

Migrace dat a metadat bude provedena po provedení analýzy Dodavatele. Obsahem Analýzy bude navržení oblastí k migraci z původního systému. Požadavek na migraci je uveden v:

- Příloze Technické specifikace IS WEB MV č. 4 – Funkční a nefunkční požadavky na listu Ostatní.
- Požadavek na strategii provedení Migrace je uveden v dokumentu Technická specifikace Migrace (Příloha č. 5 – Technická specifikace požadavků na migraci)

8 Bezpečnostní testování

Provedení bezpečnostních testů pro Redakční systém a Publikační část a API aplikace.

Pro zvýšení bezpečnosti budou v souladu s požadavkem VyKB §13 písm. f) provedeny penetrační a bezpečnostní testy (testy zranitelností) probíhající i na produkčním prostředí, které provede nezávislá organizace, tak aby byl zajištěn atribut nestrannosti. Toto testování, včetně konfiguračního review, bude provedeno předimplementací informačního systému pro ověření správnosti nastavení celého prostředí.

8.1 Požadavky na bezpečnostní testování

Požadovaný rozsah kyberbezpečnostního testování:

- Testovaní zranitelnosti/zranitelností
- Penetrační testování
- Kyberbezpečnostní kontrola zdrojového kódu
- Soulad s legislativními požadavky
- Testování DDoS
- Testování sociálního inženýrství
- Bezpečnostní audit konfigurace
- Ověření kvality logování a monitoringu
- Bezpečnostní audit SDLC v souvislosti s dosavadním a plánovaným procesem vývoje

V rámci každé výše uvedené oblasti bude testování provedeno náhodným výběrem minimálně jednoho většího hlavního webu a jednoho mikro-webu.

Viz také zaslaný návrh rozsahu kyberbezpečnostního testování nových webů MV a jejich Detailního časového rozpočtu.

8.2 Dokumentace

8.2.1 Výstupy

Minimální potřebné výstupy k prováděným bezpečnostním testům

Souhrnná závěrečná zpráva.

Dílčí zprávy pro každé provedené testování:

- Závěrečná zpráva z Testovaní zranitelnosti/zranitelností
- Závěrečná zpráva z Penetračního testování
- Závěrečná zpráva z Kyberbezpečnostní kontroly zdrojového kódu

- Závěrečná zpráva z Testování souladu s legislativními požadavky
- Závěrečná zpráva z Testování DDoS
- Závěrečná zpráva z Testování sociálního inženýrství
- Závěrečná zpráva z Bezpečnostního auditu konfigurace
- Závěrečná zpráva z Ověření kvality logování a monitoringu
- Závěrečná zpráva z Bezpečnostního auditu SDLC v souvislosti s dosavadním a plánovaným procesem vývoje.
- Ke každé dílčí zprávě je nutné vytvořit samostatnou zprávu z provedeného retestování.

Osobní prezentace výstupů, konzultace výstupů pro detailní probrání detailů zprávy a doporučených opatření, případně související školení k identifikovaným nálezům a jejich řešení.

8.2.2 Struktura a obsah zpráv

Souhrnná závěrečná zpráva i dílčí závěrečné zprávy musí mít jednotnou strukturu a musí obsahovat:

- Úvod
  - Manažerské shrnutí. Shrnutí pro strategické směřování, které má sloužit jako high-level shrnutí, o rizicích i možných dopadech. Důležité je být stručný a jasný, srozumitelný i netechnickému čtenáři pro získání přehledu o bezpečnostních problémech uvedených ve zprávě. Tato část je určena primárně vedoucím pracovníkům, kteří nemusí rozumět technickým detailům, které jsou uvedeny dále ve zprávě, ale business rizikům, aby mohli učinit informovaná rozhodnutí.
  - Představení typu testování a jeho významu.
  - Cíl a rozsah konkrétního testování.
  - Testované oblasti.
  - Stručný přehled nálezů seřazených podle závažnosti a podle oblastí podle testovaných systémů.
- Popis testovacích postupů a jejich zdůvodnění.
- Specifikace testovaných scénářů.
- Popis použité metodiky.
- Popis použitých nástrojů a zdůvodnění jejich použití.
- Popis zjištěných omezení testování.
- Detailní popis nálezů:
  - Kategorizace zranitelností podle jejich závažnosti dle CVSS (poslední verze).
  - Zřejmý popis možných technických a business dopadů a pravděpodobnosti.
  - Nezpochybnitelné důkazy o nálezech (screenshoty, logy apod.).
  - Postup krok za krokem, který vede či vedl k nálezu a z nějž je možné nález opětovně simulovat.
  - Ve všech možných případech nálezů budou uvedeny časy, kdy byly nálezy učiněny s přesností alespoň na minutu.
  - Slouží pro technické pracovníky, kteří potřebují učinit rychlé a jasné rozhodnutí o tom, jak nejlépe vyřešit nálezy. V tomto případě je nutné být technicky a kontextuálně přesný.
  - Doporučení – konkrétní kroky k odstranění zjištěných bezpečnostních nedostatků.

- Musí být natolik detailní, aby bylo možné podle něj provést co nejdříve nápravu, přičemž nelze předem předpokládat, že ICT pracovníci vědí, jak nález odstranit. Lze uvést více možností pro nápravu.

- Návrhy na zlepšení bezpečnostních opatření a procesů.
- Kompletní logy a reporty ze všech použitých nástrojů, použité skripty a další relevantní data.

8.2.3 Ostatní požadavky

Souhrnná závěrečná zpráva i dílčí závěrečné zprávy musí být:

- Vysoce kvalitní z pohledu slovního popisu, správné metodiky, použití obrázků.
- Doplněny o další informace, které bude požadovat bezpečnostního testování.
- V českém jazyce, vyjma původně cizojazyčných pojmů, které jsou v České republice oborově ustáleny (například anglicismy).
- Dodány v následujících formátech: DOCX, PDF.
- Předány pouze předem určené osobě ze strany Odběratele.
- Označena podle míry své citlivosti informací dle pravidel pro klasifikaci citlivosti informací e bezpečnostního testování. Zprávy a všechny jejich náležitosti musí být předány jen způsobem, stanoveným pravidly e bezpečnostního testování pro určenou klasifikaci citlivosti předávaných informací.

9 Seznam schémat a tabulek

9.1 Přehled schémat (Obrázků)

9.2 Přehled tabulek

10 Seznam zkratek a vysvětlivky

Zkratka	Popis
AD	Active Directory. Adresářová služba od firmy Microsoft, která je postavená na protokolu LDAP sloužící k autorizaci a autentizaci uživatelů nebo zařízení.
AI	Artificial Intelligence. Umělá inteligence.
AIS	Agendový informační systém.
API	Application Programming Interface. Rozhraní pro programování aplikací.
ASCII	American Standard Code for Information Interchange. Americký standardní kód pro výměnu informací. Jedná se o kódovou tabulku, která definuje znaky anglické abecedy a jiné znaky používané v informatice.
CaaS	Content-as-a-Service. Obsah jako služba.
CSRF	Cross Site Request Forgery. Jedná se o techniku, která umožňuje útočníkovi podvrhnout formulář na jiné stránce nebo pomocí některých HTTP metod přesměrovat prohlížeč oběti na skript zpracovávající legitimní formulář aplikace s daty, která mohou oběť poškodit.
DOCX	Dokument Microsoft Word formátovaný formátem Open XML.
RS (CMS)	Content management system. Systém pro správu obsahu. Jedná se o software zajišťující správu dokumentů, nejčastěji webového obsahu.
CMS 2.0 nebo CMS	Centrální místo služeb verze 2.0. Poskytuje zabezpečený přístup ke všem agendám státní správy, a to i po odpojení od veřejného internetu.
FE	Frontend. Označení části webu viditelné běžným návštěvníkům, kterou přímo ovládá uživatel.
GDPR	General Data Protection Regulation. Obecné nařízení o ochraně osobních údajů.
HTML	Hypertext Markup Language. Značkovací jazyk používající se k vytváření základní obsahové kostry webových stránek.
HZS	Hasičský záchranný sbor.
IČO	Identifikační číslo osoby.
IDM	Identity Management. Správa rolí. Řízení uživatelských identit, oprávnění a rolí.
IMEI	International Mobile Equipment Identity. Jedná se o unikátní číslo přidělené výrobcem mobilnímu telefonu.
Instance	Část prostředí vymezená pro aplikační část (aplikace, DB, uložiště, nástroje) pro jeden Subjekt
IS	Informační systém.
ISMS MV	Information Security Management System.
ISVS	Informační systém veřejné správy.
IT OPS architektura	OPS = operations. Ve smyslu toho požadavku pojem znamená, že přesměrování bude provedeno mimo systém RS, ale na úrovni konfigurace webového serveru či jiné komponenty.
IS UPAAS	IS Univerzální prostředí pro provoz aplikací a služeb.
IS WEB MV	Informační systém webů ministerstva vnitra.
LDAP	Lightweight Directory Access Protocol. Protokol pro ukládání a přístup k datům na adresářovém serveru.
MV	Ministerstvo vnitra.
NAKIT	Národní agentura pro komunikační a informační technologie.

NTH	Nice To Have.
OD	OpenData. Otevřená data. Informace a data bezplatně a volně dostupná na internetu ve strojově čitelném formátu.
ODK	Odbor dozoru a kontroly veřejné správy.
OOÚ	Ochrana osobních údajů.
OWASP/ASVS	Open Web Application Security Project / Application Security Verification Standard.
PČR	Policie České republiky.
PDF	Portable Document Format. Přenosný formát dokumentů. Souborový formát vyvinutý pro ukládání dokumentů nezávisle na softwaru i hardwaru, na kterém byly pořízeny.
PO	Právnická osoba.
RSS	Really Simple Syndication. Formáty určené pro čtení novinek na webových stránkách.
RS	Redakční systém.
RZ	Registrační značka.
SAML	Security Assertion Markup Language. Standard založený na XML poskytující mechanismus pro výměnu autentizačních a autorizačních dat mezi zúčastněnými stranami.
SEO	SEO (zkratka z anglického Search Engine Optimization, česky optimalizace pro vyhledávače) je soubor technik a postupů, které mají za cíl zlepšit pozici webové stránky ve výsledcích vyhledávání, jako je Google. Cílem je, aby se stránka zobrazovala na předních místech pro relevantní dotazy uživatelů.
SLA	Service Level Agreement. Dohoda o úrovni poskytovaných služeb.
SSO	Single Sign-On. Jednotné přihlášení.
UI	User Interface. Uživatelské rozhraní. vizuální podoba produktu nebo systému, se kterou uživatel přímo interaguje, např. Podoba tlačítek, ikon, menu, texty a další prvky, a jak jsou uspořádané.
URL	Uniform Resource Locator. Řetězec znaků sloužící k přesné specifikaci umístění zdrojů informací na Internetu.
UX	User Experience. Česky uživatelská zkušenost: zabývá se tím, jak snadné, příjemné a efektivní je pro člověka používání nějakého online produktu, služby nebo systému.
VIN	Vehicle Identification Number. Unikátní identifikátor vozidla.
VIS	Významný informační systém
VŘ	Veřejná zakázka.
XML	Extensible Markup Language. Značkovací jazyk umožňující snadné vytváření konkrétních značkovacích jazyků (aplikací) pro různé účely a různé typy dat.

11 Přílohy

Příloha č. 1 – Základní popis RS

Příloha č. 2 – Schémata

a) Schéma, které vyznačuje Předmět poptávané dodávky
b) Schémata byznys vrstev
c) Schéma aplikační vrstvy
d) Schémata technologické vrstvy (sítě a servery)

Příloha č. 3 – Role a oprávnění

Příloha č. 4 – Funkční a nefunkční požadavky

Příloha č. 5 – Technická specifikace požadavků na migraci

Příloha č. 6 – Checklisty k aplikacím

Příloha č. 7 - Odpovědnost subjektů pro integraci

Příloha č. 8 – Výchozí popis věcných správců