

Technická specifikace

-

Zajištění provozu a rozvoje integrační platformy Azure ESB

1. Cíl veřejné zakázky

Cílem veřejné zakázky je zajištění služeb podpory provozu a rozvoje integrační platformy Azure ESB, vybudované Objednatelům v cloudové platformě Microsoft Azure.

2. Předmět veřejné zakázky

Předmětem veřejné zakázky je poskytování expertních služeb pro zajištění podpory provozu a rozvoje integrační platformy Azure ESB na dobu 4 let od podpisu smlouvy.

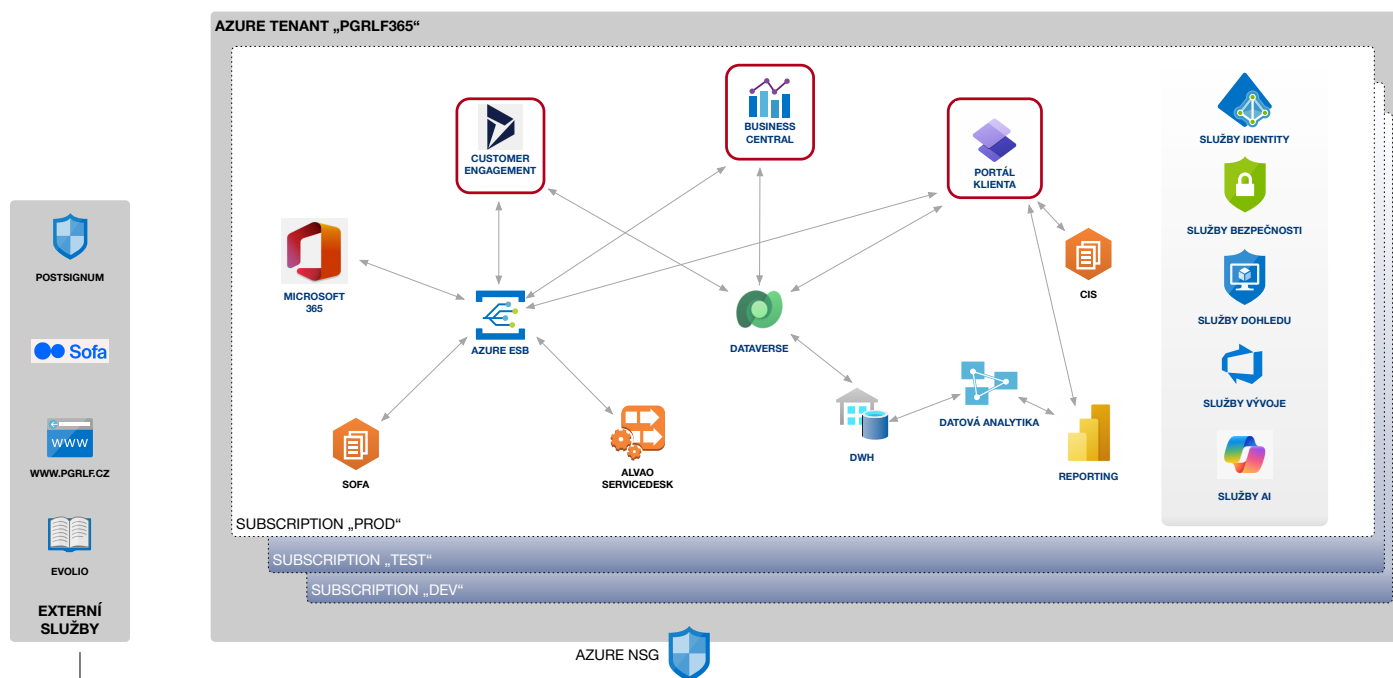
Detailní rozsah poptávaných služeb je vymezen v následujících kapitolách.

3. Technická specifikace plnění

3.1. Současný stav

Objednatel provozuje v prostředí Azure cloudu plně cloudový informační systém. V rámci jednoho tenantu PGRLF jsou v samostatných subskripcích vytvořena prostředí pro vývoj, testování a produkci.

Rámcová architektura systému je znázorněna na následujícím obrázku:



Objednatelům vybudovaná integrační služba Azure ESB je technologicky založena na využití následujících cloudových komponent:

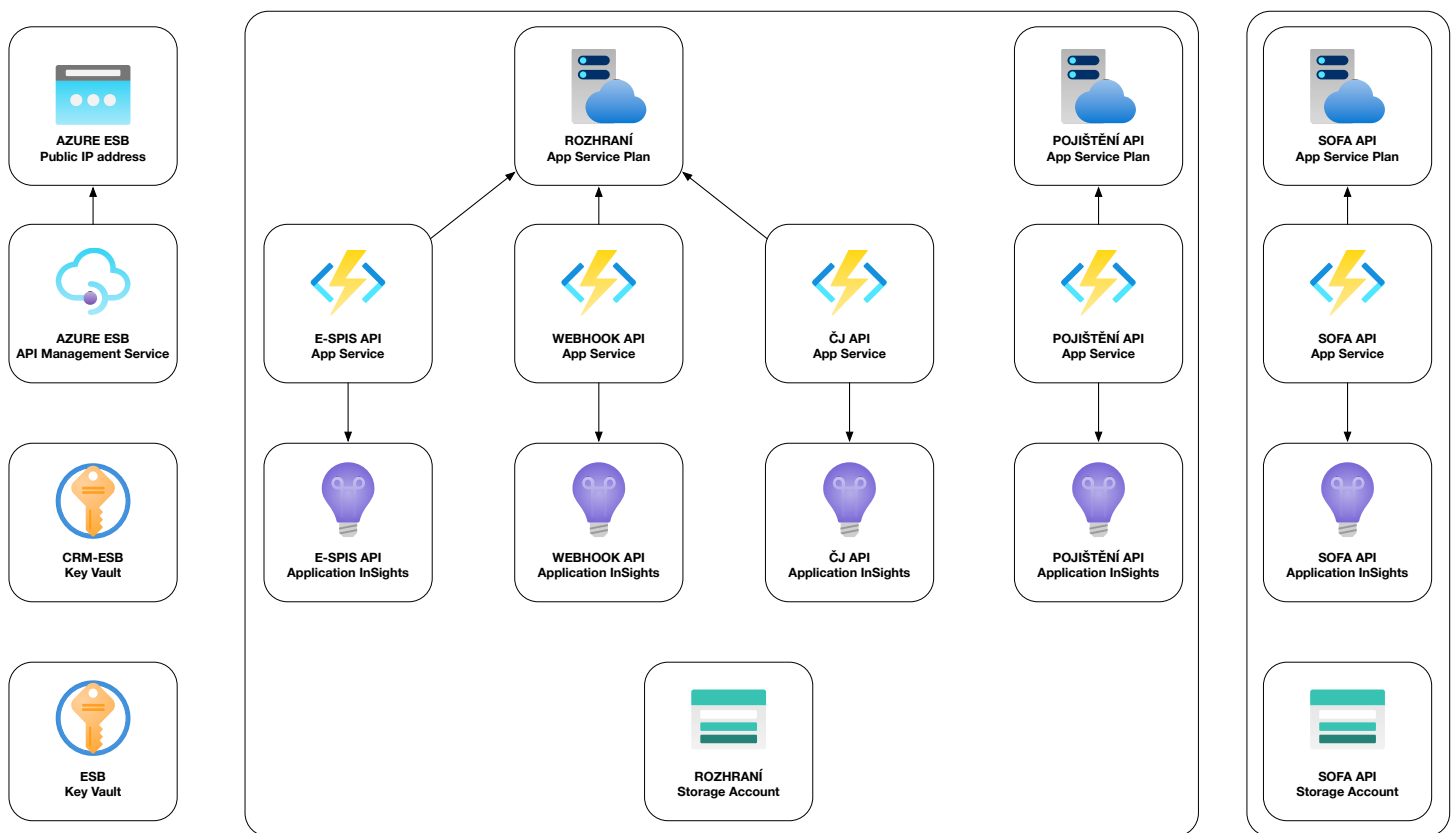
- **Azure API Management**, na kterém jsou vytvářena a publikována jednotlivá API rozhraní
- **Azure Function**, které zajišťují zpracování dat, přijímaných nebo odesílaných přes API rozhraní
- **Azure Storage**, tedy prostor pro ukládání dat v rámci služby Azure ESB.

V souladu s rámcovou architekturou je služba Azure ESB nasazena ve 3 prostředích:

- Vývojové (DEV)
- Testovací (TEST)
- Produkční (PROD).

Každé prostředí je umístěno v samostatné subscripci v tenantu PGRLF, má samostatnou konfiguraci a oddělené deployment pipelines.

Vlastní technické řešení služby Azure ESB vypadá následovně:



Jednotlivé komponenty mají následující určení:

JMÉNO	POPIS	TYP	UMÍSTĚNÍ
AZURE ESB	Služba pro správu API – umožňuje publikovat, zabezpečit, monitorovat a analyzovat API rozhraní. Pro PROD prostředí je využíván PREMIUM tier této služby, TEST a DEV prostředí běží v tieru Developer (no SLA).	API Management service	West Europe
ROZHRANÍ	Plán, který určuje, jaké výpočetní prostředky (CPU, paměť) budou použity pro hostování aplikací v Azure App Service. Umožňuje škálování a volbu cenové úrovně. Pro všechna prostředí je zvolen shodný plán v úrovni B1.	App Service plan	West Europe
POJIŠTĚNÍ API	Plán, který určuje, jaké výpočetní prostředky (CPU, paměť) budou použity pro hostování aplikací v Azure App Service. Umožňuje škálování a volbu cenové úrovně. Pro všechna prostředí je zvolen shodný plán v úrovni B1.	App Service plan	West Europe
SOFA API	Plán, který určuje, jaké výpočetní prostředky (CPU, paměť) budou použity pro hostování	App Service plan	West Europe

	aplikací v Azure App Service. Umožňuje škálování a volbu cenové úrovně. Pro všechna prostředí je zvolen shodný plán v úrovni B1.		
E-SPIS API	Služba pro monitorování výkonu aplikací, sledování telemetrie, chyb a uživatelského chování. Součást Azure Monitor.	Application Insights	West Europe
WEBHOOK API	Služba pro monitorování výkonu aplikací, sledování telemetrie, chyb a uživatelského chování. Součást Azure Monitor.	Application Insights	West Europe
SOFA API	Služba pro monitorování výkonu aplikací, sledování telemetrie, chyb a uživatelského chování. Součást Azure Monitor.	Application Insights	West Europe
ČJ API	Služba pro monitorování výkonu aplikací, sledování telemetrie, chyb a uživatelského chování. Součást Azure Monitor.	Application Insights	West Europe
POJIŠTĚNÍ API	Služba pro monitorování výkonu aplikací, sledování telemetrie, chyb a uživatelského chování. Součást Azure Monitor.	Application Insights	West Europe
E-SPIS API	Hostuje Azure Functions – bezserverové funkce, které se spouštějí na základě událostí. Umožňuje psát kód bez správy infrastruktury. Slouží pro komunikaci a přenos dokumentů s aplikací E-SPIS (původní spisovna používaná ro roku 2025, dnes nahrazena vlastním modulem v prostředí CRM Dynamics 365 CE).	Function App	West Europe
WEBHOOK API	Hostuje Azure Functions – bezserverové funkce, které se spouštějí na základě událostí. Umožňuje psát kód bez správy infrastruktury. Kontrolní utilita pro zajištění kontroly nových dokumentů k přenosu mezi CRM a SOFA.	Function App	West Europe
SOFA API	Hostuje Azure Functions – bezserverové funkce, které se spouštějí na základě událostí. Umožňuje psát kód bez správy infrastruktury. API Endpoint pro přenos dokumentů, konverze DOCX na PDF/A a zařazení do SOFA fronty.	Function App	West Europe
ČJ API	Hostuje Azure Functions – bezserverové funkce, které se spouštějí na základě událostí. Umožňuje psát kód bez správy infrastruktury. API Endpoint k propojení s aplikací Generátor ČJ (unikátní aplikací sloužící pro generování čísel jednacích pro všechny aplikace v rámci systému PGRLF).	Function App	West Europe
POJIŠTĚNÍ API	Hostuje Azure Functions – bezserverové funkce, které se spouštějí na základě událostí. Umožňuje psát kód bez správy infrastruktury. API Endpoint ke zpracování přijetí datových dávek o transakcích klientů od připojených pojišťoven.	Function App	West Europe
ESB	Bezpečné úložiště pro tajné klíče, certifikáty a hesla. Umožňuje řízený přístup a šifrování.	Key vault	West Europe
CRM-ESB	Bezpečné úložiště pro tajné klíče, certifikáty a hesla. Umožňuje řízený přístup a šifrování.	Key vault	West Europe

AZURE ESB	Veřejná IP adresa pro přístup k Azure zdrojům z internetu.	Public IP address	West Europe
ROZHRANÍ	Účet pro ukládání dat v Azure (Blob, File, Queue, Table). Základní stavební prvek pro ukládání souborů a objektů.	Storage account	West Europe
SOFA API	Účet pro ukládání dat v Azure (Blob, File, Queue, Table). Základní stavební prvek pro ukládání souborů a objektů.	Storage account	West Europe

Mimo výše uvedených komponent jsou dále využívány globální komponenty typu Log Analytics Workspace, Smart Detector Alert Rule a další.

Z důvodu bezpečnosti a ochrany dat Objednatele budou detailní technické podklady, zdrojové kódy a další náležitosti, nezbytné pro plnění dodavatele, předány vybranému dodavateli až po podpisu smlouvy.

3.2. Podpora provozu

3.2.1. Provozní parametry a SLA

V souladu s potřebami Objednatele na **dostupnost služeb Azure ESB řešení stanovena v úrovni 99,95% v režimu 7x24**. Tato dostupnost vychází z dostupnosti jednotlivých komponent:

- Azure API Management: 99.99 % dostupnost v Premium tier
- Azure Functions: 99.95 % dostupnost (v rámci App Service Environment)
- Azure Key Vault: 99.99 % dostupnost

SLA parametry jsou definovány úrovní použitého předplatného u Microsoftu – je možné je ověřit v rámci Azure Portal Objednatele, nebo proti oficiálním SLA dle dokumentace Microsoftu.

3.2.2. Parametry provozní podpory

Z hlediska způsobu provozu služby je Azure ESB provozována Objednatelem v Azure tenantu Objednatele (viz výše). Objednatel požaduje zajištění služby podpory provozu od dodavatele následovně:

- Zdroje potřebné pro službu Azure ESB v jednotlivých subskripcích jsou vytvořené a hrazené Objednatelem v rámci jeho Azure kreditů. Objednatel rovněž zajišťuje potřebné licence a certifikáty.
- Příslušní pracovníci dodavatele bude mít zajištěn přístup ke zdrojům v úrovni Contributor, aby mohli provádět administraci a správu služby Azure ESB dle požadavků Objednatele
- Dodavatel bude odpovídat za provoz a správu celé služby Azure ESB dle stanovených požadavků na dostupnost služby Azure ESB.

Objednatel pro zajištění provozní podpory požaduje, aby:

- Dodavatel zajistil službu servicedesku, na který bude Objednatelem určená skupina zaměstnanců (Objednatel požaduje min. 3 zaměstnance) oprávněna zadávat jednotlivé provozní incidenty. Služba musí být dostupná minimálně v čase 06.00 – 20.00 v pracovní dny, negarantovaně v režimu 24x7.
- Pro zadané provozní incidenty se stanovují následující SLA parametry, které jsou pro jejich řešení dodavatelem závazné:

Incident	Popis	Max. odezva (HOD)	Max. doba odstranění (HOD)
Kritický	Vada způsobující úplnou nedostupnost klíčových funkcí nebo bezpečnostní incident	1	4

Střední	Částečné omezení funkcí, které má dopad na některé uživatele	4	24
Nízký	Drobné chyby bez významného dopadu na provoz	NBD (Next Business Day)	5 pracovních dní

- Dodavatel zajistil po celou dobu trvání smlouvy průběžnou službu provozní podpory v následujícím rozsahu:
 - o Zajištění nepřetržité dostupnosti technické podpory na úrovni L3 pro kritické incidenty typu „Server Down“ dle klasifikace Microsoft Severity A. Cílem je minimalizovat výpadky a obnovit provoz ve stanovených SLA parametrech.
 - o Monitoring změn jednotlivých zdrojů (resource) a Azure služeb využívaných v rámci služby Azure ESB a výrobcem (Microsoft) vydávaných update a upgrade, informování Objednatele o jejich dopadech a realizace nezbytných úprav služby Azure ESB a jednotlivých zdrojů a zákaznický vyvinutých komponent pro zajištění provozu ve stanovených SLA parametrech
 - o Bezpečnostní monitoring externích/interních rozhraní a návrh úprav služby Azure ESB pro zajištění vysoké úrovně bezpečnosti. Sledování lhůt platnosti certifikátů využívaných pro ochranu komunikační vrstvy a včasná notifikace Objednatele při jejich vypršení.
 - o Provozní monitoring služby Azure ESB a jejích jednotlivých komponent s důrazem na monitoring dostupnosti a kvality služeb a provádění provozních činností v oblasti správy služby Azure ESB, úprav komunikace (síťové i datové) a řešení bezpečnosti služby.
- Dodavatel si aktivně budoval znalost procesů a datové základny Objednatele, které využívají službu Azure ESB tak, aby byl schopen efektivně provozovat a rozvíjet službu Azure ESB při zajištění požadovaných SLA parametrů.

Služba provozní podpory bude Objednatelem hrazena paušálně, vždy dopředu na období jednoho roku, který se bude počítat ode dne zahájení plnění dle této smlouvy.

3.3. Rozvoj řešení

3.3.1. Požadovaný rozsah služby

Objednatel předpokládá v průběhu plnění rozšiřování a rozvoj služby Azure ESB v souladu se svými potřebami a legislativními požadavky a při zohlednění následujících cílů služeb poskytovaných Dodavatelem:

- Zajištění rozšiřování a úprav API rozhraní,
- Zajištění integrace interních a externích systémů,
- Zajištění standardizace datových typů a formátů,
- Zvýšení bezpečnosti a spolehlivosti provozu,
- Zajištění technického řízení životního cyklu API.

Rozvojové činnosti pro službu Azure ESB budou zahrnovat **návrh, vývoj a implementaci nových integračních rozhraní**, která umožní efektivní propojení systémů a služeb v rámci ekosystému Objednatele. Dodavatel bude v interním prostředí propojovat/integrovat aplikace a data zejména v platformách Microsoft Dataverse, Power Automate, Power Apps, Dynamics 365 a Software602 SOFA, přičemž je požadováno, aby využíval standardizované postupy a nástroje pro zajištění bezpečné, škálovatelné a dlouhodobě udržitelné integrace. U integrace systémů a dat třetích stran se předpokládá primárně integrace pomocí API rozhraní, detailní parametry budou závislé na cílovém externím systému.

Součástí rozvoje je také testování, dokumentace a případná optimalizace stávajících řešení s cílem zajistit jejich bezproblémový provoz a rozšiřitelnost (blíže popsáno v následující kapitole tohoto dokumentu).

Klíčové oblasti rozvoje budou následující:

- Rozšiřování současných **externích API rozhraní** a vytváření nových pro nové subjekty, zejména pak hlavně pojišťovny a jejich specifické datové potřeby a zabezpečení (viz <https://www.pgRLF.cz/o-nas-ke-stazeni-pro-partnery/>).
- Optimalizaci, aktualizaci a rozšiřování integrace interních aplikací a datových zdrojů v IS Objednatele a to zejména:

- o **Integrace se SOFA a Dynamics 365 Sales/Customer Engagement**

SOFA je v prostředí Objednatele nasazena jako centrální platforma pro správu životního cyklu dokumentů – od jejich generování, přes schvalování, podepisování až po dlouhodobé bezpečné ukládání, archivaci, publikaci (např. do registru smluv) a skartaci. Vlastní řízení životního cyklu provádí interně vyvinutý DMS modul v prostředí Microsoft Dynamics 365 Customer Engagement (CRM), který prostřednictvím služby Azure ESB a jednotlivých API rozhraní řídí manipulaci s dokumenty v SOFA. Popsaný způsob je základem pro plně digitalizované a automatizované procesy Objednatele.

Pro každou agendu, která je v CRM řešena a pracuje s dokumentu/soubory, existuje samostatné integrační rozhraní ve službě Azure ESB. Jednotlivá rozhraní jsou obousměrná. Jednotlivé agendy využívají rozhraní pro dávky od jednotek záznamů až po několik tisíc datových záznamů v jediné dávce.

Objednatel, v souladu se svými potřebami, předpokládá postupný vývoj dalších agend, pravidelně dochází k aktualizaci a úpravám stávajících agend a s tím souvisí pravidelný vývoj a rozvoj jednotlivých rozhraní v rámci služby Azure ESB.

- o **Rozhraní pro podání žádostí a čj.**

Objednatel má vyvinutý vlastní portál el. podání žádostí klientů (<https://zadost.pgRLF.cz>) a současně vlastní interní aplikaci pro generování čísel jednacích podle pravidel a požadavků interní evidence dokumentů. Služba Azure ESB obsahuje specifická rozhraní pro přístup interních aplikací Objednatele ke generátoru čj. a rozhraní pro manipulaci s přijatými žádostmi. Veškeré zmíněné služby prochází pravidelným rozvojem a aktualizacemi.

- Vývoj **nového rozhraní** mezi PGRLF a CRIF – Czech Credit Bureau, a.s
Cílem nového rozhraní je umožnit výměnu dat (komplexního spektra informací), umožňujících Objednateli vyhodnotit úvěrové riziko klienta s využitím informací sestavených z datových zdrojů CRIF.

Integrační řešení předpokládá minimálně 15 typů dotazů/datových vět, které se budou sestavovat z datových podkladů v CRM Objednatele a budou zasílány na API rozhraní CRIF. Dotazy budou na API Objednatele zasílány přímo z CRM, API dotaz předá na rozhraní na straně CRIF, kde se sestaví odpověď a tato bude opět skrz API rozhraní předána zpět na PGRLF. Objednatel předpokládá minimálně následující parametry řešení:

- o Rozhraní bude asynchronní, aby bylo možné zajistit bezproblémovou komunikaci mezi systémy v případě zpracování odpovědí na složitější a komplexní dotazy objednatel
- o Rozhraní bude komunikovat na bázi SOAP protokolu (výměna pomocí XML zpráv) s popisem rozhraní ve formátu WSDL a definicí obsahu XML ve formátu XSD
- o Veškerá komunikace bude protokolem TLS v1.3
- o Veškerá komunikace bude výhradně datová, rozhraním se nebudou přenášet soubory.
- o Autentizace a autorizace k rozhraní bude využívat metodu OAuth2 + klientský certifikát, přičemž systém se bude identifikovat příslušným aplikačním klíčem (API key). Certifikát musí být mezinárodně uznávaný a veřejně ověřitelný. Autentizace jménem a heslem nebude přípustná.
- o K rozhraní bude Dodavatelem vyvinuta aplikace/modul v prostředí Power

Platform/Power Automate, která bude zajišťovat:

- Předzpracování přijatých dat a jejich transformace
- Sestavení cílových reportů z dat, dle metodiky poskytnuté Objednatelem
- Uložení klíčových výsledků do CRM Objednatele a celých reportů do Power BI Objednatele
- Udržování databáze kompletní historie dotazů a odpovědí zpracovaných rozhraním, včetně kompletního záznamu datových vět a chybových stavů.
- Možnost ovládání rozhraní na základě pravidel pro dotazy (např. pokud bude stanoveno, že platnost odpovědi na dotaz typu X je Y dní, nebude možné po dobu Y dní poslat dotaz na CRIF a rozhraní jako odpověď vrátí výsledky poslední platné komunikace).

Pro oblast rozvoje

K veškerým výstupům v oblasti rozvoje a vývoje služby Azure ESB, které vzniknou v průběhu plnění, získává Objednatel automaticky plnohodnotnou nevýhradní licenci/uživací práva k užívání a modifikaci dle svých potřeb. Tato licence nesmí být zpoplatněna a její nasazení do produkce obdobně nezakládá právo Dodavatele na navýšení jakýchkoliv poplatků, včetně poplatků za podporu provozu dle kap. 3.2 tohoto dokumentu. Nedílnou součástí licence jsou úplné a kompletní zdrojové kódy daného výstupu.

Úhrada za služby rozvoje bude dána výhradně oboustranně schváleným objemem člověkodní (MD), jejichž nacenění se provede při objednání/zadání požadavku na vývoj Objednatelem.

3.3.2. Požadavky na vývoj a release management

Objednatel požaduje zajištění technického řízení životního cyklu API s využitím nástroje Azure DevOps a dalších. Klíčové požadavky jsou následující:

- Build & release pomocí Azure DevOps YAML pipeline, přičemž pro release bude zajištěna sekvence jednotlivých release po prostředích DEV – TEST – PROD.
- automatizované verzování API,
- nasazení přes APIM ARM/Terraform šablony.

Cílem je převést prostředí služby Azure ESB na řešení „infrastruktury jako kódu“ s využitím nástroje Terraform, včetně automatizace nasazení prostřednictvím DevOps pipeline, což zajistí konzistenci, škálovatelnost a snadnou správu prostředí.

Požadavky na jednotlivé technologie a bezpečnost jsou následující:

- **XML požadavky:**
 - validace proti XSD (součástí vývoje),
 - namespaces povinné,
 - XSD ukládat do repozitáře a verzovat,
 - velikostní limity elementů (typicky do 1 MB, není-li domluveno jinak).
- **WSDL požadavky:**
 - SOAP 1.1/1.2 dle požadavků partnera,
 - oddělené WSDL + XSD (import),
 - verzování: WSDL musí být neměnné → změna = nová verze.
- **Bezpečnostní požadavky:**
 - Autentizace a autorizace
 - OAuth 2.0 / client credentials,
 - Azure AD App Registrations,
 - minimální zabezpečení TLS 1.3.
 - Bezpečnost API (APIM policies)
 - IP filtering,
 - subscription keys / JWT validace,

- rate limit + quota,
- logování všech request/response do App Insights.
- Compliance
 - žádná citlivá data v chybových hláškách (interní zjištění z testů),
 - detailní evidence přístupů.
- Přístup k citlivým datům
 - všechny tajné klíče pouze v Key Vault,
 - žádná konfigurace v repozitáři,
 - auditní záznamy při přístupu k tajným údajům.

V rámci vývoje rozhraní bude Dodavatel zajišťovat i **testování rozhraní**, a to minimálně v rozsahu:

- Unit testy,
- Integrační testy,
- Zátěžové testy (APIM scaling).

Objednatel dále požaduje vytvoření a průběžnou aktualizaci **dokumentační základny služby Azure ESB** ve smyslu zprovoznění dokumentace API pomocí Swaggeru a vytvoření uživatelského portálu API, který umožní snadný přístup k popisům jednotlivých služeb a jejich parametrům. Každý API endpoint musí mít dokumentaci:

- OpenAPI/Swagger specifikaci (JSON + UI),
- XSD/WSDL pro XML služby,
- příklady požadavků a odpovědí,
- seznam chybových kódů,
- diagram sekvence integrace.

Každé rozhraní musí být dokumentováno i pro externí partnery, publikovaná dokumentace rozhraní se vytváří minimálně v rozsahu:

- Metodika rozhraní
- Technická specifikace rozhraní

Primárním jazykem dokumentace rozhraní je český jazyk. Z důvodu komunikace s globálními partnery je dokumentace pro některá rozhraní vytvářena v anglickém jazyce, dodavatel je proto povinen zajistit vytváření dokumentace v obou jazycích, dle zadání objednatele. Ukázka rozsahu dokumentace je k nahlédnutí na webu Objednatele (viz <https://www.pgrlf.cz/o-nas-ke-stazeni-pro-partnery/>).

3.3.3. Požadovaný objem služby

Objednatel v oblasti rozvoje řešení požaduje zajištění kapacit v rozsahu **150 MD ročně, tj. celkem 600 MD za dobu plnění** (4 roky). Pro tyto kapacity platí následující:

- plnění není nárokové a Objednatel bude čerpat kapacity dle svých skutečných potřeb a na základě jednotlivých objednávek,
- každá objednávka bude hrazena na základě samostatné faktury vždy po úspěšné akceptaci předmětu celé objednávky,
- dodavatel je povinen pro tyto kapacity stanovit jedinou sazbu za člověkodenní bez ohledu na roli, která bude plnění vykonávat. Cena za člověkodenní bude platná po celou dobu trvání smlouvy.
- Dodavatel je povinen vykazovat a účtovat čerpání vývojových kapacit s rozlišením na 30 min (půl člověkohodiny).