Příloha č. 2

Rozsah, harmonogram a cena realizace 1. etapy Migrace eSeL

Obsah

1 Vymezení 1. etapy

1.1 Cíle 1. etapy

Cílem 1. etapy je připravit technické prostředky pro vytvoření prototypu, který prokáže funkčnost provozu systému eSeL ve veřejném cloudu. Prokázané dosažení cílů 1. etapy bude migrace definované části aplikačního SW ze stávající kontejnerové platformy do Azure Kubernetes Service (dále jen „AKS") a jeho funkčnost v novém prostředí po migraci.

Plnění 1. etapy nezahrnuje integrace na okolní systémy a podpůrné systémy běžící mimo stávající Openshift. Součástí 1. etapy je také analýza a časově vymezené ověření integrace na Bezpečnostní monitoring Poskytovatele.

1.2 Součinnost pro 1. etapu

K zajištění plnění 1. etapy je nutná vzájemná součinnost a koordinace Objednatele, poskytovatele a jeho poddodavatele, kteří mají za úkol cíl splnit. Neidentifikované aktivity, které se v průběhu realizace vyskytnou budou řešeny spoluprací všech stran. Základní rozsah součinnosti je uveden v části „Požadavky na součinnost Objednatele" této Nabídky.

2 Rozsah analytických činností a příprava Cloudových služeb

Analytické a ověřovací činnosti realizované v 1. etapě jsou poskytované jako Ostatní činnosti dle pododst. 3.3.2.1 Smlouvy, tj. jako Ostatní činností.

2.1 Činnosti SPCSS a poddodavatele

V tomto odstavci uvádíme činnosti Poskytovatele a Poddodavatele v členění dle jednotlivých milníků a dle odpovědnosti.

Legenda k tabulce:

- **G** – garant dohlíží na aktivitu a zodpovídá za dodání;
- **R** – hlavní realizátor zodpovědný za technickou realizaci;
- **S** – součinnost, kterou potřebuje R při technické realizaci;
- **M** – milník, ve které se aktivita bude realizovat;
- Smluvní strany a poddodavatel:
  - Poskytovatel – **S**,
  - Poddodavatel – **A,**
  - Objednatel – **V**.

Činnost	Popis činností	Ověření činností	G	R	S	M
Vytvoření Plánu pro Etapu 1	Vytvoření podrobného plánu pro Etapu 1 včetně základního schématu výsledné architektury	Detail podrobného plánu pro Etapu 1 je k dispozici	S	A	V	M0
Vytvoření tenantů v Azure	Vytvoření nového tenantu v MS Azure pomocí Azure Portal nebo Azure CLI a MS Azure Stack Hub HCI.	Tenant byl úspěšně vytvořen. Tenant je viditelný v Azure Portal.	S	S	A	M1
	Vytvoření potřebných přístupových práv a pověření ve vytvořených tenantech v MS Azure a MS Azure stack hub.	Přístupová práva jsou popsána. Práva jsou aplikována v tenantu. Práva jsou předána ACE.	S	S	A	M1
	Konfigurace základních nastavení tenanta (např. název, doména).	Základní nastavení tenanta odpovídá zvyklostem SPCSS.	S	S	A	M1
	Implementace rolí, přístupů a bezpečnostních opatření (např. MFA, role-based access control).	Role a přístupy včetně bezpečnostních opatření jsou implementována - MFA a RBAC fungují podle očekávání.	S	S	A	M1
	Vytvoření resource group pro potřeby IS ESEL aplikační vybavení	RG byly vytvořeny podle jmenné konvence MS AZURE	A	A	S	M1
	Vytvoření network resource group	Pro potřeby správy sítí. Network resource groups jsou vytvořeny a dostupné.	S	S	A, V	M1
	Základní nastavení FinOps: - struktura reportů o consumption - nastavení alertů, reporting	FinOps reporting je nastaven a je pravidelně odesílán	S	S		M1
	Ověření, že tenant splňuje standardy SPCSS	Auditní zpráva potvrzuje shodu s	S	S	A	M1

Činnost	Popis činností	Ověření činností	G	R	S	M
	prostřednictvím dokumentace / auditní zprávy	bezpečnostními standardy SPCSS.				
Ukládání kódu	Vytvoření Gitlab prostředí pro projekt ESEL	Gitlab projektu IS ESEL je vytvořen	S	S	A	M1
	Nastavení služby Gitlabu a poskytnutí přístupů	Gitlab repozitář je zpřístupněn a funkční	S	S	A	M1
	Definice layoutu repository a design projektů v Gitlabu: - vytvoření Gitlab projektů a subgroup - pravidla přístupu, povolení a zpřístupnění uživatelů do Gitlab (maintener, owner, developer) - branching strategy pro aplikační a infrastrukturní kód - nastavení CI/CD (Gitlab runner)	Design je zdokumentován a odsouhlasen. Následně je struktura vytvořena	A	A		M1
	Vytvoření repository a nahrání zdrojového kodu	Existující kód je nahrán v repositářích	A	A		M1
	Nasazení artifactory - lokální v Gitlabu - package registry a ACR v Azure - nastaveni pro container images a helm charts - nastaveni sync (pipelines)	Artifactory jsou nastaveny. - Manuální testy nahrání testovacího containeru a Helm chartu jsou úspěšné,	A	A		M2
	Nastavení Pipelines v Gitlabu: - migrace z Jenkins - úpravy pro Gitlab	- Pipelines jsou správně nakonfigurovány. - Funkčnost nástrojů je ověřena.	A	A		M2
	Test build Pipeline pro automatizaci sestavení.	Pipeline byla úspěšně vytvořena. - Všechny kroky Pipeline fungují správně.	A	A		M2
	Dokumentace procesu buildu a nasazení a školení týmu na nové postupy.	- Dokumentace procesů je k dispozici. - Tým byl vyškolen a	A	A		M2

Činnost	Popis činností	Ověření činností	G	R	S	M
		rozumí novým postupům.				
Migrace z OpenShift do AKS	Analýza stávajícího řešení na OpenShift (architektura, závislosti)	Analýza je dokumentována. - Klíčové komponenty jsou identifikovány.	A	A		M2
	Desing služeb AKS a doplňkových služeb podle analýzy		A	A		M2
	Příprava prostředí AKS: - vytvoření clusteru, - konfigurace node pools - konfigurace CNI - nastavení síťování a prostupů - konfigurace scalingu (HPC, scaling rules)	Cluster AKS je úspěšně vytvořen. - CNI je správně nakonfigurováno.	A	A		M2
	Konfigurace storage	Storage account je nakonfigurován	A	A		M2
	Konfigurace služeb a nástrojů potřebných pro AKS: - sítě Ingress, Load Balancer - network policies - RBAC v AKS - storage - ephemeral a permanent (Azure Disk, Azure Files)	Všechny služby a nástroje jsou správně nakonfigurovány. - Funkčnost služeb je ověřena.	A	A		M2
	Testy AKS: - vytvoření testovacích podů ověření dostupnosti - test intra cluster komunikace - testování PVC (storage)	Úspěšné vytvoření všech testů.	A	A		M2
Migrovatelnost kontejnerů	Identifikace služeb, kontejnerů a nodů, které budou migrovány pro experimentální prostředí	Seznam kontejnerů a nodů je vytvořen. - Identifikované kontejnery jsou připraveny k migraci.	A	A		M2

Činnost	Popis činností	Ověření činností	G	R	S	M
	Získání informací o všech službách a kontejnerech podle checklistu	Vyplněný checklist ke všem službám, které budou nasazeny v rámci kontejnerů	A	A		M2
	Vyhodnocení potřebných úprav pro rebuild kontejnerů (např. aktualizace Dockerfile). - volby base images - úpravy dockerfile - seznamy dependencies - health checks, monitoring, logování	Potřebné úpravy jsou zdokumentovány - změny podle nového standardu	A	A		M2
	Vytvoření nových build container images pro vybrané služby v experimentálním prostředí - deploy do registries - vulnerabilites scans (trivy, snyk apod.)	Nové container image jsou k dispozici v registries. - images mají vulnerability scan	A	A		M2
	Manuální deploy služeb do AKS	Služby jsou nasazeny v AKS	A	A		M2
	Testování funkčnosti migrovaných kontejnerů a nodů.	Migrované služby, kontejnery a nody fungují správně. - provedeny ad-hoc / regresních testů	A	A	S, V	M2
	Dokumentace provedených úprav a testovacích výsledků.	Kompletní dokumentace s výsledky testů a provedenými úpravami je k dispozici.	A	A		M2
Propojení a cloudových on-premise	Design propojení Azure a Azure stack	Dokumentace designu, klíčové komponenty jsou identifikovány a jejich konfigurace je známa.	V	A	S	M1

Činnost	Popis činností	Ověření činností	G	R	S	M
	Implementace potřebných síťových komponent (např. brány, routování).	Všechny síťové komponenty byly úspěšně implementovány. - Funkčnost komponent je ověřena.	S	A,S	V	M1
	Testování latence a prostupnosti mezi cloudovým a on-premise prostředím.	Latence a prostupnost jsou měřeny. - výsledky testů jsou dokumentovány.	A	A	S	M2
	Dokumentace výsledků testů a případných doporučení pro optimalizaci.	zpráva o testování je k dispozici. - Doporučení pro zlepšení výkonu jsou formulována.	A	A		M2
Testování komponent v on-premise prostředí	Identifikace komponent, které budou testovány – databáze.	Seznam komponent je vytvořen a jejich konfigurace je zdokumentována	A	A		M2
	Nasazení komponent pro testování – databáze, migrace testovacích dat	Databáze je nasazena je přístupná, napojená na monitoring	A	A		M2
	Příprava testovacího prostředí a scénářů pro testování.	Testovací prostředí je správně připraveno – prostupy, monitoring - Testovací data jsou namigrovány - Scénáře pro testování jsou definovány.	A	A	S	M2
	Provádění testů a sledování výkonu komponent.	Testy byly úspěšně provedeny. - Výkon komponent je sledován a analyzován.	A	A		M2

Činnost	Popis činností	Ověření činností	G	R	S	M
	Analýza výsledků testů a identifikace případných problémů.	- Analýza výsledků je k dispozici. - Identifikované problémy jsou zdokumentovány.	A	A		M2
	Komunikace výsledků testů, doporučení pro zlepšení. Rozhodnutí o dalších krocích.	- Zpráva o testování je k dispozici. - Doporučení pro zlepšení výkonu jsou formulována.	A	A		M2
Integrace na Bezpečnostní monitoringu	Napojení MS Azure na Bezpečnostní monitoring SPCSS	Úspěšné napojení na Bezpečnostní monitoring SPCSS	S	A	V	M3
	Napojení Bezpečnostního monitoringu na DCeGOV	Úspěšné zpracování bezpečnostních logů na DCeGOV v rozsahu dle závěru analýzy (M1)	S	S	V	M3
Ostatní	Detailní návrh plánu realizace navazujících etap včetně požadavků na součinnosti	Detailní návrh plánu je k dispozici	V	A	S	M3
	Detailní návrh integrace komponent třetích stran (eLDAX, Unify, TSA IZOL) včetně požadavků na součinnosti	Detailní návrh integrace je k dispozici	S	A	V	M3
Výstavba BM	Analýza a následná výstavba BM v rozsahu Analýzy/PoC pro 1.etapu	Úspěšné předání Analýzy/PoC	S	S	A + V	M3

2.1.1 Odborné role poddodavatele pro realizaci analytických činnosti

Rozsah analytických činností poddodavatele v členění dle Odborných rolí dle Příloha č. 1 Smlouvy:

ID Odborné role	Název Odborné role	Počet člověkodnů
6	DevOps engineer junior	93
11	Systémový architekt / Infrastrukturní systémový architekt	122
35	Databázový specialista	6
59	Specialista konzultant Elasticsearch	15
2	Tester senior	33
Celkem		**269**

2.1.2 Odborné role Poskytovatele pro realizaci analytických činností

Rozsah analytických činností Poskytovatele v členění dle Odborných rolí dle Příloha č. 1 Smlouvy:

ID Odborné role	Název Odborné role	Počet člověkodnů
10	Administrátor Microsoft technologií (MS)	12
14	IT analytik / IT architekt	30
13	Administrátor síťových technologii (NET)	15
7	Aplikační administrátor	7
21	Business analytik/architekt	10
23	Správce identit a integrací	10
Celkem		**84**

2.2 Činnosti a externí služby nezahrnuté do 1. etapy

Zde uvádíme činnosti, které nejsou zahrnuté do plnění 1. etapy, ale budou součástí analytických výstupů 1. etapy:

- Licence a implementace DB na ukládání pdf. (eLDAX);
- Technologie Unify a implementace – sběrnice;
- Služby třetích stran – pečetění a časová razítka (TSA IZOL).

K rozsahu plnění milníku M3 – Ostatní Aktivita "Detailní návrh integrace komponent třetích stran (eLDAX, Unify, TSA IZOL) včetně požadavků na součinnosti" dle odst. 2.1 uvádíme, že výstupem této činnosti bude pouze popis v části analytického dokumentu. Součástí 1. etapy není implementace komponent eLDAX, Unify a TSA IZOL.

3 Rozsah činností v oblasti kybernetické bezpečnosti pro 1. etapu

Činnosti v oblasti kybernetické bezpečnosti jsou pro 1. etapu rozděleny následovně:

3.1 Analytické činnosti v oblasti bezpečnosti

Analytické činnosti zahrnují práce Odborných rolí na Analýze, která je výstupem M1 a zahrnuje vymezení Bezpečnostního monitoringu pro M3 a pro 2. etapu migrace eSeL, která bude řešená samostatným smluvním vztahem.

V rámci analytických činností v M1 zpracuje Poskytovatel analýzu napojení na Bezpečnostní monitoring SPCSS pro M3 a analýzu zpracování bezpečnostních logů na DCeGOV pro M3 v součinnosti s Objednatelem a poddodavatelem, kde potřebné součinnosti budou zejména sdílení podkladů a informací o stávajícím bezpečnostním monitoringu eSeL.

3.1.1 Odborné role Poskytovatele pro realizaci analytických činnosti v oblasti bezpečnosti

Rozsah analytických činností Poskytovatele pro zpracování analýzy v členění dle Odborných rolí dle Příloha č. 1 Smlouvy:

ID Odborné role	Název Odborné role	Počet člověkodnů
2	Architekt KB	11
1	Analytik KB	4
6	Manažer rozvoje služeb KB	10
Celkem		**25**

3.2 Bezpečnostní monitoring

Bezpečnostní monitoring v rámci M3 zahrnuje činnosti Odborných rolí při napojení MS Azure na Bezpečnostní monitoring SPCSS a při napojení Bezpečnostního monitoringu na DCeGOV na dobu 1 měsíce v termínu dle rozhodnutí Objednatele a dle podrobného plánu činností Poskytovatele a poddodavatele, který je výstupem M0 dle vymezení milníků uvedeném v odst. 2.1 této přílohy.

Odborné role se budou v rámci M3 podílet na ověřování služeb Bezpečnostního monitoringu pro experimentální prostředí systému eSeL v rozsahu stanoveném v rámci plnění M1.

3.2.1 Odborné role Poskytovatele pro Bezpečnostní monitoring

Rozsah analytických činností Poskytovatele pro Bezpečnostní monitoring v členění dle Odborných rolí dle Příloha č. 1 Smlouvy:

ID Odborné role	Název Odborné role	Počet člověkodnů
2	Architekt KB	5
1	Analytik KB	4
Celkem		**9**

4 Řízení Služeb 1. etapy

4.1 Rozsah Řízení služeb

Řízení Služeb 1. etapy je rozděleno v návaznosti na stranu poskytující tyto činnosti, a to takto:

- Odborné činnosti projektového řízení prostřednictvím Odborné role Projektový manažer poddodavatele, který zajišťuje projektové činnosti poddodavatele a jeho Realizačního týmu,
- činnosti projektového řízení prostřednictvím Odborné role Projektový manažer, Manažer služeb a Obchodní manažer Poskytovatele, který zajišťuje koordinaci činností poddodavatele, Poskytovatele a Objednatele.

Rozsah činností Odborné role je uveden v Příloze č. 1 Smlouvy a pro 1. etapu bude rovněž zajišťovat následující činnosti:

- účast na jednáních týmu Objednatele a na jednáních týmu Poskytovatele,
- komunikace v rámci realizačního týmu Poskytovatele a poddodavatele,
- zpracování obvyklých projektových dokumentů – vedení tabulky úkolů, kontrola projektové dokumentace a ověřování výstupů plnění,
- příprava programu jednání, udržování sdílených adresářů a administrace přístupů, vedení evidence rizik, aktualizace realizačního plánu – harmonogramu,
- kontrola akceptačních protokolů.

4.2 Odborné role pro realizaci řízení Služeb

ID Odborné role	Název Odborné role	Počet člověkodnů
Odborné role poddodavatele		
14	Projektový manažer	55
Celkem		**55**
Odborné role Poskytovatele		
15	Manažer služeb	10
16	Projektový manažer	20
Celkem		**30**

5 Související analytické činnosti

V rámci přípravy a ověřování experimentálního prostředí zajistí Poskytovatel následující související analytické činností:

- Ověření využitelnosti a pilotní testování cloudových služeb pro AI Assistant, vč. poskytnutí přehledů o aktivitách formou čerpání kreditů,
- analýza stavu a příprava specifikace experimentálního prostředí, účast Odborných rolí na technických jednáních s cílem definovat rozsah a rizika migrace systému eSeL do nového prostředí.

5.1 Odborné role pro realizaci souvisejících analytických činností

ID Odborné role	Název Odborné role	Počet člověkodnů
Odborné role pro analýzu Cloudových služeb pro AI Assistant		
10	Administrátor Microsoft technologií (MS)	5
Celkem		**5**
Odborné role Poskytovatele pro analýzu stavu a přípravu specifikace experimentálního prostředí		
10	Administrátor Microsoft technologií (MS)	5
14	IT analytik / IT architekt	3
13	Administrátor síťových technologii (NET)	4
21	Business analytik/architekt	4
23	Správce identit a integrací	1
Celkem		**17**

6 Harmonogram

Pro účely této Nabídky jsou pro realizaci 1. etapy stanoveny Milníky plnění – M0, M1, M2 a M3. Rozsah činností realizovaných v rámci každého milníků je uveden v odst. 2.1 této přílohy, a to takto:

Milník	Termín poskytnutí plnění **od termínu dle odst. 7.4 Smlouvy**
M0	do 7 kalendářních dnů
M1	do 50 kalendářních dnů
M2	do 90 kalendářních dnů
M3	do 90 kalendářních dnů

7 Cena Ostatních činností

7.1 Cena dle jednotlivých oblastí plnění

Cena Ostatních činností je členěná podle jednotlivých oblastí analytických a souvisejících analytických činností, činností v oblasti kybernetické bezpečnosti a činností poddodavatele.

ID	Oblast činností	Odstavec dle této přílohy	Cena bez DPH	Cena s DPH
1	Analytické činnosti a příprava Cloudových služeb, z toho:	odst. 2	4 765 900 Kč	5 766 739 Kč
1.1	• činností Poskytovatele, z toho:	odst. 2.1	1 190 200 Kč	1 440 142 Kč
1.2	• činnosti poddodavatele;	odst. 2.1	3 575 700 Kč	4 326 597 Kč
2	Činnosti v oblasti kybernetické bezpečnosti pro 1. etapu, z toho:	odst. 3	542 600 Kč	656 546 Kč
2.1	• analytické činnosti v oblasti bezpečnosti;	odst. 3.1	398 900 Kč	482 669 Kč
2.2	• bezpečnostní monitoring;	odst. 3.2	143 700 Kč	173 877 Kč
3	Řízení Služeb 1. etapy, z toho:	odst. 4	1 249 700 Kč	1 512 137 Kč
3.1	• činnosti Poskytovatele;	odst. 4	408 000 Kč	493 680 Kč
3.2	• činnosti poddodavatele;	odst. 4	742 500 Kč	898 425 Kč
4	Související analytické činnosti, z toho:	odst. 5	307 100 Kč	371 591 Kč
4.1	• analýza Cloudových služeb pro AI Assistant;	odst. 5	65 000 Kč	78 650 Kč
4.2	• analýza stavu a příprava specifikace experimentálního prostředí.	odst. 5	242 100 Kč	292 941 Kč
Celkem Ostatní činnosti			**6 766 100 Kč**	**8 186 981 Kč**

7.2 Cena dle jednotlivých milníků

Poskytovatel bude předkládat k akceptaci rozsah činností dle jednotlivých milníků v souladu s odst. 7.7 Smlouvy.

ID	Milník dle Harmonogramu	Cena bez DPH	Cena s DPH
1	M0	**209 700 Kč**	**253 737 Kč**
2	M1	**2 248 200 Kč**	**2 720 322 Kč**
3	M2	**2 838 800 Kč**	**3 434 948 Kč**
4	M3	**1 469 400 Kč**	**1 777 974 Kč**
Celkem Ostatní činnosti		**6 766 100 Kč**	**8 186 981 Kč**

Každý milník bude fakturován, na základě akceptace samostatného akceptačního protokolu za daný milník.

Podmínky využití poskytnutých informací Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách https://www.first.org/tlp/). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:	
Štítek	**Podmínky použití**
TLP: RED	Informace není určena pro jiné než určené osoby (určuje původce); poskytnutí informace dalším subjektům ze strany příjemce lze učinit pouze s předchozím souhlasem původce informace.
TLP: AMBER	Informaci je možné sdílet pouze s omezeným okruhem osob (určuje původce); příjemci mohou sdílet tyto informace pouze s členy své organizace a s dodavateli nebo zákazníky, kteří nezbytně potřebují tyto informace znát, aby se chránili nebo zabránili vzniku další škody; původce informace může rozsah sdílení dále omezit.
TLP: GREEN	Informace je určena k omezenému zveřejnění; omezeno na komunitu (organizace příjemce a další partnerské subjekty příjemce informace), avšak nikoliv s využitím veřejně dostupných komunikačních kanálů; příjemce nesmí informaci šířit mimo určenou komunitu (určuje původce).
TLP: CLEAR	Zveřejnění informace není omezeno; tímto ustanovením není dotčeno omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran.