Způsob realizace předmětu plnění veřejné zakázky

1. OBSAH

2. DODÁVKA NÁSTROJE IDM

2.1. PŘEDMĚT DODÁVKY

Předmětem dodávky je dodání kompletního SW licenčního vybavení nástroje pro správu identit (nástroj IDM) dle požadavků stanovených Zadávací dokumentací včetně jejích příloh (dále jen „***Dodávka***").

Součástí Dodávky je poskytnutí kompletních licenčních dokumentů a klíčů, instalačních médií, standardní technické dokumentace výrobce SW nezbytné pro instalaci IDM nástroje a souvisejícího SW vybavení a následný provoz IDM nástroje a souvisejícího SW vybavení a potvrzení o zajištění maintenance výrobcem nástroje Objednateli.

2.2. SEZNAM DODÁVANÝCH SW PRODUKTŮ

Součástí dodávky bude akceptační protokol, který bude obsahovat soupis veškerých poskytovaných licencí včetně dokumentace se závazkem Poskytovatele, že se jedná o kompletní seznam následujících licencí nezbytných pro implementaci nástroje IDM v požadovaném rozsahu.

Seznam licencí:

Pro produkty IBM Security Identity Governance and Intelligence nejsou třeba žádné aktivační klíče. Zde je třeba pouze stáhnout instalační média z Passport Advantage portálu.

Název licence	Výrobce	Part Number	Popis	Množství
Dodávané Licence pro zajištění funkčnosti nástroje IDM				
IBM Security Identity Governance and Intelligence Enterprise Edition	IBM	D1K1GLL	IBM Security Identity Governance and Intelligence Enterprise Edition Install License + SW Subscription & Support 12 Months	6584,00
IBM Security Secret Server for Privileged Users per User Value Unit License	IBM	D21ZQLL	IBM Security Secret Server for Privileged Users per User Value Unit License + SW Subscription & Support 12 Months	15,00

Poskytovatel prohlašuje, že navrhovaných a nabídnutých 6584 licencí odpovídá požadavku Zadavatele na 1500 interních uživatelů a 100 000 externích uživatelů systému. Přepočet byl proveden na základě konverzní a licenční tabulky, která byla dodána spol. IBM.

Součástí dodávky licence je zároveň SW Subscription *(+SW Subscription&Support 12 Months*), která umožňuje mimo jiné přístup ke stažení nových verzí dodaného produktu po dobu platného SW Subscription. Celý popis SW Subscription je uveden zde:
https://www.ibm.com/software/uk/passportadvantage/software_subscription_support_ov.html

Dodaný nástroj IDM splňuje tyto funkční vlastnosti:

ID	Kategorie	Požadavek
1	Funkcionalita	Systém umožňuje práci minimálně s 5 nezávislými úrovněmi (typy) identit, kdy pro každou úroveň (typ) lze stanovovat vlastní politiky/pravidla/vlastnosti
2	Funkcionalita	Pro každý typ identit lze definovat datové struktury (atributy) identit s vlastními vlastnostmi (např. jmenná konvence user name, kontrola dané hodnoty, atd.)
3	Funkcionalita	Řešení umožňuje přidělování, odebrání, reorganizaci a modelování rolí (na úrovni business rolí)
4	Funkcionalita	Systém umožňuje ohodnocení objektů (atributů, povolení) na základě analýzy rizik
5	Funkcionalita	Systém umožňuje grafické zobrazení přístupových práv jednotlivých uživatelů v interaktivní mapě, která zobrazuje i návrhy možných rolí
6	Funkcionalita	Systém umožní revizi přístupů a jejich certifikaci včetně zneplatnění
7	Funkcionalita	Umožňuje konfiguraci a validaci politik minimálních privilegií
8	Funkcionalita	Umožňuje konfiguraci a validaci SoD - Separation of Duties
9	Funkcionalita	V systému musí být možno vytvořit vlastní struktury organizace, které reflektují skutečnost. (např.: rozdělení mezi regiony, interní členění, různé organizační struktury, partneři)
10	Funkcionalita	Systém umožňuje založení, změnu, dočasné i trvalé zneplatnění, vymazání uživatele
11	Funkcionalita	Možnost definovat vlastní politiky provisioningu identit a rolí, hesel a tvorby identit
12	Funkcionalita	Systém dokáže identifikovat nepoužívané účty
13	Funkcionalita	Systém rozlišuje systémové a technické účty od uživatelských účtů
14	Funkcionalita	Systém musí umožňovat definování statických a dynamických rolí, které jsou přiřazovány na základě atributů uživatele
15	Funkcionalita	Systém musí umožňovat pokročilou administraci rolí v rámci základní licence (tvorba "what-if" analýz)
16	Funkcionalita	Musí umožňovat víceúrovňové schvalovací procesy (workflow) pro správu rolí, oprávnění i samotného řízení identit
17	Funkcionalita	Obsahuje nástroje pro modelování workflows včetně vizualizace a umožňuje definování workflows bez nutnosti znalosti programovacích jazyků
18	Funkcionalita	Musí umět pracovat s vlastními uživatelsky definovanými atributy včetně jejich správy a nástroji pro modelování rolí

19	Funkcionalita	Systém musí být schopen zabránit přidělení oprávnění/role/přístupu, pokud by mělo dojít ke střetu zájmů (SoD - Separation of Duties)
20	Funkcionalita	Musí umožňovat delegace pravomocí
21	Funkcionalita	Podporuje přidělování oprávnění na základě rolí, nebo na základě požadavků, případně kombinací obojího
22	Funkcionalita	Možnost pokročilého vyhledávání účtů pomocí předpřipravených filtrů (non-compliant účty, osiřelé účty apod.)
23	Funkcionalita	Systém musí podporovat vytvoření hierarchického modelu rolí
24	Funkcionalita	Řešení musí obsahovat záchrannou síť proti administrativním manuálním chybám - musí umět simulovat dopad a umožnit náhled před aplikováním změn politik
25	Funkcionalita	Řešení umožňuje online synchronizaci dat IDM, zdroje identit a cílových aplikací a nespoléhá pouze na plánované noční batch operace
26	Funkcionalita	Systém umí připojit více uživatelských identit k jednomu reálnému uživateli
27	Funkcionalita	Systém dokáže spravovat sdílené účty (privilegované uživatele)
28	Funkcionalita	Umožňuje monitorovat uživatele používající privilegované účty a umí uchovávat záznamy o historii užívání
29	Funkcionalita	Systém dokáže zaznamenat a zpětně přehrát operace, které byly provedeny s pomocí sdílených účtů, a také vyhledávat v tomto záznamu
30	Funkcionalita	U privilegovaných účtů uchovává hesla v bezpečném trezoru
31	Funkcionalita	Umožňuje měnit hesla sdílených účtů po každém použití pro zachování bezpečnosti
32	Funkcionalita	Systém musí být schopen zabezpečit sdílené účty používané aplikacemi a skripty a sledovat jejich aktivity
33	Funkcionalita	Systém umožňuje centrální změnu hesla sdíleného účtu bez nutnosti úpravy skriptů a aplikací
34	Funkcionalita	Systém umí časově omezit délku využívání sdíleného účtu
35	Integrace	Synchronizace hesel a účtů v rámci všech systémů, včetně podpory změny hesla přímo z prostředí Windows desktop
36	Integrace	Systém musí podporovat různé operační systémy (Windows Server, Linux, AIX)
37	Integrace	Systém musí podporovat různá databázová úložiště (Oracle, MS SQL, IBM DB2)
38	Integrace	Systém musí podporovat různé implementace LDAP (MS AD, SAP LDAP, IBM Security Directory Sever, Oracle Directory Server)

39	Integrace	Systém musí umožňovat integraci pro správu uživatelů na systémy MS Exchange a Office Online (Office 365)
40	Integrace	Komunikace mezi všemi komponentami celého řešení musí probíhat zabezpečeně (např. certifikáty, TLS, SSO)
41	Integrace	Systém musí umožňovat podporovat integraci řešení s různými typy autentizace (AD, AD FS, IDM třetích stran, SAML)
42	Integrace	Systém obsahuje „out of the box" základní adaptéry (Unix, Linux, AIX, Active Directory, LDAP, DB2, Oracle DB, Sybase)
43	Integrace	Systém v základu obsahuje nástroj pro tvorbu vlastních adaptérů, a to v grafickém prostředí a bez nutnosti znalosti programovacích jazyků
44	Integrace	Musí nabízet širokou škálu API pro možností přizpůsobení celého systému včetně standardů WebService a REST
45	Integrace	Řešení může být nasazeno jako virtual appliance
46	Integrace	Řešení musí detekovat změny ve zdrojích identit on-line a následně propagovat do cílových systémů na základě událostí
47	Integrace	Systém musí umožňovat organizaci a přemisťování konfiguračních jednotek a balíčků mezi vývojovým, testovacím a produkčním prostředím
48	Report	Řešení a jeho reporty musí být akceptovatelné interními i externími auditory, a to v souladu s požadavky ISO 27000 a ZoKB
49	Report	Systém umožňuje compliance reporty
50	Report	Systém musí umožňovat reportování a následný export reportů do formátů CSV, HTML, PDF a MS Office
51	Report	Systém umožňuje report historie změn uživatelů
52	UI	Systém bude možné ovládat kompletně z webového rozhraní
53	UI	Uživatelské rozhraní podporuje běžné prohlížeče v aktuálních verzích (MS Internet Explorer, Mozilla Firefox a Google Chrome)
54	UI	Systém obsahuje administrátorské rozhraní pro správu aplikace
55	UI	Systém obsahuje „Self service" rozhraní pro koncové uživatele, které musí umožňovat změnu hesla, obnovu zapomenutého hesla, zobrazení seznamu zdrojů a služeb, ke kterým má uživatel přístup, možnost požádat o přístup a také možnost sledovat stav žádostí
56	UI	Rozhraní pro administrátory může být upraveno tak, aby zobrazovalo pouze tu část, kterou má administrátor na starosti
57	UI	Základní úkony uživatelů je možné provádět z aplikace pro mobilní zařízení (požadavek na přidělení/změnu přístupu) podporující minimálně platformy Android a iOS

58	UI	Systém musí být plně upravitelný do vzhledu společnosti (web, notifikace, formuláře, reporty, emaily)

2.3. HARMONOGRAM A ZPŮSOB PŘEVZETÍ DODÁVKY

Celkový termín dodání Dodávky je stanoven na maximálně **15 kalendářních dní** ode dne nabytí účinnosti Smlouvy.

Způsob a formát předání dodávky:

Licence SW produktu IBM Security Identity Governance and Intelligence Enterprise Edition uvedené v nabídce budou zadavateli zpřístupněny skrze službu IBM Passport Advantage (dále jen PA). Odkaz na uvedenou službu: https://www.ibm.com/software/passportadvantage/pacustomers.html

Zadavatel dostane k dispozici instalační balíčky produktů, licenční certifikáty a hlášení s podrobným popisem procesu formou návodu od výrobce IBM. Předmětný dokument bude Zadavateli předán až v rámci resp společně s dodávkou.

Aktivační klíče IBM Security Secret serveru dostane Zadavatel při předání a akceptaci produktu. Licenční klíč dorazí emailem na adresu, kterou uvedl Zadavatel: ondrej.smejkal@szif.cz

Předmět dodávky převezme Oprávněná osoba na straně Objednatele. Předmět Dodávky bude předávat Oprávněná osoba na straně Poskytovatele. Součástí předání ze strany Poskytovatele bude rovněž Akceptační protokol s kompletním výčtem předmětu Dodávky.

Pro akceptační proceduru a lhůty potvrzující předání a převzetí Dodávky se uplatní ustanovení kapitoly č. 9 Smlouvy. Tzn. že licence a aktivační klíče budou předány dle požadavků Zadavatele.

3. IMPLEMENTACE NÁSTROJE IDM

Předmětem implementace (dále jen „***Implementace***“) je zajištění následujících služeb nezbytných pro uvedení IDM nástroje do produktivního užívání:

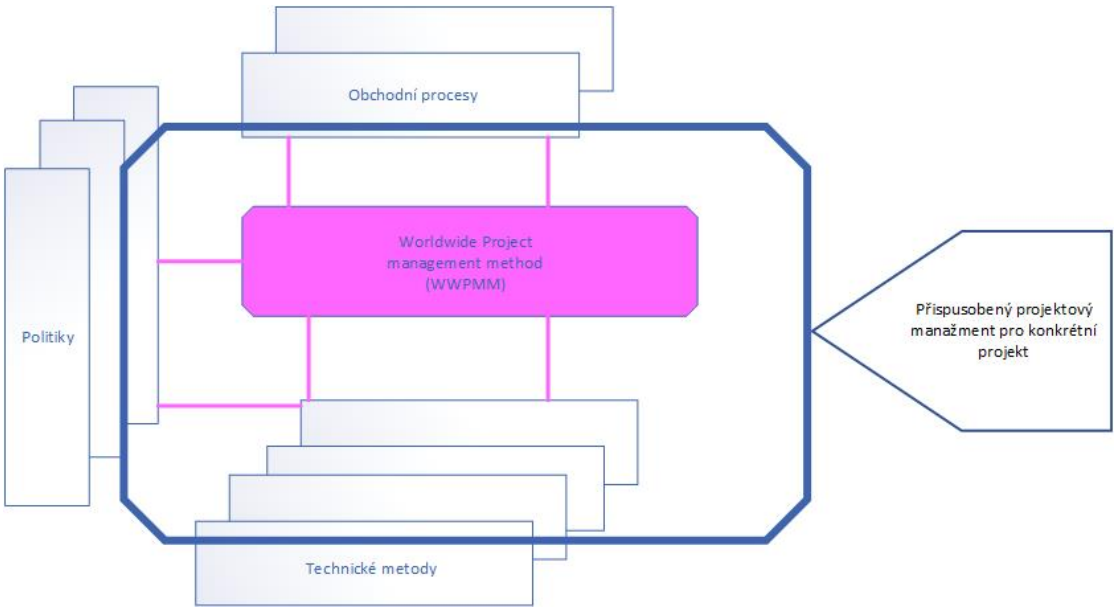
- Instalace nástroje ve virtualizovaném prostředí Objednatele
- Plná integrace nástroje IDM na:
    - HR systém OKBase
    - Microsoft Active Directory
    - Správu uživatelů (CUA SAP) a LDAP SAP
- Příprava nástroje pro další implementační a rozvojové práce:
    - Integraci na jednotlivé moduly informačního systému SAP
    - Integraci na interní podpůrné systémy zajišťující výkon činností SZIF
    - Zajištění realizace procesů správy identit a údajů uživatelů IS SZIF
- Testy funkčnosti IDM nástroje
- Školení administrátorů IDM a zpracování dokumentace
- Uvedení do produktivního provozu

3.1. METODIKA ŘÍZENÍ PROJEKTU IMPLEMENTACE/ZÁKLADNÍ POPIS PRINCIPU ŘÍZENÍ PROJEKTU

3.1.1. Způsob realizace projektu

Organizace projektu popisuje celkový přístup k dodávce navrhovaného řešení. Díky využití metodologie „World Wide Project Management Methodology (WWPMM)“ nabízí vysoce kvalitní nástroje a procesy pro kontrolu a řízení projektu a reporting.

Poskytovatel řídí projekty s cílem je přizpůsobit potřebám Zadavatele tak, aby pokryla veškeré jeho požadavky. Výsledkem je strukturovaný řídicí přístup tak, jak je znázorněn v následujícím schématu:



Obrázek 1 - Obecný pohled na WWPMM

Jak ukazuje schéma, Project Management System je souhrnem metod, organizačních procesů a zásad pro konkrétní projekt. V následujících částech podrobně popisujeme integrační body Poskytovatele pro metody a potenciální podnikové procesy.

Požadovaná součinnost ze strany Zadavatele, jak je definovaná v kapitole 3.4.1, bude objednána prostřednictvím emailu zaslaného na Vedoucího projektu Zadavatele minimálně 3 pracovní dny před výkonem konkrétního požadavku na součinnost ze strany Zadavatele. V rámci součinnosti je tento požadavek uveden níže v kapitole Součinnost pro zajištění implementace.

3.1.2. Struktura projektu

Smluvní strany ustanoví tým ručitelů za každý dílčí systém projektu ze strany Poskytovatele i ze strany Zadavatele, který bude schválen na Kick-off jednání. Členové těchto týmů musí mít dostatečnou úroveň oprávnění při poskytování informací druhé straně, aby byla zajištěna maximální efektivita spolupráce obou týmů na projektu. V rámci obou týmů bude vytvořena organizační struktura vedení projektu, která definuje styk mezi Poskytovatelem a Zadavatelem, jakož i povinnosti obou partnerů.

Řídicí výbor

Řídicí výbor má nejvyšší úroveň odpovědnosti nad celým projektem. Řídící výbor se schází nepravidelně, vždy na základě požadavku některého z členů. Řídící výbor má lichý počet členů. Řídící výbor tvoří jak zástupci Poskytovatele, tak zástupci Zadavatele.

Stanovená struktura projektového týmu

Stanovená struktura projektového týmu vychází z metodiky projektového řízení a celkově koresponduje a zapadá do předpokládaných možností Zadavatele. Je možné upravovat obecný náhled na jednotlivé role a případné obsazení. Nicméně pro některé klíčové role není možné akceptovat jejich vypuštění z projektu, nebo sdílení několika pracovníky. A to jak na straně Zadavatele, tak na straně Poskytovatele.

3.1.3. Základní projektové role

Výkonný pracovník projektu Zadavatele

Výkonný pracovník projektu Zadavatele je osoba, která dohlíží nad projektem z hlediska spokojenosti organizace Zadavatele. Výkonní pracovníci projektu Zadavatele a Poskytovatele se scházejí pravidelně jednou za měsíc. Výkonní pracovníci projektu Zadavatele a Poskytovatele přijímají rozhodnutí, která překračují rozsah odpovědnosti vedoucího pracovníka projektu. Výkonní pracovníci projektu Zadavatele a Poskytovatele nesou odpovědnost za řešení případných problémů, které se vyskytnou v průběhu projektu, a které jim vedoucí projektu postoupili. Výkonní pracovníci projektu Zadavatele a Poskytovatele jsou v rámci řízení projektu povinni respektovat rozhodnutí řídícího výboru.

Výkonný pracovník projektu Poskytovatele

Výkonný pracovník projektu Poskytovatele je osoba, která ponese odpovědnost za projekt vůči Zadavateli. Tato osoba nese odpovědnost za vedení a řízení vztahu se zadavatelem a řídícím výborem. Tato osoba bude jediným kontaktním bodem pro práce na projektu, řešení problémů a celkové řízení a usměrňování členů týmu.

Výkonný pracovník projektu Poskytovatele zajišťuje řízení kontinuity a přechodu pro různé pracovní harmonogramy a týmy během celého procesu. Výkonný pracovník projektu Pokytovatele nese odpovědnost za celkové smluvní řízení, personální obsazení, finanční plány, spokojenost Zadavatele a řešení problémů. Pro tento projekt obsadí Poskytovatel tuto klíčovou funkci člověkem, který má rozsáhlou praxi ve veřejném sektoru a dovede řídit projekt daný rozsahem a komplexností Zadavatele.

Vedoucí projektu Poskytovatele

Vedoucí projektu Poskytovatele je osoba, která nese odpovědnost za plánování, organizaci, usměrňování a řízení každodenních činností projektu, dodržování harmonogramu projektu a dodržování cílů projektu. Tato osoba bude jediným kontaktním bodem projektu pro personální obsazení, přidělení úkolů, plánování a reporting.

Tato osoba zabezpečuje každodenní koordinaci a kontrolu všech činností projektu a ověřuje, zda jsou používány správné metody a postupy pro všechny činnosti projektu. Řídí rizika projektu a kontroluje, zda jsou uplatňovány plány kontroly pro všechny problémy. Stejně tak nese společně s výkonným pracovníkem projektu odpovědnost za projektové plány a výstupy Poskytovatele.

Vedoucí projektu rovněž zajišťuje vedení týdenních porad o stavu projektu, provádí revizi problémových položek a činností k řešení v závislosti na požadovaném datu řešení. Problémové položky/činností, které nebudou vyřešeny v přiměřené lhůtě, budou postoupeny dále v souladu s procesem řešení problémů.

Vedoucí projektu bude podřízen výkonnému pracovníkovi projektu Poskytovatele a vedoucímu projektu Zadavatele, přičemž bude poskytovat pravidelné aktuální informace o předpokládaném čerpání zdrojů projektu Poskytovatele. Pro tento projekt Poskytovatel obsadí tuto pozici zkušenou osobou s odpovídající zkušeností, která dokáže řídit a vést rozsáhlý projekt návrhu a implementace.

Tato osoba bude mít předchozí praxi s řízením projektů v oblasti informačních technologií pro veřejnou správu a bude mít přehled o způsobu realizace tohoto řešení.

Role vedoucího projektu Poskytovatele bude obsazena projektovým manažerem Poskytovatele (PM).

Vedoucí projektu Zadavatele

Vedoucí projektu Zadavatele nese odpovědnost za plánování, organizaci, usměrňování a řízení každodenních činností projektu, dodržování harmonogramu projektu a dodržování cílů projektu. Tato osoba bude jediným kontaktním bodem projektu pro řízení projektu s Vedoucím projektu Poskytovatele.

Tato osoba zabezpečuje každodenní koordinaci a kontrolu všech činností projektu za stranu Zadavatele a ověřuje, zda jsou používány správné metody a postupy pro všechny činnosti projektu. Řídí rizika projektu a kontroluje, zda jsou uplatňovány plány kontroly pro všechny problémy.

Vedoucí projektu rovněž zajišťuje vedení týdenních porad o stavu projektu, provádí revizi problémových položek a činností k řešení v závislosti na požadovaném datu řešení. Problémové položky/činností, které nebudou vyřešeny v přiměřené lhůtě, budou postoupeny dále v souladu s procesem řešení problémů.

Vedoucí projektu bude podřízen Zadavateli projektu. Vedoucí projektu bude Projektový manažer za stranu Zadavatele.

Vedoucí integrace Poskytovatele

Vedoucí integrace je seniorní pracovník Poskytovatele. Tato osoba nese odpovědnost za vedení plánování, které povede k vypracování návrhu designu řešení a plnění požadavků Zadavatele.

Vedoucí integrace poskytuje významnou podporu a konzultační vedení týmů a vedoucímu projektu Poskytovatele během vypracování návrhu i celé implementační činnosti. Nese odpovědnost za veškeré výstupy a potvrzení plánu a strategického plánu implementace.

Tento vedoucí bude poskytovat podporu a zajistí vedení technického týmu Poskytovatele během činností vypracování návrhů a implementace. Bude ověřovat kvalitu komponent dodávaného řešení.

Vedoucí integrace bude Analytik IDM řešení.

Člen technického týmu Poskytovatele

Úkolem člena technického týmu Poskytovatele, tedy technického specialisty, je poskytovat podporu při vypracování návrhu a instalaci nových systémů. Během fáze vypracování návrhu bude tato osoba spolupracovat se Zadavatelem na vytvoření prostředí nezbytného pro přípravu systému.

Členem technického týmu Poskytovatele budou Senior analytik IDM řešení a Analytik Bezpečnosti – Informační/Kybernetické bezpečnosti.

Člen technického týmu Zadavatele

Úkolem člena technického týmu Zadavatele je poskytovat podporu při vypracování návrhu a instalaci nových systémů. Během fáze vypracování návrhu bude tato osoba spolupracovat s Poskytovatelem na vytvoření prostředí nezbytného pro přípravu systému.

Členové technického týmu Zadavatele budou jmenováni Zadavatelem, dle požadavků Poskytovatele na jejich odbornost.

Požadované projektové role na straně Zadavatele

Na straně Zadavatele jsou požadované tyto role:

Zadavatel projektu

Vedoucí projektu Zadavatele

Člen/Členové technického týmu (Zadavatele).

Obě strany se dohodly, že Zadavatel v rámci kickoffu jmenuje a oznámí všechny členy řídícího výboru Zadavatele. Zároveň se obě smluvní strany dohodly, že projektový tým bude možné rozšířit o další projektové role, pokud to bude projekt vyžadovat.

3.1.4. Řízení rizik

Riziko je možná událost, nebo situace v budoucnosti, které mohou mít nepříznivý dopad na projekt. Rizika vznikají na základě **rizikových faktorů.** Pokud se vyskytne riziko, jeho **důsledky** mohou mít dopad na projekt.

Rizikový faktor

Riziko může být způsobeno více než jedním rizikovým faktorem, a naopak jeden rizikový faktor může indikovat více než jedno riziko. Rizika se identifikují, popisují a následně analyzují z následujících hledisek:

- pravděpodobnost výskytu,
- dopad důsledků rizika na projekt,
- období, kdy mohou důsledky nastat.

Na základě analýzy rizik lze rizika řídit. K dispozici jsou obecně 4 možné reakce:

- **Akceptace**. Akceptace možnosti, že nastanou důsledky rizika, a to bez jakékoliv další činnosti. Nicméně s průběžným sledováním toho, zda se pravděpodobnost výskytu podobného rizika nezvyšuje.
- **Přesun rizika.** Přenesením celé odpovědnost za zvládání rizik nebo jejich částí na Zadavatele nebo Poskytovatele.
- **Využití rezervy** vytvářené na krytí rizik. Rozhodnutí použít zdroje z rezerv řízení rizik nebo rizikových rezerv.
- **Omezení rizik**. Existují dva typy omezení rizik dle definice v WWPMM:
  - **Zmírnění rizika.** Podniknutí kroků pro působení na rizikové faktory tak, aby se snížila pravděpodobnost výskytu jeho důsledků, pokud by riziko nastalo.
  - **Plánování rizikových rezerv** (risk contingency planning). Vypracování **plánu rizikových rezerv** pro zvláštní nebo vícečetná rizika.

Skutečné rizikové faktory a možné reakce na ně budou řešeny v průběhu celého trvání projektu.

3.1.5. Vyhodnocení rizik

Níže v tabulce je uveden obecný příklad výčtu způsobu vyhodnocení rizik.

Zdroje	ID	Riziko	Úroveň	Omezení rizika
Připomínky k současnému stavu řešení uvedenému v dokumentaci obchodní soutěže	1	Změna konečného řešení	Střední	• Ověření předpokladů • Analýza • Úprava • Akceptace konceptu a projektu
	2	Nesprávně stanovené náklady, čas, zdroje	Střední	• Úprava / vyladění • Akceptace
Zainteresované třetí strany	3	Legislativní proces může mít vliv na koncepci anebo způsobit její změnu	Střední	• Ověření formou konzultací
	4	Možné zablokování celého projektu	Vysoká	• Ověření formou konzultací • Předběžné dohody se třetími stranami

Tabulka 1: Návrh způsobu vyhodnocení rizik, demonstrativní výčet

- Obě smluvní strany se dohodly, že rizika budou identifikována a vyhodnocována průběžně během celého trvání projektu.

3.1.6. Metodologie

Přístup Poskytovatele k řízení projektu zahrnuje čtyři základní principy:

- Proces projektového managementu – zahrnuje práce na definici, plánování a realizaci projektu, pro zajištění odpovídajících činností na straně Zadavatele a Poskytovatele, které povedou k realizaci záměru projektu při akceptaci projektových principů, včetně projektových rizik.

- Organizace projektu a odpovědnost za něj – definování a dohoda, kdo bude klíčovými aktéry, kteří budou spolupracovat s cílem dosáhnout úspěšného výstupu – zejména pak organizace, která realizaci projektu požaduje (jejíž činnost má výstup projektu podporovat) a která ponese odpovědnost za provoz a používání výstupních dokumentů a služeb. Smluvní strany se dohodly, že organizace projektu a odpovědnosti budou schváleny na Kick-off meetingu.
- Fáze projektu – zaručuje, že práce bude rozdělena do jednotlivých fází, které vedení umožňují opakovaně odhadovat rizika v klíčových bodech během projektu.
- Systém projektového managementu – zavedení systému řízení, který vyžaduje přiměřený stupeň kontroly nad všemi činnostmi a zohledňuje předmět projektu.

Cílem metodiky je poskytnout opakovatelné prostředky vývoje řešení, které v konečném důsledku přinášejí úspěšné projekty a spokojené zákazníky.

- Obě smluvní strany se dohodly, že tyto principy, vyžadující včasnou koordinaci mezi Poskytovatelem a Zadavatelem, poskytují základní strukturu projektu a tvoří mapu úspěšné cesty k jeho dokončení. Proto budou obě smluvní strany aktivně řešit nastalé situace a připravovat taková řešení, která budou směřovat k úspěšnému dokončení celého projektu.

3.1.7. Plánování projektu

Hlavní činností v rámci plánování projektu je vývoj a vedení podrobného plánu projektu. Tento proces vytváří harmonogram pro projekt a na samotném počátku projektu potvrzuje jeho proveditelnost a rozsah. Poskytovatel nadefinuje plán projektu ve spolupráci s projektovým týmem Zadavatele. Vypracování plánu projektu zahrnuje vytvoření měřitelných úkolů, identifikaci výstupů, stanovení kritické cesty a milníků projektu. Tento plán projektu bude obsahovat jasnou definicí úkolů a odpovědnosti jednotlivých členů.

3.1.8. Kontrola plnění harmonogramu projektu

Jako základ pro řízení projektu bude sloužit nástroj MS Project. Tento nástroj poskytuje řídícím týmům obou smluvních stran společnou základnu pro vykazování stavu projektu a podpoří shromažďování žádostí, výsledků rozhovorů, záznamů ze zasedání, výsledků projektu, řízení problémů, položek činností a kontrolu změn projektu. Využití tohoto nástroje vylepšuje schopnost týmu Poskytovatele poskytnout řídícímu týmu Zadavatele kompletní přehled o činnostech projektu a stav realizace v „reálném čase".

3.1.9. Vykazování stavu

Vykazování stavu projektu bude probíhat na vícero úrovních, včetně týdenní porady o stavu s projektovým týmem. Pravidelné reporty Poskytovatele o stavu projektu pro Zadavatele budou zahrnovat úkoly dokončené v daném období projektovým týmem. Na straně Zadavatele bude vytvořena role **Výkonný pracovník projektu**. Tato osoba nese odpovědnost za vedení a řízení vztahu s Poskytovatelem a řídícím výborem. Tato osoba bude kontaktním bodem pro Výkonného pracovníka projektu Poskytovatele. Řeší problémy a celkově řídí a usměrňuje členy týmu.

3.1.10. Každodenní řízení projektu

Každodenní řízení projektu zahrnuje položky, které vedoucí projektu Poskytovatele realizuje denně pro zajištění hladké realizace projektu. Tyto činnosti zahrnují: řešení problémů, řízení změn projektu, řízení plnění zdrojů, zajišťování řízení úkolů, vedení projektu a komunikace s uživateli a zajišťování souhlasů a závazků.

3.1.11.Řízení změn

Za pochopení rozsahu projektu a potřeby pečlivě řídit změny s ohledem na stanovený rozsah projektu po celou dobu trvání projektu nesou společnou odpovědnost všichni členové týmu; výkonný pracovník projektu, členové řídicího výboru, projektového týmu, jakož i koncoví uživatelé Zadavatele.

To dává oběma smluvním stranám možnost změny projektu. Tuto změnu je nezbytné zaznamenat a řídit. Vzhledem k tomu, že změny jsou poměrně obvyklé, se obě strany dohodly, že „řízení změn" je nedílnou součástí řízení projektu. Je tím zajištěno, že obě smluvní strany mají možnost reagovat na změny, které se během projektu nevyhnutelně vyskytnou. Nástroj MS Project pomůže při zdokumentování změn s ohledem na celkový rozsah a časové hledisko projektu.

Obecně existují pouhé čtyři parametry, které lze měnit s cílem vypořádat se se změnou – rozsah, harmonogram, zdroje a náklady. Všechny změny projektu, které významně zasáhnou do celkového plnění díla musí být vypořádány dle platného legislativního rámce.

Řízení rozsahu projektu je velmi důležité. Prvním krokem řízení a kontroly rozsahu je dosažení jasného porozumění definice projektu společným týmem. V případě změny rozsahu bude mít oznámení změny formu žádosti o změnu projektu (Project Change Request - PCR). PCR musí popisovat změnu, zdůvodnění změny a dopad, který změna bude mít na projekt. Písemnou PCR musí podepsat obě strany, aby tím schválily realizaci změny rozsahu.

Následující odstavce popisují navrhovaný proces řízení změn:

Konfigurace projektu – řízení změny

Potřeba změny se může projevit dokonce i po podepsání dohody a vytvoření podrobné koncepce řešení, a to v důsledku identifikace dalších požadavků, přehodnocení priorit požadavků, změny rozsahu nebo termínů atd. V takových případech je nevyhnutelné vytvořit žádost o změnu, aby se spustil proces změny. Poskytovatel vyhodnotí následky navrhované změny v souladu s pravidly uvedenými v následujících odstavcích. Výkonní pracovníci projektu Zadavatele i Poskytovatele následně posoudí názor vedoucích projektu a rozhodnou o přijetí nebo zamítnutí žádosti o změnu.

Inicializace žádosti o změnu

Kterýkoliv člen projektového týmu může inicializovat žádost o změnu. Každá žádost o změnu se zaznamená na zvláštní formulář „žádosti o změnu" a stane se součástí projektové dokumentace. Žádost o změnu bude předložena vedoucím projektu.

Vedoucí projektu Poskytovatele ve spolupráci s vedoucím projektu Zadavatele zhodnotí, a v případě potřeby, upraví žádost o změnu. Vedoucí projektu Poskytovatele jmenuje člena projektového týmu pověřeného prošetřením žádosti o změnu. V případě potřeby Zadavatel poskytne dodatečné informace tak, aby na základě návrhu řešení této změny bylo možné stanovit prioritu a termín žádosti o změnu.

Hodnocení žádostí

Během hodnocení bude identifikován dopad žádosti o změnu a nezbytné úkoly. Posouzeny budou rovněž následky případného zamítnutí žádosti o změnu. Současně bude posouzeno, jak může žádost o změnu ovlivnit projekt z hlediska rozsahu, výstupu a nákladů.

Výsledky hodnocení budou zdokumentovány ve formuláři „žádost o změnu" a výsledky budou předloženy vedoucímu projektu Poskytovatele a vedoucímu projektu Zadavatele pro příslušné posouzení.

Řešení žádostí o změnu

Vedoucí projektu vypracují své posudky pro každou žádost o změnu. V případě, že změna nemá dopad na rozsah nebo náklady projektu, rozhodnou o přijetí změny nebo jejím zamítnutí.

V případě, že má žádost dopad na celkové náklady, funkčnost nebo harmonogram projektu, vypracují podrobný odhad skutečných nákladů a dopadů na plán projektu a žádost postoupí, společně se svými

vlastními posudky, Výkonným pracovníkům projektu k rozhodnutí. Pokud Výkonný pracovník projektu Zadavatele žádost schválí, spustí se postup změny k diskusi o změnách dohody, nebo bude odpovídajícím způsobem upraven harmonogramu projektu.

Schválená žádost o změnu bude realizována a zdokumentována jako sledovaná úloha. Stav žádosti o změnu a souvisejících činností se bude hlásit na poradách Výkonných pracovníků projektu.

3.1.12.Řízení problémů, eskalace problémů

Východiskem řízení problémů je snaha o ulehčení včasné identifikace problémů a co nejrychlejší řešení veškerých problémů, které se v průběhu realizace projektu vyskytnou. Problémy jsou rozděleny do kategorií: tj. technické, funkční, školící atd. a sledují se na více úrovních v rámci projektu. Vedoucí projektu povede seznam problémů, který sleduje stav nevyřízených problémů projektu. Projektový tým bude případné problémy projektu rovněž uvádět ve svých týdenních reportech o stavu a prezentovat je na poradách týmu o stavu projektu.

Obě smluvní strany se dohodly, že Vedoucí projektu Poskytovatele předloží klíčové problémy nebo žádosti o změnu na pravidelné poradě o stavu projektu (porada Vedoucích projektu). Tyto budou během porady projednány s Vedoucím projektu Zadavatele. Společně je buď vyřeší během porady vedoucích nebo je v případech rozporu postoupí na rozhodnutí řídícímu výboru.

3.1.13.Kontrola, sledování a reporting projektu

Tento proces zahrnuje realizaci projektu jako takovou, nebo realizaci plánu projektu, tj. sledování, kontrolu a dokumentaci činností projektu a řízení změn. Hlavní činnosti zahrnují:

- hodnocení úkolů vůči zdrojům,
- vedení a kontrola pracovních procesů,
- spolupráce s vedoucími týmů,
- spolupráce s vedením společnosti,
- koordinace projektových procesů s vedoucím projektu Zadavatele,
- rozhodování v případě výskytu problémů atd.

Pokrok projektu bude kontrolovat harmonogram projektu a vedoucí projektu Poskytovatele povede podrobný pracovní plán. Pokrok projektu bude pravidelně sledován a kontrolován vedoucími projektu, kteří se budou pravidelně setkávat během celé doby trvání projektu, přičemž řídicí výbor zajistí dohled.

Jako prostředek kontroly projektu se povede následující projektová dokumentace:

- Pracovní plán, který obsahuje projektové činnosti, přidělené lidské zdroje a stav dokončení všech úkolů.
- Report o stavu projektu vypracovaný pro každou poradu vedoucích projektu.
- Zápisy/záznamy z porad (pravidelných či eskalačních) vypracované zodpovědným/jmenovaným zaměstnancem Poskytovatele.
- Žádosti o změnu obsahující podrobný popis důvodů změny, stávající stav, řešení, hodnocení rizik a navrhované pokračování.
- Požadavky na poskytnutí součinnosti ze strany Objednatele
- Akceptační protokol/dokumentace

3.1.14.Správa projektu

Dokumentace o průběhu projektu se povede v tzv. kontrolní knize projektu (PCB – Project Control Book). PCB je nástroj využívaný společností Poskytovatele k dokumentaci, řízení a sledování projektu. Obsahuje veškeré informace o projektu včetně popisu rizik, změn, zápisů ze schůzek, rozhodnutí, milníků a sporných problémů.

Pro zajištěni fungovaní PCB poskytne Zadavatel sdílené úložiště na infrastruktuře spravované Zadavatelem. (viz požadavky na součinnost Zadavatele)

3.1.15.Formuláře komunikace projektového týmu, formy a způsoby komunikace

Porady o stavu projektu

O stavu projektu se bude diskutovat v rámci pravidelných kontrolních porad uspořádaných vedoucím projektu a zdokumentovaných v reportech o stavu projektu, které budou stručně a přesně popisovat stav projektu, definovat činnosti pro následující období, stejně jako případné postupy žádostí o změny. Frekvence, způsob a účastníky pravidelných kontrolních porad bude specifikovat komunikační matice projektu a obě smluvní strany se dohodly, že definování periody porad bude provedeno během inicializačního Kick-off střetnutí projektu.

Komunikace mezi Zadavatelem a Poskytovatelem bude probíhat e-mailem, telefonicky, osobně, či prostřednictvím videokonference. Všechny formy komunikace jsou rovnocenné.

Po zahájení projektu bude připraven komunikační plán pokrývající dohodnuté způsoby komunikace a komunikační plán projektu

Šablony projektových dokumentů

V rámci dodávky projektu budou použity dohodnuté šablony projektových dokumentů

a) Záznam/zápis z jednání týmu/projektového týmu
b) Zápis z jednání eskalační úrovně projektu
c) Požadavky na poskytnutí součinnosti ze strany Zadavatele
d) Žádost o změnu
e) Akceptační protokol/dokumentace

3.1.16.Nástroje řízení projektu

Hlavním nástrojem řízení projektu bude nástroj MS Project.

Nástroj MS Project bude sloužit jako hlavní zdroj plánu projektu a změny plnění v tomto plánu budou průběžně sledovány, obvykle jednou týdně. Smluvní strany budou využívat analytických dovedností těchto nástrojů, reportingu aktuálního harmonogramu a zobrazení případných prodlení.

Poskytovatel navrhne šablonu plánu projektu, vycházející z rozsahu práce požadované Zadavatelem. Tento plán se bude v průběhu projektu dále vyvíjet v závislosti na identifikaci nových úkolů a plnění původních. Plán se bude obvykle jednou týdně aktualizovat na základě informací od týmů a následně proběhne automatické plánování v závislosti na vzájemných vazbách projektu a vyvažování zatížení personálu tak, aby odrážel aktuální harmonogram projektu. V případě zjištění odchylek od plánu bude vedoucí projektu Poskytovatele spolupracovat s vedoucím projektu Zadavatele na řešení otázek personálního zajištění nebo plánování.

Využití nástroje automatického plánování a sledování projektu je důležité pro udržení kontroly nad projektem, což vedoucím projektu umožňuje vypracovávat odhady a řešit problémy s harmonogramem či zdroji dříve, než budou mít na projekt dopad.

3.1.17.Zápisy z porad projektového týmu

Ze všech pravidelných i nepravidelných střetnutí projektového týmu, řídicího výboru a zároveň ze všech ad-hoc setkání členu projektového týmu budou vznikat zápisy z porad. Tyto zápisy budou vypracované určeným členem projektového týmu. Forma zápisu bude obvykle elektronická. Zápis bude po schválení doručen vedoucímu týmu Poskytovatele, který zabezpečí distribuci zápisu podle dohodnuté komunikační matice na příslušné členy projektového týmu a zabezpečí uložení tohoto zápisu k projektové dokumentaci v nezměněné podobě.

3.1.18.Popis způsobů akceptace dílčích etap/celku

Akceptaci dílčí etapy i akceptace celku iniciuje vždy vedoucí projektu poskytovatele, který vyzve k akceptaci vedoucího projektu zadavatele. O provedené akceptaci dílčí etapy bude proveden písemný záznam. V případě, že zadavatel stanoví, použije se přiměřeně článek č. 9 Smlouvy.

Akceptace celku bude provedena v souladu s článkem č. 9 Smlouvy a bude zahrnovat požadavky zadavatele, které stanovil v kapitole pro akceptaci řešení. (viz. kap. 3.5 Akceptační kritéria implementace)

3.1.19.Inicializační střetnutí projektu – kickoff

Nejdéle do 5ti pracovních dní od nabytí účinnosti smlouvy iniciuje a do 9ti pracovních dní od nabytí účinnosti smlouvy realizuje Poskytovatel úvodní projektové setkání, tzv. projektový kickoff. Na tomto setkání bude ustanoven a bude definováno obsazení Řídícího výboru projektu. Řídící výbor následně potvrdí iniciální harmonogram projektu, proces pro řízení změn, proces pro řízení rizik, proces pro řízení problémů, eskalační proceduru a komunikační plán projektu – tedy **Základní popis principu řízení projektu** a zaváže pracovníky projektu a řídící pracovníky projektu k jejich dodržování.

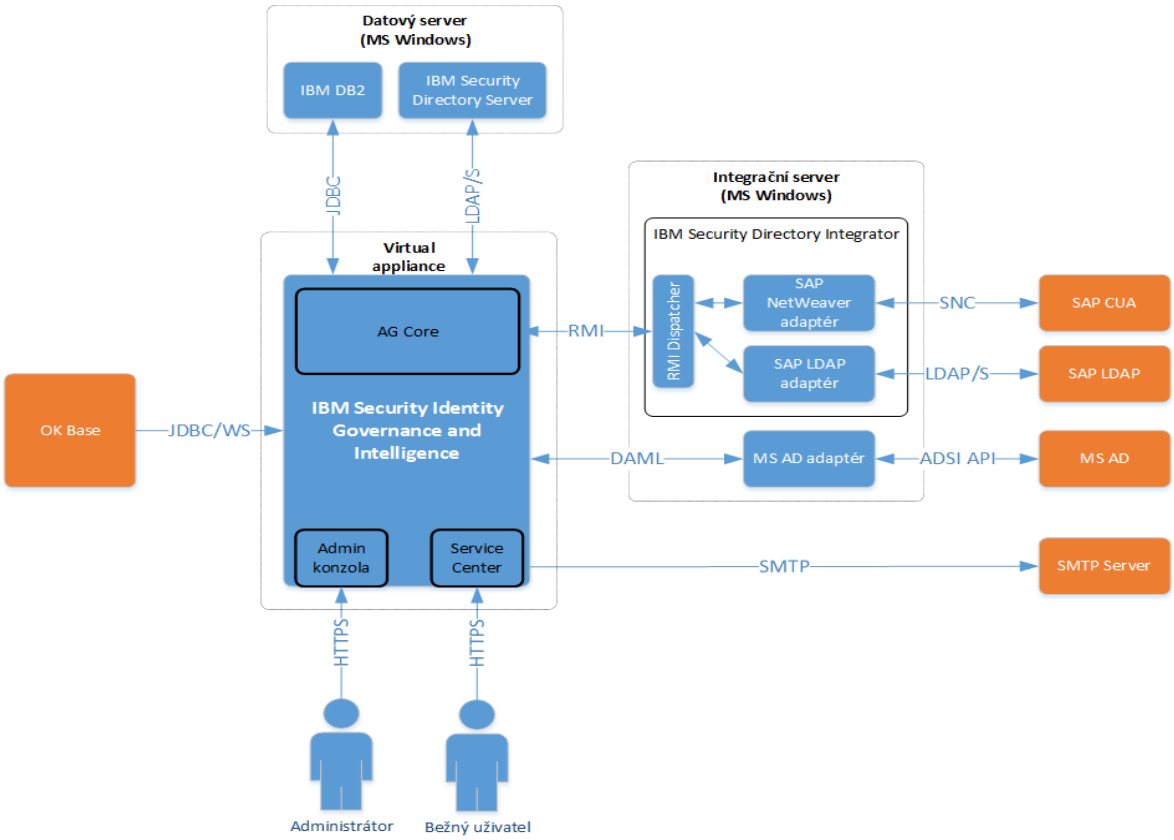
3.2.DETAILNÍ SPECIFIKACE IMPLEMENTACE

3.2.1. Základní architektura řešení

Jádrem dodávaného řešení je software IBM Security and Intelligence. Na níže uvedeném diagramu je uvedena předpokládaná architektura řešení a níže v textu jsou popsány jednotlivé části a jejich základní funkcionalita. Obě strany se dohodly, že finální verze Architektury bude představena Zadavateli v rámci fáze analýzy a bude Zadavatelem schválena.

IBM Security Identity Governance and Intelligence (aktuální verze 5.2.6)

IBM Security Identity Governance and Intelligence (IGI) je strategickou platformou IBM pro oblast řízení přístupů a governance (IGA), poskytuje zabezpečené automatizované řešení založené na politikách, které pomáhá efektivně spravovat uživatelské účty, přístupová oprávnění a hesla od vytvoření až po vyřazení v kompletním prostředí IT systémů. IGI pomáhá automatizovat procesy tvorby a poskytování nebo odmítnutí uživatelských oprávnění po celý životní cyklus uživatele.



Obrázek 2 – High level architektura řešení

Základní vlastnosti a schopnosti IGI

IBM Security Identity Governance and Intelligence (IGI) poskytuje bezpečné, automatizované řešení založené na politikách, které pomáhá efektivně spravovat uživatelské účty, přístupová oprávnění a hesla od vytvoření až po vyřazení v kompletním prostředí IT systémů. IGI pomáhá automatizovat procesy tvorby a poskytování nebo odmítnutí uživatelských oprávnění po celý životní cyklus uživatele. Některé klíčové funkcionality jsou uvedeny níže:

- IGI poskytuje identity governance infrastrukturu s ohledem na business prostředí a business požadavky – nejedná se tedy pouze o IT pohled na tuto problematiku.
- Prostřednictvím IGI modulu Access Governance Core může administrátor řešení definovat a spravovat organizační strukturu, uživatele, účty, role, oprávnění, spravované systémy a aplikace. Tento modul umožňuje modelovat organizaci z pohledu řízení přístupu a provozních procesů.
- Zároveň je možné automatizovat procesy životního cyklu (vytváření, modifikace a mazání) přístupů pro uživatele. K dispozici jsou auditní záznamy a detailní reporty, pravidelné recertifikace oprávnění a detekce a oprava účtů, které jsou v rozporu s politikami.
- Segregation of Duties (SoD) v rámci IGI podporuje koncept, jehož cílem je zabezpečit správu konfliktních oprávnění, respektive business aktivit. Uživatel nemůže standardně získat konfliktní oprávnění do systémů a aplikací – IGI považuje porušení SoD za specifický typ rizika. Podpora správy tohoto typu rizika je k dispozici v rámci IGI modulu Access Risk Controls.
- Pokud jde o SAP SoD, IBM poskytuje integrovanou podporu pro správu rolí s předdefinovanými pravidly až po úroveň transakcí SAP a autorizačních objektů. Konflikty mohou být snadno objeveny a popsány v rámci podnikatelského kontextu s využitím modelovacího přístupu založeného na činnostech. Díky granulární podpoře pro prostředí SAP i non-SAP je možné snížit náklady na řízení SoD v rámci celé organizace.

- Navíc IGI nabízí analýzu pravidel SoD v reálném čase a umožňuje organizacím průběžně monitorovat případné konflikty. Posouzení rizik může být součástí pracovního postupu žádosti o přístup, kdy mohou být konfliktní žádosti automaticky zamítnuty, eskalovány, případně povoleny jako výjimky. Kontrola SoD v reálném čase pomáhá zaměřit pozornost na oblasti, které představují největší riziko.

Access Governance Core

- Access Governance Core (AGCore alias AGC) je základní modul celého řešení. Využívají ho i ostatní moduly. Jeho cílem je správa základních objektů celého řešení – uživatelů, rolí, organizační struktury či integrovaných aplikací, ve kterých IGI spravuje účty a oprávnění. Poskytuje konfigurační možnosti, správu objektů, monitorování, nástroje pro hromadný import dat či definici notifikací prostřednictvím e-mailů a SMS.

Grafické prostředí a samoobslužný portál

IGI používá dvě moderní grafická webová rozhraní:

- **Administration Console**

  Administrační konzole je určená především administrátorům IGI. Poskytuje všechny nástroje potřebné pro administraci aplikace IGI formou přístupu k jednotlivým IGI modulům.

- **Service Center**

  Toto rozhraní je určené pro koncové uživatele, včetně manažerů. Poskytuje přístup k žádostem, schválením, recertifikacím či reportům. Slouží i jako samoobslužný portál. Zaměstnanci mohou využít samoobslužný webový portál pro změnu svého hesla a k aktualizaci bezpečnostních otázek. Mohou také nahlížet na status požadavku na změnu hesla. Samoobslužný portál také umožňuje zaměstnancům zobrazit dostupná oprávnění, případně požádat o udělení nového oprávnění. Tyto žádosti jsou poté dle nastaveného workflow schvalovány. Prostředí je intuitivní a vzhledem k používání modelu business rolí i srozumitelné, noví uživatelé si tak dokážou zažádat o přístupy bez nutnosti asistence Help Desku nebo manažera.

Datový server

- **Relační databáze**

  IGI umožňuje použít interní PostgreSQL nebo externí databázový systém (DB2 nebo Oracle). Interní databáze je určená i pro produkční použití. Zjednodušuje celkové náklady na administraci řešení, protože v tomto případě nejsou potřeba žádné DBA znalosti. Na druhou stranu však neumožňuje detailní konfigurační možnosti jako externí databáze, protože PostgreSQL je integrální součástí IGI VA. Obě smluvní strany se dohodly, že definitivní rozhodnutí o nasazení DB2 bude potvrzeno během fáze analýzy.

- **Directory Server**

  Komunikace se spravovanými systémy vyžaduje adresářový server (LDAP), do kterého si adaptéry ukládají informace týkající se rekonciliace. Podporovaný je IBM Security Directory Server (ISDS).

Integrační server

Integrační server je centrální komponenta zajišťující integraci na zdrojové a cílové systémy. Zdrojovým systémem pro informace týkající se identit bude OK Base systém, na který se z pohledu technologického bude přistupovat prostřednictvím JDBC rozhraní/protokolu. Cílovými systémy budou

Microsoft Active Directory a SAP CUA/LDAP. Pro tyto systémy se budou v rámci integrace používat standardní adaptéry, které jsou pro takový typ integrace již vytvořeny.

- Active Directory: *IBM Security Identity Adapter for Windows AD*
- SAP CUA: *IBM Security Identity Adapter for SAP NetWeaver*
- SAP LDAP: *IBM Security Identity Adapter for LDAP*

Uvedené adaptéry cílových systémů jsou součástí dodávaného řešení. RMI Dispatcher je součástí integračního frameworku adaptérů.

Obě strany se dohodly, že plnou integrací je chápáno napojení na systémy za účelem komunikace a zjišťování nebo propagaci rolí, vlastností, atributů a dalších parametrů. Toto nastavení bude popsáno v rámci analýzy a obě strany jej budou moci připomínkovat a následně akceptovat v dalších fázích projektu. Plná integrace musí zajistit takové napojení systémů (zdrojových i cílových), aby byla zajištěna akceptace řešení tak, jak je stanoveno v kapitole 0 – Akceptační kritéria implementace.

Zdrojový systém

OK Base je pro SZIF systém klíčovým zdrojem správy identit a informací o

- Interních identitách
- Organizační struktuře

Dodávané řešení bude přistupovat k datům uloženým v OK Base prostřednictvím JDBC nebo Web services rozhraní a předpokládá se, že bude obsahovat všechna data, metody nebo služby pro úspešnou integraci a propagaci na cílové systémy.

Cílové (spravované/manažované) systémy

Cílové systémy jsou systémy/aplikace, v kterých dodávané řešení spravuje účty a oprávnění. Tak jak bylo uvedeno v odstavci týkajícím se komponenty *Integrační server*, se v rámci implementace cílových systémů předpokládá integrovat a napojit tyto cílové systémy:

- Microsoft Active Directory
- SAP LDAP
- SAP CUA

SMTP Server

SMTP server slouží jako brána pro odesílání emailových upozornění/notifikací při různých událostech v rámci systému správy identit.

3.2.2. Způsob instalace ve virtuálním prostředí Objednatele

Dodávané řešení je složeno z více komponent. Jednotlivé komponenty jsou popsány níže. Zároveň se obě strany dohodly, že všechny technické požadavky a celkový rozsah implementovaných komponent a parametrů bude v rámci fáze Analýzy revidován a bude zpřesněn dle zjištěných informací a stavu. U všech komponent jsou uváděny doporučené konfigurace, které se mohou měnit.

IBM Security Identity Governance and Intelligence

IGI bude instalováno ve formě Virtual Appliance na platformě Hyper-V. Na základě dohody obou smluvních stran, bude během fáze Analýzy upřesněno cílové nasazení IBM IGI. Doporučené předpoklady jsou uvedeny níže.

- Instalovaná verze IGI: aktuálně dostupná v čase instalace
- Virtualizace: Hyper-V

- Produkční prostředí
    - CPU: 16 cores
    - RAM: 256 GB
    - Disk: min 150 GB
    - NIC: 3 ks (1 Gbps)
- Testovací a Vývojové prostředí
    - CPU: 4 cores
    - RAM: 16 GB
    - Disk: min 150 GB
    - NIC: 3 ks (1 Gbps)

Datový server

Na základě dohody obou smluvních stran bude během fáze Analýzy upřesněno cílové nasazení Datového serveru. Operační systém datového serveru je Microsoft Windows Server (tento může být virtualizován např. Hyper-V dle možností Zadavatele). Instalované budou aktuálně platné a podporované verze dvou následujících produktů:

- IBM DB2
- IBM Security Directory Server

Licence, instalaci a konfiguraci operačního systému MS Windows Server zajišťuje Zadavatel. Doporučené předpoklady pro instalaci datového serveru:

- Operační systém: MS Windows Server
- Produkční prostředí
    - CPU: 6 cores
    - RAM: 48 GB
    - Disk: min 250 GB
    - NIC: 1 ks (1 Gbps)
- Testovací a Vývojové prostředí
    - CPU: 4 cores
    - RAM: 16 GB
    - Disk: min 250 GB
    - NIC: 1 ks (1 Gbps)

Integrační server

Na základě dohody obou smluvních stran bude během fáze Analýzy upřesněno cílové nasazení. Operační systém integračního serveru je Microsoft Windows Server (tento může být virtualizován např. Hyper-V dle možností Zadavatele). Instalované budou aktuálně platné a podporované verze následujících produktů:

- IBM Security Directory Integrator
- IBM Security *Identity Adapter RMI Dispatcher for Security Directory Integrator v7.x*
- Adaptér *IBM Security Identity Adapter for Windows AD*
- Adaptér *IBM Security Identity Adapter for SAP NetWeaver*
- Adaptér *IBM Security Identity Adapter for LDAP*

Doporučené předpoklady pro instalaci integračního serveru:

- Operační systém: MS Windows Server (poskytne Zadavatel)
- Produkční prostředí
    - CPU: 4 cores
    - RAM: 16 GB
    - Disk: min 250 GB
    - NIC: 1 ks (1 Gbps)
- Testovací a Vývojové prostředí

- CPU: 2 cores
- RAM: 8 GB
- Disk: min 250 GB
- NIC: 1 ks (1 Gbps)

Celkové nároky a přesné specifikace budou upřesněny v rámci Fáze 1 – Architektura prostředí.

3.2.3. Způsob integrace IDM nástroje na systémy, které budou na IDM nástroj napojeny v rámci integrace a způsob komunikace mezi všemi těmito systémy

V následující části jsou uvedené informace, systémy a popisy integrací, které je možné v rámci analýzy řešení dále upřesňovat.

Základní a klíčovou komponentou pro nasazení a řešení problému s managementem identit v rámci organizace je navržený produkt společnosti IBM, Identity Governance and Intelligence, který je plně schopen řešit všechny požadavky na správu a management identit, včetně řešení problému se Segregation of Duties *(v rámci významu jde o slovníkově stejný pojem jako Separation of Duties)*, Campaigns apod ... Detailní funkcionalitu popisují následující kapitoly.

Při implementaci a integraci systému pro správu identit, jsou navržené procesy zcela klíčové. Obě strany se dohodly, že navrhované procesy pro implementaci celého řešení správy identit, které Zadavatel předložil, budou použité jako základ pro analýzu řešení centrální správy identit a pro správné nastavení v rámci design fáze řešení. Poskytovatel bude z těchto procesů vycházet a vyvine maximální úsilí pro zajištění integrace v rámci navrženého řešení. Zároveň se obě strany dohodly, že i přesto může dojít k situaci, která znemožní nasazení navrhovaného procesu v původních parametrech a ten bude muset být v těchto parametrech modifikován na straně Zadavatele, případně bude jeho implementace modifikována Poskytovatelem. Taková změna bude zanesena do kontrolní knihy projektu (PCB).

Obě smluvní strany jsou si vědomy, že implementace procesů je úzce spjata s technickými možnostmi řešení a spoléhá se na funkcionalitu navrženého řešení a jsou známé jeho limitace. Obě strany se dohodly, že jediným vyvíjeným adaptérem pro integraci zdrojových a cílových systémů bude adaptér na HR systém (zdrojový systém), který není v rámci navrhovaného řešení standardně vyvinutým adaptérem od vendora řešení. Ostatní systémy (cílové) budou připojeny prostřednictvím standardních adaptérů, které jsou poskytnuty vendorem řešení a to v posledních verzích.

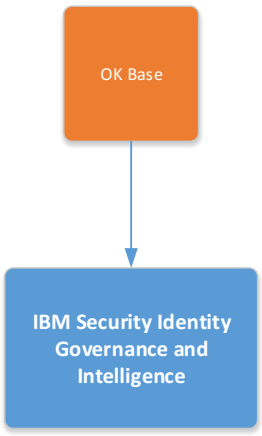
V rámci analýzy bude provedena Poskytovatelem revize interních procesů a možností nasazení adaptérů na systémy. Na základě zjištění z analýzy se obě strany dohodnou na dalším postupu implementace.

Rozhodnutí a návrhy implementací musí být stanoveny nejpozději během fáze Analýzy a odsouhlaseny oběma smluvními stranami.

Jak již bylo uvedeno základní komponentou je produkt IBM Identity Governance and Intelligence.
Níže jsou uvedeny zcela základní prvky a funkcionality, které mají poskytnout Zadavateli představu o produktu a navrženém řešení.

Zdrojový systém - OK Base

JDBC zdroje identit (v tomto je HR systémem řešení OK Base) je možné integrovat přímo do IGI prostřednictvím ovladače JDBC tak, jak je zobrazeno na obrázku níže. Mapování atributů mezi zdrojem (OK Base) a cílem (IGI) je součástí vlastní integrace a bude popsáno v Analýze. Předpoklad napojení a využití JDBC ovladače bude potvrzen, případně modifikován během analýzy řešení.



Obrázek 3 – Schéma napojení zdrojového systému

Řízení cílových systémů

Integrace systémů automatizuje proces sběru dat z cílových systémů a odráží změny provedené v IGI v těchto cílových systémech. Tyto systémy jsou uživatelské repositáře uchovávající informace o účtech.

IGI poskytuje dvě metody integrace s cílovými systémy, a to s použitím Identity Brokerage Adapters nebo Enterprise Connectors.

Identity Brokerage je brána pro přímou integraci IGI s cílovými systémy pomocí IBM Security Identity Adapters. Flexibilní architektura systému IGI umožňuje používat adaptéry dvěma způsoby:

- Instalace kódu (adaptéru) přímo na řízenou platformu, která poté komunikuje se serverem řešení IGI a provádí příkazy místně pomocí nástrojů nativní správy nebo API volání spravovaného cíle.
- Instalace kódu (adaptéru) na vzdálený systém (systém proxy), který obsahuje nástroje pro správu pro daný cílový systém. Tento přístup se často používá v databázových prostředích, kde je proxy systémem oddělený od databázového serveru, nebo tam, kde nemusí být žádoucí nainstalovat kód adaptéru přímo na spravovaný cíl.

Při administraci cílových systémů je možné provádět:

- Import profilu systému
- Import mapování atributů účtu
- Konfiguraci výchozích atributů účtu
- Vyhledávání, přidávání, modifikování a mazání systémů
- Rekonciliaci

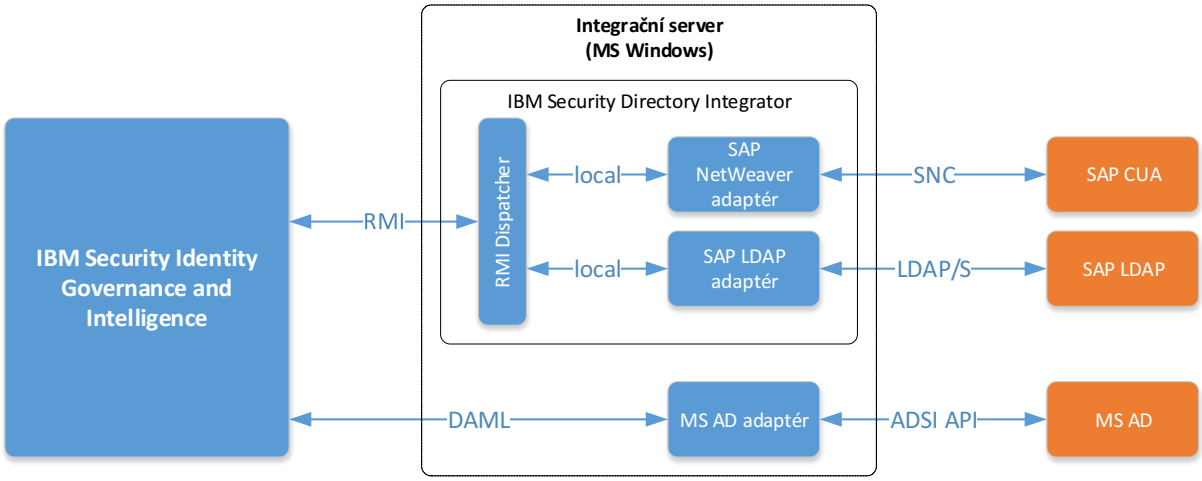
Enterprise Connectors je vhodné použít k integraci systémů, které Identity Brokerage nepodporuje. Jedná se například o některé HR systémy nebo CSV soubory.

Obě strany se dohodly, že v rámci procesu integrace systému do prostředí SZIF bude použita pro integraci cílových systémů Identity Brokerage, Zároveň se strany dohodly, že v průběhu analýzy může být toto upraveno. S *IBM Security Identity Governance and Intelligence* je k dispozici skupina adaptérů pro několik desítek často používaných systémů a aplikací. V prostředí SZIF budou implementované následující adaptéry, pro jednotlivá prostředí:

- *1ks IBM Security Identity Adapter for Windows AD*

- *1ks IBM Security Identity Adapter for SAP NetWeaver*
- *1ks IBM Security Identity Adapter for LDAP*

Způsob integrace a použití a související protokoly jsou zobrazené na níže uvedeném obrázku.



Obrázek 4 – Schéma napojení cílových systémů

SAP Adaptéry

- SAP NetWeaver adaptér komunikuje s SAP prostřednictvím SNC (Secure Network Communication). Umožňuje integraci v CUA a NON-CUA módu. Implementace v prostředí SZIF předpokládá nasazení v CUA módu. Konfiguraci na straně SAP zajišťuje Zadavatel, dle pokynů Poskytovatele.
- LDAP adaptér bude komunikovat se SAP LDAP prostřednictvím zabezpečeného LDAPS protokolu. Detaily SAP LDAP objektů (účty, oprávnění) poskytne Objednavatel v rámci analýzy.

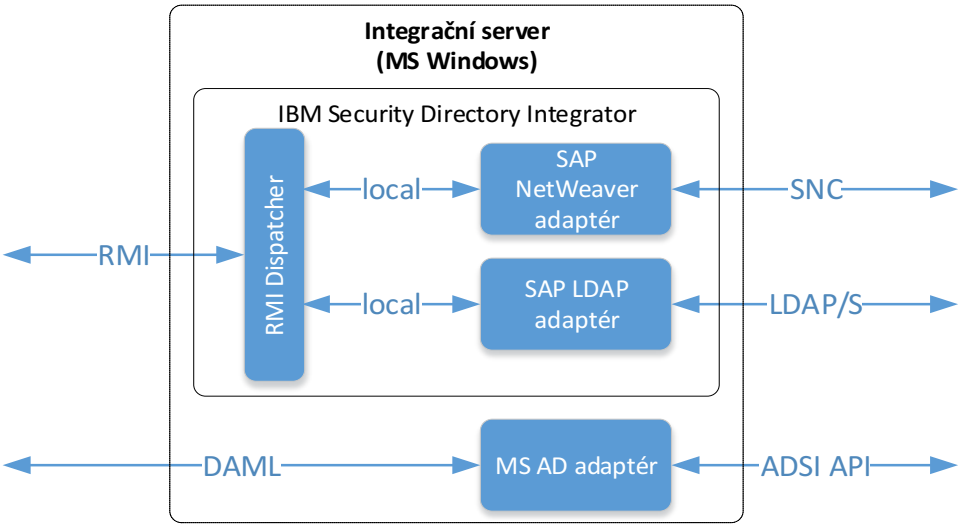
MS AD adaptér

- MS AD adaptér komunikuje s IGI prostřednictvím DAML (Directory Access Markup Language) protokolu zajištěného X.509 certifikáty. Adaptér běží jako Windows služba a s doménou komunikuje prostřednictvím Microsoft ADSI (Active Directory Service Interfaces) API.

Obě strany se dohodly, že budou použity pouze adaptéry, které jsou uvedeny výše v popisu řešení. Zároveň pak, že implementace adaptérů bude provedena dle analýzy. Zadavatel souhlasí, že poskytne všechny X.509 certifikáty, na základě specifikace a podkladů, které budou upřesněny v rámci analýzy. Obě strany si jsou vědomy možných dopadů při těchto změnách.

Security Directory Integrator

Tato interní univerzální integrační platforma *IBM Security Directory Integrator* (SDI) je základem pro implementaci a napojení cílových systémů v prostředí SZIF. Obecně je v prostředí IGI umožněn vývoj IGI adaptérů, integrace na HR systém či integrace se SIEM.



Obrázek 5 – Schéma Integračního serveru

IBM Security Directory Integrator

SAP Netweaver a LDAP adaptér využívají společnou platformu pro vývoj a exekuci IGI adaptérů (*IBM Security Directory Integrator*). Předřazený *RMI Dispatcher* je server, který přijímá všechny požadavky na provisioning a distribuuje je na správný cílový adaptér. RMI komunikace bude zabezpečená prostřednictvím X.509 certifikáty. Obě strany se dohodly, že změny nasazení je možné provést během implementační analýzy. Komunikace mezi RMI Dispatcher a adaptéry je na lokální úrovni v rámci Java procesu.

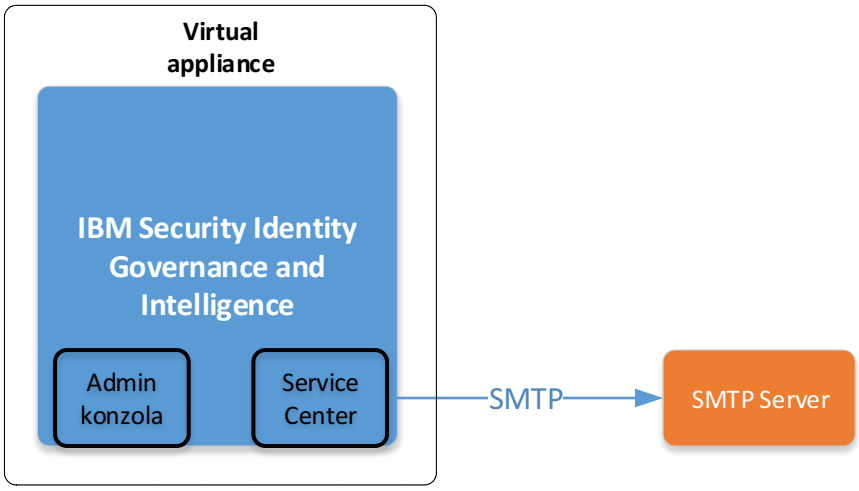
Integrační možnosti jsou téměř neomezené. Jakmile má integrovaná komponenta komunikační rozhraní, tak je IBM SDI schopný ho využívat. Má předdefinované velké množství konektorů pro běžné technologie – JDBC, LDAP, WebServices, AD, FTP, CLI, MQ, souborový systém apod. Zároveň je možné použít vlastní Java knihovny implementující potřebnou funkčnost.

Otevřenost znamená, že IBM SDI používá dobře zdokumentované principy a postupy, otevřené standardy a jednoduchý skriptovací jazyk – JavaScript. Pro vývoj stačí v tomto kontextu znalost principů – není potřebná znalost žádného proprietárního jazyka. Poskytovatel zároveň uvádí fakt, že výsledný „produkt" není kompilovaným kódem, ale konfiguračním XML souborem.

Jednoduchost vývoje souvisí se standardním Eclipse rozhraním, jednoduchým integračním konceptem, drag-and-drop možnostmi, a jak již bylo výše zmíněno, s použitím jednoduchého skriptovacího jazyka. Vývojář je odstíněný od specifik komunikačních technologií – nepotřebuje znát LDAP protokol a JNDI API na to, aby integroval adresářový server.

SMTP Server

Poslední součástí je SMTP server a jeho napojení pro odesílání notifikací jednotlivým uživatelům dle nastavení. Nejedná se vlastní integraci, jako spíše o využití stávajícího SMTP serveru, který již v organizaci běží a jeho využití na standardních portech pro zasílání zpráv.



Obrázek 6 – Schéma komunikace se SMTP serverem

3.2.4. Výčet jednotlivých kroků realizovaných v rámci implementace, který zahrnuje veškeré oblasti Implementace dle kapitoly 2.2 Přílohy č. 10 Zadávací dokumentace: Specifikace předmětu plnění a logickou následnost těchto kroků, aby bylo možné Implementaci realizovat.

Tato kapitola obsahuje veškeré oblasti Implementace dle kapitoly 2.2 Přílohy č.10 Zadávací dokumentace: Specifikace předmětu plnění a jejich logické následnosti a návaznosti těchto kroků. Jednotlivé činnosti specifikované v kapitole 2.2 Přílohy č.10 Zadávací dokumentace: Specifikace předmětu plnění se v rámci Fází mohou prolínat a proto jsou dle dohody obou smluvních stran detailněji popsány v návrhu Harmonogramu. Samotný návrh Harmonogramu bude dále upravován v rámci Analýzy, a následně bude schválen oběma smluvními stranami ve Fázi 1, bod 3.

Jednotlivé kroky realizované v rámci implementace jsou popsány v kapitole 3.3 Harmonogram implementace.

V této kapitole je uvedený stručný popis základních implementačních kroků, detaily jednotlivých kroků budou uvedeny v rámci projektového plánu po počáteční analýze. Součástí implementace jsou tři prostředí (DEV/TEST/PROD). Zadavatel zajistí prostředky pro instalaci těchto prostředí na základě detailní specifikace, která bude uvedena v analýze. Dále Zadavatel zajistí vlastní přípravu prostředí (zdrojové a cílové systémy) tak, aby byly v souladu s odpovídajícím zabezpečením a příslušnou legislativou. Zároveň se obě smluvní strany dohodly, že charakter plnění povinností vyplývajících ze ZoKB ze strany Poskytovatele a rozsah testů provedených v rámci implementace řešení, budou blíže specifikovány v průběhu fáze Analýzy řešení na základě vzájemné dohody mezi Zadavatelem a Poskytovatelem řešení. Poskytovatel bude průběžně v rámci Fáze 1 a 2 vytvářet uživatelskou a technickou dokumentaci, která bude finalizovaná ve Fázi 2, kapitole 4. Školení a akceptace

Fáze 0

Během této fáze bude svolán úvodní kickoff meeting, na kterém se představí implementační tým na straně Poskytovatele i Zadavatele a budou **navrženy a schváleny Základní principy řízení projektu**. Bude představen harmonogram, který se bude dále upřesňovat ze strany Zadavatele, postupy a další kroky, které jsou popsány v Metodice řízení projektu viz. kap.3.1

Fáze 1

V této fázi jsou zahrnuté aktivity související s implementací řešení definované v kapitole 2.2.1 a., 2.2.1 b., Přílohy č.10 Zadávací dokumentace: Specifikace předmětu plnění, blíže rozpracované v Harmonogramu plnění.

1. **Architektura prostředí**
   Cílem bude upřesnění a finalizace požadavků na řešení, vytvoření a zdokumentování základní architektury řešení v dokumentu „Architecture overview".

2. **Příprava/vytvoření vývojového prostředí**
   V rámci této aktivity dojde k instalaci a konfiguraci DEV prostředí (dle dohody se nainstalují všechna prostředí zároveň). Aktivity budou popsané v dokumentu „Installation and Configuration" a bude při této aktivitě nutná součinnost Zadavatele.

3. **Analýza a design řešení**
   Cílem je vytvoření detailní analýzy současného stavu a požadavků na řešení z dalších perspektiv, především z pohledu infrastruktury a výstupů a naplnění požadavků nutných pro akceptaci řešení.

   Infrastruktury

   - Integrace na OK Base
   - Integrace na SAP CUA, SAP LDAP a AD
   - Procesů životního cyklu
   - Schvalovacích procesů

   Výstupy budou zdokumentované ve dvou dokumentech:

   - Solution Requirements
   - Solution Design

Fáze 2

V této fázi jsou zahrnuté aktivity související s implementací řešení definované v kapitole 2.2.2 a 2.2.3, Přílohy č.10 Zadávací dokumentace: Specifikace předmětu plnění, blíže rozpracované v Harmonogramu plnění.

1. **Implementace**
   V rámci implementace probíhá více aktivit zároveň. Budou provedeny následující činnosti:
   - *Integrace HR systému*
     Vývoj integrace (adaptéru) na OK Base s cílem synchronizace informací o organizační struktuře a identitách/zaměstnancích.
   - *Procesy životního cyklu*
     Konfigurace procesů životního cyklu Identity v dodávaném řešení. JML (Joiner/Mover/Leaver), tzn. nástup nového zaměstnance, změna na pozici a ukončení pracovního poměru
   - *Integrace cílových systémů (Rekonciliace a Provisioning)*
     Dojde k instalaci a konfiguraci adaptérů pro správu účtů v cílových systémech
   - *Workflow*
     Dojde ke konfiguraci schvalovacího workflow
   - *Reporting/Sestavy*
     Nastavení reportingu.

   Instalační a konfigurační práce budou sepsány v dokumentu „Installation and Configuration"

2. **Testování**
   V této fázi jsou zahrnuté aktivity související s implementací řešení definované v kapitole 2.2.4, Přílohy č.10 Zadávací dokumentace: Specifikace předmětu plnění.
   Cílem testování bude vytvoření testovacího prostředí (instalace a konfigurace), přenos odpovídající části konfigurace z vývojového prostředí a provedení testů. Vlastní unit testy a

integrační testy provádí Poskytovatel v součinnosti se Zadavatelem. Akceptační testy naopak, provádí Zadavatel v součinnosti s Poskytovatelem.

3. **Nasazení do produkčního prostředí**
   V této fázi jsou zahrnuté aktivity související s implementací řešení definované v kapitole 2.2.6, Přílohy č.10 Zadávací dokumentace: Specifikace předmětu plnění.

   Během této aktivity bude vytvořené produkční prostředí (konfigurace) a přenesena odpovídající část konfigurace z testovacího prostředí.

   Do IDM řešení budou z OK Base synchronizované produkční informace o organizační struktuře a zaměstnancích. Z cílových systémů budou rekonciliací získané informace o účtech a oprávněních. Obě smluvní strany se dohodly, že plnou integrací na jednotlivé systémy se rozumí jednotlivé odsouhlasené kroky a postupy, které budou uvedeny v rámci odsouhlaseného projektového plánu a následně realizovány od DEV až na PROD prostředí.

4. **Školení a akceptace**
   V této fázi jsou zahrnuté aktivity související s implementací řešení definované v kapitole 2.2.5 Přílohy č.10 Zadávací dokumentace: Specifikace předmětu plnění.

   Budou vytvořené školící materiály dle aktuálních potřeb projektu a zrealizované školení pro Administrátory a koncové uživatele. Obě smluvní strany se dohodly, že rozsah jednotlivých kol školení bude maximálně v rozsahu 3 prac. dnů. Počet jednotlivých kol školení není omezen s ohledem na možnosti zapojování nových zaměstnanců na straně Zadavatele, nebo možnosti opakovaného přeškolení, či prohlubování znalostí zaměstnanců zadavatele. Na obsahu školení, který musí vycházet z akceptačních podmínek, se strany dohodnou v průběhu projektu před nasazením do produkčního prostředí. Zároveň se strany dohodly, že Školení „Řízení dalších úrovní uživatelských účtů (internetoví uživatelé)" bude realizováno dle stanovených technických možností a definovaných procesů. Zároveň se smluvní strany dohodly, že proběhne finalizace uživatelské a provozní dokumentace.

Jednotlivé aktivity budou vyžadovat ze strany Zadavatele součinnost ať už půjde o technické nebo, organizační aktivity. Více o součinnosti se věnuje kapitola č.3.4

Fáze 3

Během této fáze dojde k formálnímu potvrzení a akceptaci celého řešení na základě výsledků z provedeného testování a akceptačních testů.

Fáze 4

V rámci této fáze bude poskytována Post-implementační podpora tak, jak bylo specifikováno Zadavatelem. Během této fáze se budou řešit nestandardní stavy a chování systému, případně nesrovnalostí a nejasností vztahujících se k implementaci řešení.

3.3.HARMONOGRAM IMPLEMENTACE

Celkový termín realizace Implementace Dodávky je stanoven na maximálně **80 pracovních dní** ode dne nabytí účinnosti Smlouvy.

V rámci projektového plánu budou uvedeny finální termíny dle podpisu smlouvy a požadavků Zadavatele. Uvedený harmonogram je orientační, aby měl Zadavatel představu o jednotlivých úkolech, odhadované délce trvání a některých aktivitách součinnosti. Harmonogram bude upraven dle možností Zadavatele po vzájemném odsouhlasení.

Implementace bude realizována dle tohoto harmonogramu projektu:

Předpokládaný harmonogram je uveden v rámci příloh dokumentace a bude dále upřesňován během projektu. Celkově předpokládáme realizaci dle následujícího harmonogramu (bude upřesněno, potvrzeno a schváleno v projektovém plánu):

Název aktivity	Trvání až do	Zabezpečuje
Fáze č.0 - Kick-off meeting	T + 9	Poskytovatel, Zadavatel
Fáze č.1 - Analýza, design, architektura, příprava řešení	T + 55	Poskytovatel, Zadavatel
Fáze č.2 - Implementace, nasazení, testování, školení	T + 72	Poskytovatel
Fáze č.3 - Finální akceptace	T + 80	Zadavatel
Fáze č.4 - Post-implementační podpora	T + 120	Poskytovatel

Jednotlivé kroky a posloupnost jsou dány metodikou nasazení IDM systému a vychází z dlouhodobého, vyzkoušeného postupu a logických návazností. Některé z nich mohou být realizovány paralelně. Obě strany se dohodly, že harmonogram může být průběžně upravován v oblasti dílčích termínů během projektu, jak bylo uvedeno výše.

3.4.SOUČINNOST PRO ZAJIŠTĚNÍ IMPLEMENTACE

V rámci realizace Dodávky a Implementace bude ze strany Objednatele obecně zajištěna následující součinnost:

Obě smluvní strany se dohodly, že bez analýzy a dodatečných informací týkajících se prostředí Zadavatele, rolí, zkušeností (cílové systémy, verze, umístění, existence dokumentace, existence prostředí, efektivnost, možnosti využití dockers, apod.) není možné definovat předpokládaný objem požadovaných činností ani detailní specifikace. Poskytovatel proto uvádí seznam aktivit a činností, které bude nutné zajistit od Zadavatele, a tento bude během projektu doplňován na projektových schůzkách.

3.4.1. Požadavky na součinnost ZADAVATELE

Poskytovatel počítá s maximální možnou součinností Zadavatele v rozsahu:

Zadavatel, členové jeho týmu a jeho subdodavatelů budou v průběhu realizace dodávky a implementace poskytovat podporu pro nasazení IDM v pracovních dnech mezi 9-17 hodinou a nepřekročí rozsah:

- 1,5 FTE (Full Time Equivalent – při 8. hodinové pracovní době) zaměstnanců Objednatele po dobu realizace Dodávky a Implementace,
- 3 FTE (Full Time Equivalent – při 8. hodinové pracovní době) pracovníků dodavatelů, zajišťujících provoz a systémů (SAP, OK Base) integrovaných na nástroj IDM po dobu realizace Dodávky a Implementace.

Detailní specifikace požadované součinnosti v rámci jednotlivých etap projektu implementace bude upřesněna v rámci procesu řízení projektu implementace, a dle schválené Projektové dokumentace a Základního nastavení projektu. Níže jsou uvedeny základní požadavky na součinnost během jednotlivých fází projektu.

Ve fázi Kick off

a. Nominovat Výkonného pracovníka projektu Zadavatele
b. Nominovat Projektového manažera
c. Spolupracovat na přípravě kick-off
d. Nominovat projektový tým
e. Uspořádat kick-off meeting

Ve fázi Analýza

a. Zajistit aktivní účast na analytických schůzkách a workshopech (kvalifikovanými pracovníky pro danou oblast) a efektivní předání informací Poskytovateli v rozsahu nezbytném pro zpracování analýzy, zejména za oblasti:
    i. IT Security
    ii. IT Infrastruktura a provoz
        - Virtualizace (servery, storage)
        - OS administrace (RHEL, případně Windows)
        - Síťová administrace (FW prostupy)
        - Monitoring
        - Zálohování
    iii. IT správci integrovaných aplikací
    iv. HR
b. Rozsah dodávky předpokládá nejvýše 5 analytických setkání, každé v rozsahu max. 4 hodiny
c. Definovat požadavky na IDM procesy
d. Připomínkovat a schválit výstupy analýzy a návrhu
e. Zajištění analýzy. Modelování ani změna/optimalizace existujících rolí a oprávnění není součástí implementace,
f. Zjištění nastavení business rolí přes HR systém. Business role se nebudou přenášet.

Ve fázi Příprava a Nasazení řešení

Připravit virtuální infrastrukturu pro instalaci software, dle doporučení pro všechna prostředí.

a. Poskytnout nezbytnou součinnost IT (síťových administrátorů, správců VMware nebo Hyper-V, licencí OS, správců cílových systémů apod.)
b. Nastavit síťové prostupy popsané v detailním návrhu
c. Poskytnout vzdálený přístup pracovníků Poskytovatele k virtuálním strojům včetně přístupu na VMware/Hyper-V/KVM/XenServer konzoli.
d. Zadavatel poskytne nastavení (dokumentaci) a zajistí přípravu pro všechna prostředí, včetně testovacích instancí.
e. Zajistit součinnost na straně HR a cílových systémů. Zadavatel poskytne pro účely Identity Managementu přístup k aktuálním HR informacím o zaměstnancích jen v rozsahu, který je potřebný pro řízení přístupu a oprávnění v dodávaném řešení. Datový model bude dohodnut v rámci projektu.
f. Pro integraci na 3 cílové systémy (SAP LDAP, SAP CUA, MS AD (MS LDAP resp. LDAP),
g. Pro konfigurace zdrojového systému OK BASE, kde neexistuje standardní produktový adaptér, Zadavatel poskytne specifikaci rozhraní (datový model) a jednotlivých operací pro integraci na jedno prostředí daného systému. Typicky jde o následující operace:
    1. načítání účtů a oprávnění do IDM
    2. vytvoření/ modifikace/ smazání účtu
    3. aktivace/deaktivace účtu
    4. změna hesla
a. Odsouhlasení testovacích procedur
b. Spolupráce na dílčích testech

Ve fázi Implementace a Testování

a. Zajistit součinnost na straně HR a cílových systémů. Zadavatel poskytne pro účely Identity Managementu přístup k aktuálním HR informacím o zaměstnancích jen v rozsahu, který je

potřebný pro řízení přístupu a oprávnění v dodávaném řešení. Datový model bude dohodnut v rámci projektu.

b. Pro integraci na 3 cílové systémy (SAP LDAP, SAP CUA, MS AD (MS LDAP resp. LDAP),
c. Pro konfigurace zdrojového systému OK BASE, kde neexistuje standardní produktový adaptér, Zadavatel poskytne specifikaci rozhraní (datový model) a jednotlivých operací pro integraci na jedno prostředí daného systému. Typicky jde o následující operace:
    1. načítání účtů a oprávnění do IDM
    2. vytvoření/ modifikace/ smazání účtu
    3. aktivace/deaktivace účtu
    4. změna hesla
c. Odsouhlasení testovacích procedur
d. Spolupráce na E2E testech

Ve fázi Finální akceptace

a. Akceptace projektu
b. Převzetí do provozu

Průběžně po dobu implementace a nasazování, resp. celou dobu projektu

a. Zadavatele zajistí přístup a pracovní prostor v budovách, kde budou probíhat on-site aktivity
b. Umožnění vzdáleného přístupu a komunikace formou webové konference
c. Zajištění prostorů a audiovizuální techniky pro schůzky, školení a další jednání, kde je bude Poskytovatel požadovat (v prostorách Zadavatele)
d. Účast na školení a schůzkách dle stanoveného a dohodnutého termínu

Všeobecné předpoklady a ustanovení:

- Obě strany se dohodly, že cílem projektu je nasazení řešení Identity Management v prostředí Zadavatele, přičemž půjde o vybrané oblasti IGA:
    - Synchronizace s HR
    - Provisioning – technická integrace na vybrané cílové systémy
    - Schvalovací workflow pro žádosti o přístupy
    - Samoobslužné rozhraní pro žádosti o přístupy a schvalování přístupů
    - Ukázka nasazení business role pro automatické vytváření přístupů
    - Automatizace základních procesů životního cyklu identit (Joiner, Mover, Leaver)
    - Logování a auditování
- Obě strany souhlasí, že navržené řešení předpokládá maximální využití standardní funkčnosti produktu s minimalizací vývoje a zároveň se vývoj předpokládá pouze pro custom adapter pro integraci na HR systém.
- Zadavatel na začátku projektu nadefinuje stakeholdery pro oblast IDM, stejně jako projektový tým, který se bude na implementaci řešení podílet. Komunikační matici zajistí na základě těchto vstupů vedoucí projektu Poskytovatele.
- Způsob realizace projektu včetně procesu objednávání požadované součinnosti ze strany Objednatele, kdy minimální doba na zajištění požadované součinnosti bude do 3 pracovních dnů po vznesení konkrétního požadavku na součinnost ze strany Poskytovatele
- Obě strany se dohodly že, všechny licence a maintenance na instalovaný SW budou zajištěny dodávkou Poskytovatele. Jejich platnosti bude po dobu 5let od účinnosti smlouvy. (více viz kap.2)
- Zadavatel se zavazuje poskytnout licence dle kap.2 Poskytovateli v rámci součinnosti.
- Poskytovatel bude mít možnost komunikovat s podporou IBM jménem (pod ICN) Zadavatele
- Pro vzdálené videokonference zajistí Poskytovatel přístup na aplikace spol. CISCO Webex. Jestliže interní pravidla Zadavatele neumožňují použití této technologie, zajistí Zadavatel na vlastní náklady jinou technologii pro všechny členy týmu (případně licence), které je schválené Zadavatelem.
- Poskytovatel používá pro sdílené projektové dokumentace interní šifrované a zabezpečené úložiště BOX. Jestliže interní pravidla Zadavatele neumožňují použití tohoto cloud úložiště, zajistí Zadavatel na vlastní náklady jiné úložiště pro všechny členy týmu (případně licence),

které je schválené Zadavatelem ke sdílení dokumentace a je možné jej provozovat na operačních systémech MacOS a Microsoft Windows 10.

- V případě blokujícího problému, čekání na schválení ze strany Zadavatele, neposkytnutí součinnosti během implementace ze strany Zadavatele je nutné harmonogram projektu prodloužit o dobu řešení tohoto problému. Stejně tak v rámci podpory po tuto dobu musí být Poskytovateli pozastaven běh SLA.
- Podpora a veškeré aktivity týkající se instalace a integrace na cílové a zdrojové systémy, zajištění součinnosti na straně systémů mimo IGI, Directory Integrator a Directory Server budou zajištěny (zprostředkovány) Zadavatelem
- Zadavatel nebude zadržovat, ani zdržovat žádný z jednotlivých úkolů, které na něj budou kladeny pro úspěšné dodání projektu. Zadavatel vyvine maximální úsilí při řešení nestandardních situací nebo situací vyžadujících jeho aktivní součinnost.
- Místem dodávky služeb je Praha a služby budou poskytovány v CZ pracovní době (Po Pá 9:00 až 17:00, mimo státních svátků v ČR).
- Služby budou poskytovány primárně přes vzdálený přístup.
- Zadavatel zajistí veškeré přístupy do míst, kde se předpokládá plnění díla. Tyto přístupy budou zřízeny neprodleně při sestavení projektového týmu.
- Obě strany se domluvily, že předpokládaný objem prací, stanovený v rámci součinnosti vyžadované poskytovatelem, nepřekročí maximální požadavek stanovený zadavatelem v této příloze smlouvy.

Součinnost bude v průběhu realizace dodávky a implementace poskytována výhradně v pracovní dny mezi 9-17 hodinou a nepřekročí rozsah:

- 1,5 FTE (Full Time Equivalent – při 8. hodinové pracovní době) zaměstnanců Objednatele po dobu realizace Dodávky a Implementace,
- 3 FTE (Full Time Equivalent – při 8. hodinové pracovní době) pracovníků Dodavatelů, zajišťujících provoz a systémů (SAP, OK Base) integrovaných na nástroj IDM po dobu realizace Dodávky a Implementace.

Detailní specifikace požadované součinnosti v rámci jednotlivých etap projektu implementace bude upřesněna v rámci procesu řízení projektu implementace dle schválené Projektové dokumentace a Základního nastavení projektu.

3.5.AKCEPTAČNÍ KRITÉRIA IMPLEMENTACE

V průběhu realizace projektu Implementace budou v rámci projektové dokumentace konkretizována akceptační kritéria Implementace, na základě kterých bude potvrzena úspěšná Implementace nástroje IDM.

Projektově stanovená akceptační kritéria potvrdí:

- Úspěšnou instalaci nástroje IDM a souvisejícího SW vybavení na výpočetních prostředcích Objednatele
- Vytvoření tříúrovňové architektury IDM nástroje:
    - Vývojové prostředí
    - Testovací prostředí
    - Produktivní prostředí
- Plnou integraci na HR systém Objednatele (OK Base)
- Plnou integraci na Microsoft Active Directory prostředí Objednatele
- Plnou integraci na správu uživatelů v IS SAP Objednatele
- Připravenost prostředí nástroje IDM pro:
    - Další integraci na dílčí moduly IS SAP včetně popisu budoucí realizace integrace nástroje IDM
    - Další integraci na interní podpůrné systémy zajišťující výkon činností Objednatele nezbytných pro naplnění ISMS (Information Security Management System) v souladu s ISO 27001:
        - Adonis NP – systém pro správu procesního modelu SZIF
        - ARM – systém řízení rizik
        - Primavera – Systém pro řízení projektů
        - Cognos – webové a BI služby
    - Zajištění realizace procesů správy identit a údajů uživatelů IS SZIF prostřednictvím nástroje IDM tak, aby nástroj po provedení do provozu umožňoval standardní správu v následujících oblastech:
        i. Řízení business služeb a business procesů – nástroj bude připraven pro definici, správu business procesů, business rolí a budoucí integraci s nástrojem pro správu procesů.

        ii. Řízení uživatelských účtů a oprávnění na úrovni Microsoft technologií – kromě integrace s Microsoft Active Directory bude nástroj připraven pro obecnou integraci a správu Microsoft prostředí (typicky Microsoft 365/Azure AD, Exchange).

        iii. Řízení uživatelských účtů na úrovni LDAP – příprava nástroje pro řízení uživatelských účtů na úrovni LDAP.

        iv. Řízení dalších úrovní uživatelských účtů (internetoví uživatelé) – příprava nástroje pro správu internetových uživatelů, vytvoření definice identit s customizací pro evidenci atributů internetových uživatelů a žadatelů.

        v. Realizace scénářů správy identit (interních, externích, internetových uživatelů)
            - Součástí implementace IDM bude definice scénářů pro správu identit – založení, změna, dočasná změna, vytvoření nového týmu, vytvoření technické organizační struktury, přiřazení identity do technické organizační struktury; příprava základních schvalovacích schémat pro definované scénáře včetně přípravy prostředí pro administrátory i ostatní uživatele IDM nástroje.

vi. Realizace scénářů pro logování a monitoring včetně monitorování konfliktů oprávnění
   - Součástí implementace IDM bude nastavení základního monitoringu pro logování:
      a. Jakýchkoliv změn na úrovni uživatele/identity/přístupových oprávnění
      b. Systémových operací automaticky realizovaných IDM nástrojem
      c. Operací prováděných administrátory IDM nástroje
      d. Činností prováděných uživateli v IDM nástroji

vii. Řízení správy organizačních struktur včetně definice různých typů organizačních struktur (tvorba technických struktur nezávislých na organizační struktuře organizace dle definovaných parametrů).

- Plnou funkčnost nástroje IDM včetně plné integrace s ověřením následujících produktivních procesů:
   a. Nástup zaměstnance do pracovního/služebního poměru na dané místo v organizační struktuře:
      i. Zaměstnanec ještě nemá identitu v SZIF – nový zaměstnanec
      ii. Zaměstnanec již má identitu v SZIF – návrat zaměstnance na SZIF po přerušeném/ukončeném pracovním/služebním poměru

   b. Nástup zaměstnance do pracovního/služebního poměru na neurčené místo v organizační struktuře:
      i. Zaměstnanec ještě nemá identitu v SZIF – nový zaměstnanec
      ii. Zaměstnanec již má identitu v SZIF – návrat zaměstnance na SZIF po přerušeném/ukončeném pracovním/služebním poměru

   c. Změna pracovního/služebního poměru zaměstnance
      i. Přeřazení zaměstnance na jinou pozici – trvale/dočasně
      ii. Rozšíření/zúžení přístupových práv zaměstnance na základě změny pracovního/služebního poměru (např. rozšíření po splnění zkoušek státního zaměstnance)

   d. Ukončení pracovního/služebního poměru zaměstnance – trvalé/dočasné

   e. Změna organizační struktury organizace
      i. Přesun organizační jednotky v rámci stávající organizační struktury
      ii. Vznik/zánik organizační jednotky bez dopadu/s dopadem na stávající zaměstnance
      iii. Změna náplně v rámci dané organizační jednotky (změna rolí, které mohou zaměstnanci v dané organizační jednotce zastávat)
      iv. Přečíslování organizačních jednotek v rámci organizační struktury

- Plná funkčnost nástroje IDM v oblastech:
   - Plná dostupnost a funkčnost prostředí pro administrátory včetně fungování procesů správy uživatelů, identit, rolí, oprávnění, organizačních struktur
   - Plná dostupnost prostředí pro uživatele
   - Plná datová kompatibilita, tj. správnost dat v nástroji na základě ověření aktuálních dat v HR systému, MS AD a CUA SAP
   - Plná funkčnost realizovaných scénářů
   - Plná funkčnost přenosu customizací z vývojového prostředí na produkci.

- Integrace na jednotlivé systémy a jejich prostředí v rozsahu testovací a produktivní prostředí
- Plná funkčnost monitoringu prováděných operací

- Vytvoření a předání dokumentace obsahující:
    a. Kompletní projektovou dokumentaci k implementaci nástroje v českém jazyce

    b. Dokumentaci nastavení systému zahrnující protokoly o instalaci, provedení provozních, integračních, bezpečnostních testech, dále dokumentaci o realizovaných customizacích a nastavení IDM nástroje v českém jazyce

    c. Administrátorskou dokumentaci popisující procesy administrátora z hlediska technického nastavení nástroje IDM i z hlediska obsluhy aplikační vrstvy nástroje IDM

    d. Uživatelskou dokumentaci popisující ovládání nástroje IDM administrátory

    e. Uživatelskou dokumentaci popisující ovládání nástroje IDM koncovými uživateli v českém jazyce.

V rámci Implementace bude rovněž zajištěno:

- Komplexní proškolení administrátorů IDM v rozsahu:
    a. Kompletní administrátorské činnosti správy IDM nástroje – instalace, konfigurace, integrace, údržba, patchování, zálohování

        Součástí bude proškolení interních administrátorů IDM nástroje zadavatele v rozsahu, který Zadavateli umožní zajistit kompletní administraci a provoz nástroje.

    b. Implementace řízení business služeb a business procesů

        Součástí bude proškolení interních administrátorů IDM nástroje zadavatele na správu business služeb a procesů v nástroji IDM včetně proškolení na zajištění integrace prostřednictvím webových služeb.

    c. Řízení uživatelských účtů a oprávnění na úrovni Microsoft technologií – primárně Microsoft Active Directory

        Součástí bude proškolení administrátorů IDM nástroje pro správu účtů a oprávnění v MS AD prostřednictvím nástroje IDM.

    d. Řízení uživatelských účtů na úrovni LDAP

        Součástí bude kompletní proškolení interních administrátorů IDM nástroje zadavatele na řízení uživatelských účtů na úrovni LDAP.

    e. Řízení dalších úrovní uživatelských účtů (internetoví uživatelé)

        Součástí bude kompletní proškolení interních administrátorů IDM nástroje zadavatele na realizaci scénářů správy přístupů internetových uživatelů

    f. Realizace scénářů správy identit (interních, externích, internetových uživatelů)

        Součástí bude kompletní proškolení interních administrátorů IDM nástroje zadavatele pro zajištění administrace scénářů pro správu identit minimálně v rozsahu připravenosti nástroje.

g. Realizace scénářů pro logování a monitoring včetně monitorování konfliktů oprávnění

Součástí bude kompletní proškolení interních administrátorů IDM nástroje zadavatele na správu IDM nástroje v oblasti logování a monitoringu včetně vyhodnocování monitorovaných informací:

i. Jakýchkoliv změn na úrovni uživatele/identity/přístupových oprávnění
ii. Systémových operací automaticky realizovaných IDM nástrojem
iii. Operací prováděných administrátory IDM nástroje
iv. Činností prováděných uživateli v IDM nástroji

h. Řízení správy organizačních struktur včetně vícevrstevných organizačních struktur (tvorba technických struktur dle definovaných parametrů)

Součástí bude kompletní proškolení interních administrátorů IDM nástroje zadavatele na ovládání IDM nástroje v oblasti správy organizačních struktur, technických organizačních struktur

Pro akceptační procedury a lhůty potvrzující úspěšnou Implementaci se uplatní ustanovení kapitoly č. 9 Smlouvy.

4. KONZULTAČNÍ A PODPŮRNÉ SLUŽBY

Předmětem konzultačních a podpůrných služeb (dále jen „***Služby***“) bude poskytnutí kapacit specialistů ve stanovených rolích – Senior analytik IDM, Analytik IDM, Projekt manažer, Analytik bezpečnosti na základě vyžádání Objednatelem pro zajištění:

- realizace dílčích rozvojových projektů integrace IDM nástroje na nové technologie,
- plné integrace nástroje IDM na další části stávajícího IS SZIF za využití stanovených specialistů

4.1.PRINCIP OBJEDNÁVÁNÍ SLUŽEB

Konzultační a podpůrné služby jsou alokovány výhradně na základě potvrzené objednávky písemně zaslané (e-mailem) Oprávněnou osobou Objednatele a písemného potvrzení schválení Objednávky Oprávněnou osobou Poskytovatele.

Oprávněná osoba Objednatele zašle pro každé dílčí plnění Konzultačních a podpůrných služeb konkrétní požadavek na realizaci pro danou oblast Oprávněné osobě Poskytovatele včetně požadovaných termínů realizace. Oprávněná osoba Poskytovatele bez prodlení zpracuje konkrétní závaznou nabídku pro realizaci dané oblasti s uvedením osob a rolí, které se budou na realizaci požadavku podílet a s oceněním maximálního objemu prací pro jednotlivé role nezbytné pro realizaci daného požadavku a zašle zpracovanou nabídku Oprávněné osobě Zadavatele. V rámci nabídky je Poskytovatel povinen potvrdit požadované termíny dílčího plnění, případně navrhnout úpravy termínů na základě doložení konkrétních objektivních faktů, na jejichž základě úpravu termínů navrhuje.

Poskytovatel je rovněž povinen do nabídky specifikovat kompletní rozsah nezbytné součinnosti Objednatele ve formě definovaní veškerých potřebných položek (licencí SW, HW, podpory výrobce, atd.), které jsou pro úspěšnou realizaci dílčího plnění potřebné.

Na základě obdržené nabídky zpracuje Objednatel prostřednictvím Oprávněné osoby finální objednávku služeb a tu zašle potvrzenou Oprávněné osobě Poskytovatele.

Poskytování konzultačních a podpůrných služeb bude realizováno prostřednictvím rolí a osob vymezených v Příloze č. 3 Smlouvy.