

**Klasifikace: Veřejný dokument**



Technická specifikace

Příloha č. 1 zadávací dokumentace pro zadávací řízení „Výstavba systému správy identit a přístupů – organizační, procesní a datová příprava implementace systému IDM“

Obsah

[1 Seznam zkratek 2](#_Toc132037618)

[2 Úvod 6](#_Toc132037619)

[2.1 Záměr SŽ v oblasti systému pro správu identit a přístupů 6](#_Toc132037620)

[2.2 Předmět plnění veřejné zakázky 7](#_Toc132037621)

[2.3 Oblasti, které nejsou předmětem plnění veřejné zakázky 8](#_Toc132037622)

[3 Současný stav a popis prostředí 8](#_Toc132037623)

[4 Požadavky na plnění 8](#_Toc132037624)

[4.1 Identifikace systémů zdrojových dat, analýza struktury a kvality dat 8](#_Toc132037625)

[4.2 Analýza definovaných cílových systémů 10](#_Toc132037626)

[4.3 Definování systému business rolí, aplikačních a technických rolí a struktury atributů identit 11](#_Toc132037627)

[4.4 Návrh procesů správy životního cyklu identit a souvisejících obslužných procesů 12](#_Toc132037628)

[4.5 Identifikace konfliktních rolí a pravidel, definování metodiky řešení konfliktních rolí 13](#_Toc132037629)

[4.6 Vytvoření konzistentního datového modelu správy identit a souvisejícího procesního modelu 13](#_Toc132037630)

[4.7 Návrh revize funkčních a nefunkčních požadavků budoucího systému správy identit a přístupů 14](#_Toc132037631)

[4.8 Návrh postupu při napojování cílových systémů 15](#_Toc132037632)

[4.9 Návrh harmonogramu budoucí implementace systému správy identit a přístupů 15](#_Toc132037633)

[4.10 Definování nezbytné součinnosti Zadavatele při budoucí implementaci systému správy identit a přístupů 16](#_Toc132037634)

[4.11 Služby na vyžádání 16](#_Toc132037635)

[5 Fáze plnění a akceptační milníky 16](#_Toc132037636)

# Seznam zkratek

Níže uvedená tabulka obsahuje seznam zkratek a pojmů použitých v rámci této Technické specifikace.

Přehled zkratek a pojmů:

|  |  |
| --- | --- |
| Zkratka | Popis |
| AD, MS AD | Microsoft Active Directory |
| AS-IS | Současný stav |
| AKB | Architekt kybernetické bezpečnosti |
| API | Rozhraní pro programování aplikací (Application Programming Interface) |
| CA | Certifikační autorita |
| CISO | Manažer informační bezpečnosti (Chief Information Security Officer) |
| ČSN | Česká státní norma |
| DC | Domain controller. Řadič domény s Active Directory |
| GPA | Garant primárního aktiva |
| GPdA | Garant podpůrného aktiva |
| HA | Režim vysoké dostupnosti (High Availability), např. prostřednictvím redundance |
| Harmonogram | Harmonogram stanovený v příloze č. 6 „Harmonogram“ |
| HLD | Přehledový vysokoúrovňový design (High Level Design) |
| HR | Lidské zdroje |
| HW | Hardware |
| ICT | Informační a komunikační technologie (Information and Communication TechnoLogies) |
| IDM | Správa identit a přístupů (Identity and Access Management) |
| IS | Informační systém |
| ISVS | Informační systémy veřejné správy |
| ITSM | IT Service Management |
| KII | Kritická informační infrastruktura |
| LDAP | Lightweight Directory Access Protocol |
| LLD | Nízko úrovňový design (Low Level Design) |
| MB | Mega Byte |
| MCAS | Microsoft Cloud App Security |
| MD | Člověkoden, pracovní čas jedné osoby odpovídající jednomu pracovnímu dni, tedy typicky 8 hodin (man-day) |
| MDM | Správa mobilních zařízení (Mobile Device Management) |
| MFA | Vícefázové ověření (Multifactor Authentication) |
| MKB | Manažer kybernetické bezpečnosti |
| NÚKIB | Národní úřad pro kybernetickou a informační bezpečnost |
| On-premise | On-premise software je takový software, který lze instalovat a provozovat v prostorách organizace, která jej využívá |
| OS | Operační Systém |
| OTP | Jednorázové heslo (One Time Password) |
| PAM | Správa privilegovaných přístupů (Privileged Access Management) |
| PD | Pracovní Den |
| PKI | Infrastruktura správy a distribuce veřejných klíčů (Public Key Infrastructure); informační systém, produkující a využívající digitální certifikáty |
| Privilegovaný účet | Uživatelský účet informačního systému s širokou nebo neomezenou množinou administrátorských oprávnění |
| RDP | Protokol na přenos vzdálené plochy (Remote Desktop Protocol) |
| RPO | Recovery Point Objective – cílový bod zotavení |
| RTO | Recovery Time Objective – cílová doba zotavení |
| s2s VPN | Site to site VPN |
| SLA | Dohoda o úrovni poskytovaných služeb (Service Level Agreement) |
| SSH | Zabezpečený protokol pro připojení k serverům |
| SSO | Systém jednotného přihlášení (Single Sign-On) |
| SW | Software |
| SŽ | Správa železnic, státní organizace |
| Token | Dedikované HW úložiště soukromého klíče uživatele – zpravidla čipová karta. |
| UAS | Uživatelsko-aplikační síť |
| VPN | Virtuální privátní síť (Virtual Private Network) |

Seznam zkratek pro specifické aplikace, profese a organizační útvary SŽ:

|  |  |
| --- | --- |
| Zkratka | Popis |
| ASVC | Automatické stavění vlakových cest |
| DŘT | Dispečerská řídicí technika |
| DDTS | Dálková diagnostika technologických systémů |
| CDP | Centrální dispečerské pracoviště |
| CDS | Centrální dispečerský systém |
| DŽDC | Dispečer železniční dopravní cesty |
| DŽIN | Dispečer železniční infrastruktury |
| ED | Elektro dispečer |
| GVD | Grafikon vlakové dopravy |
| SSZT | Správa sdělovací a zabezpečovací techniky |
| ST | Správa tratí |
| TechDS | Technologický a dohledový systém |
| TDS | Technologická datová síť |
| TDCDP | Traťový dispečer dálkového ovládání zabezpečovacího zařízení na CDP |
| VS | Vlakové soupravy |

# Úvod

Tento dokument je přílohou a nedílnou součástí zadávacího řízení s názvem „Výstavba systému správy identit a přístupů – organizační, procesní a datová příprava implementace systému IDM“ (dále jen „veřejná zakázka“), pro organizaci Správa železnic, státní organizace (dále jen „SŽ“ nebo „Zadavatel“). Dokument popisuje technické a jiné požadavky na veřejnou zakázku.

## Záměr SŽ v oblasti systému pro správu identit a přístupů

Implementace systému Identity and Access Management (dále jen „IDM“) a jeho napojení na aktiva organizace Zadavatele je v souladu s dlouhodobou koncepcí řízení identit, přístupových oprávnění, jejich kontroly a zvýšení zabezpečení přístupů k aktivům organizace Zadavatele. S ohledem na velikost organizace Zadavatele a velké množství aktiv, neplánuje Zadavatel implementaci IDM pro všechna aktiva v jednom projektu, ale plánuje jejich postupné připojování podle technických a organizačních možností. IDM tedy není plánováno pouze pro řízení identit a přístupových oprávnění k informačním systémům spadajícím do kritické infrastruktury, ale v optimálním případě ke všem aktivům, u kterých je třeba řídit přístupová oprávnění[[1]](#footnote-2).

Hlavní cíle projektu IDM:

* implementace systému pro systematickou správu celého životního cyklu identit, řízení a kontroly přístupů identit k jednotlivým aktivům, rekonciliace a reportování;
* systematická správa a kontrola přístupových oprávnění k cílovým systémům (aktivům) včetně automatizace (založené na rolích a atributech);
* podpora automatizace souvisejících procesů (zejména navázané na HR procesy);
* podpora automatizace schvalovacích procesů, jednoznačná odpovědnost za konkrétní přístupová oprávnění;
* zvýšení bezpečnosti a plnění legislativních požadavků, eliminace části bezpečnostních hrozeb;
* systematická a automatizovaná správa technických, servisních a správcovských účtů;
* datové oddělené procesní správy životního cyklu identit od cílových systémů (včetně autorizačních a autentizačních systémů); a
* snížení nákladů na správu uživatelských účtů a HR procesů.

Implementace systému IDM v prostředí Zadavatele je rozdělena na dvě navazující Etapy:

* **Etapa 1:** organizační, procesní a datová příprava organizace Zadavatele a jejích informačních systémů pro implementaci systému řízení životního cyklu identit a přístupových oprávnění (pozn. této etapy se týká tato veřejné zakázka).
* **Etapa 2:** výběr a implementace systému IDM pro všechna definovaná aktiva, kde je nutné řídit přístupová oprávnění (pozn. tuto etapu bude případně řešit veřejná zakázka, kterou bude Zadavatel teprve připravovat).

## Předmět plnění veřejné zakázky

Cílem veřejné zakázky je uzavření smlouvy, jejímž předmětem bude zajištění přípravy implementace systému pro řízení identit, jejich životního cyklu a řízení přístupů k ICT systémům a službám Zadavatele (tj. příprava implementace systému IDM).

Předmětem plnění veřejné zakázky je poskytnutí konzultačních služeb přípravy implementace systému IDM. Nedílnou součástí plnění je také vytvoření konzistentního datového modelu správy identit, business a aplikačních rolí, pravidel apod. a jeho zpřístupnění pomocí definovaného rozhraní.

Plnění bude obsahovat následující poptávané oblasti:

**Fáze 1: Analýza systémů zdrojových dat a cílových systémů**

1. Identifikace systémů zdrojových dat, analýza struktury a kvality dat
2. Analýza definovaných cílových systémů

**Fáze 2: Definování systému identit, systemizace, rolí, procesů a metodik**

1. Definování systému business rolí, aplikačních a technických rolí a struktury atributů identit
2. Návrh procesů správy životního cyklu identit a souvisejících obslužných procesů
3. Identifikace konfliktních rolí a pravidel, definování metodiky řešení konfliktních rolí

**Fáze 3: Vytvoření datového modelu správy identit**

1. Vytvoření konzistentního datového modelu správy identit a souvisejícího procesního modelu

**Fáze 4: Revize požadavků na systém IDM, návrh budoucího postupu a součinnosti**

1. Návrh revize funkčních a nefunkčních požadavků budoucího systému správy identit a přístupů
2. Návrh postupu při napojování cílových systémů
3. Návrh harmonogramu budoucí implementace systému správy identit a přístupů
4. Definování nezbytné součinnosti Zadavatele při budoucí implementaci systému správy identit a přístupů

**Fáze 5:** **Služby na vyžádání**

1. Služby na vyžádání

Předmět plnění bude zpracováván s ohledem na požadované vlastnosti budoucího systému IDM, které jsou uvedeny v Příloze č. 3 zadávací dokumentace.

## Oblasti, které nejsou předmětem plnění veřejné zakázky

Pro vyloučení pochybností Zadavatel uvádí, že následující oblast **není** předmětem plnění veřejné zakázky:

* výběr a implementace systému IDM

Výběr technologického řešení systému IDM a jeho implementace v prostředí SŽ není předmětem této veřejné zakázky.

# Současný stav a popis prostředí

Současný stav ICT prostředí Zadavatele v oblastech z hlediska budoucího systému správy identit a přístupů je uveden v Příloze č. 2 zadávací dokumentace.

# Požadavky na plnění

Plnění veřejné zakázky se musí skládat z níže uvedených částí (kapitoly 4.1 - 4.11).

## Identifikace systémů zdrojových dat, analýza struktury a kvality dat

Zadavatel předpokládá, že primárním a autoritativním zdrojem dat o identitách, rolích a struktuře organizace Zadavatele pro budoucí systém IDM bude systém SAP HR. Po dodavateli požaduje provedení podrobné analýzy zmíněného systému co do rozsahu, struktury a kvality uložených dat.

Současně požaduje Zadavatel identifikaci případných dalších zdrojů dat a provedení obdobné analýzy i těchto doplňkových datových zdrojů.

V případě, že rozsah, struktura nebo kvalita zdrojových dat nebude odpovídat požadavkům jejich budoucího využití (návrh business rolí, návrh systemizace založené na business rolích, tvorba datového modelu, využití dat v budoucím systému IDM apod.), požaduje Zadavatel návrh změn a úprav ve zdrojích dat a návrh postupu zajištění dostatečné kvality zdrojových dat. U systému SAP HR musí dodavatel při svých návrzích změn vnímat, že primární úkol tohoto modulu je personalistika a výpočet mezd, jejichž bezchybná funkčnost nesmí být navrženými změnami ohrožena.

|  |  |
| --- | --- |
| **1** | **Identifikace systémů zdrojových dat, analýza struktury a kvality dat** |
| Popis | Dodavatel identifikuje v rámci procesů a systémů Zadavatele systémy zdrojových dat pro správu životního cyklu identit, rolí, údajů o struktuře organizace (systemizace – systemizovaná místa, jejich struktura a popis apod.), údajů o osobách evidovaných mimo systemizaci organizace (externisté s požadavkem na užívání aktiv SŽ, pracovněprávní vztahy mimo pracovní poměr, důchodci, rentisté apod.).  Dodavatel provede analýzu struktury dat v identifikovaných zdrojových systémech a případných dalších zdrojích dat s ohledem na zaměření projektu a návrh datových struktur identit, business rolí, aplikačních rolí, pravidel a dalších objektů v budoucím systému IDM.  Dodavatel provede analýzu kvality zdrojových dat a v případě nedostatečné kvality dat navrhne postup k jejich opravě.  Současně dodavatel provede identifikaci a analýzu procesů spojených se správou identit.  V případě identifikované nemožnosti využití zdrojových dat jako vstupu pro budoucí systém IDM, dodavatel navrhne odpovídající změny struktury dat a postupy pro zajištění dostatečné kvality vstupních dat.  V rámci provedené identifikace a analýzy se dodavatel také zaměří na následující oblasti a otázky:   * jaké typy identit s rozdílným životním cyklem jsou spravovány? (např. zaměstnanci – pracovní poměr, dohoda o pracovní činnosti, dohoda o provedení práce; externisté (partneři, dodavatelé), administrátoři apod.) * má identita v rámci organizace jeden nebo více uživatelských účtů? * jaký je životní cyklus uživatelského účtu (vytvoření, aktivace, blokace, odblokování, deaktivace, výmaz) * kde vznikají jednotlivé typy identit? (personální systém, popř. jiný systém apod., včetně systémů zdrojových dat týkající se externistů) * jaký je životní cyklus identit a jak je řešen? Zejména: jak dochází ke změně atributů při změně zařazení v organizační struktuře, změně lokalizace, změně vedoucího zaměstnance, mateřské dovolené, dlouhodobé nepřítomnosti, jak je řešena zastupitelnost, ukončení pracovního poměru nebo smluvního vztahu apod. * jaký je jedinečný identifikátor osoby/uživatele; popř. návrh na vytvoření jedinečného identifikátoru osoby * jaká jsou pravidla pro správu atributů osoby/uživatele * jak jsou nastaveny procesy aktualizace identity, kdo a jakým způsobem je informován o změnách identity v průběhu jejího životního cyklu.   V případě, že pro návrh datového modelu a souvisejících procesů (viz kapitola 4.6), popř. pro budoucí systém IDM nebudou některá data dostupná v IT systémech nebo dokumentaci Zadavatele, navrhne dodavatel způsob doplnění potřebných dat. |
| Výstupy | Výstupem tohoto kroku bude dokument obsahující alespoň:   * seznam systémů zdrojových dat, popis dat a jejich struktury využitý pro další postup projektu a pro budoucí systém IDM; * vyhodnocení kvality dat v identifikovaných zdrojových systémech; * popis existujících procesů souvisejících se správou identit; * případný návrh na změny ve struktuře dat a případný návrh postupu pro zajištění dostatečné kvality zdrojových dat pro budoucí systém IDM; * případný návrh na doplnění zdrojových dat o chybějící oblasti a údaje. |

## Analýza definovaných cílových systémů

V rámci tohoto kroku provede dodavatel analýzu cílových (koncových systémů) určených k napojení[[2]](#footnote-3) na budoucí systém IDM (tj. systém IDM bude systémem řídícím uživatelské účty, role, přístupy apod. v cílových systémech).

Seznam cílových systémů a jejich základní charakteristika jsou uvedeny v Příloze č. 4 zadávací dokumentace.

|  |  |
| --- | --- |
| **2** | **Analýza definovaných cílových systémů** |
| Popis | Dodavatel provede analýzu všech cílových (koncových) systémů definovaných v Příloze č. 4 zadávací dokumentace. Analýza cílových systémů bude provedena zejména z hledisek správy uživatelských účtů, rolí, skupin a oprávnění, způsobů autorizace a autentizace pro každý definovaný systém. Současně dodavatel identifikuje technické možnosti napojení cílových systémů. |
| Výstupy | Výstupem tohoto kroku bude dokument obsahující pro každý požadovaný cílový systém alespoň:   * způsob správy uživatelských účtů, rolí, skupin a oprávnění; * identifikované skupiny a role (aplikační, technické apod.); * způsob správy autorizace; * způsob autentizace uživatelů; * popis životního cyklu správy aplikace, popis procesu implementace změn aplikace a způsobu informování o změnách v aplikaci; * identifikované technické možnosti napojení na budoucí systém IDM. |

## 

## Definování systému business rolí, aplikačních a technických rolí a struktury atributů identit

|  |  |
| --- | --- |
| **3** | **Definování systému business rolí, aplikačních a technických rolí a struktury atributů identit** |
| Popis | Dodavatel vypracuje návrh systému business rolí, aplikačních rolí, technických rolí[[3]](#footnote-4) a struktury atributů identit s ohledem na zdrojové a cílové systémy a požadavky na automatizaci, definici základního modelu zastupitelnosti (delegování) apod.  Dodavatel dále vypracuje návrh struktury systemizace v budoucím systému IDM, založené na rolích a dalších atributech a systému zachycující správu identit mimo systemizovaná místa (např. dodavatelé, externisté apod.), opět založený na rolích a dalších atributech. Zadavatel předpokládá, že uvedených systémů/struktur může být na základě provedené analýzy zpracováno dodavatelem více.  Zadavatel požaduje vytvoření uvedených systémů a souvisejících struktur tak, aby odpovídaly činnostem v organizaci Zadavatele a jednotlivé objekty bylo možné automaticky vytvářet a měnit na základě organizačních změn evidovaných v personálním systému (SAP HR), popř. jiném identifikovaném systému zdrojových dat.  Zadavatel předpokládá, že aplikační role napříč definovanými koncovými systémy (aplikacemi) budou v návrhu dodavatele přiřazovány činnostem (business rolím). Návrh musí být zpracován tak, aby business role vycházející z pracovního zařazení uživatelů bylo možno přiřazovat a odebírat identitám automatizovaně (například na základě hodnot jejich atributů). U specifických činností nebo činností spojených s využitím privilegovaných účtů Zadavatel předpokládá jejich přiřazování po časově omezenou dobu, na základě žádostí identity a na základě definovaných schvalovacích procesů.  Zadavatel předpokládá, že vazby mezi činnostmi (business rolemi) a aplikačními rolemi potřebnými pro výkon činnosti budou definovány s ohledem na konkrétní cílový systém. Zadavatel požaduje současně zpracování definice zakázaných kombinací aplikačních rolí přiřazených současně jedné identitě (uživateli) v daném cílovém systému.  Součástí výstupů bude i návrh modelu zastupitelnosti a detailní návrh schvalovacích procesů.  Návrhy uvedených systémů dodavatel zpracuje tak, aby zachycovaly současný stav (AS-IS) a návrh optimalizace těchto systémů z hlediska jejich možné budoucí implementace do organizace Zadavatele (TO-BE). |
| Výstupy | Výstupem tohoto kroku bude dokument[[4]](#footnote-5) obsahující alespoň níže uvedené oblasti. Návrh musí zachycovat současný stav (AS-IS) i návrh optimalizace uvedených oblastí (TO-BE) společně s návrhem postupného přechodu do stavu TO-BE.  Minimální rozsah oblastí obsažených ve výstupu:   * systém business rolí, aplikačních rolí, technických rolí a struktury atributů identit s ohledem na zdrojové a cílové systémy a požadavky na automatizaci; * návrh struktury „systemizace“ založené na rolích a dalších atributech a bude v souladu se schválenou systemizací (organizační struktura, konkrétní pracovní pozice v jednotlivých organizačních útvarech atd.); * návrh struktury systému správy identit mimo systemizovaná místa založeného na rolích, atributech, popř. dalších parametrech; * pro každý cílový systém: návrh bude obsahovat vazby mezi business rolemi a aplikačními rolemi specificky pro každý definovaný cílový systém samostatně; * pro každý cílový systém: definici zakázaných kombinací aplikačních rolí, pokud je možné tyto kombinace definovat; * návrh modelu zastupitelnosti; * detailní návrh schvalovacích procesů; * identifikované technické možnosti napojení na budoucí systém IDM. |

## Návrh procesů správy životního cyklu identit a souvisejících obslužných procesů

|  |  |
| --- | --- |
| **4** | **Návrh procesů správy životního cyklu identit a souvisejících obslužných procesů** |
| Popis | Dodavatel identifikuje a detailně popíše procesy správy životního cyklu identit a procesů souvisejících. U již existujících procesů dodavatel navrhne jejich případné úpravy.  Dodavatel současně popíše vazby mezi procesy (s případnou vazbou na systémy navržené v předchozím kroku, viz kapitola 4.3) a zpracuje návrh automatizace procesů.  Pro usnadnění realizace navržené správy životního cyklu identit a včasného informování uživatelů o změně bude součástí návrhu i návrh úpravy interních směrnic a pracovních postupů souvisejících se změnou správy životního cyklu identit v organizaci Zadavatele po implementaci budoucího systému IDM.  V rámci tohoto kroku dodavatel navrhne zejména:   * proces správy životního cyklu identit * proces správy životního cyklu uživatelských účtů dle typu uživatele (zaměstnanec, externista, privilegovaný účet apod.) * definici pravidel pro atributy uživatele * definice pravidel pro atributy aplikačních rolí * proces správy životního cyklu aplikací * proces správy životního cyklu aplikačních rolí * proces správy životního cyklu business rolí * proces přidělování aplikačních rolí a business rolí identitě * proces správy konfliktních rolí * návrh notifikací (způsob notifikace, kdy notifikovat, komu, jaké informace). |
| Výstupy | Výstupem tohoto kroku budou dokumenty obsahující alespoň:   * identifikaci a detailní popis procesů správy životního cyklu identit a procesů souvisejících, včetně návrhu změn existujících procesů; * detailní popis vazeb mezi procesy; * návrh automatizace procesů v budoucím systému IDM; * návrh úpravy interních směrnic a pracovních postupů souvisejících se změnou správy životního cyklu identit. |

## Identifikace konfliktních rolí a pravidel, definování metodiky řešení konfliktních rolí

|  |  |
| --- | --- |
| **5** | **Identifikace konfliktních rolí a pravidel, definování metodiky řešení konfliktních rolí** |
| Popis | V tomto kroku dodavatel provede analýzu, zda a jakým způsobem Zadavatel pracuje s konfliktními rolemi. Konfliktní role[[5]](#footnote-6) jsou definovány jako kombinace aplikačních rolí, které z důvodu bezpečnosti realizace organizačního procesu nebo přístupu k informacím v používaných aplikacích nesmějí být současně přiděleny jednomu uživateli.  Dodavatel navrhne metodiku identifikace a správy konfliktních rolí a pravidel. Dodavatel dále navrhne postup řešení přiřazených konfliktních rolí (ať už historicky přiřazených nebo dočasně přiřazených např. pro odstranění následků havárie) a konfliktních pravidel. |
| Výstupy | Výstupem tohoto kroku budou dokumenty obsahující alespoň:   * metodika identifikace konfliktních rolí (aplikačních, popř. business rolí); * metodika identifikace konfliktních pravidel v návrhu budoucího systému IDM; * návrh metodického postupu řešení konfliktních rolí a pravidel. |

Zadavatel předpokládá, že definovanou metodiku využije dodavatel při tvorbě konzistentního datového modelu správy identit (kapitola 4.6).

## Vytvoření konzistentního datového modelu správy identit a souvisejícího procesního modelu

|  |  |
| --- | --- |
| **6** | **Vytvoření konzistentního datového modelu správy identit a souvisejícího procesního modelu** |
| Popis | Dodavatel vytvoří konzistentní datový model správy identit, rolí (business, aplikačních a technických rolí), systemizace, identit mimo systemizaci, pravidel apod.  Dodavatel požaduje, aby výsledky předchozích kroků (kapitoly 4.1 - 4.5) byly součástí datového modelu správy identit, včetně mechanismů kontroly konzistence modelu a identifikace konfliktních (vzájemně neslučitelných) objektů (rolí, pravidel apod.).  Datový model musí být zpracován jako obecný, bez vazby na konkrétní systémy IDM. Součástí datového modelu musí být i jeho zpřístupnění pro budoucí napojení na systém IDM formou technologicky neutrálního rozhraní (webová služba, API...), popř. formou uživatelsky definovaného exportního rozhraní. |
| Výstupy | Výstupem tohoto kroku bude konzistentní datový model budoucího systému IDM zahrnující výsledky předchozích kroků, včetně mechanismů kontroly konzistence modelu. Model bude naplněn daty z předchozích kroků (identity, organizační struktury/systemizace a jejich popis systémem business rolí, business role, aplikační role, atributy atd.). Součástí datového modelu bude i rozhraní pro zpřístupnění datového modelu pro jeho další strojové zpracování formou technologicky neutrálního rozhraní (API, webová služba apod.), včetně dokumentace tohoto rozhraní.  Součástí výstupů bude i dokumentace datového modelu a datových struktur v souladu s požadavky Přílohy č. 5 zadávací dokumentace (Platforma 2.0, Standardy vývoje informačních systémů, relevantní ustanovení kap. 1.5) a konceptuální datový model v „UML / Class diagram“ včetně editovatelného zdroje. |

Zadavatel požaduje v souladu s Přílohou č. 5 zadávací dokumentace (Platforma 2.0, Vymezení služeb) zpracování datového modelu v některém z následujících databázových systémů:

* MS SQL Server,
* Oracle DB a
* PostgreSQL.

Volba databázového systému z výše uvedených bude předmětem dohody dodavatele a Zadavatele.

Pro vytvoření datového modelu poskytne Zadavatel dodavateli technické prostředky (virtuální stroje, databázové stroje apod.) v souladu s Přílohou č. 5 zadávací dokumentace (Platforma 2.0, Vymezení služeb) podle specifikací dodavatele.

## Návrh revize funkčních a nefunkčních požadavků budoucího systému správy identit a přístupů

|  |  |
| --- | --- |
| **7** | **Návrh revize funkčních a nefunkčních požadavků budoucího systému správy identit a přístupů** |
| Popis | Dodavatel na základě výsledků předchozích kroků, podle svých zkušeností s obdobnými projekty a podle „best practice“ zpracuje návrh revize funkčních a nefunkčních požadavků na budoucí systém IDM uvedený v Příloze č. 3 zadávací dokumentace. |
| Výstupy | Výstupem tohoto kroku bude dokument obsahující revizi funkčních a nefunkčních požadavků na budoucí systém IDM. |

## Návrh postupu při napojování cílových systémů

|  |  |
| --- | --- |
| **8** | **Návrh postupu při napojování cílových systémů** |
| Popis | Dodavatel na základě výsledků předchozích kroků, podle svých zkušeností s obdobnými projekty a podle „best practice“ zpracuje návrh plánu postupného napojování cílových systémů definovaných Příloze č. 4 zadávací dokumentace, včetně předběžných návrhů technického řešení napojení cílových systémů.  Zadavatel předpokládá rozdělení cílových systémů do skupin, např. podle kritérií typu autorizace a autentizace, důležitosti jejich fungování pro chod organizace Zadavatele apod. (jednotlivé skupiny aplikací pak mohou být integrovány postupně). Zadavatel předpokládá, že rozdělení do skupin také umožní sjednotit budoucí způsob integrace pro cílové systémy stejné skupiny, a tak snížit počet potřebných konektorů při integraci s budoucím systémem IDM, při současném snížení nákladů na integraci a správu konektorů cílových systémů. |
| Výstupy | Výstupem tohoto kroku bude dokument obsahující:   * návrh rozdělení cílových systémů do skupin pro budoucí integraci se systémem IDM a popis kritérií tohoto rozdělení; * předběžný návrh technického řešení napojení jednotlivých cílových systémů nebo skupin cílových systémů; * návrh plánu postupného napojování cílových systémů nebo skupin cílových systémů na budoucí systém IDM. |

## Návrh harmonogramu budoucí implementace systému správy identit a přístupů

|  |  |
| --- | --- |
| **9** | **Návrh harmonogramu budoucí implementace systému správy identit a přístupů** |
| Popis | Dodavatel na základě výsledků předchozích kroků, podle svých zkušeností s obdobnými projekty a podle „best practice“ navrhne předběžný postup a harmonogram možné implementace budoucího systému IDM v prostředí Zadavatele. |
| Výstupy | Výstupem tohoto kroku bude dokument obsahující předběžný postup a harmonogram možné implementace budoucího systému IDM v prostředí Zadavatele. |

## Definování nezbytné součinnosti Zadavatele při budoucí implementaci systému správy identit a přístupů

|  |  |
| --- | --- |
| **10** | **Definování nezbytné součinnosti Zadavatele při budoucí implementaci systému správy identit a přístupů** |
| Popis | Dodavatel na základě výsledků předchozích kroků, podle svých zkušeností s obdobnými projekty a podle „best practice“ navrhne nezbytnou součinnost Zadavatele při budoucí implementaci systému IDM v prostředí Zadavatele. |
| Výstupy | Výstupem tohoto kroku bude dokument obsahující popis nezbytné součinnosti Zadavatele při budoucí implementaci systému IDM v prostředí Zadavatele. |

## Služby na vyžádání

|  |  |
| --- | --- |
| **11** | **Služby na vyžádání** |
| Popis | Dodavatel poskytne Zadavateli služby konzultace na vyžádání, zejména v oblasti využití výstupů při přípravě implementace budoucího systému IDM, popř. při vlastní implementaci. Maximální souhrn těchto služeb bude činit 20 MD za celou dobu trvání smlouvy, čerpání bude probíhat dle konkrétních potřeb Zadavatele.  Dodavatel předpokládá využití služby konzultace na vyžádání zejména při koordinaci činností úvodních fází implementace budoucího systému IDM, využití vytvořeného datového modelu, analýz a metodik. |
| Výstupy | Výstupem tohoto bude poskytnutí služby konzultace na vyžádání podle potřeb Zadavatele. |

# Fáze plnění a akceptační milníky

Služby musí být dodány v níže uvedených fázích. Každá z níže uvedených fází (tj. každý řádek níže uvedené tabulky) musí být Zadavatelem separátně akceptována nejpozději v termínu uvedeném v Harmonogramu. Zadavatel akceptuje výstupy dané Fáze, jestliže je dodavatel provedl v šíři a kvalitě požadované v zadávací dokumentaci této veřejné zakázky. V opačném případě je dodavatel povinen napravit nedostatky plnění.

| **Fáze** | **Popis** | **Kapitola obsahující požadavky** |
| --- | --- | --- |
| Fáze 1 | Analýza systémů zdrojových dat a cílových systémů | 4.1 - 4.2 |
| Fáze 2 | Definování systému identit, systemizace, rolí, procesů a metodik | 4.3 - 4.5 |
| Fáze 3 | Vytvoření datového modelu správy identit | 4.6 |
| Fáze 4 | Revize požadavků na systém IDM, návrh budoucího postupu a součinnosti | 4.7 - 4.10 |
| Fáze 5 | Služby na vyžádání | 4.11 |

1. Tato aktiva tak obsahují především informační systémy kritické infrastruktury, ostatní informační systémy, systémy pro kontrolu přístupů do zabezpečených lokalit a ostatních prostor organizace. [↑](#footnote-ref-2)
2. Napojením je myšleno napojení přímé (tj. budoucí systém IDM bude řídit přímo uživatelské účty, role, přístupy apod. v cílovém systému) i nepřímé (např. uživatelské účty, role, skupiny a přístupy jsou řízeny systémem ActiveDirtectory, pro který je autoritativním zdrojem dat budoucí systém IDM). [↑](#footnote-ref-3)
3. Včetně rolí spjatých s privilegovanými účty a oprávněními. [↑](#footnote-ref-4)
4. Zadavatel předpokládá zpracování tohoto kroku společně s vytvářením datového modelu správy identit. V tomto kroku Zadavatel požaduje i čitelné výstupy (dokumentaci) návrhu systémů pokrývajících uvedené oblastí. [↑](#footnote-ref-5)
5. Také SoD (Segregation of Duties). [↑](#footnote-ref-6)