

**Klasifikace: Veřejný dokument**



## **Bližší specifikace předmětu plnění veřejné zakázky (Technická specifikace)**

Příloha č. 2 Zadávací dokumentace veřejné zakázky s názvem „Nasazení systému IdM v prostředí Správy železnic“

## Obsah

1	Seznam pojmů a zkratk	2
2	Úvod	5
2.1	Očekávání od implementace řešení	6
2.2	Předmět plnění Veřejné zakázky	7
2.3	Oblasti, které nejsou předmětem plnění Veřejné zakázky	7
3	Současný stav a popis prostředí	8
4	Požadavky na plnění	9
4.1	Implementační analýza a Analýza rizik	10
4.1.1	Implementační analýza	10
4.1.2	Analýza rizik	11
4.2	Implementace nástroje IdM a jeho integrace	11
4.2.1	Instalace IdM	11
4.2.2	Integrace zdrojových systémů pro IdM	14
4.2.3	Integrace systémů napojených na IdM	15
4.2.4	Testování	15
4.2.5	Migrace dat	15
4.2.6	Systémové a licenční požadavky	15
4.3	Dokumentace řešení	16
4.3.1	Instalační, konfigurační a související dokumentace	16
4.3.2	Spolupráce na aktualizaci vnitropodnikové dokumentační základny	17
4.4	Příprava adopční (komunikační) kampaně pro zaměstnance SŽ a externí uživatele	18
4.5	Školení uživatelů a administrátorů	18
4.6	Testovací provoz	19
4.7	Odborná technická podpora	19
4.8	Služby na vyžádání	20
5	Fáze dodávky a akceptační milníky	22

## 1 Seznam pojmů a zkratek

Zadavatel upozorňuje, že níže uvedené zkratky jsou užívané ve stejném významu ve všech přílohách Zadávací dokumentace.

Zkratka / pojem	Popis
AD	Microsoft Active Directory,
ADFS	Active Directory Federation Services
BAPI	Komunikační rozhraní (typické pro komunikaci se SAP)
CMDB	Konfigurační databáze
CDP	Centrální dispečerské pracoviště
CTD	Centrum telematiky a diagnostiky
Dodavatel	Vybraný dodavatel Veřejné zakázky
Dotčený systém	Systémy, které budou napojovány na nástroj IdM (zdrojový nebo koncový)
DB	Databáze
E-ZAK	Elektronický nástroj pro zadávání veřejných zakázek
Entra	MS Entra, součást řešení pro M365 pro správu identit a řízení přístupu (starší názvy: Azure AD, AAD)
ERP	Enterprise resource planning – podnikový centrální systém
GDPR	Nařízení Evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), včetně související legislativy
HA	High availability (režim vysoké dostupnosti)
HR	Podnikový personální systém
Harmonogram	Harmonogram stanovený ve Smlouvě o dílo, konkrétně v její příloze „Harmonogram“
ICT	Informační a komunikační technologie (Information and Communication Technologies)
ID	Identifikační číslo, řetězec
Identita	Identita představuje záznam nebo objekt v IdM, který jednoznačně identifikuje konkrétního uživatele. Může

	obsahovat informace jako uživatelské jméno, unikátní identifikátor aj. Každá identita může mít více účtů, rolí a práv.
IdM	Identity management (systém pro řízení a správu identit), systém hlavní instance aplikace a podřízených IdM sond, které s hlavní instancí zabezpečeně komunikují
IdM sonda	Podřízená instance IdM (nebo jeho část) implementovaná do oddělené části infrastruktury SŽ za účelem segmentace běžného uživatelského prostředí a technologického prostředí
IS	Informační systém
ISMS	Information Security Management System
ITSM	IT Service Management
JIRA SD	JIRA Atlassian (cloudové servicedeskové řešení), aplikace SD
KII	Kritická informační infrastruktura
KLU	Klíčový uživatel
LDAP	Lightweight Directory Access Protocol, označení platí i pro šifrovanou verzi LDAPS.
MD	Člověkodén, pracovní čas jedné osoby odpovídající jednomu pracovnímu dni, tedy typicky 8 hodin (man-day)
MS	Microsoft
Offline koncový systém	Aplikace, systémy, které budou řízeny IdM manuální formou správy – tzv. řešitelskou skupinou
OU	AD Organizační skupina
OWASP	Open web application security project – projekt v oblasti bezpečnosti webových aplikací
PAM	Privileged access management – aplikace pro správu privilegovaných účtů
REST API	Komunikační rozhraní typu REST
Řešitelská skupina	Definovaná skupina uživatelů tvořená Garantem aplikace/klíčovým uživatelem, nadřízeným pracovníkem případně další nominovanou osobou, která bude na základě definovaných oprávnění schvalovat žádosti o přidělení přístupového oprávnění do jím spravované aplikace. Schválené žádosti budou následně garantem aplikace zaneseny do aplikace.
SAP	Podnikový systém ERP - SAP
SAP HR	Personální systém SAP HR

Selfservice	Rozhraní pro uživatele (samoobslužné)
SD	Service desk (v prostředí SŽ - JIRA Atlassian ITSM)
SLA	Dohoda o úrovni poskytovaných služeb (Service Level Agreement)
ST	Systémové testy
SW	Software
SŽ	Správa železnic, státní organizace
TDS nebo TECHLAN	Technologické datové sítě (soubor technologických sítí)
Use-case	Příklad užití
Účastník	Subjekt, který se účastní tohoto zadávacího řízení o realizaci Veřejné zakázky s názvem „Nasazení systému IdM v prostředí Správy železnic“
Veřejná zakázka	Veřejná zakázka s názvem „Nasazení systému IdM v prostředí Správy železnic“.
VoKB	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů
Workflow	Pracovní postup
ZD	Zadávací dokumentace na Veřejnou zakázku
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

### Vztahy mezi základními pojmy

Osoba = fyzický jedinec, ke kterému je přiřazena jedna nebo více identit (s unikátním identifikátorem v systému SAP).

Identita = centrální logický záznam v IdM, který propojuje Osobu s různými účty

Účet = technický prostředek, který umožňuje přístup do jednotlivých systémů a aplikací, přičemž je spravován prostřednictvím identity.

## 2 Úvod

Tento dokument je přílohou a nedílnou součástí zadávací dokumentace Veřejné zakázky „Nasazení systému IdM v prostředí Správy železnic“, pro organizaci SŽ. Dokument popisuje technické a jiné požadavky na Veřejnou zakázku.

SŽ, jako subjekt povinný v souladu s ustanoveními § 3 písm. c), d) ZoKB, musí používat centralizovaný nástroj pro řízení přístupových oprávnění v souladu s § 20 VoKB. Pro zajištění kybernetické bezpečnosti informačních a komunikačních systémů a informací spravovaných SŽ a v souladu s Plánem zvládnutí rizik, hodlá implementovat systém správy identit a přístupů v prostředí SŽ.

Dodavatel v rámci zakázky provede instalaci, implementaci, konfiguraci a bude zajišťovat podporu nástroje IdM v prostředí SŽ v režimu:

- vysoké dostupnosti (platí jak pro hlavní instanci IdM tak IdM sondu)
- zajišťujícím pokrytí nejen uživatelských, ale i technologických sítí a aplikací v nich provozovaných způsobem implementace hlavní instance a následně IdM sondy (podřízené instance), která bude implementována v technologické síti, bude zabezpečeně komunikovat s hlavní instancí, a bude řídit aplikace v technologických sítích prostřednictvím 1-n napojených instancí MS AD nebo napřímo.

Hlavní cíle Veřejné zakázky jsou:

- dodání a implementace systémového nástroje pro řízení životního cyklu identit, řízení a kontroly přístupů k jednotlivým aktivům, rekonsolidace a reportování.
- systematická správa a kontrola přístupových oprávnění k cílovým systémům (aktivům) včetně automatizace (založené na rolích a attributech),
- podpora automatizace souvisejících procesů (zejména navázané na HR procesy),
- podpora automatizace schvalovacích procesů, jednoznačná odpovědnost za konkrétní přístupová oprávnění,
- napojení zdroje identit na systém IdM,
- migrace, tvorba a případná korekce business a aplikačních rolí určujících přístupová práva k vybraným informačním systémům do IdM,
- konfigurace workflow schvalovacích procesů, určující jednoznačnou zodpovědnost za konkrétní přístupová oprávnění,
- postupné napojení informačních systémů na IdM, prostřednictvím MS AD, manuálně nebo i přímo,
- zvýšení bezpečnosti a plnění legislativních požadavků, eliminace části bezpečnostních hrozeb,
- systematická a automatizovaná správa technických, servisních a správcovských účtů,

- datové oddělení procesní správy životního cyklu identit od cílových systémů (včetně autorizačních a autentizačních systémů),
- snížení nákladů na správu uživatelských účtů a HR procesů.

## 2.1 Očekávání od implementace řešení

SŽ očekává dosažení následujících cílů v rámci plnění Veřejné zakázky:

- Zvýšení bezpečnosti ICT prostředí SŽ (snížení bezpečnostních hrozeb, souvisejících se správou uživatelských účtů a přístupů).
- Zajištění systematické a strukturované správy identit a přístupů k ICT systémům.
- Snížení náročnosti souvisejících procesů na zdroje a snížení jejich chybovosti prostřednictvím automatizace souvisejících procesů.
- Naplnění legislativních požadavků v kontextu správy identit a přístupů (GDPR, ZoKB, VoKB).

### Požadavky na rozsah řešení

Pro naplnění projektu SŽ požaduje nasazení řešení na následující prostředí v SŽ:

1. Implementace nástroje IdM v prostředí SŽ pro uživatelskou síť a technologické sítě
2. Integrace nástroje IdM na zdrojové systémy (SAP HR, MS AD, JIRA CMDB)
3. Integrace nástroje IdM na 1-n instancí MS AD a JIRA SD
4. Zprovoznění a otestování integrací systémů dodavatelů třetích stran integrovaných skrze AD
5. Migrace dat a podpora Zadavatele při implementaci Byznysových a Činnostních rolí
6. Testovací provoz
7. Odborná technická podpora
8. Služby na vyžádání.

Celková aktivita implementace systému IdM v prostředí Zadavatele byla rozdělena na dvě vzájemně 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 netýká tato Veřejná zakázka, etapa již byla realizována a výstup této etapy v rozsahu nezbytném pro podání nabídky v rámci zadávacího řízení na Veřejnou zakázku bude zpřístupněn Dodavateli v rámci prohlídky místa plnění postupem dle čl. 8 zadávací dokumentace Veřejné zakázky).
- **Etapa 2:** implementace systému IdM pro všechna definovaná aktiva, kde je nutné řídit přístupová oprávnění (řešeno v rámci této Veřejné zakázky).

## 2.2 Předmět plnění Veřejné zakázky

Předmětem plnění Veřejné zakázky je dodávka aplikačního nástroje IdM (řešení) včetně jeho implementace a integrace s dotčenými systémy spolu s testováním, migrací dat, přípravou implementační analýzy, vytvořením veškeré provozní a konfigurační dokumentace, školením administrátorů a uživatelů spolu s návrhem adopční (komunikační) kampaně dle potřeb SŽ. Nedílnou součástí plnění je také technická podpora nakonfigurovaného řešení a dodávka veškerých licencí souvisejících s provozem nástroje IdM. Dodavatel bude v rámci implementačního procesu poskytovat metodickou supervizi garantům dotčených systémů.

Tato Veřejná zakázka bude obsahovat následující poptávané oblasti:

- Implementace IdM nástroje včetně IdM sondy v prostředí SŽ a jeho integrace se zdrojovými a koncovými systémy (včetně technické podpory dodavatelů koncových systémů při integracích a testování)
- Komplexní testování implementovaného nástroje IdM včetně všech realizovaných integrací
- Migrace dat
- Dokumentace zachycující implementační a konfigurační postupy, návrh aktualizace provozních dokumentací zapojených systémů a aktualizace dotčených vnitropodnikových dokumentů SŽ.
- Příprava adopční (komunikační) kampaně pro zaměstnance SŽ a externí uživatele
- Realizace školení pro uživatele i administrátory řešení.
- Testovací provoz zakončený akceptací a převzetím IdM do produkčního provozu
- Odborná technická podpora
- Služby na vyžádání
- Dodávku licencí souvisejících s implementací a provozem IdM nástroje

## 2.3 Oblasti, které nejsou předmětem plnění Veřejné zakázky

Pro vyloučení pochybností SŽ uvádí, že následující oblasti **nejsou** předmětem plnění Veřejné zakázky:

- Úprava systémů Dodavatelů třetích stran, u nichž bude probíhat napojení na nástroj IdM (vyjma poskytnutí součinnosti pro analytické činnosti a technickou podporu při integraci a testování integračních a konfiguračních vazeb IdM a koncového systému skrze AD a identifikaci problémů při realizaci integračních vazeb se zapojenými systémy)
- Dodávka uživatelských licencí pro AD
- HW vybavení, včetně operačních systémů, na provoz nástroje IdM.



### 3 Současný stav a popis prostředí

Současný stav ICT prostředí SŽ a základní premisy z návrhu budoucího stavu IdM služeb (výstup Etapy 1 - Analýza) je popsán:

- v příloze č. 7 zadávací dokumentace – Popis prostředí, kde jsou uvedeny informace k datovým centrům, doménovému prostředí a informace k provozovaným systémům v rámci SŽ
- v příloze č. 10 zadávací dokumentace – Podklady pro cílové řešení, kde jsou uvedeny základní specifikace cílového řešení
- v příloze č. 10a zadávací dokumentace - Podklady pro cílové řešení - schéma, kde je uvedeno graficky znázorněné funkční schéma cílového řešení
- a příloze č. 3 zadávací dokumentace – Analýza a návrh implementace systému IdM, která obsahuje informace z výstupu dříve realizované Etapy 1 nezbytné pro realizaci Veřejné zakázky. Tato příloha bude Dodavateli zpřístupněna v rámci prohlídky místa plnění postupem dle čl. 8 zadávací dokumentace Veřejné zakázky. Kompletní výstup Etapy 1 bude následně Dodavateli předán na úvodním setkání po podpisu Smlouvy o dílo. Rozsah plnění je definován zadávací dokumentací Veřejné zakázky s názvem „Výstavba systému správy identit a přístupů – organizační, procesní a datová příprava implementace systému IDM“ dostupné na: [https://zakazky.spravazeleznic.cz/contract\\_display\\_13119.html](https://zakazky.spravazeleznic.cz/contract_display_13119.html). Příloha č. 3 zadávací dokumentace - Analýza a návrh implementace systému IdM nemusí jednoznačně odpovídat aktuálnímu stavu mj. z důvodů časové prodlevy mezi tvorbu analýzy a termínem veřejné zakázky. Případné odchylky budou řešeny s vybraným dodavatelem v rámci Implementační analýzy.

#### **Zdrojové systémy pro IdM**

##### SAP HR

Primárním autoritativním zdrojem dat pro systematickou správu životního cyklu identit a byznys rolí bude systém SAP HR spravující mj. data o zaměstnancích (pracovně právních vztazích), organizační strukturu, a systemizaci organizace a externistech. Způsob integrace bude stanoven v rámci implementační analýzy, přičemž se předpokládá integrace formou napojení na DB (ze SAP do IdM) a formou API (z IdM do SAP).

##### JIRA Atlassian (CMDB + Service desk)

Zdrojem informací o aplikacích, které mají být řízeny IdM, bude JIRA CMDB, která bude předávat seznam aplikací včetně potřebných atributů do IdM prostřednictvím vhodné integrace, přičemž se předpokládá integrace formou API. Zároveň budou z IdM zpět do JIRA předávány informace o všech rolích a jejich skladbě a rolích aktérů v jednotlivých workflow.

JIRA Service desk bude zároveň umožňovat outsourcing schvalovacího workflow pro IdM a zajišťovat zrcadlení všech akcí provedených v rámci workflow do IdM tak, aby IdM zůstalo řídicím systémem, ale schvalovací workflow probíhalo v service desku.

### Koncové (cílové) systémy

V budoucnu SŽ předpokládá, že IdM bude zajišťovat řízení životního cyklu identit a přístupových oprávnění pro všechna aktiva, u kterých je nutné řídit přístupová oprávnění. SŽ aktuálně disponuje portfoliem cca 500 aplikací, přičemž IdM musí mít schopnost zajistit řízení celkového počtu aplikací portfolia, nicméně v rámci této Veřejné zakázky SŽ vyžaduje napojení pouze 30 systémů, přičemž některé z nich mohou existovat ve více oddělených instancích nebo se skládají z vícero oddělených modulů, kde každý modul má vlastní správu uživatelů a přístupů.

Cílovými (koncovými) systémy v rámci VZ budou zejména:

- systémy Active Directory (očekává se napojení na více instancí - forestů),
- vybrané systémy kritické informační infrastruktury (vybraná technická aktiva),
- vybrané systémy mimo kritickou informační infrastrukturu (vybraná technická aktiva),
- systémy typu Privileged Access Management (PAM) pro správu technických, servisních a správcovských účtů,
- systémy interních certifikačních autorit,
- systém SAP,
- systém JIRA,
- dodávaný nástroj IdM.

V rámci VZ musí být systémy napojovány a řízeny následovně:

- přímou integrací - budou napojeny pouze systémy SAP (BAPI), MS AD (LDAPS) a JIRA (REST API)
- napojení prostřednictvím MS AD – řízení prostřednictvím skupin za účelem autentizace nebo zároveň autorizace
- řízení formou manuálního zadávání uživatelů a přiřazování rolí v aplikacích, přičemž IdM bude v tomto případě namísto propagace do koncových systémů provádět notifikace na určené specifické uživatelské skupiny, které provedou manuální realizaci změn v koncových aplikacích a následně zpětně potvrdí IdM výsledek manuální realizace.

## 4 Požadavky na plnění

Plnění Veřejné zakázky se musí skládat alespoň z níže uvedených fází, které jsou následně podrobně popsány níže v jednotlivých podkapitolách:

- Implementační analýza a Analýza rizik
- Dodávka a implementace nástroje IdM a jeho integrace se zdrojovými systémy, vícero instancemi (forestry) AD, JIRA a zapojenými systémy (30 zapojených systémů)
- Dokumentace řešení
- Školení uživatelů a administrátorů
- Příprava adopční (komunikační) kampaně pro zaměstnance SŽ a i externí uživatele
- Testovací provoz
- Odborná technická podpora
- Služby na vyžádání
- Dodávka licencí k nástroji IdM

Výčet funkčních a nefunkčních požadavků je umístěn v příloze č. 13 zadávací dokumentace Seznam požadavků na systém IdM – funkční a nefunkční vlastnosti.

## 4.1 Implementační analýza a Analýza rizik

### 4.1.1 Implementační analýza

#### Předpokládaný postup projektu

Cílem implementační analýzy bude zpracovat analýzu obsahující minimálně tyto body:

- UX řešení
- Analýza zdrojových systémů a dat a cílových systémů a způsobů napojení
- Analýza identit, rolí, procesů a metodik
- Definování business rolí, aplikačních a technických rolí a forem jejich tvorby (příprava migračního plánu do nástroje IdM)
- Analýza a návrh provozního modelu v rámci infrastruktury, potřebných zdrojů, sizingu
- Návrh procesů správy životního cyklu identit
- Návrh schvalovacích workflow pro napojované systémy (UAS, TDS)
- Analýza a dopřesnění datového modelu správy identit vytvořeného v rámci Etapy 1
- Návrh postupu pro napojování systémů (bude sloužit jako podklad pro dodavatele těchto systémů k integraci na IdM)
  - Pro zdrojové systémy (SAP, JIRA)
  - Pro systémy napojené prostřednictvím AD včetně způsobu napojení na MS AD samotné
  - Pro koncové systém napojené přímo na IdM
  - Pro PAM
- Podrobný harmonogram implementace IdM

- Osnova, rozsah a harmonogram školení pro administrátory a garanty (klíčové uživatele) zapojených systémů
- Návrh testovacích scénářů a use-casů
  - Návrh metodiky/postupu testování
  - Návrh use-casů (dopřesnění use-case proběhne v rámci implementace)
  - Návrh testovacích scénářů (dopřesnění testovacích scénářů proběhne v rámci implementace)

Součástí Implementační analýzy bude zpracování metodiky pro implementaci řešení dle navrženého stavu včetně dokumentace z jednotlivých fází.

#### 4.1.2 Analýza rizik

Součástí Implementační analýzy bude realizace Analýzy rizik implementace IdM s návrhem relevantních opatření, které eliminují identifikovaná implementační a provozní rizika.

### 4.2 Implementace nástroje IdM a jeho integrace

Cílem této fáze bude dodávka a implementace nástroje IdM v prostředí SŽ a realizace všech souvisejících implementací a integrací se zdrojovými systémy a s koncovými systémy, jejichž uživatelská základna bude zpravována pomocí nástroje IdM. Součástí milníku je i migrace dat do nástroje IdM.

ID	Oblast	Popis
P1	Funkční a nefunkční požadavky na nástroj IdM	Funkční a nefunkční požadavky jsou definovány v příloze č. 13 zadávací dokumentace - Seznam požadavků na systém IdM – funkční a nefunkční vlastnosti.

#### 4.2.1 Instalace IdM

Dodavatel provede instalaci IdM do třech nezávislých prostředí SŽ (Vývoj, Test, Produkce). Produkční instance bude provozována v režimu HA. Počet nodů a hardwarové požadavky budou upřesněny v rámci Implementační analýzy, případně jsou dále popsány v dalších přílohách této zadávací dokumentace. Vzhledem k tomu, že SŽ hodlá provozovat instance MS AD v technologických sítích, požaduje zároveň instalaci IdM sondy (další instance nebo oddělená část IdM) v technologické síti. IdM sonda musí zabezpečeně komunikovat s hlavní instancí IdM a řídit identity a role v aplikacích v technologické síti. IdM sonda bude obsahovat vždy pouze identity a role nutné ke správě aplikací v dané technologické síti.

Řízené koncové systémy budou připojeny prostřednictvím:

- konektoru LDAP nebo prostřednictvím MS AD
- proprietárního konektoru
- databázového konektoru
- rozhraní webových služeb

Off-line koncové systémy budou řízené formou manuální správy identit uživatelů a řízení rolí v koncových aplikacích řešitelskou skupinou (skupina osob s byznys rolí aktéra k dané aplikaci), přičemž IdM zajistí správu identit a rolí a schválení. Řešitelská skupina následně zajistí na základě požadavku generovaného IdM (nebo JIRA) manuální nastavení konkrétních úkonů (uživatelů, oprávnění) včetně zadání zpětné vazby o realizaci požadavků zpět do IdM (nebo JIRA, která bude tuto skutečnost propagovat do IdM).

#### **4.2.1.1 Požadavky na životní cyklus identit**

Kompletní přehled funkčních a nefunkčních požadavků kladených na řešení IdM je uveden v příloze č. 13 zadávací dokumentace, níže je prezentovaný pouze stručný výčet pro potřeby tohoto dokumentu.

SŽ požaduje implementaci následujícího životního cyklu pro načítané objekty:

- Načítání personálních informací o identitách z autoritativního zdroje SAP v definovaných periodách, jejich konsolidaci a vytvoření unikátní identity.
- Dynamické vytváření objektů organizační struktury v IdM dle organizační struktury v HR systému zadavatele.
- Dynamické vytváření uživatelů v IdM, atributy uživatele evidované IdM provázané s HR, procesy (založení, aktualizace, aktivace/deaktivace identity, přejmenování, změna organizační struktury, operace s aplikačními rolemi apod.) a mechanismus generování centrálního username, password a e-mailové adresy. E-mailové notifikace. Doručení iniciálního hesla vedoucímu novému uživateli e-mailem.
- Tvorba byznys rolí
  - Organizační byznys role
  - Činnostní byznys role
  - Byznys role vytvořené na základě dalších požadavků věcnými garanty
  - Role aktérů ve schvalovacích řízeních a řešitelských skupinách
- Automatizace přiřazení do byznys rolí na základě informací z HR.
- Generování unikátního ID (neměnné číslo) pro každou identitu nebo přiřazení jedinečného identifikátoru osoby ze SAP, kde bude použit atribut „ID identity IDM“. IdM musí zajistit případnou propagaci tohoto identifikátoru až do koncového systému.
- Vytváření IdM procesů v návaznosti na informace z HR a do koncových systémů (založení, aktualizace, aktivace/deaktivace identity, přejmenování, změna organizační struktury, operace s aplikačními rolemi apod.)

- Aktualizace uživatele v koncových systémech:
  - Aktualizace všech atributů identity, které jsou vzájemně evidovány v IdM a koncových systémech na základě informací z HR.
- Aktivace a deaktivace v koncových systémech:
  - Pokud to koncový systém dovoluje, aktivování nebo deaktivování uživatele v koncovém systému na základě informací z HR a atributů platnost od a do.
- Přiřazení a odebrání aplikačních rolí:
  - Přiřazování a odebrání aplikačních rolí v koncových systémech na základě Business rolí, nebo ručním zásahu administrátora.
- Načítání uživatelů v koncových systémech a narovnání zjištěných nesouladů mezi koncovým systémem a IdM.
- Vícekrokové workflow pro přidání/odebrání rolí uživateli včetně schvalování, které bude prostřednictvím integrace přenášeno do JIRA.
- Rozhraní pro uživatele (selfservice), které bude zobrazovat profil uživatele, tedy obsahovat přehled aktuálně platných rolí v aplikacích daného uživatele, možnost žádat o přidělení nových byznys rolí, aplikačních rolí, možnost změny hesla. V případě vedoucích pracovníků musí toto rozhraní zobrazovat profily uživatelů podřízených danému vedoucímu dle schématu organizační struktury. Zároveň bude obsahovat možnost přepínání pracovněprávního vztahu.
- Vytvoření rolí, které zajišťují autorizaci uživatele pro práci v IdM (např. administrátor, správce rolí, aktér ve schvalovacích řízeních, člen řešitelské skupiny provádějící manuální nastavení v koncových systémech, koncový uživatel apod.)
- E-mailové notifikace s ohledem na operace s uživateli a prostředí pro jejich správu (tvorbu, úpravy).
- Dodávku následujících reportů:
  - Report oprávnění, která jsou u uživatele přiřazena v koncovém systému, ale nejsou přiřazena jako role v IdM.
  - Report účtů, ke kterým existuje v IdM vlastník, ale které vznikly mimo vědomí IdM.
  - Uživatelský report, auditní report (změny provedené přes IdM), rekonciliační report.
- Přístup externích správců oprávněných osob, kteří budou pouze ve vlastní organizační skupině (vlastní organizační struktuře) spravovat své identity a žádat o jejich role. Nová žádost o identity zadaná externím správcem do IdM je prostřednictvím integrace odesílána do SAP formou žádosti a následně v SAP po přidělení ID a validaci zařazena do odpovídající organizační struktury a odeslána zpět do IdM s ostatními identitami a aktivována.

## 4.2.2 Integrace zdrojových systémů pro IdM

### **SAP - Personální systém**

Napojení ze SAP do IdM

SŽ požaduje napojení (čtení) autoritativního zdroje dat z HR systému vedeném v ERP SAP. Integrace bude realizována formou exportu do DB tabulek. Konsolidace dat bude upřesněna v rámci implementační analýzy a je požadována v rámci tohoto projektu.

Z autoritativního zdroje budou do IdM načítány minimálně tyto typy objektů:

- Zaměstnanci (PP, DPČ, DPP)
- Spolupracující externisté
- Externisté smluvní (dodavatelé aj.)
- Externisté zákazníci (dopravci aj.)
- Organizační struktura a její parametry
- Ostatní parametry nutné pro správný chod a funkčnost IdM

### **Napojení z IdM do SAP**

SŽ požaduje vytvoření rozhraní umožňující odesílání nově vytvořených žádostí o identitu v IdM do SAP k jejich validaci (zpravidla u externistů typu dopravce).

### **Active Directory**

SŽ požaduje obousměrnou integraci na vícero instancí MS Active Directory, přičemž integrace bude mj. zahrnovat přenos informací o identitách, uživatelích, uživatelských účtech, organizačních strukturách, rolích, a to ze všech instancí AD, které jsou nebo budou v rámci infrastruktury SŽ vytvořeny, včetně technologických.

### **JIRA Atlassian – Service desk (Cloud)**

SŽ požaduje obousměrnou integraci na JIRA včetně CMDB, přičemž CMDB bude zdrojem dat o aplikacích včetně parametrů.

SŽ požaduje, aby v rámci integrace IdM předávalo do JIRA veškerá data potřebná pro outsourcing schvalovacího procesu (workflow) do JIRA. Vytvořené tickety budou přenášeny do JIRA včetně aktérů (schvalovatelů). Veškeré činnosti, včetně výsledku workflow ticketů v rámci JIRA pak následně musí být ihned zrcadleny do IdM tak, aby byla za každého stavu zajištěna konzistence schvalovacího procesu v obou aplikacích, JIRA jako nástroj pouze zprostředkovávala schvalovací workflow a IdM zůstalo řídicím prvkem.

Detailnější informace o funkčním modelu jsou k dispozici v neveřejné části zadávací dokumentace - příloze č. 10 zadávací dokumentace – Podklady pro cílové řešení.

#### 4.2.3 Integrace systémů napojených na IdM

SŽ předpokládá integraci 30 koncových systémů, přičemž je lze rozdělit do několika skupin dle formy integrace:

- Systémy napojené přímo na IdM (SAP) prostřednictvím vhodné integrace (webová služba, DB, BAPI)
- Systémy napojené prostřednictvím MS AD
  - IdM zajišťuje propagaci účtů a rolí na základě zavedení do bezpečnostní skupiny v MS AD
  - koncové aplikace provádí autentizaci nebo zároveň i autorizaci vůči MS AD.
- Systémy off-line, kde IdM provádí formální evidenci, správu a schvalování požadavků na identity, uživatele a role a ty jsou pak manuálně zadávány do koncových systémů prostřednictvím řešitelské skupiny.

Dodavatel bude v rámci integračních procesů odpovědný za případnou identifikaci chybových stavů při realizaci a testování integračních vazeb nástroje IdM a koncových systémů až na úroveň kompletní funkcionality zajišťované IdM nástrojem pro koncové systémy.

#### 4.2.4 Testování

Rozsah testování je popsán v příloze č. 12 zadávací dokumentace – Testování systému IdM.

#### 4.2.5 Migrace dat

V rámci implementace nástroje IdM budou do nástroje migrovány data ze zdrojových systémů (Organizační a činností role, organizační struktura, identity, platnosti smluv a další identifikované údaje definované implementační analýzou) a z napojovaných systémů (aplikační role a další identifikované údaje definované implementační analýzou). Přesný rozsah migrace dat bude definovat Implementační analýza.

#### 4.2.6 Systémové a licenční požadavky

Systém IdM musí být v souladu se specifiky stanovenými přílohou č. 9 Zadávací dokumentace – Platforma SŽ.

SŽ požaduje:

- Počet identit byl minimálně 40 000



- Neomezené počty instancí IdM, přičemž se předpokládá hlavní instance (v HA režimu 3 nodů) a instance IdM sondy (v HA režimu 2 nodů)
- Neomezené počty koncových (cílových) systémů
- Neomezené počty konektorů a integrací na okolní systémy

SŽ požaduje, aby v rámci plnění zakázky byly dodány všechny zdrojové kódy, které dodavatel vytvořil v rámci plnění zakázky, přičemž budou dodány a průběžně aktualizovány dle přílohy č. 8 - Zvláštní obchodní podmínky k ICT zakázkám. .

Zadavatel požaduje, aby v rámci Veřejné zakázky byly zahrnuty i licence třetích stran a používání implementovaného nástroje IdM jako celku nevyžadovalo žádné další dodatečné náklady (tím není myšleno licence koncových (cílových) systémů).

## 4.3 Dokumentace řešení

### 4.3.1 Instalační, konfigurační a související dokumentace

Cílem této fáze je zpracování kompletní instalační a konfigurační dokumentace.

Dodavatel zpracuje kompletní a podrobnou dokumentaci všech instalačních a konfiguračních procesů, včetně konkrétního nastavení souvisejících služeb a nástrojů pro prostředí SŽ.

Minimální požadavky na výstupní dokumentaci obsahuje následující tabulka:

	Oblast	Popis
	Kompletní instalační a konfigurační dokumentace	<p>Zpracování kompletní a podrobné dokumentace všech instalačních a konfiguračních procesů, včetně konkrétního nastavení SW komponent pro prostředí SŽ a souvisejících nástrojů, které jsou předpokladem pro úspěšné nasazení a provozování IdM nástroje a jsou také předmětem implementace (až do úrovně snímků obrazovek jednotlivých komponent). Instalační a konfigurační dokumentace musí být natolik podrobná, aby na základě dokumentace pracovníci SŽ byli schopni instalační a konfigurační práce provést.</p> <p>Jako součást dokumentace požaduje SŽ také zpracování odhadu pracnosti implementace a konfigurace (např. v MD), které bude muset SŽ vynaložit k dokončení implementace podle návrhu.</p> <p>Části dokumentace popisující prostředí systémů (dokumentace výrobce a snímky obrazovek) mohou být v anglickém jazyce.</p>

		Dokumenty pro koncové uživatele (návody, popis procesů) musí být v českém jazyce.
	Související dokumentace	Zpracování plánů kontinuity (BCP) a plánů obnovy (DRP). BCP a DRP budou zpracovány v podobě dostatečné pro jejich budoucí využití v reálné krizové situaci. BCP a DRP budou přehledné, jasné a funkční. Zpracovaný DRP bude formalizovaným pro zachování alespoň omezeného fungování služby technickým postupem obnovy provozu služby a bude obsahovat nezbytné části pro jeho realizaci, tzn. zejména jeho cíle, parametry obnovy, dopady výpadku, organizaci a odpovědnosti, nástroje a procedury obnovy. BCP jakožto postup / procesu bude obsahovat náhradní průběh poškozené služby / procesu a zdroje pro zajištění dočasného náhradního fungování (zejména prostory, lidské zdroje, technologie, nástroje).
	Exit plán	SŽ požaduje zpracování exit plánu, který bude definovat rozsah součinnosti Dodavatele IdM nástroje, popis způsobu exportu všech dat z nástroje IdM, popis datové struktury.
	Minimální požadovaná struktura dokumentace	SŽ požaduje zpracování dokumentace odpovídající požadavkům ISMS a ITSM. Požadavky na dokumentaci jsou uvedeny v interním předpisu č.j. 56805/2018-SŽDC-GŘ-O30 (viz příloha č. 1 Zadávací dokumentace).

#### 4.3.2 Spolupráce na aktualizaci vnitropodnikové dokumentační základny

Dodavatel zajistí návrh doplnění provozních dokumentací všech dotčených systémů implementací nástroje IdM (30 provozních dokumentací) a revize vnitropodnikových politik, směrnic a pokynů SŽ.

Cílem aktualizace dotčených dokumentů je popsat způsob jakým bude probíhat proces správy uživatelských oprávnění a změny hesel v kontextu implementace nástroje IdM v rámci SŽ a jednotlivých zapojených systémů. Dodavateli budou poskytnuty všechny provozní dokumentace k systémům a relevantní vnitropodnikových politik, směrnic a pokynů SŽ, dodavatel formou revizí navrhne jejich aktualizaci a v rámci akceptace je předloží ke schválení Garantovi každého systému.

Zadavatel nepředpokládá, že se jedná o více než 35 dokumentů a rozsah aktualizace dokumentů bude pouze v kontextu implementace nástroje IdM.

## 4.4 Příprava adopční (komunikační) kampaně pro zaměstnance SŽ a externí uživatele

Dodavatel zajistí přípravu komplexní adopční (komunikační) kampaně určené pro zaměstnance SŽ a i všechny externí uživatele. Parametry kampaně jsou definovány v samostatné příloze, kde jsou popsány cíle, minimální rozsah, forma a harmonogram realizace. Adopční kampaň by měla současně působit jako školicí nástroj pro běžné uživatele.

	Oblast	Popis
	Adopční	Minimální požadavky a rozsah adopční (komunikační) kampaně je definován v příloze č. 11 zadávací dokumentace - Komunikační kampaň

## 4.5 Školení uživatelů a administrátorů

Dodavatel zajistí školení pracovníků SŽ v oblasti administrace, provozu a uživatelském používání implementovaného nástroje IdM.

Minimální požadavky obsahuje následující tabulka:

	Oblast	Popis
	Zajištění školení	<ul style="list-style-type: none"> <li>Výstupem budou školicí manuály pro guaranty/klíčové uživatele, běžné uživatele i provozní administrátory.</li> <li>Dodané manuály budou poskytnuty v podobě přizpůsobené k pozdějším úpravám (doc, pdf).</li> <li>Pro účely školení administrátorů bude využita instalační a konfigurační dokumentace. Dodavatel zajistí školení pověřených pracovníků v oblasti provozní administrace pro cca 10 osob v rozsahu instalační a konfigurační dokumentace tak, aby byli administrátoři řešení schopni úspěšně spravovat na úrovni L1 a L2. Školení proběhne v prostorách SŽ za přítomnosti školitelů Dodavatele v minimálním rozsahu 1 MD.</li> <li>Pro účely školení garantů/klíčových a běžných uživatelů Dodavatel vytvoří školicí manuál, jenž bude podkladem pro osobní školení garantů/klíčových uživatelů všech napojovaných systémů na IdM.</li> <li>Školení garantů/klíčových a běžných uživatelů (maximálně 45 fyzicky přítomných osob) proběhne fyzicky v prostorách Zadavatele v prostorách SŽ za přítomnosti školitelů</li> </ul>

		<p>Dodavatele s možností se ke školení přihlásit i vzdáleně v minimálním rozsahu 1 MD každého školení.</p> <ul style="list-style-type: none"> <li>• Součástí školícího manuálu pro garanty/klíčové uživatele a běžné uživatele musí být podrobný popis všech činností koncových uživatelů týkajících se ovládání portálu IdM, přihlašování do aplikací, žádosti o přidělení přístupu a změny hesel.</li> <li>• Po skončení školení zpracuje Dodavatel do školícího manuálu zpětnou vazbu a připomínky vyškolených administrátorů.</li> <li>• Zadavatel požaduje, aby pro administrátory byly realizovány 2 školení v různých termínech, pro garanty/klíčové a běžné uživatele byly realizovány 3 školení v různých termínech.</li> <li>• Ze všech školení bude Zadavatelem pořízen záznam, který bude moci Zadavatel dále využívat jako školící materiál.</li> </ul>
--	--	--

## 4.6 Testovací provoz

Před uvedením IdM do produkčního prostředí bude Dodavatel ve spolupráci se Zadavatelem provozovat IdM nástroj v testovacím provozu. Cílem tohoto období bude identifikace případných provozních/konfiguračních nedostatků a jejich oprava před uvedením nástroje do plného provozu. V rámci tohoto období bude Dodavatel poskytovat zvýšenou podporu (nikoliv Odbornou technickou podporu) při řešení identifikovaných nedostatků.

Testovací provoz bude zakončen akceptací a převzetím IdM jako celku do produkčního provozu.

## 4.7 Odborná technická podpora

Dodavatel zajistí odbornou technickou podporu k implementovanému řešení po dobu 5 let od převzetím IdM jako celku do produkčního provozu (ukončení Fáze 6).

Detailní požadavky obsahuje následující tabulka:

	Oblast	Popis
	Zajištění odborné technické podpory implementovaných technologií	<p>Dodavatel zajistí odbornou technickou podporu implementovaného řešení:</p> <p>(1) poskytování expertních služeb, které budou využívány zejména pro podporu činností SŽ v případě řešení</p>

	Oblast	Popis
		<p>nestandardních stavů a pro profylaxi řešení, aby se předcházelo omezením jeho správné funkčnosti.</p> <p>(2) Instalaci aktualizací IdM nástroje a jednotlivých dodaných komponent</p> <p>(3) Odborná technická podpora bude poskytována po dobu 5 let od převzetím IdM jako celku do produkčního provozu (ukončení Fáze 6).</p> <p>(4) odborná technická podpora bude poskytována v souladu s ustanoveními Zvláštních obchodních podmínek pro Zakázky v oblasti ICT (Příloha č. 5 Závazného vzoru smlouvy) podle servisního modelu A5). Plánované změny či významné změny (aktualizace atp.) budou ze strany Dodavatele poskytnuty (uvolněny) SŽ vždy v pracovních dnech, a to konkrétně v pondělí a ve středu. V případě, že plánovaná změna či významná změna a její poskytnutí vychází na státní svátek, vyzve Dodavatel SŽ k upřesnění poskytnutí (uvolnění).</p> <p>(5) Poskytování služeb Helpdesku ze strany Dodavatele bude realizováno po celou dobu trvání odborné technické podpory v souladu s čl. 10.1.2 Zvláštních obchodních podmínek pro Zakázky v oblasti ICT (Příloha č. 5 Závazného vzoru smlouvy) v Režimu 4 (5×8, tj. v pracovních dnech v době od 7:00 do 15:00).</p> <p>(6) Měření SLA bude realizováno na straně Dodavatele.</p> <p>(7) Součinnost při auditech řešení, opravu a zapracování identifikovaných nedostatků</p>

## 4.8 Služby na vyžádání

Dodavatel poskytne SŽ služby na vyžádání, přičemž půjde o:

- Poskytnutí až 500 MD, které bude moci Zadavatel využít k v rámci zvýšené technické podpory, k rozvoji nástroje IdM nebo vytvoření přímé integrační vazby s dalšími systémy provozovanými SŽ (zdrojové/koncové systémy)
- integraci dalších koncových systémů do nástroje IdM pomocí AD 's

SŽ není povinna služby na vyžádání čerpat.

## 5 Fáze dodávky a akceptační milníky

Dodávka má být dodána v níže uvedených následujících fázích. Každá z níže uvedených fází (tj. každý řádek níže uvedené tabulky) musí být SŽ separátně akceptována nejpozději v termínu uvedeném v Harmonogramu. SŽ akceptuje výstupy dané Fáze, jestliže je Dodavatel provedl v šíři a kvalitě požadované ve výzvě k podání nabídek této Veřejné zakázky. V opačném případě je Dodavatel povinen napravit nedostatky dodávky.

Fáze	Popis	Ukončení fáze	Kapitola obsahující požadavky
<b>F1.1</b>	Implementační analýza – Plán nasazení IdM a připojení systémů	Fáze F1 bude ukončena akceptací dokumentu akceptačním protokolem.	4.1.1
<b>F1.2</b>	Implementační analýza – Analýza rizik		4.1.2
<b>F2.1</b>	Implementace (instalace) nástroje IdM	Fáze F2.1, F2.2 a F2.3 budou ukončeny splněním všech vhodných testů F2.4 akceptačním protokolem. Fáze F2.5 bude ukončena splněním testů migrace dat akceptačním protokolem.	4.2.1
<b>F2.2</b>	Integrace zdrojových systémů		4.2.2
<b>F2.3</b>	Integrace systémů napojených na IdM		4.2.3
<b>F2.4</b>	Testování		4.2.4
<b>F2.5</b>	Migrace dat		4.2.5
<b>F3.1</b>	Dokumentace řešení - Instalační, konfigurační a související dokumentace	Fáze F3 bude ukončena akceptací dokumentace akceptačním protokolem.	4.3.1
<b>F3.2</b>	Dokumentace řešení - Spolupráce na aktualizaci vnitropodnikových norem		4.3.2
<b>F4</b>	Příprava adopční (komunikační) kampaně	Fáze F4 bude ukončena akceptací výstupů akceptačním protokolem	4.4
<b>F5</b>	Školení uživatelů a administrátorů	Fáze F5 bude ukončena akceptací provedených školení akceptačním protokolem	4.5
<b>F6</b>	Testovací provoz zakončený akceptací a převzetím IdM do produkčního provozu	Fáze F6 bude ukončena akceptačním protokolem.	4.6
<b>F7</b>	Odborná technická podpora	Fáze F7 bude vykazována na základě pravidelných výkazů.	4.7

<b>Fáze</b>	<b>Popis</b>	<b>Ukončení fáze</b>	<b>Kapitola obsahující požadavky</b>
<b>F8</b>	Služby na vyžádání	Fáze F8 bude ukončena akceptačním protokolem objednaných služeb.	4.8