Klasifikace: Veřejný dokument

SPRÁVA ŽELEZNIC

Příloha č. 1 zadávací dokumentace veřejné zakázky s názvem „Zavedení systému PAM v prostředí SŽ“

Technická specifikace

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

Obsah

1 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
DR	Disaster Recovery (obnova po havárii)
EPS	Elektronické protipožární systémy
EZS	Elektronické zabezpečovací systémy
GPA	Garant primárního aktiva
GPdA	Garant podpůrného aktiva
HA	Režim vysoké dostupnosti (High Availability), např. prostřednictvím redundance
Harmonogram	Harmonogram stanovený ve Smlouvě o dílo, konkrétně v její příloze „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
ISMS	Information Security Management Systém (systém řízení bezpečnosti informací)
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)
MPLS	Multiprotocol Label Switching / Multiprotokolové přepojování
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)
OT	Operational Technology / Operační technologické sítě a prvky
PAM	Správa privilegovaných přístupů (Privileged Access Management)
PIM	Správa privilegovaných identit (Privileged Identity 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
UI	Uživatelské rozhraní (User Interface)
VPN	Virtuální privátní síť (Virtual Private Network)
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), v aktuálním znění
ZoKB	Zákon 181/2014 Sb., o kybernetické bezpečnosti, v aktuálním znění

Seznam zkratek pro specifické aplikace 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
SŽE	Správa železniční energetiky
TechDS	Technologický a dohledový systém
TDS TECHLAN	Technologická datová síť
TDCDP	Traťový dispečer dálkového ovládání zabezpečovacího zařízení na CDP
VS	Vlakové soupravy

2 Úvod

Tento dokument je přílohou a nedílnou součástí zadávací dokumentace veřejné zakázky „Zavedení systému PAM v prostředí SŽ" (dále jen „veřejná zakázka"), pro organizaci Správa železnic, státní organizace (dále jen „SŽ"). Dokument popisuje technické a jiné požadavky na veřejnou zakázku.

2.1 Záměr SŽ v oblasti systému pro správu privilegovaných účtů a přístupů (PAM/PIM)

Implementace systému PAM[1] (Privileged Access Management) a jeho napojení na aktiva organizace je v souladu s dlouhodobou koncepcí řízení privilegovaných účtů a přístupových oprávnění, jejich kontroly a zvýšení zabezpečení přístupů ke správě aktiv SŽ. S ohledem na velikost organizace, složitost ICT prostředí a velké množství aktiv, neplánuje SŽ zavedení systému PAM/PIM pro všechna aktiva v jednom kroku, ale plánuje postupné připojování podle technických a organizačních možností. V cílovém stavu je plánována správa privilegovaných účtů a přístupů systémem PAM/PIM k systémům kritické informační infrastruktury i podpůrným a technickým aktivům.

Cílem projektu „Zavedení systému PAM v prostředí SŽ" a s tím spojené veřejné zakázky je revize současného systému PAM[2] a jeho rozšíření na definované cílové systémy (vybraná podpůrná a technická aktiva, vybrané systémy KII), kde SŽ požaduje oddělenou implementaci PAM/PIM pro prostředí UAS a prostředí TDS.

Hlavními cíli zavedení systému PAM/PIM v prostředí SŽ jsou zejména:

- zvýšení bezpečnosti ICT prostředí SŽ, ochrana před hrozbami krádeže privilegovaných účtů a zneužití privilegovaných oprávnění;
- zajištění systematické a strukturované správy privilegovaných identit a účtů a na ně navázaných privilegovaných přístupů ke správě ICT systémů SŽ;
- nastavení procesů řízení, monitorování, zabezpečení a audit všech lidských i automatizovaných privilegovaných identit a činností při správě systémů SŽ;
- splnění legislativních požadavků vyplývajících ze ZoKB a VoKB.

V současnosti SŽ provozuje systém PAM/PIM založený na technologii CyberArk pro jednotky cílových systémů. V rámci této veřejné zakázky SŽ požaduje také provedení revize stávajícího systému s ohledem na změny v architektuře a technologiích ICT prostředí SŽ a dále rozšíření systému PAM/PIM pro správu definovaných IT aktiv.

[1] V této veřejné zakázce je pod pojmem PAM zahrnuta i funkcionalita PIM (Privileged Identity Management).

2.2 Předmět plnění veřejné zakázky

Cílem veřejné zakázky je uzavření smlouvy, jejímž předmětem bude revize současného systému pro správu privilegovaných účtů, jejich životního cyklu a řízení privilegovaných přístupů (PAM) k aktivům SŽ a rozšíření implementace systému PAM/PIM na definovaná aktiva SŽ. Nedílnou součástí služeb bude i provedení podrobné předimplementační analýzy a vypracování prováděcího projektu a harmonogramu implementace.

Předmětem plnění veřejné zakázky je:

- poskytnutí služeb předimplementační analýzy, detailního návrhu řešení a prováděcího projektu,
- revize současného systému PAM a implementace systému PAM/PIM na definovaná aktiva SŽ,
- dodávka nezbytných chybějících[3] licencí systému PAM/PIM,
- zajištění služeb technické podpory výrobce systému PAM/PIM pro všechny využité licence,
- zajištění školení pracovníků SŽ na dodané technologie a konkrétní implementaci,
- služby na vyžádání,
- post-implementační technická podpora systému PAM/PIM.

Plnění bude obsahovat následující poptávané oblasti:

Fáze 1: Předimplementační analýza

Zpracování podrobné předimplementační analýzy zavedení systému PAM/PIM v prostředí SŽ pro aktiva definovaná v příloze č. 3 zadávací dokumentace (podpůrná a technická aktiva, systémy KII), včetně definování požadavků na fyzický HW a virtuální stroje pro provoz systému PAM/PIM.

Předimplementační analýza zahrnuje i revizi konfigurace stávající implementace PAM a její využití v dalších částech implementace.

Předimplementační analýza bude obsahovat také detailní návrh řešení a prováděcí projekt včetně harmonogramu dalších kroků a definice požadavků na nezbytnou součinnost SŽ.

Fáze 2: Implementace PAM/PIM pro úvodní dva cílové systémy z prostředí UAS, pilotní provoz implementace, školení

SŽ požaduje na základě schválených výstupů předimplementační analýzy provedení realizace implementace systému PAM/PIM pro úvodní dva systémy definované v příloze č. 3 zadávací dokumentace.

Implementace PAM/PIM pro definované systémy bude ověřena pilotním provozem v délce minimálně 4 kalendářních týdnů. V průběhu pilotního

[3] SŽ již disponuje perpetuálními licencemi PAM/PIM – jejich seznam je uveden v příloze zadávací dokumentace.

provozu poskytne dodavatel SŽ součinnost při provedení bezpečnostních testů implementace PAM/PIM a před ukončením pilotního provozu dodavatel odstraní případné neshody.

V rámci pilotního provozu zajistí dodavatel školení vybraných pracovníků SŽ v oblasti správy a provozu systému PAM/PIM.

Fáze 3: Rozšíření implementace PAM/PIM na zbývající definované systémy

Na základě schválené předimplementační analýzy a harmonogramu realizace provede dodavatel implementaci systému PAM/PIM pro zbývající systémy definované v příloze č. 3 zadávací dokumentace formou dílčích implementací po skupinách aktiv dle předimplementační analýzy.

Každá dílčí implementace PAM/PIM bude ověřena pilotním provozem v délce minimálně 2 kalendářních týdnů. V průběhu pilotního provozu poskytne dodavatel SŽ součinnost při provedení bezpečnostních testů implementace PAM/PIM a před ukončením pilotního provozu každé dílčí implementace dodavatel odstraní případné neshody.

Fáze 4: Implementace PAM/PIM pro jeden cílový systém v prostředí TDS a pilotní provoz implementace

SŽ požaduje na základě schválených výstupů předimplementační analýzy provedení realizace implementace systému PAM/PIM pro jeden systém KII v prostředí TDS definovaný v příloze č. 3 zadávací dokumentace.

Implementace PAM/PIM pro definovaný systém bude ověřena pilotním provozem v délce minimálně 4 kalendářních týdnů. V průběhu pilotního provozu poskytne dodavatel SŽ součinnost při provedení provozních a bezpečnostních testů implementace PAM/PIM a před ukončením pilotního provozu dodavatel odstraní případné neshody.

Fáze 5: Průběžná dodávka chybějících licencí

Pro každou dílčí implementaci PAM/PIM (fáze 2, fáze 3, fáze 4) dodavatel zajistí dodávku chybějících SW licencí. Licence musí plně pokrývat implementované části systému PAM/PIM. V případě dodávky časově omezených licencí (subskripce) musí být dodané licence platné minimálně po dobu tolika měsíců, kolik jich zbývá do uplynutí doby 48 měsíců od ukončení Fáze 2. Součástí licencí musí být i služba technické podpory výrobce PAM/PIM v délce stejné jako platnost licencí. Pro SŽ vlastněné perpetuální licence zajistí dodavatel technickou podporu výrobce těchto perpetuálních licencí v délce 48 měsíců.

Fáze 6: Technická podpora implementovaného řešení

Pro implementované řešení poskytne dodavatel službu technické podpory implementovaného řešení v délce 48 měsíců. Technická podpora je poskytována od uvedení první dílčí implementace PAM/PIM do produkce.

Fáze 7: Služby na vyžádání

Dodavatel poskytne SŽ služby konzultace na vyžádání. Služby mohou být čerpány především pro rozšiřování implementace systému PAM/PIM na další koncové systémy, a to jak pro podpůrná a technická aktiva, tak i pro systémy KII.

2.3 Oblasti, které nejsou předmětem plnění veřejné zakázky

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

- hardware pro provoz systému PAM/PIM,
- hardware/systém pro ukládání a archivaci relací,
- perpetuální licence PAM/PIM, které jsou již ve vlastnictví SŽ[4].

Pro provoz systému PAM/PIM SŽ poskytne dostatečné HW zdroje formou fyzických nebo virtuálních strojů v příslušných lokalitách podle technických a výkonnostních specifikací dodavatele, včetně systémů pro ukládání a archivaci dat a síťového prostředí. Virtuální stroje budou poskytnuty v souladu s kapitolou 5.1.1 přílohy č. 7 zadávací dokumentace (Platforma 2.0).

3 Technické podmínky veřejné zakázky

Řešení PAM/PIM plánuje SŽ v budoucnu nasadit na většinu prostředí informačních a komunikačních systémů SŽ. Část těchto systémů je klasifikována jako systémy KII v rámci ZoKB a VoKB. V rámci projektu „Zavedení systému PAM/PIM v prostředí SŽ" předpokládá SŽ zajištění správy privilegovaných účtů a přístupů pro aktiva definovaná v příloze č. 3 zadávací dokumentace.

Podpůrná a technická aktiva a systémy KII jsou provozována v poměrně složitém ICT prostředí, včetně odpovídající infrastruktury a infrastrukturních služeb. Z tohoto důvodu nejsou v současnosti u všech aktiv určených k napojení na PAM/PIM splněny předpoklady k úspěšné implementaci PAM/PIM (zejména dostupnost potřebných infrastrukturních služeb, dokončení segmentace sítí apod.). Bližší popis ICT prostředí SŽ je uveden v příloze č. 2 zadávací dokumentace.

Z výše uvedených důvodů předpokládá SŽ postupnou implementaci PAM/PIM a napojování koncových systémů v závislosti na splnění implementačních prerekvizit pro koncové systémy a lokality.

Z důvodu požadavků na bezpečné oddělení systémů kritické informační infrastruktury je požadována implementace oddělených systémů PAM/PIM. Je tedy požadována implementace systému PAM/PIM zajišťující správu privilegovaných účtů a přístupů aktiva v prostředí UAS (viz příloha č. 3 zadávací dokumentace) a oddělená

[4] Viz příloha č. 4 této zadávací dokumentace

implementace PAM/PIM pro správu privilegovaných účtů a přístupů pro systémy KII v prostředí TDS (viz příloha č. 3 zadávací dokumentace).

3.1 Základní požadované funkcionality řešení

Nástroj PAM/PIM musí být centralizované řešení (samostatně pro prostředí UAS a prostředí TDS), které bude zajišťovat zejména následující hlavní funkcionality:

- Správu privilegovaných účtů, která zahrnuje jejich autentizaci, autorizaci a ochranu privilegovaných hesel,
- Zaznamenávání aktivit privilegovaných účtů (tzv. „session recording"),
- Řízení konkrétních aktivit (operací) prováděných administrátory na koncových zařízeních.

Řešení PAM/PIM bude poskytovat řízení a správu privilegovaných účtů na následujících vrstvách:

- Aplikační[5],
- Infrastrukturní, která zahrnuje zejména:
  - operační systémy,
  - databázové systémy,
  - bezpečnostní systémy,
  - komunikační prvky,
  - datová úložiště,
  - adresářové služby,
  - systémy pro vzdálenou správu,
  - virtualizační nástroje (hypervizory).

Řešení PAM/PIM musí umožňovat řízení a správu následujících typů privilegovaných účtů:

- účty administrátorů (interní zaměstnanci i externí dodavatelé),
- servisní (systémové) účty,
- aplikační účty.

Řešení PAM/PIM musí umožňovat následující základní funkcionality, které jsou detailněji specifikovány v následujících podkapitolách této technické specifikace a v příloze č. 6 zadávací dokumentace. Jedná se především o následující oblasti:

- Řízení přístupu k PAM/PIM,
- Řízení a ochrana privilegovaných účtů a hesel, SSH klíčů,
- Řízení a analýza relací, nahrávání privilegovaných relací,
- Integrace PAM/PIM řešení s okolími systémy a systémy kybernetické bezpečnosti,
- Auditing.

[5] v případě, že z předimplementační analýzy vyplyne existence rozhraní pro napojení dané aplikace do PAM/PIM, popř. je možno takové rozhraní v rámci implementace PAM/PIM doplnit.

Požadavky na funkční a nefunkční vlastnosti, které musí systém PAM/PIM splňovat, jsou uvedeny v příloze č. 6 zadávací dokumentace.

Vlastnosti systému uvedené v oblastech L a M v příloze č. 6 zadávací dokumentace označené jako „Požadované" musí systém splňovat, avšak licence na tyto vlastnosti nemusí být součástí nabídky a dodávky řešení.

SŽ upozorňuje, že nabízené řešení musí splňovat všechny vlastnosti označené v příloze č. 6 zadávací dokumentace jako „Požadované".

3.1.1 Řízení přístupu k PAM/PIM

3.1.1.1 Identifikace a autentizace uživatelů PAM/PIM

Systém PAM/PIM musí fungovat jako prostředník mezi administrátorem a koncovým zařízením/systémem, ke kterému se daný administrátor chce přihlásit (např. server, aplikace, komunikační prvek). Administrátor bude přistupovat k UI rozhraní PAM/PIM a bude se autentizovat za využití vícefaktorové autentizace.

Autentizační systém může být pro různé spravované systémy různý, dodavatel musí počítat s možností autentizace vůči různým autentizačním službám (viz též popis prostředí v příloze č. 2 zadávací dokumentace).

Přihlašování k vybranému privilegovanému účtu na vybraném koncovém zařízení bude dále muset probíhat pomocí automatizovaného přihlášení (SSO) bez nutnosti znalosti a zadávání hesla administrátorem.

Přihlášení bude probíhat buďto přímo v prohlížeči prostřednictvím prohlížeče, který otevře okno s příslušnou klientskou aplikací, bez nutnosti její lokální instalace, nebo bude využito systému jump serverů.

Podporovány musí být běžné protokoly a aplikace:

- SSH
- Telnet
- Remote Desktop (RDP)
- Webové aplikace
- Aplikace spouštěné v prostředí Microsoft Windows.

Při návrhu identifikace a autentizace musí dodavatel také počítat s budoucí integrací PAM/PIM na systém správy identit a přístupů (IDM), kdy IDM bude sloužit jako zdroj identit pro PAM/PIM.

3.1.1.2 Autorizace

Po úspěšné identifikaci a autentizaci bude administrátor autorizován a získá množinu privilegovaných účtů, kterými bude moci disponovat. Kromě účtů, které bude mít administrátor k dispozici, může mít také přiřazeny účty, ke kterým může získat přístup až po udání důvodu nebo po schválení jiným uživatelem nebo skupinou uživatelů. Takový přístup bude moci získat na definovanou dobu (omezenou dobu nebo na stálo). Dodavatel musí počítat s integrací této funkce na externí nástroj typu ServiceDesk nebo jiný nástroj pro schvalovací workflow.

3.1.1.3 Emergency (nouzové) přístupy

V případě nouzové situace, kdy je potřeba získat okamžitě přístup k heslu privilegovaného účtu a není dostupná příslušná odpovědná osoba, musí nástroj PAM/PIM podporovat tzv. „Breaking glass" proces. V takovém případě jsou definovány zástupné osoby, které si mohou vyžádat přístup k danému privilegovaného účtu (za současného zaznamenání této operace, nahrávání session a notifikace odpovědné osoby).

Nástroj PAM/PIM musí podporovat následující procesní opatření týkající se použití nouzových (emergency) účtů na koncových zařízeních v případě nefunkčnosti PAM/PIM nástroje.

3.1.2 Řízení a ochrana privilegovaných účtů a hesel

3.1.2.1 Zabezpečené úložiště hesel

Hesla a další informace o privilegovaných účtech (zejména uživatelské jméno, heslo, práva, odkazy do integrovaných systémů) musí být uložena v zabezpečeném on-premise úložišti PAM/PIM (datový trezor), tyto údaje musí být šifrovány. Veškeré operace spojené s použitím privilegovaného účtu a hesla, musí být zaznamenány a evidovány (auditní stopa).

Veškeré komponenty řešení, ve kterých se nachází citlivé informace (včetně databází) musí zajistit, aby v nich uložené informace byly nativně šifrovány bez nutnosti použít šifrování třetí strany. Tato funkcionalita musí být dodána společně s řešením.

Dodané řešení musí z hlediska využití kryptografických prostředků splňovat minimálně standard FIPS 140-2 (nebo podobný standard s minimálně stejnou úrovní bezpečnosti) a současně splňovat doporučení NÚKIB „Minimální požadavky na kryptografické algoritmy v3.0" ze dne 1. července 2023.

3.1.2.2 Politika hesel

Nástroj PAM/PIM musí zajišťovat ochranu hesel privilegovaných účtů. Nástroj musí umožňovat nastavit politiku hesel (např. minimální délka hesla, maximální stáří hesla, požadavky na komplexitu hesla, opakované použití hesel z historie). Na základě této politiky hesel systém automaticky generuje nebo mění hesla ke spravovaným privilegovaným účtům (např. po každém použití privilegovaného hesla nebo v definovaném intervalu). Politika hesel musí odpovídat specifikaci ZoKB a VZoKB.

3.1.3 Politika automatického objevování (discovery) účtů

PAM/PIM musí obsahovat funkcionalitu automatického objevování (tzv. account discovery) systémů a účtů, která je spouštěna v pravidelné frekvenci. Nově objevené účty musí být před přidáním do systému PAM/PIM posouzeny odpovědnou osobou, zda se jedná o uživatelský účet patřící konkrétní identitě nebo o sdílený privilegovaný účet. Odpovědná osoba rozhodne o zařazení do správy systému PAM/PIM a přiřadí privilegovaný účet příslušným administrátorům a nastaví odpovídající politiku hesel.

3.1.3.1 Účty aplikací

Systém PAM/PIM musí umožňovat spravovat také účty aplikací a poskytuje mechanismy pro omezení použití otevřeného hesla přímo ve zdrojovém kódu aplikace nebo skriptu (tzv. „application-to-application" funkcionalita).

3.1.4 Nahrávání a řízení privilegovaných relací

Systém PAM/PIM musí obsahovat funkcionalitu nahrávání relací (tzv. „Session recording"), při které je snímána obrazovka a logovány vstupy, které administrátor zadá. V případě, že je nahrávání pro daný privilegovaný účet zapnuto, je nahrávána každá akce (stisk klávesy, změna obrazovky atd.). Lze tedy jednoznačně dohledat, kdo daný privilegovaný účet použil a jaké operace byly pod tímto účtem provedeny.

3.1.4.1 Zálohování a archivace nahrávek

Nahrávky musí být pravidelně zálohovány, musí být zajištěna dostupnost těchto záloh a ochrana proti neoprávněnému smazání. PAM/PIM musí umožňovat řídit životní cyklus nahrávek po dobu minimálně 18 měsíců (tj. nahrávky by měly být okamžitě k dispozici bez nutnosti jejich vyvolání z archivu). Nahrávky musí být archivovány po dobu minimálně 2 roky. Nahrávky musí být v souladu se ZoKB a VoKB.

3.1.4.2 Zabezpečení nahrávek

Nahrávané relace mohou obsahovat citlivé informace, proto musí být zajištěna důvěrnost, integrita a dostupnost nahrávaných záznamů po celou dobu, kdy jsou pod správou PAM/PIM. Dále musí být zajištěno bezpečné řízení přístupu k nahrávkám. Musí být zajištěno, že pouze autorizované osoby mohou mít k pořízeným záznamům přístup.

3.1.4.3 Rozsah nahrávaných relací

Přesné politiky pro nahrávání administrátorů budou stanoveny v průběhu analytické fáze dodávky v rámci předimplementační analýzy. Základním požadavkem je, že systém PAM/PIM musí být kapacitně schopen nahrávat současně relace **všech** administrátorů, kteří s PAM/PIM pracují.

Pro efektivní využívání kapacity datových úložišť musí PAM/PIM umožňovat efektivní záznam a přenos nahrávek (např. pomocí komprimace, zaznamenávání pouze změn v relaci apod.). Musí být podporovány minimálně následující formáty:

- Video nebo jiný obrazový formát (pro RDP relace).
- Metadata - např. názvy oken na obrazovce, stisknutá tlačítka, výstup příkazů na obrazovce, otevřené soubory apod. Struktura metadat musí být v souladu minimálně se specifikací ZoKB a VoKB.
- Textový přepis relace (u protokolu SSH a Telnet).

3.1.4.4 Řízení a analýza relací

PAM/PIM musí umožňovat vyhledávání v rámci nahrávaných relací (dle klíčových slov a dalších parametrů – metadat).

PAM/PIM musí umožňovat připojení třetí osoby (např. bezpečnostního administrátora PAM/PIM) k probíhající relaci z důvodu kontroly. Třetí osoba může probíhající relaci předčasně ukončit.

3.1.4.5 Řízení privilegovaných operací a zdrojů

SŽ požaduje řešení, které technickými prostředky umožní řízení a kontrolu privilegovaných operací, které může daný administrátor provádět. Jedná se zejména o řízení:

- příkazů na spravovaném systému/zařízení, které administrátor může/nemůže spouštět (tzv. „white listing/black listing"),
- zdrojů (např. souborů nebo adresářů) na koncovém zařízení, které administrátor může/nemůže využívat,
- časových oken definujících, kdy je možné ke správě systému/zařízení přistupovat.

3.1.4.6 Auditní záznamy

Nástroj PAM/PIM vytváří centrální log, kde jsou strukturovaně zaznamenány veškeré operace:

- administrátorů, kteří používají PAM/PIM řešení pro přístup ke spravovaným systémům/zařízením,
- bezpečnostních správců nástroje PAM/PIM, kteří provádí konfiguraci nástroje a správu politik.

Nástroj musí podporovat vytváření auditních reportů, které je možno parametrizovat. Výstupem jsou strukturované logy nebo reporty; logy jsou dále zpracovávány nástrojem typu SIEM (viz požadavky na integraci PAM/PIM).

3.1.4.7 Analytické nástroje

SŽ požaduje PAM/PIM řešení, které v sobě již obsahuje nástroje (popř. pro které existuje externí modul), které umožňují využívat behaviorálně analytické funkcionality nad probíhajícími privilegovanými relacemi. Nástroj se učí na základě běžného chování administrátorů a v případě vyhodnocení neobvyklého chování pod daným privilegovaným účtem dokáže automaticky zasáhnout do probíhající relace nebo upozornit bezpečnostního administrátora PAM/PIM. V případě, že tato funkcionalita je zajišťována externím modulem, musí být tento modul součástí dodávky a musí být řádně licencován.

3.1.5 Integrace PAM/PIM

Primárním zdrojem autentizace a autorizace privilegovaných účtů a jejich aktivit jsou adresářové služby Active Directory (dále jen „AD") a LDAP. Popis prostředí AD SŽ je uveden v příloze č. 2 zadávací dokumentace – Popis prostředí.

PAM/PIM musí umožňovat integraci a pravidelnou synchronizaci s uvedenými adresářovými službami a musí umožňovat i využití jiných autentizačních a autorizačních služeb (zejména pro prostředí TDS).

Současně je požadováno, aby PAM/PIM umožňoval správu i lokálně vytvořených privilegovaných účtů na koncových zařízeních, tj. účty, které nejsou založeny v AD nebo LDAP (zde SŽ předpokládá využití požadované funkcionality automatického objevování (Discovery) účtů).

3.1.5.1 Integrace s nástroji pro bezpečnostní monitoring

PAM/PIM musí být integrován do stávajících bezpečnostních dohledových nástrojů – konkrétně je požadována integrace minimálně s nástrojem typu SIEM a Log management nástroj.

V rámci integrace s nástrojem typu SIEM je požadován minimálně záznam aktivit PAM/PIM operace ve formě strukturovaných logů, které jsou dále v čase blízkém reálnému přenášeny a vyhodnocovány v SIEM nástrojích a ukládány pro případnou zpětnou analýzu, včetně napojení na nástroj Log managament.

V dokumentaci řešení dodavatel uvede strukturu logů z PAM/PIM (nebo odkaz na jednoznačnou dokumentaci), aby bylo možné vytvořit korelační pravidla pro SIEM.

Rozsah a struktura logů musí být v souladu s požadavky ZoKB a VoKB.

3.1.5.2 Schvalovací workflow

PAM/PIM musí umožňovat podporu procesů a schvalovacích workflow v rámci integrace s nástrojem Service Desk. Je požadováno, aby byly podporovány alespoň následující scénáře:

- Požadavek na řízení privilegovaných účtů, zejména:
  - přiřazení privilegovaného účtu konkrétnímu uživateli,
  - použití privilegovaného účtu,
  - aktivace privilegovaného účtu,
  - zrušení privilegovaného účtu,
  - obnova hesla atd.
- Požadavek na nahrávání nebo zrušení nahrávání relací u vybraného privilegovaného účtu nebo skupiny účtů.

3.1.6 Licence

Nezbytnou součástí plnění je i dodávka SW licencí systému PAM/PIM. Dodavatel zajistí dodávku chybějících SW licencí tak, aby systém PAM/PIM převedený do produkčního prostředí byl plně licencován – licence musí plně pokrývat aktuální implementované části systému PAM/PIM převedené do produkce. V případě dodávky časově omezených licencí (subskripce) musí být dodané licence platné minimálně po dobu tolika měsíců, kolik jich zbývá do uplynutí doby 48 měsíců od ukončení Fáze 2. Aktivace příslušných licencí proběhne vždy při převodu dílčí části implementace PAM/PIM do produkce[6]. Součástí licencí musí být i služba technické podpory výrobce PAM v délce stejné, jako

[6] tj. po provedení akceptačních funkčních, výkonnostních a zátěžových testů, ukončení pilotního provozu a převodu systému do produkce.

platnost licencí. Pro SŽ vlastněné perpetuální licence zajistí dodavatel technickou podporu výrobce těchto perpetuálních licencí v délce 48 měsíců.

Příloha č. 5 zadávací dokumentace určuje v tabulce "Požadavky na licenční pokrytí PAM/PIM" maximální parametry licenčního pokrytí, které může být součástí dodávky SW licencí. Rozsah licencí definovaný přílohou č. 5 zadávací dokumentace je nutno vnímat jako maximální a SŽ tento rozsah nemusí využít, kromě závazku k odběru licencí v minimálním objemu tak, jak je definován níže a v příloze č. 5 zadávací dokumentace Data pro sizing. Dodavatel bere na vědomí, že bez jakékoli sankce či poplatku SŽ, nemusejí být uvedené maximální hodnoty SŽ úplně využity.

Zadavatel se současně zavazuje k odběru licencí v minimálním objemu 250 licencí nad rámec perpetuálních licencí PAM/PIM, které SŽ již vlastní, avšak vzhledem k průběžné dodávce chybějících licencí se nezavazuje k využití licenčního pokrytí (podpory výrobce) těchto 250 nově pořizovaných licencí po celou dobu 48 měsíců.

Dodané řešení musí umožnit rozšíření řešení nad úroveň definovanou v požadavcích v příloze č. 5 zadávací dokumentace pouze dokoupením licencí bez nutnosti pořízení dalších SW modulů nebo HW.

V nabídce lze použít licence pro tzv. externí administrátory, pokud jsou ve standardní licenční nabídce výrobce a neomezují potřebnou funkčnost. Dodavatel dodá přehledovou tabulku v rozdílu funkčností, mezi plnou a omezenou (externí) licencí.

SŽ požaduje, aby v řešení byly plně využity perpetuální licence PAM/PIM, které SŽ již vlastní a jejichž seznam je uveden v příloze č. 4 zadávací dokumentace.

3.1.6.1 Licence pro testovací prostředí

SŽ požaduje, aby licence, které jsou součástí plnění, současně pokryly možnost instalace samostatného testovacího prostředí PAM/PIM, s plnou funkčností jako je systém PAM/PIM převedený do produkce a v rozsahu minimálně 10% licencovaného produkčního prostředí.

3.1.7 Další technické podmínky

3.1.7.1 Vysoká dostupnost řešení

SŽ požaduje, aby dodávané PAM/PIM řešení bylo navrženo a provozováno v režimu vysoké dostupnosti formou Active/Active, kdy výpadek části řešení znamená, že je automaticky zachována plná funkcionalita. Musí být zajištěno, aby při výpadku jedné části systému nebyla dotčena funkčnost řešení a privilegovaní uživatelé se mohli dále přihlašovat a spravovat koncové systémy/zařízení. Současně musí být zajištěno alespoň jedno DR řešení.

Řešení vysoké dostupnosti musí být automatické. Řešení, která vyžadují jakoukoliv manuální intervenci ze strany operátora dohledového centra (např. přepnutí mezi instancemi v případě vzniku chybového stavu) nejsou přípustná. Vysoká dostupnost musí být zajištěna plně na úrovni dodávaného PAM/PIM řešení, tedy buď na úrovni samotné aplikace a/nebo operačního systému.

Dodavatel navrhne HA architekturu v rámci předimplementační analýzy a definuje požadavky na hardwarovou a virtualizační vrstvu, kterou zajistí SŽ podle specifikací dodavatele, přičemž SŽ požaduje, aby požadavky na virtualizační vrstvu byly ve shodě s čl. 5.1.1 přílohy č. 8 zadávací dokumentace (Platforma 2.0), u hardwarové vrstvy (fyzického hardware) požaduje SŽ návrh na technologii x86/x64.

3.1.7.2 Cloudové řešení PAM/PIM

Řešení PAM/PIM, které je provozováno výhradně v cloudu, je pro účely této veřejné zakázky nepřípustné. Zejména je nepřípustné, aby v cloudu byly provozovány části řešení zajišťující bezpečné úložiště hesel, autentizaci a řízení přístupu k PAM/PIM, řízení a nahrávání privilegovaných relací a řízení privilegovaných operací a zdrojů. Cloudové úložiště (v přípustném rozsahu) může sloužit pouze jako aktualizační zdroj.

3.1.7.3 Velikost úložiště pro archivaci

Dodavatel navrhne vhodné formy dlouhodobého uložení nahrávek pořízených při nahrávání relací v rámci výstupů předimplementační analýzy. Zajištění úložišť pro ukládání a archivaci relací zajistí SŽ podle specifikací dodavatele.

3.1.7.4 Jazyk uživatelského prostředí PAM/PIM

SŽ připouští, aby uživatelské rozhraní systému PAM/PIM bylo v anglickém nebo českém jazyce.

3.1.7.5 Vyloučení technických a/nebo programových prostředků představující hrozbu

Dne 17. prosince 2018 vydal Národní úřad pro kybernetickou a informační bezpečnost Varování, č. j. 3012/2018NÚKIB-E/110, kde uvedl, že: *„Použití technických nebo programových prostředků následujících společností, včetně jejich dceřiných společností, představuje hrozbu v oblasti kybernetické bezpečnosti:*

- *Huawei Technologies Co., Ltd, Šen-čen, Čínská lidová republika*
- *ZTE Corporation, Šen-čen, Čínská lidová republika*"

Dne 4. ledna 2019 vydal Národní úřad pro kybernetickou a informační bezpečnost Metodiku k varování ze dne 17. prosince 2018, kde jsou mj. určeny i postupy pro aktualizaci analýzy rizik. V souladu s vydanou metodikou Zadavatel provedl analýzu rizik související s předmětnou veřejnou zakázkou na dodávky, jak je jeho povinností podle § 5 a § 8 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů. V návaznosti na to SŽ identifikovala rizika spojená s výše uvedenými technickými a programovými prostředky jako neakceptovatelná a současně opatření k jejich zvládání, kterým je nepřipuštění použití těchto prostředků v rámci plnění veřejné zakázky.

SŽ tak na základě varování NÚKIB, navazující metodiky a provedené analýzy rizik, ve spojení s § 4 odst. 4 ZoKB, nepřipouští v rámci plnění veřejné zakázky použití technických nebo programových prostředků společností (výrobců),

které jsou uvedené v současné době platném varování NÚKIB jako hrozba v oblasti kybernetické bezpečnosti.

4 Současný stav a popis prostředí

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

5 Požadavky na plnění

Plnění veřejné zakázky se musí skládat alespoň z níže uvedených částí (kapitoly 5.1 - 5.7 této technické specifikace).

5.1 Předimplementační analýza

Poz-01	**Předimplementační analýza**
Popis	Dodavatel zpracuje předimplementační analýzu pro zavedení systému PAM/PIM v prostředí SŽ. Předimplementační analýza je rozdělena na dvě navazující části (A, B)[7], součástí předimplementační analýzy bude minimálně pro část A a B: Předimplementační analýza – část A: ▪ Základní popis řešení, technologií a technických konceptů, ▪ Identifikace předpokladů úspěšné implementace PAM/PIM a stavu jejich splnění pro aktiva v prostředí UAS, jejichž seznam je uveden v příloze č. 3 zadávací dokumentace s ohledem na současný a plánovaný stav prostředí UAS, ▪ Identifikace předpokladů úspěšné implementace PAM/PIM a stavu jejich splnění pro vybrané systémy KII v prostředí TDS, jejichž seznam je uveden v příloze č. 3 zadávací dokumentace s ohledem na současný a plánovaný stav prostředí TDS, ▪ Analýza současného stavu implementace PAM/PIM a identifikace oblastí pro architektonické a konfigurační změny a návrh revize současné implementace, ▪ Základní architektura řešení (HLD) s jejím vysvětlením, ▪ Detailní návrh architektury řešení PAM/PIM pro prostředí UAS (aktiva uvedená v příloze č. 3 zadávací dokumentace) i TDS (viz příloha č. 3 zadávací dokumentace), ▪ Detailní návrh technického řešení implementace PAM/PIM pro prostředí UAS (viz příloha č. 3 zadávací dokumentace) včetně požadavků na HW zdroje, ukládání dat, síťové zdroje apod., které musí vycházet z „best practice" doporučení výrobce technologie PAM/PIM, ▪ Detailní návrh technického řešení implementace PAM/PIM pro prostředí TDS (viz příloha č. 3 zadávací dokumentace) včetně požadavků na HW zdroje, ukládání dat, síťové zdroje apod., které musí vycházet z „best practice" doporučení výrobce technologie PAM/PIM,

[7] Výstupy předimplementační analýzy – část A budou mimo jiné využity pro přípravu HW, virtuálních strojů a systémů ukládání dat podle specifikací dodavatele.

- V případě, že v návrhu řešení použije dodavatel různé typy licencí bude součástí návrhu řešení i přehledová tabulka vlastností a funkčností použitých typu licencí, včetně vyznačení rozdílů mezi typy licencí.

Předimplementační analýza – část B:

- Detailní návrh procesů a služeb systému s jejich rozpisem a vysvětlením jejich účelu v rámci řešení,
- Detailní návrh integrační architektury s infrastrukturními systémy SŽ (SIEM, SNMP, AD, SMTP, NTP),
- Popis nakládání s daty, jejich uložení, zabezpečení, ochrana,
- Detailní síťový a komunikační model řešení včetně interní komunikace mezi vnitřními prvky řešení,
- Návrh politik PAM/PIMřešení detailně specifikovaných během analýzy a vycházející z „best practice" doporučení výrobce technologie,
- Návrh maximálně automatizovaného discovery procesu privilegovaných účtů po zavedení PAM,
- Detailní návrh harmonogramu a detailní prováděcí projekt implementace PAM/PIM pro prostředí UAS (aktiva uvedená v příloze č. 3 zadávací dokumentace) a prostředí TDS (systém KII uvedený v příloze č. 3 zadávací dokumentace),
- Detailní návrh požadavků na součinnost ze strany SŽ při implementaci systému PAM/PIM pro prostředí UAS a TDS,
- Detailní návrh na napojení systému PAM/PIM na systém bezpečnostního monitoringu (SIEM, Log management systém a Service Desk),
- Detailní popis zálohování a obnovy PAM/PIM systému, řešení DR scénářů včetně návrhů testovacích scénářů zahrnujících totální výpadek a obnovy do provozního stavu,
- Návrh metodiky nakládání s „break-glass" účty a scénáře na jejich otestování,
- Návrh na provádění assesment analýz systému PAM/PIMzaměstnanci SŽ (četnost, rozsah, hlavní oblasti assesmentu, automatizace assesment procesu, scoring apod.),
- Scénáře pro DR a break-glass musí minimálně zahrnovat:
  - kompletní výpadek celého PAM/PIM systému,
  - výpadek některého ze základních systémů SŽ, např. virtualizační platformy,
  - výpadek konektivity na některé ze základních prvků PAM/PIM,
  - selhání některého z prvků PAM/PIM a doporučený postup pro jeho zálohování a obnovu,
  - výpadek bezpečného úložiště dat (datového trezoru) včetně fatálního výpadku (primární i sekundární nod apod.),
  - výpadek webového rozhraní PAM/PIM a scénáře pro přístup k úložišti dat,
  - doporučené postupy na zajištění dostupnosti webového rozhraní,
  - výpadek konektivity v prostředí SŽ a řešení přihlašování privilegovaných uživatelů v takovém scénáři,
- Doporučené postupy pro nasazení break-glass účtů, způsob úschovy, periodicita změn, nakládání s nimi apod.,
- Podklady pro analýzu rizik implementace PAM/PIM pro prostředí UAS a TDS,
- Návrh metodiky a plánu provedení akceptačních funkčních, výkonových a zátěžových testů řešení, včetně návrhu testů obnovy a zotavení pro vybrané typy událostí/závad (včetně výkonnostních parametrů obnovy a zotavení – RPO, RTO apod.). Návrh metodiky akceptačních testů musí pokrývat testování funkčních požadavků na systém PAM/PIM,

	▪ Návrh metodiky testů měření dostupnosti systému PAM/PIM.
Výstupy	Výstupem předimplementační analýzy bude soubor dokumentů pokrývající výše uvedené oblasti (pro část A i část B). 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. 21 zadávací dokumentace).

5.2 Implementace PAM/PIM pro úvodní dva cílové systémy (aktiva) v prostředí UAS, pilotní provoz implementace, školení

Poz-02	**Implementace PAM/PIM pro úvodní dva cílové systémy, akceptační a bezpečnostní testy, pilotní provoz implementace**
Popis	Dodavatel provede úvodní implementaci systému PAM/PIM pro koncové systémy v prostředí UAS definované (označené) v příloze č. 3 zadávací dokumentace a konfiguraci všech komponent systému. Součástí implementace je i revize konfigurace stávajícího systému PAM/PIM (popř. zcela nová implementace, tak jak určeno v akceptované předimplementační analýze). Součástí implementace musí být také ▪ nastavení politik pro PAM/PIM, ▪ nastavení nahrávání privilegovaných relací, ▪ integrace koncových systémů/zařízení, ▪ integrace s dalšími systémy prostředí SŽ (zejména AD/LDAP a SSO, nástroje pro bezpečnostní a provozní monitoring, integrace se Service Desk apod.), ▪ nastavení zálohování atd. Po provedení implementace provede dodavatel v souladu s metodikami definovanými v rámci předimplementační analýzy akceptační funkční, výkonové a zátěžové testy a odstraní případné neshody. Dodavatel dále poskytne součinnost při provedení bezpečnostních testů řešení PAM/PIM a odstraní případné neshody. Po provedení akceptačních a bezpečnostních testů a odstranění případných neshod dodavatel převede systém PAM/PIM do pilotního provozu v délce minimálně 4 kalendářních týdnů a v rámci pilotního provozu dodavatel odstraní případné provozní závady. Po vyhodnocení pilotního provozu bude systém PAM/PIM převeden do produkce a dodavatel v souladu s požadavkem odst. 5.6 této technické specifikace zajistí technickou podporou řešení.

	V rámci této fáze dodavatel vybuduje také testovací prostředí systému PAM/PIM s plnou funkčností produkčního prostředí a v rozsahu minimálně 10 % licencovaného produkčního prostředí. HW zdroje formou virtuálních strojů a síťové prostředí pro testovací prostředí zajistí SŽ podle specifikace dodavatele. Virtuální stroje budou poskytnuty v souladu s kapitolou 5.1.1 přílohy č. 7 zadávací dokumentace (Platforma 2.0).
Výstupy	Výstupem bude: ▪ Úvodní implementace systému PAM/PIM a jeho napojení na definované koncové systémy a integrace s prostředím SŽ, ▪ Protokoly z akceptačních funkčních, výkonnostních a zátěžových testů a protokol odstranění případných neshod, ▪ Protokol o provedení bezpečnostních testů a odstranění případných neshod, ▪ Dokument vyhodnocení pilotního provozu, ▪ Testovací prostředí systému PAM/PIM.

Poz-03	**Dokumentace implementace systému PAM/PIM**
Popis	Jako součást plnění (implementace systému PAM/PIM) zpracuje dodavatel dokumentaci systému minimálně v následujícím rozsahu: a) Produktová dokumentace ke všem dodávaným modulům PAM/PIM, popř. dalšímu SW dodaným v rámci implementace, b) Detailní popis architektury, instalační a implementační dokumentace, dokumentace k napojení koncových systémů, dokumentace k integraci s prostředím SŽ (AD, ServiceDesk apod.), c) Administrátorské a uživatelské příručky, popis konfigurace, instalační procedury, dokumentace DR řešení, d) Dokumentace ke všem logům – zejména popis struktury logů, seznam událostí s jejich charakteristikou a strukturou. Kromě výše uvedeného musí v rámci bodu c) dodavatel vytvořit návrh konkrétních kroků včetně stanovení odpovědností pro tyto body: • Vytvoření nového uživatele v PAM/PIM – *Založení nového účtu na úrovni PAM/PIM řešení pro uživatele PAM/PIM (např. interní/externí administrátor, správce PAM, auditor, popř. další subjekty).* • Zrušení uživatele PAM/PIM – *Zrušení účtu na úrovni PAM/PIM řešení v případě, že účet není nadále používán (např. v případě ukončení zaměstnaneckého poměru zaměstnance u SŽ, odebrání účtu externího dodavatele apod.).* • Dynamické přidělování/odebírání licencí pro externí uživatele PAM/PIM– *Návrh postupu dynamického přidělování/odebírání licencí externích uživatelů, který bude optimalizován podle maximálního počtu souběžně připojených externích uživatelů PAM/PIM a povede k efektivnímu využití licencí externích uživatelů PAM.* • Přidělení/odebrání role uživateli PAM/PIM– *Přidělení/odebrání role (např. správce PAM, uživatel, auditor) uživateli PAM.* • Přidání nového privilegovaného účtu do PAM/PIM– *Přidání privilegovaného účtu do PAM/PIM (např. v případě objevení nového privilegovaného účtu, který má být spravován pomocí PAM), nastavení politik a přidělení privilegovaného účtu k používání konkrétním uživatelům PAM/PIM (tj. administrátorům).*

	• Použití privilegovaného účtu – *Poskytnutí přístupu uživatele PAM/PIM (interního/externího administrátora) k privilegovanému účtu prostřednictvím PAM/PIM řešení (tj. v případě že má uživatel přístup schválen).* • Použití privilegovaného účtu na vyžádání (elevace oprávnění) – *Poskytnutí přístupu uživatele PAM/PIM (interního/externího administrátora) k privilegovanému účtu na vyžádání na definované časové období (tj. v případě že daný administrátor nemá standardně k privilegovanému účtu oprávnění, přístup je umožněn pouze na dočasnou dobu na základě schválení). Popis bude zahrnovat i případný onboarding nového účtu, a to se zaměřením na externí privilegované uživatele*. • Použití privilegovaného účtu (nouzový přístup) – *Poskytnutí nouzového přístupu v případě, kdy je potřeba získat okamžitě přístup k privilegovanému účtu a není dostupný příslušný odpovědný administrátor.* • Disaster recovery proces – *Poskytnutí přístupu k privilegovaným účtům v případě, že PAM/PIM infrastruktura nebo její část není dostupná (např. z důvodu havárie nebo jiné neočekávané události).* • Žádost o změnu konfigurace – *Zpracování žádosti o změnu konfigurace PAM/PIM (např. vytvoření nové/změna stávající politiky).* • Revize uživatelů PAM/PIM– *Provedení revize uživatelů PAM/PIMa privilegovaných účtů, kterými jednotliví uživatelé disponují (může být vyřešeno v rámci bodů pro Discovery a Assesment procesy).* • Sledování či ukončení relace – *Sledování aktivní relace nebo její předčasné ukončení odpovědnou osobou (např. člen dohledového týmu).* • Žádost o nahrávání relace – *Zpracování žádosti o nahrávání relací pro konkrétního uživatele (na vyžádání, pokud PAM/PIM systém není nastaven k nahrávání všech relací).* • Žádost o zpřístupnění nahrávky – *Zpracování žádosti o zpřístupnění nahrávky relace pořízené pomocí PAM/PIM řešení.* Dokumentace uvedená výše v b) až d) této technické specifikace je požadována v českém jazyce. Produktová dokumentace od výrobce je akceptovatelná v anglickém nebo českém jazyce. Pravidelná aktualizace dokumentace bude prováděna v rámci napojování dalších koncových systémů/zařízení a v rámci technické podpory řešení, a to pravidelně při aktualizacích (patchování, upgrade) implementovaného PAM/PIM řešení.
Výstupy	Dokumentace implementovaného systému PAM/PIM. 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. 21 zadávací dokumentace)

Poz-04	**Školení pracovníků SŽ**
Popis	Požadovanou součástí plnění je zajištění školení IT specialistů na implementovaný systém PAM/PIM (viz následující tabulka).

	Typ školení	Název – obsah školení	Počet osob proškolených osob	Rozsah (v MD)
1.	Administrace a provoz systému PAM/PIM	Školení zaměřená na základní správu a provoz systému PAM/PIM.	Minimálně 5 maximálně 8	2 MD
2.	Pokročilá administrace systému PAM/PIM, způsoby integrace	Praktické procvičování dovedností správců PAM/PIM, včetně procesů obnovy a zotavení, řešení definovaných use-case. Školení v oblasti integračních rozhraní a napojování koncových systémů.	Minimálně 5 maximálně 8	2 MD

Školení č. 1 proběhne v rámci pilotního provozu úvodní implementace řešení PAM/PIM (viz požadavek č. P02), školení č. 2 proběhne po uvedení systému PAM/PIM do produkce.

Školení proběhne v prostorách SŽ. Konkrétní termíny a místo školení určí SŽ. Školení proběhne v českém nebo slovenském jazyce.

Školení poskytne určeným pracovníkům komplexní informace v takovém rozsahu, aby tito pracovníci dokázali samostatně a dlouhodobě spravovat a provozovat dodané řešení.

Školitel bude disponovat certifikací výrobce dodávané technologie, resp. Výrobců všech technologií, ze kterých bude složena dodávka (pokud výrobci takové certifikace vystavují). Certifikát je možno nahradit čestným prohlášením výrobce o způsobilosti daného školitele. Certifikát a/nebo čestné prohlášené předloží dodavatel SŽ nejpozději pět (5) pracovních dní přede dnem konání školení.

Výstupy	Protokoly o provedených školení pracovníků SŽ na dodané technologie a konkrétní implementaci PAM/PIM.

5.3 Rozšíření implementace PAM/PIM na zbývající definované systémy

Poz-05	**Rozšíření implementace PAM/PIMna zbývající definované systémy**
Popis	Dodavatel provede rozšíření systému PAM/PIM na další systémy definované v příloze č. 3 zadávací dokumentace (podpůrná a technická aktiva). SŽ předpokládá rozšiřování implementace PAM/PIM po skupinách aktiv. Rozšíření bude provedeno podle harmonogramu a prováděcího projektu vypracovaných v rámci předimplementační analýzy a odsouhlasených SŽ. Každá dílčí implementace systému PAM/PIM (rozšíření o další koncové systémy) bude obsahovat také pilotní provoz v délce minimálně dva (2) kalendářní týdny a po jeho

	vyhodnocení a odstranění případných neshod bude dílčí část systému převedena do produkce a zařazena do služby technické podpory. Součástí každé dílčí implementace bude i dodávka chybějících licencí (dle požadavku č. Poz-07), bude-li taková dodávka licencí zapotřebí. SŽ si vyhrazuje možnost u dílčích implementací požadovat provedení akceptačních funkčních, výkonnostních a zátěžových testů a odstranění případných neshod.
Výstupy	Rozšíření implementace systému PAM/PIM o další aktiva podle prováděcího projektu a harmonogramu definovaných ve výstupu předimplementační analýzy. Dokument vyhodnocení pilotního provozu každé dílčí implementace PAM/PIM.

5.4 Implementace PAM/PIM pro jeden cílový systém v prostředí TDS, pilotní provoz implementace

Poz-06	**Implementace PAM/PIMpro jeden cílový systém v prostředí TDS, akceptační a bezpečnostní testy, pilotní provoz implementace**
Popis	Dodavatel provede úvodní implementaci systému PAM/PIM pro koncový systém KII v prostředí TDS definovaný (označený) v příloze č. 3 zadávací dokumentace a konfiguraci všech komponent systému. Součástí implementace musí být také ▪ nastavení politik pro PAM/PIM, ▪ nastavení nahrávání privilegovaných relací, ▪ integrace koncových systémů/zařízení, ▪ integrace s dalšími systémy prostředí Zadavatele (zejména AD/LDAP a SSO, nástroje pro bezpečnostní a provozní monitoring, integrace se Service Desk apod.), ▪ nastavení zálohování atd. Po provedení implementace provede dodavatel v souladu s metodikami definovanými v rámci předimplementační analýzy akceptační funkční, výkonové a zátěžové testy a odstraní případné neshody. Dodavatel dále poskytne součinnost při provedení bezpečnostních testů řešení PAM/PIM a odstraní případné neshody. Po provedení akceptačních a bezpečnostních testů a odstranění případných neshod dodavatel převede systém PAM/PIM do pilotního provozu v délce minimálně 4 kalendářních týdnů a v rámci pilotního provozu dodavatel odstraní případné provozní závady. Po vyhodnocení pilotního provozu bude systém PAM/PIM převeden do produkce a dodavatel v souladu s požadavkem odst. 5.6 této technické specifikace zajistí technickou podporou řešení.
Výstupy	Výstupem bude:

	▪ Úvodní implementace systému PAM/PIM v prostředí TDS a jeho napojení na definovaný koncový systém KII a integrace s prostředím SŽ, ▪ Protokoly z akceptačních funkčních, výkonnostních a zátěžových testů a protokol odstranění případných neshod, ▪ Protokol o provedení bezpečnostních testů a odstranění případných neshod, ▪ Dokument vyhodnocení pilotního provozu, ▪ Dokumentace implementovaného systému podle požadavků definovaných v kapitole 5.2, požadavek č. 3 této technické specifikace.

5.5 Průběžná dodávka chybějících licencí

Poz-07	**Průběžná dodávka chybějících licencí**
Popis	Součástí plnění je i dodávka SW licencí systému PAM/PIM. Dodavatel zajistí dodávku chybějících SW licencí tak, aby systém PAM/PIM převedený do produkčního prostředí byl plně licencován – licence musí plně pokrývat aktuální implementované části systému PAM/PIM převedené do produkce. V případě dodávky časově omezených licencí (subskripce) musí být dodané licence platné minimálně po dobu tolika měsíců, kolik jich zbývá do uplynutí doby 48 měsíců od ukončení Fáze 2. Aktivace příslušných licencí proběhne vždy při převodu dílčí části implementace PAM/PIM do produkce (tedy v rámci provádění plnění dle kapitoly 5.2, 5.3 a 5.4 této technické specifikace). Součástí licencí musí být i služba technické podpory výrobce PAM/PIM v délce stejné, jako platnost licencí. Pro SŽ vlastněné perpetuální licence zajistí dodavatel technickou podporu výrobce i těchto perpetuálních licencí v délce 48 měsíců. SŽ tedy předpokládá dodávku odpovídajících licencí vždy při dílčí implementaci systému PAM/PIM (úvodní implementace a následné napojování koncových systémů) při převodu dílčí části implementace PAM/PIM do produkce.
Výstupy	Dodávka SW licencí systému PAM/PIM, včetně technické podpory výrobce.

5.6 Technická podpora řešení

Pro implementovaný systém PAM/PIM požaduje SŽ poskytování služby technické podpory v délce 48 měsíců.

Služby jsou rozděleny na pravidelně vykonávané a individuálně, samostatně objednávané činnosti.

Poz-08	**Průběžně prováděné a pravidelné měsíční činnosti**
Popis	Průběžně prováděné a pravidelní měsíční činnosti zahrnují: ▪ Provádění údržby systému: min. 1x měsíčně, ▪ Kontrola provozních systémových logů s následným řešením případných incidentů,

	▪ Kontrola funkčnosti a bezpečnosti úložiště hesel: min 1x měsíčně, ▪ Zajištění služeb servisní podpory pro řešení SW vad, včetně identifikace a analýzy neshod, ▪ Pravidelná profylaxe systémových prostředků systému, včetně návrhu řešení nalezených problémů nebo rozvoje systému, ▪ Vedení systémové dokumentace včetně změnových požadavků, ▪ Provoz kontaktního místa prostřednictvím webové aplikace, emailu a telefonní hot-line v českém jazyce zdarma nebo za běžný účastnický tarif, ▪ Vypracování protokolu o údržbě s detailním popisem veškerých nalezených nedostatků a postupu pro jejich odstranění: 1x měsíčně.
Výstupy	Výstupem tohoto bude poskytnutí služby technické podpory prováděné průběžně nebo pravidelně měsíčně v termínech stanovených SŽ.

Poz-09	**Pravidelné půlroční činnosti**
Popis	Průběžně prováděné a pravidelní měsíční činnosti zahrnují: ▪ Test přechodu na DR řešení a zpět, ▪ Kontrola záloh, případná obnova v test prostředí, ▪ Funkčnost/platnost rekonciliačních účtů a platnost vybraných uložených hesel.
Výstupy	Výstupem tohoto bude poskytnutí služby technické podpory prováděné jednou za půl roku v termínech stanovených SŽ.

Poz-10	**Individuálně objednávané činnosti technické podpory řešení**
Popis	Individuálně objednávané činnosti technické podpory zahrnují zejména: ▪ Instalace nejnovějších opravných balíčků a relevantních nových verzí SW, dle doporučení výrobce, ▪ Konfigurace požadavků na změnu dle potřeb SŽ, ▪ Řešení provozních incidentů uživatelů, které nejsou způsobeny prokazatelnou vadou SW nebo implementace, ▪ Diagnostika systému PAM/PIM, resp. závad, v místě plnění nebo prostřednictvím vzdáleného přístupu dle žádosti správce aplikace, ▪ Obnovení uložiště hesel ze zálohy na žádost správce aplikace, ▪ Provedení testu obnovy uložiště hesel ze zálohy, ▪ Školení bezpečnostního týmu po implementaci zásadních změn.
Výstupy	Výstupem tohoto bude poskytnutí služby technické podpory prováděné na žádost SŽ v termínech dle příslušného SLA.

Technická podpora bude poskytována v souladu ustanoveními Zvláštních obchodních podmínek pro Zakázky v oblasti ICT (Příloha č. 9 zadávací dokumentace) podle servisního modelu A4.

5.7 Služby na vyžádání

Poz-11	Služby na vyžádání
Popis	Dodavatel poskytne SŽ služby konzultace na vyžádání. Služby mohou být čerpány především pro rozšiřování implementace systému PAM/PIM na další koncové systémy, a to jak pro podpůrná a technická aktiva, tak i pro systémy KII. Maximální souhrn těchto služeb bude činit 50 MD za celou dobu trvání smlouvy, čerpání bude probíhat dle konkrétních potřeb SŽ, a to na základě objednávek.
Výstupy	Výstupem tohoto bude poskytnutí služby konzultace, implementace a konfigurace systému PAM/PIM na vyžádání podle potřeb SŽ.

6 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 SŽ separátně akceptována nejpozději v termínu uvedeném v Harmonogramu, tj. v příloze č. 8 zadávací dokumentace. SŽ 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 dodávky.

Fáze	Popis	Kapitola obsahující požadavky
Fáze 1-A	Předimplementační analýza – část A	5.1
Fáze 1-B	Předimplementační analýza – část B	5.1
Fáze 2	Implementace PAM/PIM pro úvodní dva cílové systémy (aktiva) v prostředí UAS, pilotní provoz implementace, školení	5.2
Fáze 3	Rozšíření implementace PAM/PIM na zbývající definované systémy	5.3
Fáze 4	Implementace PAM/PIM pro jeden cílový systém v prostředí TDS, pilotní provoz implementace	5.4
Fáze 5	Průběžná dodávka chybějících licencí	5.5
Fáze 6	Technická podpora řešení	5.6
Fáze 7	Služby na vyžádání	5.7