Technická specifikace

Správa a monitoring privilegovaných účtů – PIM

OBSAH

Seznam obrázků

Seznam tabulek

1 ÚČEL DOKUMENTU

Tento dokument obsahuje specifikaci řešení a technických požadavků na systém pro správu a monitoring aktivit privilegovaných účtů ICT systémů Ministerstva Zemědělství České republiky. Dokument tvoří přílohu zadávací dokumentace veřejné zakázky „Správa a monitoring privilegovaných účtů - PIM“ a obsahuje představení požadovaného konceptu řešení, základní popis poptávaného řešení a požadavky závazné pro všechny potenciální uchazeče o zajištění realizace zakázky.

2 PŘEHLED ZÁKLADNÍCH POJMŮ

Termín	Význam
AD	Microsoft Active Directory
AK	Aplikační katalog
CAL	Client Access License
DB	Databáze
DC	Datové centrum
EP	End Point – řízený koncový systém (Win, Linux, DB, Router, SAP …)
DRP	Disaster recovery plan
HA	High Availability – režim vysoké dostupnosti (např. redundance)
HP BAC	HP Business Availability Center – nástroj pro End-to-end monitoring
HW	Hard-Ware
ICT	Informační a komunikační technologie (Information and Communication Technologies)
IDM	Identity Management – správa uživatelských účtů
LDAP	Lightweight Directory Access Protocol
Objednatel/Zadavatel/MZe	Česká republika – Ministerstvo zemědělství
OID	Oracle Internet Directory – LDAP systém od Oraclu, který je implementován v prostředí MZe
OIM	Oracle Identity Manager – IDM systém od Oraclu, který je implementován v prostředí MZe
OS	Operační Systém
OSS	Organizační složka státu – organizace podřízená ministerstvu
PAM	V kontextu Unix/Linux PAM - Pluggable Authentication Modules umožňující např. delegaci autentizace na externí adresář (LDAP/AD) Privileged Account Management - správa privilegovaných identit/účtů
PIM	Privileged Identity Management - správa privilegovaných identit/účtů
Privilegovaný účet	Uživatelský účet informačního systému s širokou nebo neomezenou množinou administrátorských oprávnění, který je zpravidla nepersonalizovaný a může být sdílen mezi vícero uživateli.
PuTTY	Klient protokolů SSH, Telnet, rlogin a holého TCP.
RDP	Remote Desktop Protocol – protokol na přenos vzdálené plochy
RODC	Active Directory Read-Only Domain Controller
SIEM	Security Information and Event Management - správa bezpečnostních informací a událostí
Smlouva	Smlouva o poskytnutí řešení „Správa a monitoring privilegovaných účtů – PIM“

SNMP	Simple Network Management Protocol
SSO	Single sign on - systém jednotného přihlášení
SUR	Aplikace pro správu uživatelů a rolí
SW	Software
TS	Terminálový server
WMI	Windows Management Instrumentation
Zhotovitel, Dodavatel	Subjekt, který je jako Zhotovitel/Dodavatel definován v záhlaví Smlouvy

Tabulka 1 - seznam zkratek a pojmů

3 AKTUÁLNÍ STAV

Informační prostředí MZe je tvořeno velkým množstvím informačních systémů a rozlehlou síťovou infrastrukturou, na kterém je závislý chod celé organizace. Každý z prvků tohoto prostředí obsahuje privilegované účty, které jsou využívány pro jejich administraci, běžnou obsluhu, nebo se jedná o servisní účty použité v rámci integrací. K takovým účtům mají přístup jak zaměstnanci MZe, tak externí dodavatelé, kteří zajišťují provoz a rozvoj IT systémů a služeb MZe.

Současný stav řešení problematiky správy privilegovaných účtů je shrnut v následujících odstavcích:

3.1 Organizační opatření

1. Proces přidělování a manipulace s uživatelskými účty, včetně těch privilegovaných, je organizačně řízen podle vnitřní směrnice.
2. Osoba disponující privilegovaným účtem se musí zavázat k dodržování pravidel informační bezpečnosti (déle jen „prohlášení“). Toto prohlášení jasně definuje způsob manipulace s těmito účty a jejich používání jako například:
    a. Politika hesel – složitost hesla, stáří hesla, unikátnost hesla (stejné heslo není použito pro více účtů).
    b. Účet není dovoleno nikde ukládat pro použití v rámci automatizovaného přihlašování.
3. Tato organizační opatření jsou vynucována pouze na systémech a aplikacích, které umožňují definovat politiku hesel. Kontrola nastavení politiky hesel je však prováděna pouze občasně a nesystematicky.

3.2 Přístup k účtům a jejich evidence

1. Neexistuje centrální evidence všech privilegovaných účtů (jen některých, většinou na úrovni infrastruktury), ani osob, které k nim mají přístup.
2. Některé účty jsou sdíleny mezi více osobami.
3. Záměrem je však, tam kde je to možné, používat osobní účty. V rámci jednotlivých technologií je používán následující přístup:
    a. **Unix/Linux** (HP-UX, RedHat, CentOS) – veškeré účty jsou lokální. Pro administrátory jsou vytvořeny lokální osobní účty. Pro přístup k privilegovaným účtům (root, oracle, …) se používá *sudo*.
    b. **Windows** – většina Windows serverů je zapojena do AD domény MZe. Účty jsou tedy používány převážně osobní doménové. Administrátoři serverů mají své účty přiřazené na jednotlivých serverech do lokální skupiny Administrator (buď napřímo nebo přes doménovou skupinu). Frontend Windows servery (DMZ1) nejsou zapojeny do domény, tudíž správa uživatelů a oprávnění je pouze lokální.
    c. **Network** (routery, switche, firewall, WCF, IPS, IDS, WIFI atd.) – kde je to možné, jsou použity osobní účty administrátorů. Např. Cisco zařízení jsou napojeny na Cisco ACS, který slouží jako centrální autentizační a autorizační bod, na kterém má každý

z uživatelů svůj osobní účet - systémový privilegovaný účet je tedy použit jako záložní varianta pouze v případě výpadku ACS serveru. Pro správu je zpravidla použit buď:

i. Tlustý klient nebo tenký klient.
ii. SSH
iii. Telnet

d. **VMWare** – ESXi servery jsou zapojeny do AD domény, používají se tedy osobní doménové účty. Systémový účet root je používán výjimečně (např. upgrade). Pro přístup k serveru se používá jak tlustý tak tenký vSphere klient.
e. **Citrix XenApp** – pro autentizaci a autorizaci je použita AD doména. Oprávnění se však řídí z adresáře LDAP, ze kterého jsou synchronizovány do AD. Citrix se používá pro publikaci „tlustých“ aplikací jak pro MZe tak podřízené OSS. Publikováno je interně (do lokální sítě) a také externě prostřednictvím externího portálu.
f. **LDAP** – pro administraci se využívají výhradně osobní účty LDAPu. Výjimku tvoří vytváření skupin, které může být prováděno servisními účty napojených aplikací.
g. **Active Directory a Exchange** – pro administraci se využívají osobní doménové účty. Výjimečně je nutné použít přímo účet doménového administrátora, proto je heslo k tomuto účtu sdíleno v rámci Windows týmu.
h. **SAP** – pro správu účtů je použit SAP Solution Manager. Používány jsou převážně lokální osobní účty.
i. **Databáze** (Oracle, MS SQL, PostgreSQL) – převážně se používají osobní lokální účty. V některých případech se používají servisní administrátorské účty, které jsou sdíleny (jak z nutnosti, tak kvůli usnadnění). Pro přístup k databázi se používají zejména standardní management nástroje: Oracle SQL Developer, Microsoft SQL Management Studio. Běžný je také přístup přímo z napojené aplikace, která v sobě přístupové údaje k databázi uchovává, tudíž je administrátor ani nemusí znát.
j. **Aplikační servery** (WebLogic, JBoss, Tomcat, Oracle AS, GlassFish) – pokud server umožňuje administraci prostřednictvím web GUI, jsou použity lokální sdílené administrátorské účty.

4. Hesla administrátorských účtů jsou po jejich vygenerování a nastavení vytisknuty, vloženy do obálky a založeny ve fyzickém trezoru u bezpečnostního manažera MZe. K heslu mají však přístup také správci příslušných systémů, kteří ho mohou v případě potřeby využívat.
5. Není nijak stanoveno, jak hesla k privilegovaným účtům uchovávat, ani způsob jejich předávání (obzvláště u sdílených účtů).
6. Účty jsou používány v rámci skriptů a integračních komponent informačních systémů, kde mohou být uloženy buď v otevřené formě, nebo v zabezpečeném úložišti.

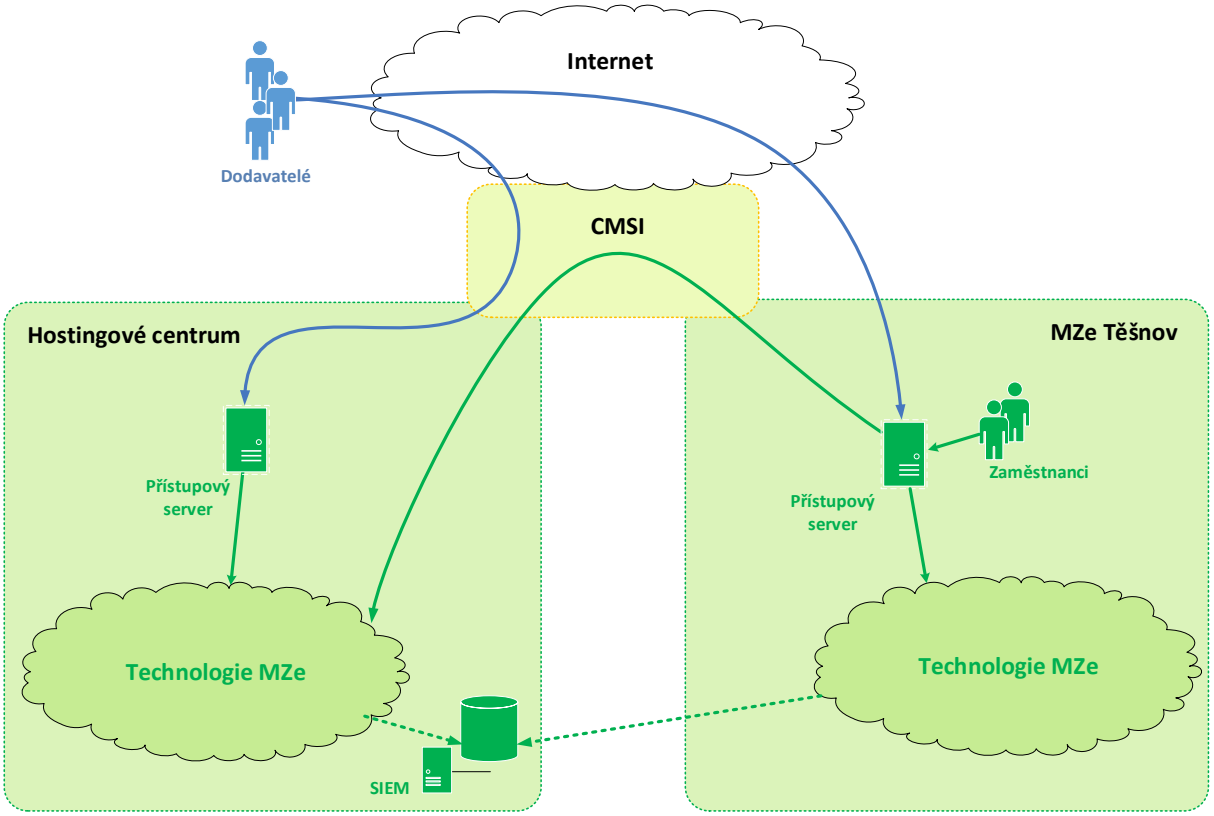
3.3 Aktivita účtů

1. Aktivita těchto účtů většinou není nijak monitorována, pokud monitorována je, děje se tak zpravidla až na aplikační úrovni a nejednotným způsobem.
2. Logování systémů o aktivitě privilegovaných účtů není standardizováno, tedy není stanoveno, jaké události se mají monitorovat ani jak dlouho se mají uchovávat, či centrálně shromažďovat a vyhodnocovat (SIEM).

3.4 Přístupové body

Infrastruktura MZe se skládá ze dvou geograficky oddělených datových center, která jsou hostována v HC Nagano a HC Chodov, a infrastruktury provozované v lokalitě Těšnov. Tyto tři lokality jsou připojeny do společné MPLS sítě, která je přes CMSI připojena do Internetu. Lokalita Těšnov je navíc ještě připojena do Internetu vlastní linkou. Ve všech lokalitách jsou provozovány EP, které jsou spravovány externími dodavateli ze sítě Internet, nebo interními zaměstnanci MZe z lokality Těšnov.

Zadavatel v tuto chvíli používá pro zajištění přístupu dodavatelů a zaměstnanců MZe ke spravovaným technologiím farmu Windows terminálových serverů, tak jak je znázorněno na obrázku Obrázek 1. Jak je z tohoto obrázku zřejmé, použity jsou dva přístupové servery, které jsou umístěny HC (1x Nagano, 1x Chodov), a jeden terminálový server, který je provozován v lokalitě Těšnov. Jako přístupové servery jsou používány terminálové servery OS Windows 2012 R2 Standard instalované ve virtuální infrastruktuře VMWare.



Obrázek 1 - současné přístupové body (high-level architektura)

4 POŽADOVANÝ STAV A MOTIVACE

Privilegované účty umožňují takřka neomezený přístup ke zdrojům příslušných systémů včetně manipulace s nimi (např. root, Administrator, sys, sa, atp.), proto jsou významným bezpečnostním rizikem. Oprávnění disponovat takovým účtem mají jak interní zaměstnanci, tak externí dodavatelé a takové oprávnění často není nijak evidováno. Znalost přihlašovacích údajů je navíc zpravidla sdílena mezi více uživateli, tudíž odpovědnost za případné zneužití je velice těžko dohledatelná, nebo dokonce není vůbec prokazatelná. Toto riziko se vztahuje na všechny systémy, počínaje operačními systémy, databázemi, síťovými prvky až na komplexní informační systémy distribuované jako produkt, nebo vyvinuté na míru. Ať už přímo nebo nepřímo se tedy problém dotýká všech informačních systémů, včetně systémů potenciálně identifikovaných jako „Významný informační systém“ nebo „Kritická informační infrastruktura“ v rámci zákona č. 181/2014 Sb., zákon o kybernetické bezpečnosti, který vychází z doporučené normy ISO/IEC 27001. Proto je nutné zavést správu přístupu k těmto účtům a monitoring veškeré aktivity účtů s vazbou na konkrétní osobu, která jím právě disponuje.

Řešením správy privilegovaných účtu je nasazení tzv. **Privileged Identity Management** Systému (PIM, nebo také Privileged Account Management – PAM). PIM můžeme rozdělit do následujících tří oblastí, které spolu úzce souvisí:

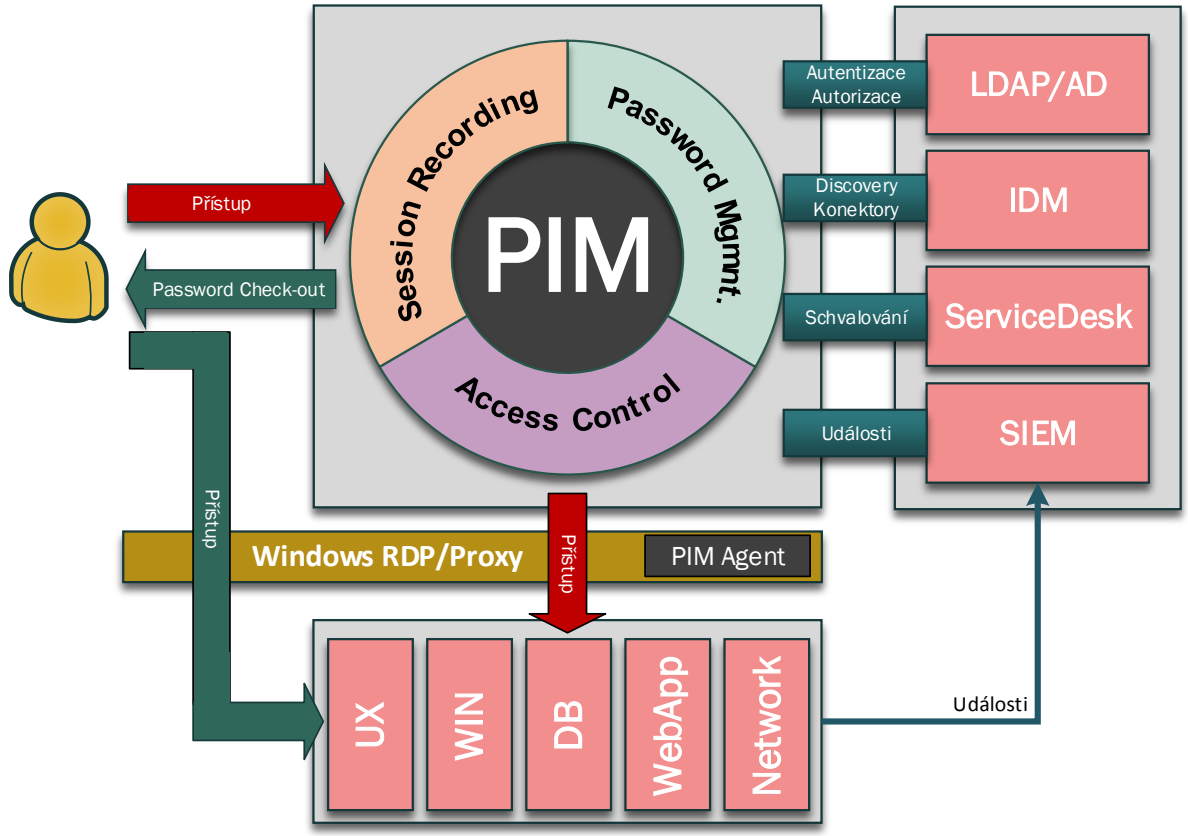
1. **Password Management** – centrální správa privilegovaných účtů se zabezpečeným úložištěm hesel a správou přístupů k těmto účtům.
2. **Session Recording** – zaznamenávání aktivit privilegovaných účtu včetně nahrávek obrazovek a stisků kláves (key-logging).
3. **Access Control** – kontrola přístupu k systému pomocí privilegovaných účtů, zvýšení granularity oprávnění těchto účtů, detekce a ochrana prostředků systému na základě definovaných politik.

Z důvodů urychlení nasazení řešení rizik je požadováno implementovat pouze první dvě oblasti **Session Recording** a **Password Management**, které pokryjí většinu identifikovaných rizik a zároveň umožní naplnit nařízení v rámci návrhu zákona a kybernetické bezpečnost, konkrétně:

Druhá část, HLAVA II – Technická opatření:

- *Nástroj pro ověřování identity uživatelů*
  Stanovení politik hesel, které řeší právě Password Management.
- *Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a správců*
  Zaznamenávání činnosti privilegovaných účtů, které řeší Session Recording.

Zahrnutí oblasti **Access Controlu** v rámci tohoto projektu není požadováno. Je však vyžadováno, aby nasazované řešení tuto funkcionalitu podporovalo a bylo tak možné celou problematiku pokrýt v rámci jednoho řešení pouze jeho rozšířením.



Obrázek 2 - koncept PIM řešení

5 POPIS POŽADOVANÉHO ŘEŠENÍ

Tato kapitola obsahuje popis řešení, které je předmětem zakázky. Účelem kapitoly je poskytnout uchazeči ucelený přehled nad požadovaným řešení, ze kterého vyplývají konkrétní požadavky uvedené v další kapitole, které musí nabízené řešení splňovat a bude předmětem vyhodnocování nabídky.

5.1 Password Management

Jedná se o systém s centrálním vysoce zabezpečeným úložištěm privilegovaných účtů a příslušných hesel spolu s konektory na koncové systémy (EP) s řízenými účty a uživatelským rozhraním, nad kterým je postavena logická vrstva v podobě procesů a politik.

Uživatelé (zaměstnanci/externí dodavatelé) přistupují do systému pomocí uživatelského rozhraní na základě autentizace proti lokálnímu, nebo externímu adresáři (AD/LDAP). Lokální autorizací, nebo autorizací proti stejnému adresáři uživatel získává množinu privilegovaných účtů, kterými může disponovat. Takové účty je možné použít dvěma způsoby:

1. **Heslo** je možné si nechat **zobrazit** na obrazovce a následně použít standardním způsobem.
2. Použít **automatizované přihlášení** (SSO) k systému pomocí privilegovaného účtu bez nutnosti prozrazení hesla. Přihlášení probíhá buďto přímo v prohlížeči prostřednictvím pluginu prohlížeče, který otevře okno s příslušnou klientskou aplikací, bez nutnosti její lokální instalace, nebo je využito lokální klientské aplikace na koncové stanici uživatele, které je heslo předáno pomocí skriptu. Tímto způsobem jsou podporovány běžné protokoly/aplikace:
    - SSH, Telnet;
    - RemoteDesktop;
    - HTTP(s)/Web aplikace;
    - Libovolná aplikace běžící v prostředí MS Windows;

    Takový přístup výrazně zvyšuje uživatelský komfort, jelikož uživatelé nejsou nuceni s hesly privilegovaných účtů vůbec pracovat, veškerá akce probíhají automaticky na pozadí (tzv. privileged SSO). Uživatelé si tak např. nemusí pamatovat mnoho dalších hesel, ale využívají jen heslo svého účtu.

Pro zobrazení/použití hesla uživatel spustí akci check-out, při které je za pomoci konektoru heslo změněno, stejně jako po ukončení práce s účtem, kdy je volána akce check-in. Při použití automatizovaného přihlášení dochází k akci check-out/in automaticky. Tímto je zaručena jasná evidence toho, kdo má k jakým účtům přístup a v jaké chvíli je využíval.

Kromě účtů, které má uživatel volně k dispozici, může mít také přiřazeny účty, ke kterým získá přístup až po udání důvodu, nebo po **schválení** jiným uživatelem, nebo skupinou uživatelů. Takový přístup může získat buď na omezenou dobu, nebo na stálo. Schvalovací workflow je možné libovolně strukturovat, nebo je možné využít napojení na externí service desk.

V případě nouzové situace, kdy je potřeba získat přístup k heslu privilegovaného účtu okamžitě, existuje proces, který takovou akci podporuje, za současného zalogování a odeslání notifikace na určenou kontaktní osobu.

Pro spravované účty jsou definovány **politiky hesel**, které jasně definují složitost hesla a jeho stáří – dle těchto politik jsou generována náhodná hesla, která jsou aktivně propisována do EP pomocí konektorů. V pravidelném intervalu je naplánována kontrola, zda nedošlo ke změně hesla privilegovaného účtu při externím zásahu mimo PIM systém. Detekovaný zásah je aktivně notifikován. Zároveň je plánováno pravidelné **discovery** účtů na EP – zde je vhodná interakce s IDM, aby bylo možné jednoznačně odlišit, zda se jedná o uživatelský účet patřící konkrétní identitě, nebo o sdílený privilegovaný účet. Takové účty jsou reportovány odpovědné osobě, která je na základě definovaného procesu zařadí příslušným uživatelům a nastaví odpovídající politiky hesel.

Kromě přístupu uživatelů k privilegovaným účtům, systém obsluhuje také **přístup aplikací**. Je poskytnut aplikační interface umožňující provést check-out hesla k účtu, čímž poskytuje možnost vyvarovat se použití otevřeného hesla přímo v kódu skriptu/aplikace. Standardně je v rámci řešení password managementu možné integrovat mechanizmus pro získávání hesla přímo do aplikačních serverů, které jej mohou používat k získání přístupu k různým datovým zdrojům (databáze). Tímto jednoduchým mechanizmem je možné zbavit se uložených přístupových údajů bez nutnosti upravovat aplikaci.

5.2 Session Recording

Další důležitou oblastí je detailní audit aktivity privilegovaných účtů. Password Management zajišťuje přehled o přístupu k účtům, nikoliv však přehled aktivit, které jsou s takovým účtem konány. To je zajištěno nahráváním uživatelských relací - snímáním obrazovky a logování uživatelského vstupu (key-logging). Každá akce (stisk klávesy, změna obrazovky apod.) privilegovaného účtu je nahrávána a je jednoznačně přiřazena konkrétní osobě. Nahrávky jsou zabezpečeným způsobem přenášeny do centrálního úložiště, kde jsou dlouhodobě uchovávány. Takové nahrávky jsou klíčovým důkazem, kterým je možné uživateli jednoznačně prokázat veškeré jeho aktivity. Zároveň však mohou obsahovat velice citlivé informace. Proto je nutné dodržovat základní bezpečnostní triádu CIA (confidentiality, integrity, availability):

- **Confidentiality** (důvěrnost) – nahrávky jsou po celou dobu uchovávány v zašifrované podobě - tedy od jejich zaznamenání, až po konečné uložení do centrálního repository a jejich archivace. Dále je zaručeno, že k těmto nahrávkám mohou přistupovat pouze autorizované osoby, aby nemohlo dojít k jejich zneužití. U vysoce citlivých/kritických systémů je možné aplikovat metodu čtyř očí, kdy je k zobrazení záznamu podmíněno schválením další osoby.
- **Integrity** (celistvost) – je nutné zabránit jakékoliv manipulaci s nahrávkami po celou dobu jejich existence, aby nemohlo dojít ke zpochybnění její prokazatelnosti. Toho je možné dosáhnout digitálním podpisem každé z nahrávek.
- **Availability** (dostupnost) – klíčovost těchto nahrávek implikuje nutnost zaručit jejich dostupnost. Nahrávky jsou pravidelně zálohovány, současně je zajištěno, že nemohou být jednoduše odstraněny.

Nahrávky jsou efektivním způsobem zaznamenávány a přenášeny (komprimace, zaznamenávání pouze aktivní relace), aby nedocházelo ke zbytečnému zatěžování prostředků (úložiště, síť).

Aby měl systém nahrávání relací vůbec význam, je nutné zajistit, aby ho nebylo možné jednoduše obejít. Toho je dosaženo následujícími prvky:

1. Uživatelé přistupují k EP výhradně prostřednictvím jednoho, nebo více bodů, na kterých je systém nahrávání provozován.
    - Může se jednat o prvek, který funguje jako **síťová proxy**, tedy je přes něj směrována veškerá síťová komunikace od uživatele k EP, která je zaznamenávána.
    - Další variantou je využití vyhrazených **terminálových serverů** (TS) nebo zařízení, které jsou využívány jako jediný bod zprostředkovávající komunikaci uživatele s EP (dále jen „přístupový bod“). Veškeré aktivity na tomto přístupovém bodě jsou zaznamenávány.
2. Síťová pravidla jsou nastavena takovým způsobem, aby byl umožněn přístup výhradně přes tyto vyhrazené body (proxy/přístupový bod), pokud to prostředí podporuje. Jakýkoliv pokus přihlášení k EP z jiného než vyhrazeného bodu je detekován a buď aktivně přerušen, nebo alespoň notifikován. K tomuto účelu se předpokládá využití systému SIEM (nasazení této funkcionality provede zadavatel, s dodavatelem bude pouze konzultován návrh realizace).
3. V případě výpadku linky, přes kterou jsou nahrávky přenášeny do centrální databáze, je nahrávka ukládána lokálně na přístupovém bodu, a to do objemu, který je definován konfigurovatelným parametrem, aby nedošlo k její ztrátě. Po obnovení linky je lokálně uložená nahrávka přenesena do centrální databáze.

Nahrávky obsahují kromě samotných obrazovek a uživatelského vstupu také příslušná **metadata** – např. názvy oken na obrazovce, stisknutá tlačítka, výstup příkazů na obrazovce, otevřené soubory, atp. Všechny tyto údaje jsou **indexovány** tak, aby v nich bylo možné efektivně vyhledávat a z výsledku vyhledání moci přejít rovnou na relevantní místo v nahrávce, bez nutnosti sledovat kompletní záznam.

5.3 Access Control

Tato oblast se zabývá řízením přístupu privilegovaných účtů, tedy kontrolu nad tím, jaké aktivity může jaký uživatel s privilegovaným účtem provádět. Můžeme chápat jako přidání další vrstvy oprávnění na koncovém systému, kde je účet využíván.

Tato funkcionalita není v rámci tohoto projektu vyžadována. Je však vyžadováno, aby nasazované řešení tuto funkcionalitu podporovalo, aby bylo možné celou problematiku pokrýt v rámci jednoho řešení pouze jeho rozšířením.

Access control je tedy určen **sadou politik**, které se skládají z následujících pravidel:

1. Výčet příkazů, které uživatel může/nemůže spouštět.
2. Výčet zdrojů, které uživatel může/nemůže využívat – např. soubory, adresáře.
3. Výčet kanálů, které uživatel může/nemůže využívat pro přístup k systému.
4. Časová okna definující, kdy je možné k systému přistupovat.

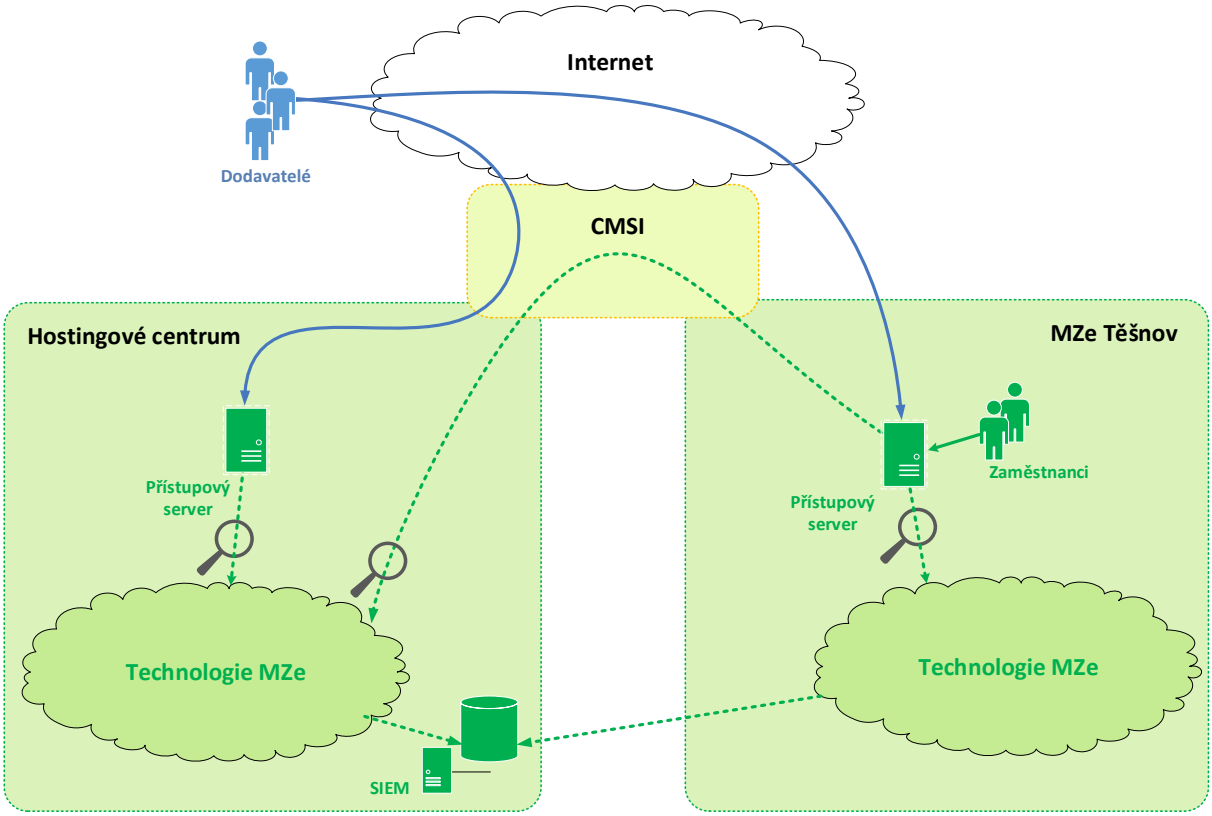
Omezení mohou být buď přímo vynucena, nebo pouze auditována, kdy vyhodnocení pravidla v případě porušení může spustit generování události do systému SIEM nebo notifikaci.

Politiky jsou **centrálně** spravovány a je zajištěna jejich distribuce a deployment na koncové systémy a to buď manuální (politiky jsou EP ručně přiřazeny), nebo automatická (na základě typu nebo kategorie EP).

5.4 Řízení přístupu k EP

Komunikační schéma na obrázku (Obrázek 3) znázorňuje požadovaný cílový stav, který musí být řešením PIM zajištěn. Řešení PIM tak musí umožňovat řídit a monitorovat přístup:

- externích dodavatelů přistupujících z Internetu k EP hostovaným v HC Nagano a HC Chodov;
- externích dodavatelů přistupujících z Internetu k EP hostovaným v lokalitě Těšnov;
- interních zaměstnanců MZe přistupujících z lokality Těšnov k EP hostovaným v HC Nagano, HC Chodov a v lokalitě Těšnov;



Obrázek 3 - topologie přístupových bodů (high-level architektura)

5.5 Integrace

Dodané řešení PIM je integrováno s ostatními systémy organizace dle následujícího popisu.

5.5.1 LDAP/AD

Adresářová služba LDAP nebo Active Directory je využita jako primární zdroj autentizace a autorizace uživatelů pro všechny jejich aktivity. Autorizace opravňuje uživatele k těmto aktivitám:

1. Aktivity v rámci systému na řízení PIM, tedy příslušnost základních rolí:
    a. **Administrátor** – konfiguruje systém nebo jeho část, může vytvářet/upravovat/odstraňovat objekty systému (kromě odstraňování auditních informací a nahrávek).
    b. **Auditor** – má přístup k auditním informacím a nahrávkám.
    c. **Uživatel** – je mu umožněn přístup k systému PIM a jeho běžné používání.
2. Aktivity spojené s privilegovanými účty:
    a. **Vlastník** – nastavuje, kdo má k účtu přístup, případně schvaluje přístup v rámci workflow, přiřazuje politiky hesel.
    b. **Uživatel** – může účet buď přímo používat, nebo je mu umožněno o přístup k účtu zažádat.

Struktura oprávnění je zpravidla ještě dále členěna, jedná se pouze o základní pohled. Konečný výčet rolí a jejich obsah vyplyne z analýzy během dodávky.

5.5.2 IDM

V rámci analýzy během dodávky bude za součinnosti zadavatele a správce IDM navržena kooperace systému IDM a PIM při discovery účtů na EP, kdy je potřeba zjistit, zda nově nalezený neřízený účet patří identitě (osobě), nebo se jedná o sdílený privilegovaný účet, na základě čehož je účet předán do správy buď IDM nebo PIM systému.

5.5.3 Logování a SIEM Systém

PIM loguje jak veškeré aktivity prováděné administrátory nad řešením, tak i veškeré operace uživatelů používajících PIM. Všechny tyto logované záznamy jsou v reálném čase přenášeny do systému pro bezpečnostní monitoring (SIEM) k jejich vyhodnocení a uložení na centrálním bezpečném místě pro případnou zpětnou analýzu.

Do SIEM sytému se rovněž integrují i logy ze systémů a aplikací na EP, aby bylo možné vyhodnotit dodržování pravidel pro přístup daných PIM řešením (např. že uživatelé přistupují k EP přes vyhrazené přístupové řešení a ne napřímo). Nasazení této funkcionality provede zadavatel, s dodavatelem bude pouze konzultován návrh realizace.

5.5.4 Service Desk

Schvalování uživatelských akcí je buď řešeno přímo v systému PIM, nebo je možné využít integrace se Service Desk systémem, na který je schvalování zcela, nebo jen částečně delegováno. Schvalování může být vynuceno v následujících případech:

1. Přiřazení privilegovaného účtu uživateli.
2. Použití privilegovaného účtu (např. při inicializaci relace).
3. Přístup k nahrávce uživatelské relace.

6 PŘEHLED POŽADAVKŮ

Objednatel v rámci výběrového řízení požaduje zajištění kompletní dodávky řešení PIM, které vyhovuje požadavkům uvedeným v této kapitole.

6.1 Funkční požadavky

Součástí této Technické specifikace je Příloha A s tabulkou ve formátu Excel, která obsahuje seznam požadavků na funkcionalitu řešení PIM (dále jen „Tabulka požadavků“). Pokud je v Tabulce požadavků některý požadavek označen jako **povinný**, nebude řešení, které takovému požadavku nevyhovuje, akceptováno a nabídka takového uchazeče bude vyřazena. Ostatní funkční požadavky uvedené v Tabulce požadavků jsou **volitelné** a budou předmětem hodnocení.

Tabulka požadavků je rozdělena celkem do třech částí:

A. Základní vlastnosti a obecné požadavky,
B. Session Recording,
C. Password Management.

Bude-li uchazečem předkládaný návrh technického řešení splňovat konkrétní volitelný funkční požadavek, bude mu přiděleno bodové hodnocení stanovené zadavatelem ve vztahu k takovému funkčnímu požadavku. Nebude-li uchazečem nabízené řešení příslušný volitelný funkční požadavek splňovat, obdrží uchazeč v jeho rámci 0 bodů.

Ve sloupci „Popis naplnění požadavku“ uvedeném v Tabulce požadavků uchazeč popíše způsob naplnění požadavku. Z obsahu samotného popisu musí být zřejmé, zda jsou stanovené funkční požadavky naplněny. Popis může být rozšířen o odkaz na příslušnou část dokumentace výrobce ve sloupci „Doplňující odkaz na externí zdroj“, který bude mít pouze účel upřesnění, informace o naplnění požadavku musí být zřejmá již ze samotného popisu.

Tabulku požadavků musí uchazeč pouze doplnit o informaci, zda jeho řešení splňuje („ANO“/„NE”) spolu s popisem naplnění požadavku ve smyslu předchozích odstavců. Uchazeč je povinnen předat soubor v elektronické podobě pouze s doplněným svým obsahem dle popisu výše (modře podbarvené buňky). Zároveň je povinen zachovat veškerý obsah (zeleně podbarvené buňky), který mu nepřísluší měnit, zachovat formát a podobu tabulky, včetně formátu excelovského souboru.

Pokud uchazeč u požadavku uvede, že jeho řešení PIM jej splňuje, rozumí se tím, že bude požadavek naplněn v rámci dodávky, tedy součástí dodávky budou veškeré licence, vývojové/implementační práce, případně jiné části dodávky potřebné k naplnění tohoto požadavku.

6.2 Rozsah

V této sekci je definován rozsah dodávaného řešení.

6.2.1 Řízené systémy/aplikace

Cílem je do Session Recordingu a Password Managementu[1] postupně zahrnout následující systémy a aplikace:

	Systém/Aplikace (typ EP)	Protokol/Rozhraní	Počet systémů/apl.
1.	Fyzické servery s operačním systémem • Unix/Linux – HP-UX, RedHat, CentOS • Windows (standalone, nebo zapojené do domény)	**SSH – Unix/Linux** **RDP/WMI – Windows**	**100**
2.	Virtuální servery s operačním systémem • Unix/Linux – RedHat, CentOS • Windows (standalone, nebo zapojené do domény)	**SSH – Unix/Linux** **RDP/WMI – Windows** **VMWare**	**250**
3.	Infrastrukturní a bezpečnostní prvky (routery, switche, firewall, WCF, IPS, IDS, WIFI atd.)	**SSH/Telnet,** **HTTP(S) (webové rozhraní)**	**70**
4.	VMware ESXi 5.1.0	**Tlustý klient/web** **vSphere**	**Fyz. serverů: 16** **CPU 12 core: 6** **CPU 8 core: 24** **CPU 6 core: 4** **CPU 4 core: 6**
5.	Citrix XenApp platforma, včetně session recordingu deployovaných aplikací.	**Tlustý klient/web** **ICA**	**2**
6.	LDAP (Oracle Internet Directory)	**LDAP**	**2**
7.	Microsoft Active Directory (přístup k doméně privilegovanými osobními účty nelze omezit, proto bude řešeno monitoringem SIEM systémem)	**LDAP/RDP**	**3**
8.	SAP • SAP Business Warehouse • SAP ERP (systémy R3, AF, EP)	**Tlustý klient/web**	**1**
9.	Databáze (Oracle, MS SQL)	**SQL/Tlustý klient** **Oracle** – SQL*Plus, SQL Developer **MS SQL** – SQL Server Management Studio	**15 (instance)**
10.	Aplikační servery s administračním web GUI (JBoss, WebLogic, GlassFish, Oracle AS, Tomcat)	**Webové rozhraní**	**35**
11.	Ostatní aplikace využívající webové rozhraní nebo tlustého klienta, např.: *SUR, AK, OIM, dohledové systémy, zálohovací systémy, SIEM, ServiceDesk*	**Tlustý klient/web**	**30**

[1] Pokud nebude možné některé z aplikací/systémů uvedených v řádcích 3, 8, 10, 11 tabulky Tabulka 2 zařadit do plného Password Managementu z důvodu nemožnosti jednoduše měnit hesla k účtům, bude v takovém případě heslo alespoň evidováno a v pravidelném intervalu měněno správcem aplikace/systému manuálně.

	Některé z těchto aplikací využívají jako úložiště uživatelů LDAP/AD, proto správa hesel k účtům spadá pod správu hesel k LDAP/AD.		
12.	Aplikace/skripty a aplikační servery využívající aplikačního rozhraní na získání hesla k účtu prostřednictvím PIM	**Java** **.NET** **Unix/Linux shell script** **Windows batch**	**Vlastní aplikace: 1** **JBoss: 1** **WebLogic: 1** **Oracle AS: 1** **Tomcat: 1**

Tabulka 2 - typy a počty EP

Součástí dodávky budou licence, které pokryjí napojení všech systémů/aplikací uvedených v tabulce výše (Tabulka 2).

Z důvodu urychlení nasazení budou v rámci implementace napojeny pouze některé ze zmíněných systémů/aplikací, další integrace proběhnout následně proškoleným personálem zadavatele. Seznam systémů/aplikací k integraci je uveden v kapitole 6.3.3 Implementace.

6.2.2 Počet uživatelů

Počet uživatelů využívající PIM pro přístup k systémům je následující:

- Celkový počet uživatelů: **260**;
- Maximální počet současně přistupujících uživatelů: **70**;
- Průměrný počet přistupujících uživatelů za den: **70**;
- Průměrná délka uživatelské relace za den: **5 hodin**;

Licence potřebné k pokrytí výše uvedených parametrů budou součástí dodávky.

6.2.3 Archivace nahrávek

Nahrávky Session Recordingu je požadováno uchovávat **5 let** na bezpečném úložišti. Z tohoto úložiště nemusí být nahrávky nutně okamžitě dostupné, je možné využít tzv. cold archive, tedy archivu, ze kterého je nutné před jejich prohlížením nejprve nahrávky přenést na určené místo (vyvolat). Nahrávky, které nejsou starší než **8 měsíců** by měli být dostupné bez nutnosti jejich vyvolávání.

Pro výpočet velikosti úložiště lze použít údaje z odstavce 6.2.2 Počet uživatelů.

6.2.4 Přístupové body

Řešení PIM musí v lokalitě MZe Těšnov obsahovat alespoň jeden přístupový bod, který bude zajišťovat nahrávání uživatelských relací a řízení přístupu k EP provozovaných jak v lokalitě Těšnov, tak i v HC Nagano a HC Chodov. Dále řešení PIM musí obsahovat alespoň jeden přístupový bod v HC Nagano/Chodov, který bude rovněž zajišťovat nahrávání uživatelských relací a řízení přístupu k EP provozovaných v HC Nagano a HC Chodov. Všechny přístupové body musí být nasazeny v režimu **vysoké dostupnosti**. Řešení vysoké dostupnosti přístupového bodu musí ve všech případech obsahovat minimálně dva samostatné přístupové servery a v případě HC Nagano/Chodov musí být tyto přístupové servery geograficky odděleny do jednotlivých datových center. Každý ze serverů musí sám zajistit požadované výkonnostní parametry, tak jak je uvedeno v kapitole 6.2.2.

PIM řešení musí umožňovat řídit přístup k EP na dvou úrovních:

1. Na základě řízení **oprávnění** k rozhraní EP (Password Management), tedy poskytnutím přístupových údajů, případě automatické přihlášení k příslušnému rozhraní (SSH, RDP, HTTP, HTTPS, apod.), tak jak je popsáno v kapitole 5.1 Password Management.
2. Na základě řízení **dostupnosti** (Remote Access Control) buď rozhraní jednotlivých EP, nebo rozhraní skupiny EP. V tomto případě musí řízení přístupu uživatelům (dodavatelům, zaměstnancům) zajistit dostupnost pouze těch rozhraní EP/skupiny EP, pro která mají oprávnění. Ostatní rozhraní EP musí být pro uživatele z přístupových bodů kompletně nedostupná, tedy bez jakékoliv možnosti k rozhraní přistoupit - vyvolat přihlašovací dialog (např. každý dodavatel bude mít vyhrazen vlastní přístupový bod v režimu vysoké dostupnosti, ze kterého budou dostupná pouze a jen ta rozhraní, která daný dodavatel potřebuje pro správu technologií).
   V případě řízení přístupu ke skupinám EP v HC Nagano/Chodov je požadováno, aby dodané PIM řešení umožňovalo zajistit tento výlučný přístup minimálně k **deseti skupinám rozhraní EP**, které nemusí být disjunktní. V lokalitě Těšnov je vyžadováno, aby PIM řešení umožňovalo zajistit stejný výlučný přístup minimálně ke **třem skupinám rozhraní EP**. Pro tuto architekturu platí rovněž požadavek na zajištění vysoké dostupnosti přístupových bodů pro každou skupinu EP.
   Pokud není možné zajištění výlučného přístupu dosáhnout čistě na úrovni PIM řešení např. dostupností pouze odkazu pro přístup ke konkrétnímu rozhraní EP a pomocí SSO, ale je zapotřebí vybudovat více přístupových bodů pro každou skupinu EP a výlučný přístup zajistit nastavením filtrování na úrovni sítě, není zařízení pro nastavení filtrování síťové komunikace (firewall) požadováno jako součást dodaného PIM řešení. Filtrování bude zajištěno centrálním firewallem v HC Nagano a HC Chodov, případně firewallem v lokalitě Těšnov.

Pokud řešení vyžaduje farmu Windows terminálových serverů a zároveň uživatelské CAL licence, není vyžadováno, aby tyto CAL licence byly součástí řešení. Zadavatel díky současnému řešení přístupu dodavatelů disponuje dostatečným počtem uživatelských CAL licencí na pokrytí všech uživatelů přistupujících prostřednictvím terminálových serverů. Licence OS je však vyžadována jako součást dodávaného PIM řešení.

6.2.5 Prostředí

V rámci dodávky je požadována instalace **dvou** prostředí PIM:

- **Produkční**
- **Vývojové/Testovací**

Požadavky na produkční prostředí vyplývají z této Technické specifikace.

Vývojové/testovací prostředí bude sloužit k testování patchů a nových verzí systému dodaných výrobcem. Zároveň v něm bude probíhat vývoj a testování funkcionalit v rámci rozšiřování systému (konektory, skripty pro automatizované přihlašování, schvalovací WF, integrace, atp.).

Testovací/vývojové prostředí musí zajistit všechny požadované funkční parametry jako prostředí produkční a musí obsahovat minimálně po jedné z komponent použité v produkčním prostředí, aby

tak obě prostředí byla identická z pohledu podporovaných funkcí a komponent, a bylo tak možné v testovacím/vývojovém prostředí řádně otestovat veškeré funkcionality a vlastnosti konfigurovatelné v produkčním prostředí. Testovací/vývojové nemusí být nasazeno v režimu vysoké dostupnosti.

Všechny změny v rámci PIM řešení, zejména upgrade, bezpečnostní záplaty, nové funkcionality a další nové verze PIM řešení nebo jeho částí, musí být řádně otestovány Dodavatelem, ještě před nasazením do produkčního prostředí Objednatele. V rámci implementace PIM řešení se produkční prostředí považuje za testovací až do fáze akceptačních testů (etapa B.6. dle harmonogramu).

6.2.6 Vysoká dostupnost

V rámci řešení je požadováno, aby produkční prostředí bylo instalováno v režimu vysoké dostupnosti. Každá z komponent tedy musí obsahovat minimálně dvě samostatné instance provozované v HA módu active/active, nebo active/pasive. Řešení vysoké dostupnosti musí být plně automatické. Řešení, která vyžadují jakoukoliv manuální intervenci pro přepnutí mezi instancemi v případě vzniku chybového stavu, nejsou přípustná. Vysoká dostupnost musí být plně zajištěna na úrovni dodávaného PIM řešení, tedy buď na úrovni samotné aplikace a/nebo operačního systému. Pokud se nejedná o instalaci OS na fyzickém HW (tj. v případě použití virtualizace), dodávané řešení nesmí spoléhat na zajištění vysoké dostupnosti nástroji a prostředky virtualizační technologie.

6.3 Fáze realizace dodávky

Následuje popis jednotlivých fází dodávky PIM řešení.

6.3.1 Analýza

Dodavatel v rámci dodávky provede nejprve analýzu nezbytnou pro instalaci a konfiguraci komponent PIM řešení, integraci všech typů EP (viz. 6.2.1 Řízené systémy/aplikace) a připraví technický popis řešení, instalační postup, detailní časový harmonogram a definuje nároky na součinnost. Na základě požadavků na PIM řešení Dodavatel připraví návrh testovacích scénářů, pokrývajících testování všech funkčních rysů implementovaného řešení, včetně testování vybraných výkonových parametrů a výpadků jednotlivých komponent. Dále Dodavatel připraví návrh integrace PIM řešení do provozního a bezpečnostního (SIEM) monitoring systému Objednatele.

Všechny požadované výstupy z etapy Analýza budou Objednateli předloženy k odsouhlasení. Objednatel prostuduje předložené výstupy a bez zbytečného odkladu posoudí, zda navrhované řešení splňuje všechny požadované vlastnosti dané touto Technickou specifikací. Pokud Objednatel shledá nesoulad nebo nejasnosti navrhovaného řešení oproti této Technické specifikaci, požádá Dodavatele o nápravu. Teprve po akceptaci bez výhrad všech požadovaných výstupů Objednatelem je etapa Analýza považována za ukončenou a Dodavatel tak může pokračovat v realizaci dodávky následnou etapou Instalace v souladu s odsouhlasenými výstupy z etapy Analýza. Akceptační řízení bude probíhat dle parametrů uvedených v čl. 4 Smlouvy, nedohodnou-li se smluvní strany jinak.

6.3.2 Instalace

Instalace řešení PIM bude provedena do vyhrazené bezpečnostní infrastruktury Objednatele, která je založena na virtuální platformě VMware a je distribuována přes obě datová centra (geocluster DC Nagano a DC Chodov) a lokalitu Těšnov. V případě nemožnosti instalace do virtuálního prostředí, zajistí Dodavatel fyzické umístění a instalaci všech HW komponent řešení do místa určení v prostředí Objednatele jako součást dodávky PIM řešení. SW prostředky dodané v rámci řešení PIM budou instalovány v poslední verzi dostupné v době plnění. Dodavatel dále zajistí nasazení a aktivaci všech licencí a licenčních klíčů. Architektura instalovaného PIM řešení, včetně identifikace komponent, přehledu instalovaných verzí a použitých licencí a licenčních klíčů bude součástí instalační dokumentace.

6.3.3 Implementace

V rámci fáze implementace bude Dodavatelem zajištěna konfigurace PIM řešení tak, aby řešení vyhovovalo požadavkům uvedeným v Technické specifikaci.

Jako součást dodávky bude provedeno:

- Konfigurace komponent PIM řešení;
- Navržení a nasazení mechanizmu vynucování a kontroly přístupu k EP výhradně přes nahrávaný kanál;
- Integrace následujících EP:

	Název systému	Počet	Přístup/Aplikace
1.	Red Hat Enterprise Linux 6 (64-bit)	1	SSH
2.	HP-UX 11i v3	1	SSH
3.	Microsoft Windows Server 2012 (64-bit)	1	WMI/RDP
4.	Microsoft Windows Server 2008 R2 (64-bit)	1	WMI/RDP
5.	Firewall Fortinet FortiGate	1	SSH/Web
6.	Switch HP 7500 (SSH)	1	SSH
7.	Switch Cisco Catalyst 4500 (Telnet)	1	Telnet
8.	Oracle RAC database 11g (11.2.0.3)	1	SQL
9.	Microsoft SQL Server 2008 R2 SP1	1	SQL
10.	Microsoft ActiveDirectory	1	RDP/LDAP(s)
11.	LDAP (Oracle Internet Directory)	1	LDAP(s)
12.	VMWare ESXi 5.1.0	1	vSphere
13.	Webová aplikace – vyplyne z analýzy	2	Web
14.	SAP – vyplyne z analýzy	1	Web/SAP klient
15.	Aplikace/systémy podporované PIM řešením, které vyplynou z analýzy	2	

Tabulka 3 - seznam EP k integraci v rámci implementace

- Vytvoření politik v souladu s bezpečnostní politikou Objednatele;
- Vytvoření schvalovacího procesu pro žádost o privilegovaný přístup;
- Vytvoření procesu pro nouzový přístup k EP v případě celkového nebo částečného výpadku PIM řešení;

- Integraci PIM řešení do provozního a bezpečnostního monitoringu provede Objednatel za součinnosti Dodavatele;
- Nastavení zálohování konfigurace a dat PIM řešení;

6.3.4 Akceptační testy

V rámci analytické fáze budou Dodavatelem navrhnuty testovací scénáře, které budou pokrývat následující oblasti a parametry řešení:

- Funkční testy

Funkční testy ověří, že implementované PIM řešení poskytuje bezchybně všechny požadované funkcionality uvedené v Technické specifikaci, včetně řádně integrace se systémy Objednatele (SIEM, SSO, apod.).

- Zátěžové testy

Jejich úkolem je ověřit, že implementované komponenty jsou schopny obsloužit požadovaný maximální počet současně přistupujících uživatelů bez výrazného dopadu na kvalitu a odezvu řešení.

- Bezpečnostní testy

Úlohou bezpečnostních testů je ověřit, že jsou všechny komponenty zabezpečeny dle požadavků definovaných v Technické specifikaci, např. je zabezpečený přístup k úložišti účtů a hesel, přístup k nahrávkám mají pouze autorizované osoby a jejich přístup je logován, zálohy konfigurace a dat jsou řádně zabezpečeny, uživatelé mají přístup pouze do přidělených bezpečnostních segmentů, apod.

- Testy zajištění kontinuity (DRP testy)

Úlohou testů je ověřit dostupnost PIM řešení v případě výpadku jednotlivých funkčních komponent a ověřit funkčnost nouzového přístupu na EP a k databázi hesel v případě nedostupnosti PIM řešení.

Testování bude provedeno Objednatelem za součinnosti Dodavatele. Dodavatel k realizaci testů zajistí:

- Nástroje a komponenty potřebné pro testování;
- Přípravu návrhu testování a hodnotících kritérií;
- Přípravu testovacích scénářů;
- Přípravu prostředí a testovacích dat (v součinnosti s Objednatelem);
- Testovací protokoly s výstupy testů;
- Seznam defektů a způsob a harmonogram jejich odstranění;

Akceptační testy jsou ukončeny nahlášením výsledku a předáním seznamu nalezených vad. Po odstranění podstatných vad budou akceptační testy celé opakovány a ověří tak kvalitu předávaného PIM řešení. U ostatních vad se provedou akceptační testy s ohledem na ověření řešení pouze příslušné vady.

Podstatné vady jsou vady, které způsobují tak závažné problémy, že Objednatel nemůže produkt nebo jeho klíčovou část používat či ovládat.

6.3.5 Dokumentace

Dokumentace dodaná v rámci řešení bude obsahovat jak originální dokumentaci dodávanou výrobcem PIM řešení, tak i dokumenty popisující nasazení PIM řešení v prostředí Objednatele.

Oficiální dokumentace výrobce produktu k PIM řešení bude předána v elektronické podobě (formát PDF nebo MS Word) a bude provedena v českém, nebo anglickém jazyce. Dokumentace od výrobce musí pokrývat minimálně následující oblasti:

- popis architektury;
- instalace řešení;
- administrace řešení;
- uživatelská příručka;

Dokumentace popisující nasazení PIM řešení v prostředí Objednatele musí být předána v elektronické podobě ve formátu MS Word a bude provedena v českém jazyce. Minimální požadavky na rozsah a obsah dodávané dokumentace je následující:

- Instalační dokumentace
  - Popis architektury;
  - Komunikační matice komponent;
  - Instalované verze;
  - Licence;
  - Instalační postup;
- Implementační dokumentace
  - Popis nastavení komponent PIM řešení;
  - Popis způsobu integrace (jednotlivých typů EP, AD, LDAP);
  - Popis konfigurace zálohování PIM řešení;
- Uživatelská příručka
  - Popis uživatelského rozhraní PIM řešení z pohledu uživatele;
  - Popis uživatelských postupů při práci PIM řešením;
- Administrátorská příručka
  - Popis uživatelského rozhraní PIM řešení z pohledu administrátora;
  - Popis základních úkonů nutných pro údržbu PIM řešení a standardní profylaktické testy;
- Zajištění kontinuity provozu
  - Popis postupu obnovy ze zálohy;
  - Doporučení pro archivaci (nahrané uživatelské relace a související data);
  - Popis postupu v případě havárie jednotlivých komponent včetně postupu obnovy do provozního stavu;
  - Popis postupu nouzového přístupu k EP v případě nedostupnosti/omezené funkčnosti PIM řešení;

6.3.6 Školení

Dodavatel zajistí proškolení minimálně 3 osob Objednatele na úrovni administrace řešení v rozsahu umožňujícím provádět:

- Běžný rutinní provoz a údržbu dodávaného PIM řešení, včetně provedení příslušných konfiguračních změn;
- Řešení obvyklých problémů;
- Správu uživatelských oprávnění;
- Integraci EP;
- Analýzu zaznamenaných uživatelských relací;
- Monitoring stavu zařízení;
- Zálohování a obnovu konfigurace a dat;
- Tvorbu pohledů a reportů;

6.4 Podpora

Dodavatel ručí za to, že PIM řešení bude funkční a použitelné v prostředí Objednatele a bude odpovídat požadavkům Objednatele uvedených v Technické specifikaci a vlastnostem deklarovaným v dokumentaci dodané Dodavatelem. Služby poskytované Dodavatelem musí vyhovovat technickým specifikacím a požadavkům výrobce.

Podpora PIM řešení zahrnuje činnosti definované ve Specifikaci katalogových listů, viz Příloha č.2 Smlouvy.

Podpora bude poskytována dle parametrů definovaných ve Specifikaci katalogových listů, viz Příloha č.2 Smlouvy a bude probíhat v českém jazyce, nedohodnou-li se pověřené osoby smluvních stran v konkrétním případě jinak.

Odstraňování vad technických prostředků bude Dodavatelem prováděno výměnným způsobem na místě s tím, že náhradní díl nebo zařízení musí být nové a bezvadné a musí být doručeny do místa provádění opravy.

6.5 Platformy

Pokud to bude PIM řešením podporováno, bude instalováno do virtuální VMware infrastruktury Objednatele. Součástí nabídky tak musí být:

- specifikace počtu požadovaných virtuálních serverů a jejich parametrů s ohledem na dostatečnou výkonnost řešení a současnou adekvátnost parametrů;
- požadavek na geografické umístění virtuálních serverů v rámci infrastruktury Objednatele s ohledem na zajištění dostupnosti a rozložení předpokládaných uživatelských relací (viz 6.2.2, 6.2.6);
- specifikace požadavků na parametry komunikačních tras a síťových prostupů mezi jednotlivými komponentami řešení PIM;

Pokud není možné řešení PIM či jeho komponentu/komponenty provozovat ve virtuálním prostředí, budou součástí nabídky i HW prostředky, které však musí být vybaveny přípojkami pro minimálně dva nezávislé přívody napájení a předozadní větrání.

Veškeré SW licence potřebné k provozu řešení PIM (např. OS, DB) musí být součástí dodávky. Výjimku tvoří Microsoft CAL licence , které jsou nyní používány v rámci současných přístupových

bodů MZe (farma terminálových serverů, viz 3.4) a dodavatel je může využít k naplnění požadavků (více v odstavci 6.2.4 Přístupové body). **Seznam všech dodaných licencí bude součástí nabídky.**

Veškeré dodané komponenty (SW, HW) budou instalovány v konfiguraci podporované výrobcem/výrobci, v konfiguraci zaručující vzájemnou kompatibilitu všech komponent a dostatečně výkonnostně nadimenzované s ohledem na parametry požadované od PIM řešení.

Veškerý dodaný software (včetně operačního systému, databazí, apod.) bude plně ve správě Dodavatele a je poskytnuta jeho Podpora a Maintenance dle parametrů definovaných ve Specifikaci katalogových listů, viz Příloha č.2 Smlouvy

Řešení PIM musí být v souladu s interní směrnici Objednatele „Definice závazné architektury a požadavků pro vývoj a zabezpečení provozu registrů a klíčových aplikací MZe“ (interní směrnice není přílohou zadání, bude Dodavateli k dispozici v rámci projektu - výňatek s přehledem technologií je uveden níže).

Důvodem tohoto požadavku je zajištění kompatibility se stávající infrastrukturou Zadavatele a zároveň možnost využití stávajících mechanizmů (HW/SW nástroje, personál, servisní smlouvy) pro správu a monitoring dodaných komponent řešení a jednotného přístupu, bez potřeby dalších investic na straně Zadavatele.

Výjimku tvoří řešení, které budou dodány ve formě tzv. „appliance“, tedy řešení, kdy již samotným výrobce nabízí a dodává PIM řešení či některou z jeho komponent jako společný celek softwarových a hardwarového prostředku.

Níže je vykopírován přehled platforem ze zmíněné směrnice:

- Síťové technologie
  - WAN, LAN, HW balancery – technologie Cisco, HP, F5;
  - Firewally, SSL akcelerátory – technologie Cisco, Citrix, HP, F5;
  - SAN prvky – technologie Cisco, HP, Brocade;
- Databázové systémy
  - RedHat Linux Enterprise rel. 6 a vyšší + Oracle 11g rel. 2 a vyšší;
  - Microsoft SQL server verze 2008 a vyšší (pouze pro technologické platformy neumožňující využití Oracle DB);
- Serverové operační systémy
  - Windows server 2012 R2 a vyšší;
  - Red Hat Enterprise Linux AS release 6 a vyšší (64 bit);
- Technologie pro poštovní služby a autentizaci
  - Aplikační autentizace – LDAP Oracle Internet Directory 10g rel. 2 a vyšší;
  - Poštovní služby – MS Exchange 2013 nebo vyšší;
  - Doménová autentizace a autentizace desktopových aplikací Microsoft v prostředí MZe – MS Active Directory;
- Virtualizační technologie
  - VMware ESX 5.0 a vyšší;
- Aplikační servery
  - Oracle WebLogic Server 11g rel. 1 a vyšší (64 bit) – má vlastní webserver;
  - Microsoft .NET (dot NET) – produkty v rámci MS Internet Information Server 7.0;

- JBoss – IIS 7.0 a vyšší (win) nebo Apache (linux);
- Prezentační vrstva
  - Microsoft Internet Explorer verze 10.0 a vyšší.

V případě, že zadávací podmínky této Veřejné zakázky obsahují požadavky nebo odkazy na obchodní firmy, názvy nebo jména a příjmení, specifická označení zboží a služeb, které platí pro určitou osobu, popřípadě její organizační složku za příznačné, nebo patenty, ochranné známky nebo označení původu, umožňuje Zadavatel výslovně pro plnění Veřejné zakázky použití i jiných, kvalitativně a technicky obdobných řešení, která naplní Zadavatelem požadovanou funkcionalitu (byť jiným způsobem).

PŘÍLOHA A – TABULKA POŽADAVKŮ

[samostatný dokument]