Příloha č. 1 ZD – Technická specifikace

Smlouva o dílo
Číslo smlouvy objednatele:
Číslo smlouvy zhotovitele: SOD20180051PM

Technická specifikace

Požadované minimální technické parametry předmětu plnění

Požadujeme dodání a implementaci informačního systém umožňující automatizovat správu organizačních struktur, systematizovaných míst a účtů (identit) uživatelů. Dodavatel je povinný zahrnout do nabídkové ceny všechny potřebné licence pro řádný provoz dodávaných informačních systémů. Včetně postupu nasazení systému IdM v organizaci.

Zadavatel požaduje dodávku a implementaci systémů do vlastního datového centra (on premise implementace).

Zkratky a pojmy:

IdM	**Identity Management**
AD	**ActiveDirectory**
MS	**Microsoft**
MFP	**Multi-Function Printer**
SSO	**Single sign-on**
SDS	**Software-defined storage**
HW	**Hardware**
SW	**Software**
NBD	**NextBusinessDay**
MMF	**Multimodefiber**
SMF	**Single mode fiber**
WF	**WorkFlow**
PIM	**Privileged Identity Management**
PAM	**Privileged Access Management**
IS	**Informační systém**
LDAP	**Lightweight Directory Access Protocol**
SOC	**Security Operation Centre**

1. Popis současného stavu

Zadavatel momentálně nepoužívá žádný IdM systém ani PIM/PAM nástroje.
Správa uživatelů a oprávnění se provádí v MS AD
E-mailový server Microsoft Exchange 2010
500ks WinSvrCAL SNGL SA MVL UsrCAL – nákup 1500ks do konce roku 2018
500ks Microsoft Office 20016 St.500ks Klientských stanic Win7 Pro, Win8 Pro, Win10 Pro
Servery provozovány ve VMWare prostředí verze 6.5. OS – MS Windows Server DC 2016
Databázové prostředí – MS SQL 2017
IS ServiceDesk dodavatele Alvao
DMS systém

Pro nasazení systému IDM bude využito stávající infrastruktury v DC DPO. Servery jsou na platformě INTEL, provozovány ve VMWare prostředí verze 6.5.
OS – MS Windows Server DC 2016
Databázové prostředí – MS SQL 2017
IS ServiceDesk dodavatele Alvao pro realizaci WF v rámci systému IDM.

2. IdM

Požadujeme zpracovat úvodní analýzu oprávnění, přístupových i kompetenčních kolizí, provedení návrhu WF pro správu identit a rolí a jejich implementaci do IdM včetně účtů pevně integrovaných v aplikacích.
Dodávku a nasazení „Identity management systému“ (IdM), který umožní automatizovat správu organizačních struktur, systematizovaných míst, systémových účtů a účtů (identit) uživatelů. Základním zdrojem dat pro IdMbude personální modul informačního systému HELIOS Green. IdM bude také nástrojem pro audit oprávnění uživatelů. IdM bude schopno sledování neobvyklých chování uživatelů i správců analytickými nástroji.

Základní požadavky:

- Změny organizační struktury a interních identit budou primárně v ERP Helios Green.
- IdM bude udržovat interní a externí identity a organizační strukturu ve své vnitřní databázi. Identity ve vnitřní databázi budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy.
- IdM bude obsahovat funkcionalitu Account discovery, tj. automatickou lokalizaci nově zřízených účtů nebo další ekvivalentní možnosti automatizace při přidávání účtů a systémů do IdM.
- Správa privilegovaných účtů – IdM podporuje řízení přístupu k různým druhům privilegovaných účtů (administrátor, power user, sdílené účty, servisní účty, systémové účty, ...)
- Jednotné přihlášení - Nástroj umožňuje funkcionalitu Single-Sign-On (SSO) pro spravované účty, aby nebyly zveřejněny přihlašovací údaje.
- Integrace na ostatní systémy, propagace a distribuce oprávnění v systému IdM.
- Založení identity bude zahájeno požadavkem v systému ServiceDesk, po schválení bude automaticky založen v IdM a dle popisu pracovní funkce budou přiřazeny role a oprávnění (business role) a propagovány do všech návazných systémů.
- IdM umožní nasazení na více serverů v režimu vysoké dostupnosti. Nástroj umožňuje zajištění zajištění vysoké dostupnosti - High Availability (HA) v režimu Active-Active, bez nutnosti zásahu operátora IdM. Nástroj podporuje provádění záloh interních nastavení a spravovaných dat v IdM - Backup
- IdM bude udržovat a spravovat kompletní životní cyklus identity v počtu minimálně 2500 uživatelů pro WF pro řízení life cyklu Identit bude využito systému ServiceDesk společnosti Alvao. Pozn.: Integrací je míněna možnost schvalovacího worklflow pro uživatele vyžadující přístup k účtům, ke kterým přístup uživatel doposud nemá, včetně celé historie schvalování a následného odkazu na případné nahrávky session daného uživatele.
- Zadavatel požaduje, aby systém nebyl licenčně omezen počtem uživatelů
- IdM bude obsahovat registr aplikací a jejich rolí.
- IdM bude obsahovat registr systematizovaných míst v organizaci

- IdM bude obsahovat správu uživatelských rolí, včetně zařazení uživatele do odpovídající role v daném IS.
- V IdM bude správce moci konfigurovat pravidla pro automatické začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě atributů identity a přidružených referenčních objektů. (organizační jednotka, aplikační role, systematizované místo atd.). Stejným mechanismem pravidel bude IdM moci automaticky vytvářet další účty uživatele. Pravidla budou spravována v grafickém editoru prostřednictvím webového prohlížeče.
- IdM bude implementovat princip založený na systemizovaných místech. IdM musí umožnit systemizaci pracovních míst v souladu se strukturou organizace. IdM bude spravovat jednotlivá systemizovaná místa a sadu oprávnění a rolí pro jednotlivé IS organizace vztažené ke konkrétnímu systemizovanému místu.
- IdM musí umožňovat správu emailové schránky na stávajícím poštovním serveru MS Exchange 2010 a novější, zejména musí umožnit:
  - vytvoření schránky
  - zrušení schránky a zneplatnění schránky. Řízení životního cyklu emailových schránek v IdM bude prostřednictvím správy odpovídajících aplikačních rolí uživatele.
- IdM umožní implementaci procesů a rozhraní, která jsou vyžadována v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu
- IdM bude obsahovat nástroj pro logování a audit ve formě strukturovaných logů. Dále bude evidovat logy, které zaznamenávají události systému, změnu entit evidovaných v systému, změny konfigurace nastavení systému IdM, průběh synchronizací IdM s dalšími systémy. IdM je možné integrovat s nástroji typu Syslog a SIEM. Pozn.: Integrací je míněn přenos logů a událostí do zmiňovaných nástrojů.
- IdM zaznamená auditní informace o konfiguračních změnách, které jsou spolu s log daty chráněny proti neautorizovaným úpravám/smazáním a neoprávněným čtením.
- IdM bude umožňovat export reportovaných dat v otevřeném formátu CSV nebo XML pro reportování v externích nástrojích.
- IdM bude podporovat připojení k Security Operation Center

- IdM bude používat stávající AD autentizační servery, které umožní zprostředkovávat systémům autentizační úlohy přes následující protokoly/standardy:
  - LDAP (ActiveDirectory)
  - Windows autentizaci
  - Radius
  - Ověření pomocí certifikátu
  - Podpora vícefaktorové autentizace – (Certifikát, USB token, SW token (Google, Microsoft), personalizovaná karta)

Součástí IdM bude webový portál pro správu uživatelů

Požadavky na Portál IdM:

- Portál IdM bude webová aplikace přístupná přes běžné webové prohlížeče. Minimálně IE, Edge, Chrome, Safari.

- Portál IdM bude obsahovat přehlednou a oddělenou správu samostatných identifikovatelných objektů - referenčních objektů, na které se identita odkazuje: systematizované místo, organizační jednotka, skupina, činnostní role, aplikace, skupina aplikací, aplikační role, certifikát atd. V portálu IdM bude možné tyto objekty samostatně spravovat v grafickém uživatelském rozhraní. Portál IdM musí umožňovat přidávání nových a dalších typů takovýchto referenčních objektů a zajišťovat jejich správu v grafickém uživatelském rozhraní.

- Portál IdM bude obsahovat grafické zobrazení identit (uživatelských účtů) ve stromové organizační struktuře.

- Portál IdM bude obsahovat funkcionalitu pro přesun identity mezi jednotlivými organizačními jednotkami, a kopírovaní aplikačních rolí, činnostních rolí mezi jednotlivými systematizovanými místy

- Portál IdM bude obsahovat správu uživatelů a údajů o jejich interních certifikátech. Data o certifikátech uživatelů bude navíc možné nahrávat do IdM přes webové služby IdM. Portál IdM bude obsahovat nastavení, které zajistí automatické zneplatnění certifikátů v IdM, které jsou po vypršení data platnosti. Portál IdM bude obsahovat správu nastavení, které zabrání hromadným změnám z důvodu případných chybných dat na vstupu (například z personálního systému), tak aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v ActiveDirectory).

- Portál IdM bude obsahovat modul samoobsluhy pro reset hesla pro jednotlivé účty daného uživatele. IdM bude možné napojit na SMS bránu pro generování a zasílání kódů přes zprávy SMS na daného uživatele pro potvrzení resetu hesla.

- V rámci samoobsluhy budou mít uživatelé možnost měnit heslo.

- Veškeré požadavky změn, které provedou uživatelé na Portálu IdM, budou provedeny transakčně. Budou historizovány a logovány tak, aby bylo možné zpětně prokázat kdo, kdy a co změnil v IdM identitách, referenčních objektech, ale i v administraci a konfiguraci IdM. Záznam v historii bude obsahovat původní i novou hodnotu.

- Synchronizace bude možno spouštět ručně i automaticky také v simulačním režimu, tak aby bylo možné si ověřit stav dopadu reálného spuštění předem.

- IdM umožní notifikovat emailovou zprávou vytvoření a změny identity jak schvalovateli, tak i uživateli.

- Portál IdM je možno zobrazit na mobilním zařízení s OS Android a iOS.

Požadavky na oprávnění IdM a role

- Portál IdM bude obsahovat správu jednotlivých úrovní administrátorských oprávnění k identitám a stromové struktuře. V Portálu IdM musí být zejména možnost vytvářet administrátorská oprávnění na úrovni jednotlivých organizačních jednotek.

- Portál IdM bude obsahovat editor oprávnění. V rámci editoru bude administrátor definovat oprávnění do Portálu IdM a následně tato oprávnění přiřazovat konkrétním uživatelům.

- Portál IdM bude obsahovat modul pro správu rolí / přístupů citlivým (osobní, monetizační, obchodní, apod.) údajům uchovávaných v rámci systémů organizace.

- Portál IdM bude obsahovat správu přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce. U přiřazování jednotlivých rolí bude možné nastavit datum a čas platnosti přiřazení. IdM po uplynutí tohoto intervalu rolí přiřazenému objektu odebere.
- Portál IdM bude obsahovat správu identit uživatelů (interních i externích) a jejich případnou řízenou nebo neřízenou úpravu, založení nebo zneaktivnění/smazání externích identit.

Požadavky na webové služby IdM

- IdM bude poskytovat rozhraní webových služeb pro napojení dalších systémů. Základní konfigurace přístupu k webovým službám bude přístupná v Portálu IdM.
- Webové služby IdM budou používat standardizované protokoly webových služeb.
- Volání webových služeb bude logováno a zobrazeno přímo v Portálu IdM.
- Rozhraní bude poskytovat minimálně následující služby
    - Získání organizační struktury
    - Získání hierarchie systematizovaných míst
    - Získání seznamu identit
    - Získání nadřízené osoby pro daného zaměstnance
    - Získání seznamu aplikační rolí
    - Získání seznamu uživatelů dané aplikace
    - Získání seznamu činnostních rolí přiřazených dané aplikaci
    - Zápis seznamu aplikačních rolí do IdM
    - Zápis certifikátů do IdM
    - Zápis a změna identit
- IdM bude obsahovat minimálně tyto obecné konektory pro správu identit v napojených systémech:
    - CMD – konektor umožňuje spouštět CMD příkazy
    - CSV – konektor umožňuje generovat CSV soubory
    - Databáze – konektor umožnuje spravovat identity v DB MS SQL
    - SOAP – konektor umožňuje se napojit na SOAP webové služby
    - LDAP - konektor umožňuje se napojit na LDAP
- Požadujeme plnou integraci na tyto stávající IS:
    - MS ActiveDirectory
    - Helios Green - ERP systém (AssecoSolutions, a. s.) - Aplikační Windows server (IIS) + Windows MS SQL Database
    - ServiceDesk (ALVAO) - Aplikační Windows server (IIS) + Windows MS SQL Database
    - DMS (dodavatel zatím není znám, předpoklad pořízení 4/2018)
    - MS Exchange 2010
    - Korund - systém pro plánování a řízení údržby (TescoSW) Aplikační Windows server (IIS + .NET) + Windows MS SQL Database

- BIS - docházkový systém (ESKON s.r.o.) Aplikační Windows server (IIS + .NET) + Windows MS SQL Database
- GIST controlling - Controllingový systém
- Sprinter - DISPEČERSKÝ SYSTÉM PRO DOPRAVNÍ PODNIKY (HERMAN SYSTEMS, s.r.o.,) Aplikační Windows server (IIS + .NET) + Windows MS SQL Database
- MYQ Aplikační Windows server (IIS + .NET) + Database Firebird

Plnou integrací je myšleno propojení IDM s využitím API daného IS pro plnou integraci. Cílem integrace IS je zabezpečení cílového IS a zabezpečení nakládání s oprávněním definovaným v business roli, případně v popisu systemizovaného místa. Dodavatel je povinen využít API daného systému pro integraci.

Bezpečné uložiště hesel

- Nástroj IdM využívá a poskytuje bezpečné úložiště hesel a privilegovaných účtů, které je certifikováno dle normy FIPS 140-2. V případě, že je podporováno několik úrovní FIPS 140-2, uveďte jaké a za jakých okolností je jich možné dosáhnout, a zda jsou s tímto spojeny dodatečné náklady.
- Pro uchování šifrovacích klíčů je umožněno využít nástroje Hardware Security Module (HSM). Popište případné možnosti využití HSM.
- Nástroj šifruje ukládaná data.
- Nástroj umožňuje zamezit paralelnímu využití sdíleného privilegovaného účtu různými fyzickými uživateli. Poskytněte detaily.
- Nástroj umožňuje identifikaci nesouladu uloženého hesla s heslem na koncovém zařízení.

Autentizace a řízení přístupu k IdM

- Nástroj podporuje federování identit.
- V rámci nástroje je možné přiřazovat různé uživatelské role, minimálně role: uživatel, auditor, schvalovatel, správce, atp.

Zprostředkování privilegovaných oprávnění aplikacím

- V nástroji je Správa aplikací založená na zabezpečení systému, aplikace a uživatelského profilu, který obsahuje: přístupové role, věk, riziko, nepopiratelnost vykonaných činností.
- Nástroj umožňuje správu účtu pro systémové služby či systémové aplikace.

Delegace a eskalace privilegií

- Nástroj umožňuje funkcionalitu delegace privilegií, tj. implementovat schvalovací workflow pro přidělování přístupů (na žádost uživatele) k aktuálně jemu nedostupným účtům, případně schvalovací workflow k provádění jemu aktuálně zakázaných příkazů.
- File Integrity Monitoring - Nástroj provádí kontrolu modifikací souborů a kontrolu přístupů k těmto souborům.

Spravovaná koncová zařízení podporovaných výrobcem IdM

Nástroj umožňuje spravovat následující typy OS:

- MS Windows server
- MS Windows Proffesional 10, 8, 7
- MAC OS
- SUSE Linux
- Red Hat Enterprise Linux

Nástroj umožňuje spravovat následující typy DBMS:

- MS SQL
- Firebird
- Postgre SQL

Uživatelské rozhraní SW musí být lokalizováno do češtiny.

Zajištění technické podpory systému IdM alokováním specialistů v předpokládaném objemu 1 člověkoden měsíčně. Dodavatel uvede celkové náklady na technickou podporu na 5 let jako samostatnou položku cenové nabídky.

3. Požadavky na rozšíření infrastruktury (Hardware)

3.1. Záložní napájecí zdroje (2ks)

- Tower provedení
- Výstupní výkon min. 5000VA
- UPS bude osazena LAN kartou pro správu UPS po LAN, pro její nastavování a komunikaci se zálohovanými zařízeními

3.2. Coreswitche (6 ks)

Nabízený switch **WS-C3850-12XS-S** - Cisco Catalyst 3850 12 Port 10G Fiber Switch IP Base

Požadavek zákazníka	Splněno / Parametr
Typ přepínače: L2/L3 s managementem	ANO
Protokoly pro management: SNMP 1, RMON 1, RMON 2, Telnet, SNMP 3, SNMP 2c, TFTP, SSH, CLI	ANO
Stohovatelné minimálně do počtu 8 jednotek ve stohu	ANO, až 9 jednotek
Instalace do racku	ANO
Podpora pro multicast	ANO
QoS	ANO
Správa prostřednictvím webového rozhraní	ANO
min. 12 portů 1/10Gigabit EthernetSFP+	ANO, 12 portů 1/10G SFP+
Možnost dokoupit rozšiřující síťový modul 4 porty 1/10G SFP+	ANO, modul C3850-NM-4-10G
min. 1 Konzolový port RJ-45	ANO, 1x konzolový port RJ45
min. 1 USB 2.0 port	ANO, 1x USB2 port

celková rozšiřitelnost routovaných portů ve stohu min. 208	ANO, 208 portů
Síťové standardy: IEEE 802.11ac,IEEE 802.1D,IEEE 802.1Q,IEEE 802.1p,IEEE 802.3,IEEE 802.3ab,IEEE 802.3ad,IEEE 802.3af,IEEE 802.3u,IEEE 802.3x,IEEE 802.3z	ANO
Plně duplexní režim, switch port autorecovery (err-disable recovery)	ANO
FlexibleNetflow, IGMP pozorování	ANO
Broadcaststormcontrol	ANO
DHCP server	ANO
Auto MDI/MDI-X	ANO
STP protokol	ANO
Podpora VLAN	ANO
Počet VLANs min. 4000	ANO, 4000 VLAN
Počet VLAN rozhraní min. 1000	ANO, 1000 rozhraní SVI
Celkový počet MAC adres min. 32 000	ANO, 32 000 MAC adres
kapacita přepínání min. 320 Gbit/s na switchi	ANO, 320 Gbps
propustnost na sběrnici mezi switchi ve stohu min. 480 Gbps	ANO, 480 Gbps
Podpora pro Jumbo Frames 9198 B	ANO
Přenosová rychlost min. 227Mpps	ANO, 227,28 Mbps
Access Control List (ACL)	ANO
SSH/SSL podpora, RSPAN	ANO
Šifrování/zabezpečení 802.1x RADIUS, SSH	ANO
Hlučnost při maximálním zatížení max. 45 dB	ANO, 43dB běžně, 45dB max
Typ paměti DRAM	ANO
Paměť flash min. 4GB	ANO, 4 GB
Vnitřní paměť min. 4GB	ANO, 4 GB
redundantní napájení	ANO
Nové core přepínače budou zapojeny do stávající Cisco LAN infrastruktury (stávající stack) a proto s ní musí být 100% kompatibilní	ANO
Zboží musí být určeno pro český trh a Zadavatel má právo požádat Uchazeče o potvrzení vystavené výrobcem	ANO

3.3. Příslušenství ke coreswitchům

Součástí dodávky bude:

- Stacking kabel 0,5m a stackpower kabel ke každému switchi (celkem 6 ks)
- 4ks kompatibilních transceiverů SFP-10G-ER-S= SFP+ a 2ks 10dB attenuator
- 8ks kompatibilních transceiverů SFP-10G-LR-S= SFP+
- 8ks propojovací kabely SMF, délka 2m, konektory duplexní, LC-SC
- 4ks propojovací kabely SMF, délka 5m, konektory duplexní, LC-SC
- 24ks kompatibilních transceiverů SFP-10G-SR-S= SFP+
- 10ks propojovací kabely MMF, délka 2m, 50microns, konektory duplexní LC-LC, OM3
- 10ks propojovací kabely MMF, délka 3m, 50microns, konektory duplexní LC-LC, OM3
- 4ks propojovací kabely MMF, délka 5m, 50microns, konektory duplexní LC-LC, OM3

3.4. Přístupové switche (12ks)

Nabízený switch **WS-C2960X-24TS-L** Cisco Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base

Požadavek zákazníka	Splněno / Parametr
Typ přepínače: L2 s managementem	ANO
Protokoly pro management: SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, TFTP, SSH, CLI	ANO
Stohovatelné až do počtu min. 8 prvků ve stohu	ANO, 8 prvků
Instalace do racku	ANO
Podpora pro multicast	ANO
QoS	ANO
Správaprostřednictvím webového rozhraní	ANO
min. 24 Gigabit Ethernet (10/100/1000) přepínaných ethernetových portů RJ-45	ANO, 24 portů 10/100/1000Base-T
min. 4 porty 1Gbit SFP	ANO, 4 porty SFP 1000Gbps
min. jeden Konzolový port RJ-45	ANO, 1x konzolový port RJ45
min. dva USB 2.0 porty	ANO, 2x USB2 port
Síťové standardy: IEEE 802.1ab,IEEE 802.1D,IEEE 802.1p,IEEE 802.1Q,IEEE 802.1s,IEEE 802.1w,IEEE 802.1x,IEEE 802.3,IEEE 802.3ab,IEEE 802.3ad,IEEE 802.3ae,IEEE 802.3af,IEEE 802.3ah,IEEE 802.3at,IEEE 802.3az,IEEE 802.3u,IEEE 802.3x,IEEE 802.3z	ANO
Plně duplexní režim, switch port autorecovery (err-disablerecovery)	ANO
FlexibleNetflow	ANO
Auto MDI/MDI-X	ANO
STP protokol, RSPAN	ANO
Podpora VLAN, Dynamic VLAN assignment	ANO
Počet VLANs min. 1000	ANO, 4096 VLAN, 1023 aktivních VLAN
propustnost na sběrnici mezi switchi ve stohu min. 80 Gbps	ANO, 80 Gbps
kapacita přepínání min. 200 Gbit/s	ANO, 216 Gbps
propustnost min. 100 Mpps	ANO, 108 Gbps
Podpora pro Jumbo Frames 9216 B	ANO
Přenosová rychlost 64-Byte L3 paketů min. 70 Mpps	ANO, 71,4 Mpps
MAC security, Access Control List (ACL), MAC AddressNotification	ANO
SSH/SSL podpora	ANO
Šifrování/zabezpečení 802.1x RADIUS,SSH	ANO
Hlučnost při maximálním zatížení max. 45 dB	ANO, 42dB běžně, 45dB max
Typ paměti: DRAM	ANO
Paměť flash min. 128 MB	ANO, 128 MB Flash
Vnitřní paměť min. 512 MB	ANO, 512 MB DRAM
MTBF přepínačů ve stacku: min. 17000000 hodin	ANO, 17128090 hodin
Nové přístupové přepínače budou zapojeny do stávající Cisco LAN infrastruktury a proto s ní musí být 100% kompatibilní	ANO
Zboží musí být určeno pro český trh a Zadavatel má právo požádat Uchazeče o potvrzení vystavené výrobcem	ANO

3.5. Příslušenství k přístupovým switchům

Součástí dodávky bude:

- 1ks modulů pro stohování astack kabel 0,5m ke každému switchi (celkem 12ks)
- 8ks kompatibilních transceiverů GLC-SX-MMD= (1000BASE-SX, 850-nm , DOM support, dual LC/PC connector)
- 14ks kompatibilních transceiverů GLC-LH-SMD= (1000BASE-LX/LH, 1300-nm , DOM support, dual LC/PC connector)
- 8ks propojovací kabely MMF, délka 1m, 50microns, konektory duplexní LC-SC, OM3
- 7ks propojovací kabely SMF, délka 1m, konektory duplexní LC-SC
- 7ks propojovací kabely SMF, délka 2m, konektory duplexní LC-SC

4. Instalační a implementační služby:

4.1. Zadavatel požaduje, aby součástí dodávky byly minimálně tyto práce, služby:

4.1.1. Zajištění projektového vedení realizace předmětu plnění
4.1.2. Provedení analýzy a návrhu technického řešení
4.1.3. Rekonciliaci u stávajících rolí a oprávnění v souladu s identitami v Personálním systému a evidencí v IS systémech.
4.1.4. Dodávka, instalace a konfigurace nabízeného IdM
4.1.5. Vytvoření integrací na požadované informační systémy
4.1.6. Dodání a instalace všech potřebných licencí pro řádný provoz informačního systému
4.1.7. Provedení zaškolení administrátorů pro účel správy, obsluhy a běžné údržby v rozsahu min.16 hodin.
4.1.8. Příprava školících podkladů pro uživatele v rámci e-lerningu v systému Learnis Netventic v rozsahu činností běžného uživatele.
4.1.9. Zpracování technologické dokumentace, dokumentace parametrů, konfigurací a nastavení
4.1.10. Provedení akceptačních testů

4.2. Rozsah implementace IdM (PIM/PAM)

Položka	**Počet MD**
Zajištění projektového vedení realizace předmětu plnění.	10
Provedení analýzy a návrhu technického řešení.	3
Rekonciliaci u stávajících rolí a oprávnění v souladu s identitami v Personálním systému a evidencí v IS systémech. *Tvorba autorizačních rolí – min. 50, max. 100 autorizačních rolí.* *Tvorba procesních rolí – min. 10, max. 20 procesních rolí.*	20
Dodávka, instalace a konfigurace nabízeného IdM.	4
Dodávka, instalace a konfigurace nabízeného HW.	5
Vytvoření integrací na požadované informační systémy. *Napojení adaptérů na ovládané informační systémy.* *Prvotní načtení uživatelských identit do IdM.* *Provedení rekonciliace (načtení a následné párování) účtů napojených informačních systémů oproti IdM, resp. oproti autoritativnímu zdroji.*	12
Dodání a instalace všech potřebných licencí pro řádný provoz informačního systému.	0

Provedení zaškolení administrátorů pro účel správy, obsluhy a běžné údržby v rozsahumin.16 hodin.	2
Příprava školících podkladů pro uživatele v rámci e-learningu v systému Learnis Netventic v rozsahu činností běžného uživatele.	1
Zpracování technologické dokumentace, dokumentace parametrů, konfigurací a nastavení. *Technická dokumentace implementace IdM.* *Uživatelská dokumentace implementace IdM.*	5
Provedení akceptačních testů.	3
Připojení IdM na Security Operation Centrum Uchazeče.	3

5. Akceptační kritéria a testy

Po instalaci a zprovoznění celého řešení budou před podepsáním akceptačního protokolu provedeny akceptační testy a následně provedena akceptace řešení dodaného dodavatelem. Testy bude provádět dodavatel za účasti zástupců zadavatele v místě plnění předmětu smlouvy.

5.1. Je dodán, zkompletován, nainstalován a nakonfigurován systém pro IdM
5.2. Jsou nastaveny a převedeny původní oprávnění a role z Is systémů
5.3. Jsou zavedena systematizovaná místa s popisem business role pro dané místo
5.4. Je předána technická dokumentace nastavení a nastavených hodnot
5.5. Byl proveden ověřovací provoz a technická podpora systémů IdM po dobu 30 dní

6. Ostatní požadavky

GDPR

Výsledné dílo musí splňovat požadavky na GDPR, obecné nařízení o ochraně osobních údajů (angl. General Data Protection Regulation), novou legislativu EU, která výrazně zvyšuje ochranu osobních dat.

SOC

V případě poskytování služby SOC dodavatelem požadujeme doplnit informace o poskytovaných službách v rámci SOC.

Návrh postupu implementace IdM

Uchazeč popíše rekonciliační postup v rozsahu 40 – 75 řádků (standardní A4, min. 80 znaků/řádek), ve kterém specifikuje metodiku kontroly souladu identit v Personálním systému, PIM/PAM evidenci a v dotčených systémech.

Uchazeč popíše postup mapování rolí v rozsahu 40 – 75 řádků, (standardní A4, min. 80 znaků/řádek) ve kterém specifikuje řízení rolí a obecné požadavky či doporučení na Business role.

Návrh postupu implementace IdM

V projekt Implementace IdM doporučujeme Zadavateli zohlednit následující cíle, které umožňují plnění předmětu smlouvy v Zadavatelem uvedených kritériích:

6.1. Je dodán, zkompletován, nainstalován a nakonfigurován systém pro IdM
6.2. Jsou nastaveny a převedeny původní oprávnění a role z IS systémů
6.3. Jsou zavedena systematizovaná místa s popisem business role pro dané místo
6.4. Je předána technická dokumentace nastavení a nastavených hodnot
6.5. Byl proveden ověřovací provoz a technická podpora systémů IdM po dobu 30 dní

Pro výše uvedené požadavky doporučujeme Zadavateli námi uvedený postup:

V identifikaci business rolí navrhujeme zaměření na zákonné kompetence Zadavatele, tj. identifikace popisů činností systematizovaných míst s ohledem na zákonné normy:

- **Zákon č. 181/2014 Sb.** ***o kybernetické bezpečnosti a o změně souvisejících zákonů***, především identifikaci rolí v prostředí Zadavatele, které jsou mimo působnost ICT, tj. role ***garant aktiva***, ***garant primárního aktiva*** a ***garant technického aktiva***. Dále v organizační struktuře ICT útvaru identifikovat role ***Uživatel***, ***Administrátor***, ***Manažer kybernetické bezpečnosti***, ***Architekt kybernetické bezpečnost*** a ***Auditor kybernetické bezpečnosti***.
- **Zákon č. 499/2004 Sb.** ***o archivnictví a spisové službě***, především v provázanosti procesních rolí v působnosti ICT jako jsou např. ***Garant dokumentu***[1], ***Správce Document Management Systému***, ***Správce metadat archiválií***.
- **Zákon č. 101/2001Sb.,** ***o ochraně osobních údajů***[2], především v provázanosti personálních systémů v působnosti ICT, tj. role ***Uživatel, Administrátor, Garant aplikace.*** A dále v prostředí Zadavatele, které jsou mimo působnost ICT, tj. ***Správce personálních dat zaměstnanců***, ***Správce personálních dat klientů***, ***Správce personálních dat dodavatelů***.
- **Zákon č. 563/1991 Sb.** ***Zákon o účetnictví***, především v provázanosti ekonomických systémů v působnosti ICT, tj. role ***Uživatel, Administrátor, Garant aplikace.*** A dále v prostředí Zadavatele, které jsou mimo působnost ICT, tj. ***Správce monetizačních dat***.

Uchazeči je zřejmé, že právních norem ČR k vazbě na IdM je více, ale pro první etapu projektu IdM považuje za vhodné informovat Zadavatele, že výše uvedené zákonné normy jsou zde specifikovány z důvodu zákonné penalizační restrikce nebo ze zákonem oprávněné kontroly státními orgány.

Vůči výše uvedenému postupu jsou v dalších kapitolách uvedeny naše návrhy pro detailnější implementační postup. Především k *zaměření detekce a lokalizace nesouladů mezi evidovaným stavem identit (a rolemi, oprávněními) a jejich skutečným stavem v napojených systémech (Rekonciliace)* a *metodický postup v hledání vazeb pro mapování oprávnění na business role*.

[1] Je ve smyslu zákona 181/2014 de jure ***Garant aktiva***.
[2] Tento zákon má být nahrazen „harmonizovaným zákonem s ohledem k normě EU GDPR", který je zatím ve schvalovacím procesu v Poslanecké sněmovně ČR. Uchazeč upozorňuje Zadavatele, že je typické pro ČR schválení novely zákona se zpětnou retroaktivitou a povinností. Doporučujeme tuto skutečnost zohlednit v projektových rizicích v oblasti **Legislativní faktor**.

Rekonciliační postup v IdM

Pro kontrolu souladu (integrity) seznamu uživatelských účtů na systémech HR a IdM slouží speciální postup (později nástroj) popsaný níže. Nalezené rozdíly v seznamech HR a IdM budou oznámeny obsluze IdM. Detaily implementovaného nástroje budou blíže upřesněny před jeho realizací.

Speciální postup

Tento postup/nástroj bude implementován jako workflow spouštěné ručně. Po spuštění workflow bude načten soubor se seznamem uživatelů z HR nebo načten přímo z vytvořené SQL tabulky.

1. V případě využití souboru, bude formát načítaného souboru v podobě řádkového seznamu, mající objekty oddělené čárkou. V případě načítání dat z SQL tabulky separace objektu není potřebná.

2. objekty obsahující česká slova budou překódovány do kódové stránky typu *Microsoft Windows 1250 for eastern Europe(1404)*.

3. Seznam získaný z načteného souboru nebo tabulky bude v dalším kroku workflow porovnán s aktuálním stavem uživatelských identit v Identity Manageru. Výsledek porovnání bude zobrazen jako HTML tabulka v závěrečném formuláři.

4. Porovnává se např.:

a) **Identifikátor zaměstnance** (IPD, osobní číslo, atp.) mezi HR a IdM.
b) **Datum platnosti identity**. Pokud je *datum platnosti od* menší než aktuální datum při zpracovávání nebo *datum platnosti do* je větší než aktuální datum při zpracovávání, je takto nalezená identita označena za platnou.
c) **Záznamy uložené v kontaktech identit**. Především jde o telefonní čísla, osobní čísla, atributy jako skupiny kontaktů (primární kontakt, sekundární kontakt), atp.
d) **Záznamy uložené v HR číselníku**. Nástroj se pokouší nalézt pracoviště, dle kódu v číselníku lokalit.

5. Podle výsledků porovnání dochází správcem IdM k rozhodnutí, které změny budou v IdM uplatněny (smazání, update, vložení).

Výsledný report rekonciliace by měl obsahovat následující typové stavy:

- účet neexistuje v HR
- účet neexistuje v HR, ale jde o systémový účet (např. backup, synchronize)
- účet v HR zneplatněn, ale v systémech je platný
- účet v HR aktuálně zneplatněn, ale v systémech je blokován administrátorem (např. uzamčen)
- účet v HR zneplatněn více jak 2 měsíce, ale v systémech je stále blokován administrátorem (např. uzamčen)
- účet v HR zneplatněn, ale v systémech je blokován uživatelem (např. modulu)
- účet v HR platný, ale v systémech je blokován uživatelem
- chybové stavy synchronizace metadat:
    - nesouhlasí primární skupina uživatele
    - nesouhlasí jméno
    - nesouhlasí příjmení

- nesouhlasí titul
- nesouhlasí funkce nebo není vyplněna
- nesouhlasí telefon
- nesouhlasí mobil
- nesouhlasí e-mail
- nesouhlasí společnost (u externí identity)

Výše uvedené kontroly se zpracovávají po změnách v HR systému. Zadavatel zajistí organizační opatření, kterým Personální útvar informuje správce IdM o proběhlých změnách v HR evidenci.

Mapování přístupových rolí v IdM

Z analytického pohledu je mapování přístupových rolí na Business roli, tzv. *syntéza poznatků získaných analytickými metodami v celek*. Náš postup v mapování bude zaměřen na identifikaci a specifikaci unikátní ***autorizační role***, která bude mít určeného *vlastníka* a *schvalovatele*. Takto určené a evidované autorizační role lze mapovat na následující ***procesní roli***. Unikátní *autorizační role* má v sobě evidováno nastavení v daném systému, aplikaci, službě, apod.

Autorizační role

- autorizační role je chápána jako výkon jednoho oprávnění v jednom systému.
- je reprezentována jedním identifikátorem, který je přiřazen uživatelskému účtu na daném systému (např. ERP role).
- je v daném systému unikátní.
- je pro ni definován garant (doplnit popis garanta role).

Pro *autorizační role* doporučujeme zavést samostatná workflow a formuláře pro správu *autorizačních rolí* – obdobně jako pro správu identit. Tzn.: z pohledu procesního řízení ICT služeb bude zavedeno další workflow pro řešení vazeb mezi *identitou* a *autorizační rolí*.

Název *autorizační role* má přesně definovanou skladbu („AR“+„.“+„skupina_systémů“ + „organizace“+„.“+„technický název role“). Tuto formu nevynucuje IdM. Jde o doporučenou konvenci Uchazeče. Uvedená konvence umožňuje evidenci *autorizačních rolí* v hierarchické struktuře jako objekty s atributy – nejlépe jako samostatný strom v LDAP serveru (adresářových službách).

Příklady:

- **AR.AD-DPO.NET-USER** -> Autorizační role pro *síťového uživatele* v MS Active Directory od organizace Dopravní podnik Ostrava.
- **AR.ERP-DPO.HELIOS-USER** -> Autorizační role pro *uživatele* v ERP Helios v organizaci Dopravní podnik Ostrava.
- **AR.DB-DPO.SQL-ADMIN** -> Autorizační role pro *administrátora* v SQL serveru v organizaci Dopravní podnik Ostrava.

Procesní role

- role spojující více autorizačních rolí do jedné skupiny, dle procesu.
- procesy jsou evidovány.
- uživatel zná procesy, kterých je účasten.
- uživatel je účasten více procesů (může mít více procesních rolí).
- aktuálně u Zadavatele není k dispozici popis rolí na úrovní autorizačních rolí.
- existuje pouze řídící dokumentace, ze které lze procesy v základu určit.

Procesní role odpovídají svým pojetím rolím definovaných uvnitř IdM systému. *Procesní role* sdružují více *autorizačních rolí* do skupin podle příslušnosti k firemním procesům. Pro každou procesní roli je určen její *vlastník* a *schvalovatel*, který schvaluje požadavky na přidělení této role.

Název procesní role má přesně definovanou skladbu („PR“+„.“+ název procesu +„.“+ „technický název role“). Tuto formu nevynucuje IdM. Jde o doporučenou konvenci Uchazeče.

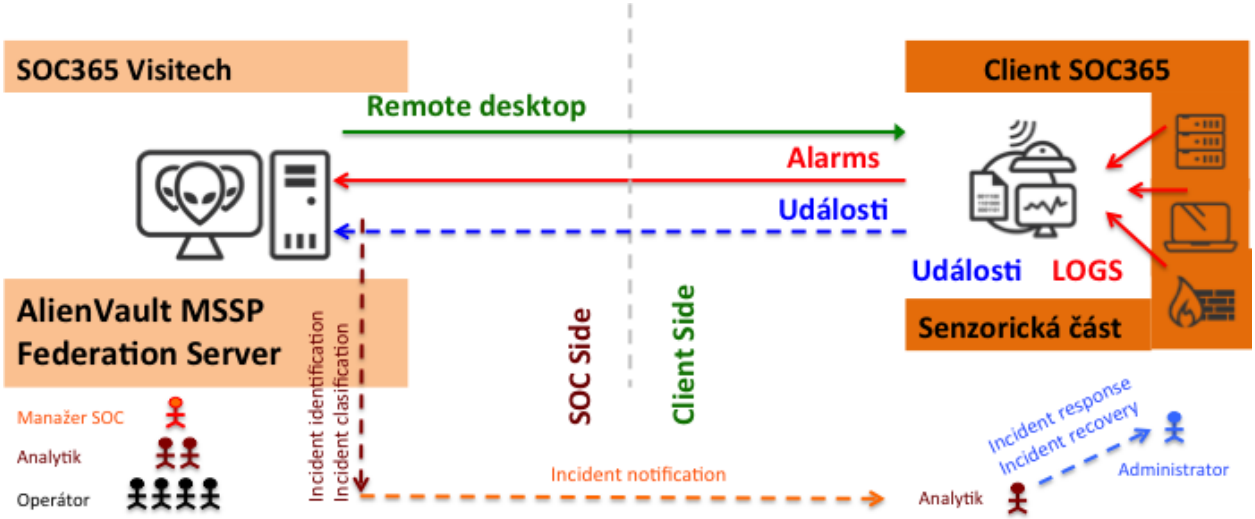
Příklady:

- **PR.ERP.CRM-USER** -> Procesní role pro *uživatele* v ERP, výhradně pro modul CRM.
- **PR.WFM.APP-ADMIN** -> Procesní role pro *administrátora* v informačním systému WorkForce Management s kompetencí správy aplikace.

V rámci analytických prací na IdM po napojení dotčených systémů může Zadavatel očekávat z naší strany definici cca 50 až 100 autorizačních rolí. Ty budou následně seskupovány do procesních rolí. V rámci implementace můžeme Zadavateli nastínit cca 10 procesních rolí, tak aby se správce IdM naučil jak technickému vedení nástroje, tak metodickému vedení procesu IdM, tj. správa *identit*, *autorizačních rolí* a *procesních rolí*.

Napojení komponent IdM na SOC

Zadavatel bude na službu SOC365 napojen interními integračními prostředky SIEM Alien Vault a dalšími software nástroji. Do federativně uspořádané centrální části SOC365 se posílají jen data typu ALARM, v případě i analytických činností také Události, tj. data typu EVENT. Ty slouží *Operátorovi* SOC365 k bližšímu pochopení kontextu přijatého Alarmu.



Operační centrum SOC365 přes role *Operátor* a *Analytik* posuzují jednotlivé Události (EVENTS) a ALARMS a notifikují roli *Analytik* u klienta. Pro specifické situace lze u klienta notifikovat roli *Incident manažer* nebo *CIO*.

Centrum SOC365 zajišťuje činnosti vyhodnocování a eskalace v případě bezpečnostních nálezů. V rámci *remote desktop funkcionality* může centrum SOC365 průběžně vykonávat profylaktické činnosti a zajišťovat aktuálně funkční konfiguraci bezpečnostních komponent klienta.

Obrázek navíc ukazuje personální pokrytí centra SOC365, které je rozšířeno o kompetenční specializace na Machine Learning, Big Data a Forensics analysis. Uvedenému trendu zvýšených potřeb na profesní specializace v kybernetické bezpečnosti bude organizace (tak jako i jiní klienti) udržovat, ať už nároky na personální zdroje a jejich praxi.

Popis vykonávaných činností ve službě SOC365

Služba Dohledu 5x8 hodin	Popis činností
Layer-1 - Operation	Přijetí hovoru na ServiceDesk provozovatele služby
Layer-1 - Operation	Průběžné sledování provozu smluvního zařízení klienta. V případě anomálie posouzení její relevance a závažnosti.
Layer-2 - Analytics	2x denně odborné posouzení bezpečnostní situace a provozního stavu
Layer-2 - Analytics	*Detection* - Posouzení a případná eskalace problému klienta na analytického specialistu. *Event & Incident management* - Detekce a vyhodnocení závažnosti identifikovaných anomálií v prostředí klienta. *Emergency* - Posouzení a případná eskalace nestandardní situace v provozu klienta na službu včasné výstrahy a reakce na incident.
Layer-3 - Služba včasné výstrahy a reakce na nestandardní situaci v prostředí klienta - Incident Response (CERT)	*TRIAGE* – podpora jednotného kontaktní místa pro sběr, třídění, seřazování, procházejících informací o anomáliích. Zajišťuje konsolidaci informací přicházejících s rozdílných zdrojů nebo v rozdílných formátech datových struktur. *HANDLING* - podpora a vedení podezřelých anomálií nebo potvrzených incidentů, hrozeb a útoků. *ANNOUNCEMENT* - přizpůsobení informací z různých formátů do podoby užitečné klientovi, informování o probíhajících hrozbách a nezbytných krocích, které klient může přijmout k ochraně před těmito hrozbami.

	FEEDBACK - poskytování zpětné vazby na bezpečnostní otázky, které se přímo netýkají konkrétních událostí klienta, nicméně mohou přispět ke zlepšování služby a interních procesů.

Služba supportu SOC365	**Popis činností**
Vizuální Dashboardy	Real-time analýza situace v napojených zařízeních podle skupin, kategorií zařízení a podle kontextu získaných záznamů nebo událostí.
Analytické reporty	Zpracování analytických scénářů na aktuální kybernetické hrozby.
Profylaxe	Periodická kontrola souladu nastavení sledovaných komponent klienta. Průběžné sledování provozu smluvního zařízení klienta. V případě anomálie posouzení její relevance a závažnosti.
Configuration & Change management	Zapracování změn podle požadavků klienta nebo podle požadavků či best-practice.
Reporting	1x za 14 dní report provozu ICT komponent, kvality ICT služeb a bezpečnosti prostředí klienta.

Služba monitoring komponent	**Popis činností**
Bezpečnostní dohled	Služba zajišťuje sběr Log dat ze systémů a aplikací, a kompletní proces *Log managementu*, archivace log dat v nezměněné podobě a vyhledávání nad nimi. Služba zajišťuje vyhodnocování Log dat, management bezpečnostních informací a událostí, a kompletní proces *Incident management*. Analytika symptomů, problémů a incidentů k určení příčin nepříznivé situace nebo původců nepříznivých jevů. Korelace všech nasbíraných údajů a jejich vyhodnocení z hlediska vlivu na bezpečnost informací. Jednotný dashboard z výše uvedených parametrů na jedné konzoli pro jednoho operátora. Jednotný alerting pomocí SMS a e-mailu, dle zadaných kritérií.

Provozní dohled	Služba zajišťuje sběr provozních a výkonnostních údajů ICT komponent, a jejich vyhodnocování pro kompletní Problem & Incident management. Provozní monitoring o stavu jednotlivých zařízení tvořících IT infrastrukturu v podobě vizuálních dashboards. Kontrola stavu ICT zdrojů a predikce vyčerpání kapacit.
Asset Management – Řízení aktiv	Průběžná evidence HW ICT komponent, SW verzí, Firmware, konfigurace, uživatel, atp., a kompletní *workflow CMDB*. Evidence a sledování využití adresace IP adresního prostoru klienta SOC365. Služba zajišťuje sběr kontextových informací o konfiguraci dohledovaných aktiv – hardware(network, storage, CPU, RAM,...), software(Operační systém, Aplikace), služby(aktivní, pasivní), uživatelé(uživatel, privilegovaný uživatel - administrátor).
Řízení zranitelností	Služba zajišťuje prověřování bezpečnostní kondice aktiv a vyhodnocení závažnosti detekovaných problémů a zranitelností. Detekce zranitelností, dle aktuálního a relevantního katalogu hrozeb.
Anomaly Detection	Služba zajišťuje sběr informací o proběhlých komunikacích a spojeních mezi aktivy, tj. sledování a analýzu datových toků v IT infrastruktuře - *NetFlow-monitoring*. Průběžným profilováním vzájemné komunikace umožňuje určit anomální chování hardware, software a uživatelů. Služba zajišťuje kontrolu změn souborů na evidovaných aktivech (File Integrity Monitoring) a změn interní konfigurace (Host Intruder Detection System) pro zajištění *ochrany informací a dat*. Sledování chování privilegovaných uživatelů.
Reporting	Automatizované generování reportů ve struktuře podle ISO/IEC 27 001.

Cenový souhrn napojení IdM na SOC

Ceny uvedené v nabídce jsou bez DPH. DPH bude připočtena k ceně díla dle platných předpisů v době zdanitelného plnění.

Napojení zařízení	cena za kus	počet	celková cena
Služba monitoring komponent klienta služby SOC365 (Bezpečnostní dohled, Provozní dohled, Asset Management – Řízení aktiv, Řízení zranitelností, Anomaly Detection)			
Application Device/System			
Počet systémů pro Autentizaci – Active Directory	xxx	1	xxx
Security Device			
Počet IdM	xxx	2	xxx
Network Device			
Počet Switchů	xxx	5	xxx
Celkem monitoring zařízení			**xxx/měsíc**
Služba supportu SOC365 (Analytické reporty, Vizuální Dashboardy, Configuration& Change management, Profylaxe)		1	xxx/měsíc
Služba dohledu 5x8 a včasné výstrahy na nestandardní situace (variantně v režimu 24x7)		1	xxx/měsíc (xxx) / měsíc
Celkem služby			**xxx/měsíc**
Celkem monitoring zařízení a služby			**xxx/měsíc**
Cena vstupní analýzy potřeb klienta a konfigurace k připojení SOC365	xxx	2 MD	xxx