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:
o vytvoření schránky
o 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