Příloha č.2 Smlouvy o dílo

P.č.	Minimální technické požadavky	Forma naplnění Ano/Ne	Doplňující popis
	IDM		
1	Změny organizační struktury a interních identit budou primárně v ERP Helios Green.	Ne	IdM nebude duplikovat evidenční funkcionality. Řešení bude respektovat jednotný (centrální) registr organizačních změn a identit. Z analýzy prostředí Zadavatele pro efektivní implementaci IdM k poskytování důvěryhodných zdrojů dat bude rozhodnuto o použití funkcí ERP Helios nebo technologie ETL (Extract, Transfer, Load) pro udržování změn organizační struktury a identit.
2	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.	Ne	IdM si v rámci rekonciliace vytvoří interní evidenci, který bude zabezpečena interními mechanismy. Tato evidence je referenčním zdrojem pro napojení na LDAP k propojení autorizační a autentizační funkce na napojené systémy.
3	IdM bude obsahovat funkcionalitu Account discovery (v našem řešení se funkce jmenuje PowerBroker Privilege Discovery and Report Tool (DART)), tj. automatickou lokalizaci nově zřízených účtů nebo další ekvivalentní možnosti automatizace při přidávání účtů a systémů do IdM.	Ano	
4	Správa privilegovaných účtů – IdM podporuje řízení přístupu k různým druhům privilegovaných účtů (administrátor, power user, sdílené účty, servisní účty, systémové účty, ...)	Ano	
5	Jednotné přihlášení - Nástroj umožňuje funkcionalitu Single-Sign-On (SSO) pro spravované účty, aby nebyly zveřejněny přihlašovací údaje.	Ano	
6	Integrace na ostatní systémy, propagace a distribuce oprávnění v systému IdM.	Ano	
7	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.	Ne	IdM má schvalovací workflow pro oprávnění a správu hesel. Zákaznicky specifická workflow je umožněno řešit přes externí interface libovolného nástroje ServiceDesk. V rámci analýzy budou určeny integrační funkcionality mezi IdM a ServiceDesk nástrojem Zadavatele.
8	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	Ano	
9	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.	Ano	
10	Zadavatel požaduje, aby systém nebyl licenčně omezen počtem uživatelů	Ano	
11	IdM bude obsahovat registr aplikací a jejich rolí.	Ano	
12	IdM bude obsahovat registr systematizovaných míst v organizaci	Ano	
13	IdM bude obsahovat správu uživatelských rolí, včetně zařazení uživatele do odpovídající role v daném IS.	Ano	
14	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.	Ano	

15	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.	Ano	
16	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.	Ano	
17	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	Ano	
18	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.	Ano	
19	IdM zaznamená auditní informace o konfiguračních změnách, které jsou spolu s log daty chráněny proti neautorizovaným úpravám/smazáním a neoprávněným čtením.	Ano	
20	IdM bude umožňovat export reportovaných dat v otevřeném formátu CSV nebo XML pro reportování v externích nástrojích.	Ano	
21	IdM bude podporovat připojení k Security Operation Center	Ano	
22	IdM bude používat stávající AD autentizační servery, které umožní zprostředkovávat systémům autentizační úlohy přes následující protokoly/standardy:	Ano	
23	o LDAP (ActiveDirectory)	Ano	
24	o Windows autentizaci	Ano	
25	o Radius	Ano	
26	o Ověření pomocí certifikátu	Ano	
27	o Podpora vícefaktorové autentizace – (Certifikát, USB token, SW token (Google, Microsoft), personalizovaná karta)	Ano	
28	Součástí IdM bude webový portál pro správu uživatelů	Ano	
29	Portál IdM bude webová aplikace přístupná přes běžné webové prohlížeče. Minimálně IE, Edge, Chrome, Safari.	Ano	
30	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.	Ano	
31	Portál IdM bude obsahovat grafické zobrazení identit (uživatelských účtů) ve stromové organizační struktuře.	Ano	
32	Portál IdM bude obsahovat funkcionalitu pro přesun identity mezi jednotlivými organizačními jednotkami, a kopírovaní aplikačních rolí, činnostních rolí mezi jednotlivými systematizovanými místy	Ano	

33	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).	Ano	
34	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.	Ano	
35	V rámci samoobsluhy budou mít uživatelé možnost měnit heslo.	Ne	V řešení je zajištěn individuální přístup k centrální správě hesel v rámci napojených systémů s využitím služby MS Active Directory Kerberos.
36	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.	Ne	Veškeré změny v nastavení jednotlivých komponent jsou auditovány. Zpracování transakcí změn navrhujeme řešit v kompetenčním nástroji typu SIEM. Řešení umí audit integrovat s následujícími nástroji: HP ArcSight connector zpracovává ve formátu Common Event Format (CEF), IBM QRadar connector zpracovává ve formátu Log Extended Event Format (LEEF) LogRhythm connector zpracovává ve formátu Log Extended Event Format (LEEF), McAfee ESM connector zpracovává ve formátu Syslog. Veškeré uvedené formáty lze využít k napojení na službu Security Operation Centrum.
37	Synchronizace bude možno spouštět ručně i automaticky také v simulačním režimu, tak aby bylo možné si ověřit stav dopadu reálného spuštění předem.	Ano	
38	IdM umožní notifikovat emailovou zprávou vytvoření a změny identity jak schvalovateli, tak i uživateli.	Ne	Řešení umí notifikovat změny a vypršení časových metrik v podobě e-mail, snmp trap nebo zápisu event záznamu do auditní služby.
39	Portál IdM je možno zobrazit na mobilním zařízení s OS Android a iOS.	Ano	
40	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.	Ano	
41	Portál IdM bude obsahovat editor oprávnění. V rámci editoru bude administrátor definovat oprávnění do Portálu IdM a následně tato oprávnění přiřazovat konkrétním uživatelům.	Ano	
42	Portál IdM bude obsahovat modul pro správu rolí / přístupů citlivým (osobní, monetizační, obchodní, apod.) údajům uchovávaných v rámci systémů organizace.	Ano	
43	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.	Ano	
44	Portál IdM bude obsahovat správu identit uživatelů (interních i externích) a jejich případnou řízenou nebo neřízenou úpravu, založení nebo zneaktivnění/smazání externích identit.	Ano	
45	IdM bude poskytovat rozhraní webových služeb pro napojení dalších systémů. Základní konfigurace přístupu k webovým službám bude přístupná v Portálu IdM.	Ne	Řešení umí v rámci komponenty ***PowerBroker Auditor and Recovery for Active Directory*** zajistit integraci přes funkci **REST API Browser** s MS Active Directory, který může sloužit jako DB. Výsledná architektura bude navržena z dosažených výsledků analytické fáze u Zadavatele.
46	Webové služby IdM budou používat standardizované protokoly webových služeb.	Ano	
47	Volání webových služeb bude logováno a zobrazeno přímo v Portálu IdM.	Ano	
48	Rozhraní bude poskytovat minimálně následující služby		
49	o Získání organizační struktury	Ne	Ano, bude realizováno přes funkci REST API Browser lze spravovat tyto atributy v MS Active Directory, který může sloužit jako LDAP DB. Výsledná architektura bude navržena z dosažených výsledků analytické fáze u Zadavatele.

50	o Získání hierarchie systematizovaných míst	Ne	Ano, bude realizováno přes funkci REST API Browser lze spravovat tyto atributy v MS Active Directory, který může sloužit jako LDAP DB. Výsledná architektura bude navržena z dosažených výsledků analytické fáze u Zadavatele. Aktuálně není uchazeči zřejmá hierarchie systematizovaných míst.
51	o Získání seznamu identit	Ne	Ano, bude realizováno přes funkci REST API Browser lze spravovat tyto atributy v MS Active Directory, který může sloužit jako LDAP DB. Výsledná architektura bude navržena z dosažených výsledků analytické fáze u Zadavatele.
52	o Získání nadřízené osoby pro daného zaměstnance	Ne	Ano, bude realizováno přes funkci REST API Browser lze spravovat tyto atributy v MS Active Directory, který může sloužit jako LDAP DB. Výsledná architektura bude navržena z dosažených výsledků analytické fáze u Zadavatele.
53	o Získání seznamu aplikační rolí	Ne	Ano, bude realizováno přes funkci REST API Browser lze spravovat tyto atributy v MS Active Directory, který může sloužit jako LDAP DB. Výsledná architektura bude navržena z dosažených výsledků analytické fáze u Zadavatele. Uchazeč pracuje s pojmy autorizační a procesní role, které jsou praktičtější v implementacích a provozu IdM. Především z pohledu změn aplikací nebo organizačních změn.
54	o Získání seznamu uživatelů dané aplikace	Ne	Ano, bude realizováno přes funkci REST API Browser lze spravovat tyto atributy v MS Active Directory, který může sloužit jako LDAP DB. Výsledná architektura bude navržena z dosažených výsledků analytické fáze u Zadavatele.
55	o Získání seznamu činnostních rolí přiřazených dané aplikaci	Ne	Ano, bude realizováno přes funkci REST API Browser lze spravovat tyto atributy v MS Active Directory, který může sloužit jako LDAP DB. Výsledná architektura bude navržena z dosažených výsledků analytické fáze u Zadavatele.
56	o Zápis seznamu aplikačních rolí do IdM	Ne	Ano, bude realizováno přes funkci REST API Browser lze spravovat tyto atributy v MS Active Directory, který může sloužit jako LDAP DB. Výsledná architektura bude navržena z dosažených výsledků analytické fáze u Zadavatele.
57	o Zápis certifikátů do IdM	Ne	Ano, bude realizováno přes funkci REST API Browser lze spravovat tyto atributy v MS Active Directory, který může sloužit jako LDAP DB. Výsledná architektura bude navržena z dosažených výsledků analytické fáze u Zadavatele.
58	o Zápis a změna identit	Ne	Ano, bude realizováno přes funkci REST API Browser lze spravovat tyto atributy v MS Active Directory, který může sloužit jako LDAP DB. Výsledná architektura bude navržena z dosažených výsledků analytické fáze u Zadavatele.
59	IdM bude obsahovat minimálně tyto obecné konektory pro správu identit v napojených systémech:		
60	o CMD – konektor umožňuje spouštět CMD příkazy	Ano	
61	o CSV – konektor umožňuje generovat CSV soubory	Ano	
62	o Databáze – konektor umožnuje spravovat identity v DB MS SQL	Ano	
63	o SOAP – konektor umožňuje se napojit na SOAP webové služby	Ano	
64	o LDAP - konektor umožňuje se napojit na LDAP	Ano	
65	Požadujeme plnou integraci na tyto stávající IS:	Ano	
66	o MS ActiveDirectory	Ano	
67	o Helios Green - ERP systém (AssecoSolutions, a. s.) - Aplikační Windows server (IIS) + Windows MS SQL Database	Ano	
68	o ServiceDesk (ALVAO) - Aplikační Windows server (IIS) + Windows MS SQL Database	Ano	
69	o DMS (dodavatel zatím není znám, předpoklad pořízení 4/2018)	Ano	
70	o MS Exchange 2010	Ano	
71	o Korund - systém pro plánování a řízení údržby (TescoSW) Aplikační Windows server (IIS + .NET) + Windows MS SQL Database	Ano	
72	o BIS - docházkový systém (ESKON s.r.o.) Aplikační Windows server (IIS + .NET) + Windows MS SQL Database	Ano	
73	o GIST controlling - Controllingový systém	Ano	

74	o Sprinter - DISPEČERSKÝ SYSTÉM PRO DOPRAVNÍ PODNIKY (HERMAN SYSTEMS, s.r.o.,) Aplikační Windows server (IIS + .NET) + Windows MS SQL Database	Ano	
75	o MYQ Aplikační Windows server (IIS + .NET) + Database Firebird	Ano	
76	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.	Ano	
77	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.	Ano	
78	Pro uchování šifrovacích klíčů je umožněno využít nástroje Hardware Security Module (HSM). Popište případné možnosti využití HSM.	Ano	
79	Nástroj šifruje ukládaná data.	Ano	
80	Nástroj umožňuje zamezit paralelnímu využití sdíleného privilegovaného účtu různými fyzickými uživateli. Poskytněte detaily.	Ano	
81	Nástroj umožňuje identifikaci nesouladu uloženého hesla s heslem na koncovém zařízení.	Ano	
82	Nástroj podporuje federování identit.	Ne	Ano, řešení tuto funkcionalitu zajišťuje hiearchizovanými procesními rolemi a metodickou definicí korporátního user_name ve vazbě na interní schvalovací workflow.
83	V rámci nástroje je možné přiřazovat různé uživatelské role, minimálně role: uživatel, auditor, schvalovatel, správce, atp.	Ano	
84	V nástroji je Správa aplikací založená na zabezpečení systému, aplikace a uživatelského profilu, který obsahuje: přístupové role, věk, riziko, nepopiratelnost vykonaných činností.	Ano	
85	Nástroj umožňuje správu účtu pro systémové služby či systémové aplikace.	Ano	
86	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.	Ano	
87	File Integrity Monitoring - Nástroj provádí kontrolu modifikací souborů a kontrolu přístupů k těmto souborům.	Ano	
88	Nástroj umožňuje spravovat následující typy OS:	Ano	
89	o MS Windows server	Ano	
90	o MS Windows Proffesional 10, 8, 7	Ano	
91	o MAC OS	Ano	
92	o SUSE Linux	Ano	
93	o Red Hat Enterprise Linux	Ano	
94	Nástroj umožňuje spravovat následující typy DBMS:	Ano	
95	o MS SQL	Ano	
96	o Firebird	Ano	
97	o Postgre SQL	Ano	
98	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.	Ano	