**Příloha č. 1 ZD – Technická specifikace**

Smlouva o dílo

Číslo smlouvy objednatele:

Číslo smlouvy zhotovitele:

# **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.

**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** Next**Business**Day

**MMF Multimode fiber**

**SMF Single mode fiber**

1. **Popis současného stavu**

Objednatel momentálně nepoužívá žádný IdM systém.

Správa uživatelů a oprávnění se provádí v AD

E-mailový server Microsoft Exchange 2010

500ks WinSvrCAL SNGL SA MVL UsrCAL

500ks Microsoft Office 2007 St. - plánovaný přechod na Microsoft Office 2016 St. do konce roku 2018

500ks Klientských stanic Win7 Pro, Win8 Pro, Win10 Pro

1. **IdM**

Požadujeme dodávku a nasazení „Identity management systému“ (IdM), které umožní automatizovat správu organizačních struktur, systematizovaných míst a účtů (identit) uživatelů. Základním zdrojem dat pro IdM bude personální modul informačního systém HELIOS Green. IdM bude také nástrojem pro audit oprávnění uživatelů.

**Základní požadavky:**

* IdM bude udržovat 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 umožní nasazení na více serverů v režimu vysoké dostupnosti.
* IdM bude udržovat a spravovat kompletní životní cyklus identity v počtu minimálně 2000 uživatelů.
* Zadavatel požaduje licencování formou multilicence.
* IdM bude obsahovat registraci aplikací a jejich rolí.
* IdM bude obsahovat správu uživatelských rolí, včetně zařazení uživatele do odpovídající role v daném IS.
* V IdM bude správce moct 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 moct 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 systematizovaná 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, 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 bude obsahovat workflow pro řízení životního cyklu změn identit.
* 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 minimálně logy, které zaznamenávají události systému, změnu entit evidovaných v systému, změny konfigurace nastavení systému IdM, průběh synchronizací IdM s dalšími systémy.
* IdM bude obsahovat autentizační server, který bude umožňovat zprostředkovávat systémům autentizační úlohy přes následující protokoly/standardy:
  + LDAP (ActiveDirectory)
  + Windows autentizaci
  + Radius
  + Ověření pomocí certifikátu
  + Podpora vícefaktorové autentizace

**Požadavky na Portál IdM:**

* Portál IdM bude webová aplikace přístupná přes běžné webové prohlížeče.
* 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 správu uživatelů a údajů o jejich 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 funkcionalitu pro přesun identity mezi jednotlivými organizačními jednotkami, a kopírovaní aplikačních rolí, činnostních rolí mezi jednotlivými systematizovanými místy
* 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 testovací režimu, tak aby bylo možné si ověřit stav dopadu reálného spuštění předem.
* IdM umožní notifikovat emailovou zprávou vytvoření a změny identity.

**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 k osobním 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 integraci na tyto stávající IS:
  + MS ActiveDirectory
  + Helios Green - ERP systém (AssecoSolutions, a. s.)
  + ServiceDesk (dodavatel zatím není znám, předpoklad pořízení 2018)
  + MS Exchange 2010
  + Korund - systém pro plánování a řízení údržby (TescoSW)
  + BIS - docházkový systém (ESKON s.r.o.)
  + GIST controlling - Controllingový systém
  + Sprinter - DISPEČERSKÝ SYSTÉM PRO DOPRAVNÍ PODNIKY (HERMAN SYSTEMS, s.r.o.,)

**Uživatelské rozhraní SW musí být lokalizováno do češtiny.**

**Zajištění technické podpory systému IdM alokováním specialistů v předpokládaném objemu 2 člověkodny měsíčně. Dodavatel uvede celkové náklady na technickou podporu na 5 let jako samostatnou položku cenové nabídky.**

1. **Požadavky na rozšíření infrastruktury (Hardware)**
   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
* Záruka 5 let
  1. **Coreswitche (6ks)**
* Typ přepínače: L2/L3 s managementem
* Protokoly pro management: SNMP 1, RMON 1, RMON 2, Telnet, SNMP 3, SNMP 2c, TFTP, SSH, CLI
* Stohovatelné minimálně do počtu 8 jednotek ve stohu
* Instalace do racku
* Podpora pro multicast
* QoS
* Správaprostřednictvím webového rozhraní
* min. 12 portů 1/10Gigabit EthernetSFP+
* Možnost dokoupit rozšiřující síťový modul 4 porty 1/10G SFP+
* min. 1 Konzolový port RJ-45
* min. 1 USB 2.0 port
* celková rozšiřitelnost routovaných portů ve stohu min. 208
* 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
* Plně duplexní režim, switch port autorecovery (err-disablerecovery)
* FlexibleNetflow, IGMP pozorování
* Broadcaststormcontrol
* DHCP server
* Auto MDI/MDI-X
* STP protokol
* Podpora VLAN
* Počet VLANs min. 4000
* Počet VLAN rozhraní min. 1000
* Celkový počet MAC adres min. 32 000
* kapacita přepínání min. 320 Gbit/s na switchi
* propustnost na sběrnici mezi switchi ve stohu min. 480 Gbps
* Podpora pro Jumbo Frames 9198 B
* Přenosová rychlost min. 227Mpps
* Access Control List (ACL)
* SSH/SSL podpora, RSPAN
* Šifrování/zabezpečení 802.1x RADIUS,SSH
* Hlučnost při maximálním zatížení max. 45 dB
* Typ paměti DRAM
* Paměť flash min. 4GB
* Vnitřní paměť min. 4GB
* redundantní napájení
* Nové core přepínače budou zapojeny do stávající Cisco LAN infrastruktury (stávající stack) a proto s ní musí být 100% kompatibilní
* Záruka 5 let s výměnou HW NBD
* Zboží musí být určeno pro český trh a Zadavatel má právo požádat Uchazeče o potvrzení vystavené výrobcem
  1. **Příslušenství ke coreswitchům**
  + Stacking kabel 0,5m a stackpower kabel ke každému switchi
  + 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
  1. **Přístupové switche (12ks)**
* Typ přepínače: L2 s managementem
* Protokoly pro management: SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, TFTP, SSH, CLI
* Stohovatelné až do počtu min. 8 prvků ve stohu
* Instalace do racku
* Podpora pro multicast
* QoS
* Správaprostřednictvím webového rozhraní
* min. 24 Gigabit Ethernet (10/100/1000) přepínaných ethernetových portů RJ-45
* min. 4 porty 1Gbit SFP
* min. jeden Konzolový port RJ-45
* min. dva USB 2.0 porty
* 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
* Plně duplexní režim, switch port autorecovery (err-disablerecovery)
* FlexibleNetflow
* Auto MDI/MDI-X
* STP protokol, RSPAN
* Podpora VLAN, Dynamic VLAN assignment
* Počet VLANs min. 1000
* propustnost na sběrnici mezi switchi ve stohu min. 80 Gbps
* kapacita přepínání min. 200 Gbit/s
* propustnost min. 100 Mpps
* Podpora pro Jumbo Frames 9216 B
* Přenosová rychlost 64-Byte L3 paketů min. 70 Mpps
* MAC security, Access Control List (ACL), MAC AddressNotification
* SSH/SSL podpora
* Šifrování/zabezpečení 802.1x RADIUS,SSH
* Hlučnost při maximálním zatížení max. 45 dB
* Typ paměti: DRAM
* Paměť flash min. 128 MB
* Vnitřní paměť min. 512 MB
* MTBF přepínačů ve stacku: min. 17000000 hodin
* Nové přístupovépřepínače budou zapojeny do stávající Cisco LAN infrastruktury a proto s ní musí být 100% kompatibilní
* záruka 5 let s výměnou HW NBD
* Zboží musí být určeno pro český trh a Zadavatel má právo požádat Uchazeče o potvrzení vystavené výrobcem
  1. **Příslušenství k přístupovým switchům**
* min. 1ks modulů pro stohování astack kabel 0,5m ke každému switchi
* 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

1. **Instalační a implementační služby:**
   1. Zadavatel požaduje, aby součástí dodávky byly minimálně tyto práce, služby:
      1. Zajištění projektového vedení realizace předmětu plnění
      2. Provedení analýzy a návrhu technického řešení
      3. Dodávka, instalace a konfigurace nabízeného IdM
      4. Dodání a instalace všech potřebných licencí pro řádný provoz informačního systému
      5. Provedení zaškolení administrátorů pro účel správy, obsluhy a běžné údržby v rozsahu min.16 hodin.
      6. Zpracování technologické dokumentace, dokumentace parametrů, konfigurací a nastavení
      7. Provedení akceptačních testů
2. **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.

* 1. Je dodán, zkompletován, nainstalován a nakonfigurován systém pro IdM
  2. Je předána technická dokumentace nastavení a nastavených hodnot
  3. Byl proveden ověřovací provoz a technická podpora systémů IdM po dobu 30 dní

1. **Další 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.