

Nadlimitní veřejná zakázka na dodávky podle zákona č. 134/2016 Sb.,
o zadávání veřejných zakázek, **otevřené řízení**

„Dodávka SW pro město Klatovy“, část 3: Identity management (IDM)

TECHNICKÉ PODMÍNKY

1	Úvod	3
1.2	Popis plnění podle této technické dokumentace	3
1.3	Seznam zkratk.....	3
2	Základní požadavky na IDM.....	4
2.2	Funkcionality IDM.....	5
2.3	Požadavky na kontrolní reporty	6
2.4	Požadavky na grafické rozhraní IDM	6
2.5	Požadavky na webové služby	7
2.6	Logy IDM.....	7
2.7	Administrace.....	8
3	Integrace IDM a migrace dat	9
3.1	Integrace IDM.....	9
3.2	Migrace dat	9
4	Implementace IDM.....	9
4.1	Dokumentace skutečného provedení	9
4.2	Instalace IDM.....	10
4.3	Konfigurace dodaného řešení pro potřeby objednatele.....	10
5	Dokumentace	11
5.1	Forma dokumentace	11
5.2	Dokumentace skutečného provedení v prostředí objednatele	11
5.3	Uživatelská dokumentace	11
5.4	Administrátorská dokumentace.....	11
6	Harmonogram	11
6.1	Harmonogram s časovými požadavky objednatele.....	11
6.2	Konkretizovaný harmonogram plnění ze strany zhotovitele	12
6.3	Testovací provoz.....	12
7	Projektové řízení.....	13
8	Legislativa	13
9	Akceptace	14
9.1	Dílčí akceptační řízení.....	14
9.2	Souhrnné akceptační řízení - akceptace díla	14
9.3	Opakované akceptační řízení	14

1 Úvod

- 1.1.1 Tento dokument je určen k popisu a definici rozsahu díla, dodávek a služeb, které objednatel poptává jako předmět plnění ve veřejné zakázce s názvem „IDM pro město Klatovy“.
- 1.1.2 Předmětem této dokumentace je popis a stanovení požadavků objednatele na dodávku a implementaci identity managementu a zpracování dokumentace.

1.2 Popis plnění podle této technické dokumentace

- 1.2.1 Předmětem plnění této technické dokumentace je dodávka a implementace identity managementu pro město Klatovy, a to včetně nedílně souvisejících požadavků typu dodání licencí a zpracování dokumentace.
- 1.2.2 Předmětem díla jsou následující činnosti zhotovitele:
- Dodávka licencí, implementace identity managementu, testovací provoz a předání do řádného užívání.
- 1.2.3 Pro výše uvedený rozsah plnění:
- provedení integrací na další systémy v prostředí objednatele i mimo něj
 - úprava dodaného řešení dle potřeb a požadavků dle pokynů objednatele
- 1.2.4 Dále je předmětem plnění dodávka
- dokumentace k dodanému plnění v požadovaném rozsahu
 - dalších licencí potřebných pro provoz identity managementu
 - listinného potvrzení dodaných licencí co do jejich počtu a rozsahu

1.3 Seznam zkratk

AIFO	Agendový identifikátor fyzické osoby
Autentizace	proces ověření proklamované identity subjektu
Autorizace	proces získávání souhlasu s provedením nějaké operace nebo povolení přístupu
Citlivá data	osobní údaje a další data, která za citlivá považuje tato Technická dokumentace a její přílohy
DB	databáze
IDM	Identity management system
IS	Informační systém
MěÚ	Městský úřad
Nařízení eIDAS	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 a o zrušení směrnice 1999/93/ES
Nařízení GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Text s významem pro EHP)

2 Základní požadavky na IDM

- 2.1.1 Předmětem dodávky je nasazení sjednocujícího řešení pro správu identit, uživatelských rolí a oprávnění uživatelů, včetně jejich evidence, v prostředí MěÚ Klatovy (cca.200 uživatelů úřadu s možností rozšířit o další 200 externích).
- 2.1.2 IDM zajistí centrální a jednoduchou správu identity, uživatelských rolí a oprávnění uživatelů v aplikacích a informačních systémech, u kterých bude provedena integrace na takové IDM.
- 2.1.3 Cílem je zefektivnit a automatizovat proces řízení identit v organizaci a zavést centrální platformu pro řízení identit v organizaci – IDM (Identity Management Systém). IDM umožní automatizovaně spravovat identity (osoby, uživatelské role a oprávnění) ve vybraných hlavních systémech organizace, a to zejména v návaznosti na personální systém a adresářové služby. Cílem je rovněž zavést samoobslužné procesy pro zadávání žádostí o oprávnění a přístupů samostatnými koncovými uživateli organizace. V IDM bude následně možné takovéto požadavky schválit a změny nastavení u identit automatizovaně předat (vypublikovat) do připojených systémů (integrovaných aplikací).
- 2.1.4 Systém Identity management bude spravovat a řídit identity (uživatele, jejich uživatelské účty a oprávnění) v rámci připojených systémů. Pro unifikovanou správu identit v systémech organizace je nutné vybudování jednotné centrální evidence uživatelů, uživatelských účtů a oprávnění uživatelů k integrovaným aplikacím. Tato evidence je spravována centrálně v systému IDM.
- 2.1.5 Současně s nasazením IDM bude potřeba konsolidovat a standardizovat procesy související s personálními obměnami v organizaci (nový zaměstnanec, odchod zaměstnance, zařazení zaměstnance na pozici, změna pozice zaměstnance a další) v této souvislosti s vývojem jejich identity (zejména nabývání a ztráta oprávnění do vybraných aplikací a informačních systémů), případně procesy existující v IDM zohlednit. Na základě takových procesů ze zdrojových systémů (personální systém) vstupují do IDM údaje o osobách, uživatelských účtech, zařazení v organizační struktuře, přiřazení pracovního místa, přiřazení do skupin atd.
- 2.1.6 Součástí nasazení takového řešení bude i vytvoření systematizovaných pracovních míst, jim odpovídajícím uživatelským rolím a dále skupin takových míst/uživatelských rolí. IDM musí dále umožnit tvorbu a správu hierarchické struktury systematizovaných míst ve struktuře organizace objednatele.
- 2.1.7 IDM bude mít provedenou vazbu na Jednotný identitní prostor (JIP) a Katalog autentizačních a autorizačních služeb (KAAS) se kterými bude spolupracovat, a to do plného rozsahu těchto IS ve vztahu k povaze objednatele jako orgánu vykonávajícímu přenesenou i samostatnou působnost pro územní samosprávný celek.
- 2.1.8 Systém IDM bude reflektovat veškeré potřebné změny související s životním cyklem identity v prostředí objednatele a ve vazbě na všechny na IDM napojené informační systémy, ve kterých bude mít daná identita uživatelské role a oprávnění. Takové změny budou reflektovány ve všech aktuálně napojených informačních systémech vždy v konkrétní rozhodné době.

- 2.1.9 Ve vztahu k napojeným systémům musí IDM zajistit samostatnou a úplnou správu v oblasti identity a uživatelských rolí ve vztahu k těmto systémům, včetně skupin uživatelů a systematizovaných míst. Ze strany objednatele není rozhodné o kolik politik a konfiguračních operací se na straně informačních systémů jedná, ale je pro něj důležitý výsledek, tedy například správné nastavení uživatelských rolí, zařazení do skupiny a konfigurace oprávnění pro všechny funkcionality Microsoft Active Directory užívané v prostředí objednatele. IDM bude autoritativním zdrojem informací o identitách a jejich účtech a přidělených rolích. IDM bude provádět správu automaticky, tak aby byly spravované systémy vždy aktuální.
- 2.1.10 IDM bude dále realizováno při naplňování nových legislativních požadavků. V případě tohoto plnění zejména s dopady Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Minimálně zajistí auditní záznamy o prováděných změnách a poskytne reporty o stavu
- 2.1.11 IDM a jeho funkcionality musí respektovat standardní architekturu IS v prostředí objednatele a pro svou integraci využít standardizovaná rozhraní a existující prostředky IS.
- 2.1.12 Součástí plnění bude dále i návrh metodiky pro správu identit
- jmenné konvence uživatelských jmen a zajištění jejich unikátnosti (sjednocení loginů)
 - mechanismu práce s hesly (přidělení, změna, samoobslužný reset...)
 - postupy správy uživatelů (zavádění, změny, rušení, nastavování oprávnění...)
 - návrh členění objektů v rámci IDM (osoby, účty, funkce, org. jednotky, skupiny...)
 - definice bezpečnostních zásad a pravidel pro práci s IDM

2.2 Funkcionality IDM

- 2.2.1 IDM musí udržovat a spravovat kompletní životní cyklus identity. Tedy v typovém případě příchod zaměstnance, jeho založení, přidělení rolí v informačním systému dle jeho organizačního zařazení (systematizovaného místa), změna rolí v případě jeho povýšení nebo změny jeho zařazení, odchod zaměstnance spočívající v deaktivaci jeho identity. Na základě informací z personálních systémů nebo ručního zadání informací přes webové rozhraní. Minimálně se jedná o následující procesy:
- vznik nové identity
 - nový pracovněprávní vztah
 - úprava identity a pracovněprávního vztahu
 - úpravy popisných atributů, např. jméno
 - úpravy organizačního zařazení
 - změny platnosti
 - automatická změna rolí na základě změny stavu / typu identity, případně jiného příznaku identity
 - změna evidenčního stavu identity
 - ukončení pracovněprávního vztahu
 - aktivace/deaktivace (ruční, automatická)
- 2.2.2 IDM musí udržovat identity, skupiny identit a organizační struktury ve své vnitřní databázi. Identity ve vnitřní databázi budou sloužit jako referenční identity pro ostatní informační systémy.

- 2.2.3 IDM musí implementovat princip založený na systemizovaných místech. IDM musí umožnit systemizaci pracovních míst v souladu se strukturou organizace, definovat jednotlivá systematizovaná místa a jejich činnosti a sadu oprávnění a rolí pro jednotlivé informační systémy organizace vztahené ke konkrétnímu systemizovanému místu.
- 2.2.4 IDM umožní přiřazení identit na takto vytvořená systematizovaná místa a to i ve vazbě M:N. Identita tedy může být v systému IDM evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit.
- 2.2.5 IDM musí umožňovat přidělení oprávnění nebo role konkrétní identitě, systemizovanému místu, skupině nebo organizační jednotce.
- 2.2.6 IDM musí umožnit správu uživatelských rolí, včetně zařazení uživatele do odpovídající role.
- 2.2.7 V IDM je možné aplikační role nastavovat dočasně. Po uplynutí nastaveného intervalu se role automaticky odebere.
- 2.2.8 IDM umožní registraci aplikací a jejich rolí a dále také import rolí přes webové služby do IDM.
- 2.2.9 IDM musí umožnit nastavení schvalovacího workflow (při přidělení práva, role atd.), včetně emailových notifikací a potvrzování.
- 2.2.10 IDM musí umožnit definovat vztahy zastupitelnosti mezi uživateli – musí umožnit uživatelům, aby v souladu se strukturou úřadu mohli delegovat v případě potřeby (nemoc, dovolená atd.) svoje role, nebo jejich část na jiné pověřené osoby, a to i tak, že jeden uživatel může mít pro každou svou činnost nastaveného jako zástupce jiného různého uživatele. Delegation oprávnění bude dočasná, kdy se po nastaveném intervalu, nastavená delegace automaticky v IDM zruší.
- 2.2.11 IDM musí umožnit dodatečné přidávání vlastních atributů k identitám.
- 2.2.12 IDM musí umožňovat přesun identity v rámci organizační struktury i mezi jednotlivými organizačními strukturami.
- 2.2.13 IDM musí mít možnost detekovat situaci, kdy se ve zdrojovém systému vyskytne nový uživatel, který již dříve byl v IDM založen a přiřadit jej k existující identitě.
- 2.2.14 IDM musí umožňovat kopírovat role mezi jednotlivými systematizovanými místy.
- 2.2.15 IDM musí obsahovat funkcionalitu kopírování veškerého nastavení oprávnění jednoho uživatele na druhého.
- 2.2.16 Veškeré požadavky, které provedou uživatelé na IDM, musí být provedeny transakčně, musí být historizovány a logovány tak, aby bylo možné zpětně prokázat kdo, kdy a co změnil v IDM identitách, referenčních objektech, ale i v administraci. Záznam v historii musí obsahovat původní i novou hodnotu.
- 2.2.17 IDM umožní autonomní správu hesel (samoobsluha).
- 2.2.18 IDM bude komunikovat v českém jazyce.

2.3 Požadavky na kontrolní reporty

- 2.3.1 IDM musí umožňovat generování min. těchto kontrolních reportů:
- přehled uživatele (uživatelů) a jejich rolí v systémech spravovaných IDM v době generování reportu,
 - report historie delegování práv uživatele/uživatelů v definovaném časovém období.
- 2.3.2 IDM musí umožnit generování těchto reportů ve strojově čitelném formátu (např. v XML).

2.4 Požadavky na grafické rozhraní IDM

- 2.4.1 IDM musí obsahovat grafické uživatelské rozhraní pro přístup administrátorů systému pro správu identit uživatelů a jejich možné založení, úpravu nebo zneplatnění.

- 2.4.2 IDM musí obsahovat grafické uživatelské rozhraní sloužící jako obsluha pro uživatele, ve kterém uživatelé mohou měnit/resetovat heslo, žádat o přidělení rolí pro sebe nebo své podřízené, schvalovat nebo zamítnout žádost a provádět další činnosti, na které mají oprávnění.

2.5 Požadavky na webové služby

- 2.5.1 IDM musí poskytovat rozhraní webových služeb pro programové napojení dalších systémů města. Toto rozhraní bude dodáno včetně jeho dokumentace, která bude určena k přímému poskytnutí dalším dodavatelům v prostředí města za účelem napojení se na takové rozhraní. Webové služby budou dostupné jako SOAP nebo REST rozhraní. Součástí takové dokumentace bude proto i popis řešení webových služeb v podobě XSD. Rozhraní a jeho konfigurace musí být součástí plnění na takové úrovni, že napojení nového informačního systému bude možné pouze za zapojení pracovníka objednatele, který provede konfiguraci rozhraní na straně IDM a dodavatele nového IS, který provede konfiguraci dle dodané dokumentace na straně nového IS, tedy vše bude možné bez aktivního zapojení dodavatele IDM.
- 2.5.2 Základní konfigurace přístupu k webovým službám musí být dostupná z grafického rozhraní IDM.
- 2.5.3 Rozhraní IDM musí poskytovat minimálně následující služby:
- získání organizační struktury,
 - získání hierarchie systematizovaných míst,
 - získání seznamu identit,
 - získání nadřízené osoby pro daného zaměstnance,
 - získání seznamu rolí pro daného zaměstnance, včetně případné informací o delegaci role,
 - zápis seznamu rolí uživatele do IDM,
 - historie uživatele a jeho oprávnění k datu uvedeném v parametru.
- 2.5.4 IDM umožní vstupně/výstupní synchronizace do připojených informačních systémů. Typy synchronizací:
- plná
 - 1 identita (možnost prosynchronizovat pouze 1 identitu bez nutnosti použít plnou nebo změnovou synchronizaci)
 - změnová (pokud to napojený IS umožní)
- 2.5.5 Plná a změnová synchronizace musí umožňovat naplánované i ruční spuštění synchronizace, synchronizace 1 identity musí umožňovat pouze ruční spuštění. Dále musí existovat možnost (trvale nebo dočasně) vyřadit identitu ze synchronizace s daným IS
- 2.5.6 IDM umožní publikaci objektů (osob, účtů, skupin, funkcí, org. jednotek...) informačním systémům přes datové rozhraní (API IDM) na principu webových služeb (SOAP). Toto API IDM musí tedy mít čtecí metody a ideálně by mělo mít i zápisové metody (součást kvalitativního hodnocení). V rámci čtecích metod musí mít dané API IDM i autentizační metody, umožňující ověřit identitu (její login/heslo) i třetím aplikacím. IDM by mělo mít historii volání API IDM z důvodu auditu (součást kvalitativního hodnocení), včetně možnosti omezit dané API IDM pro jednotlivé aplikace (pouze vydefinované metody API IDM pro potřeby dané aplikace).

2.6 Logy IDM

- 2.6.1 IDM musí umožňovat publikovat kopie logů do externího systému určeného pro sběr logů např. syslog, DB apod.
- 2.6.2 Veškeré nové moduly IDM musí vést a umožňovat jednoduchý export anonymizovaných logů o počtu užití těchto jednotlivých modulů.

2.6.3 Tyto logy musejí být natolik přehledné a oprostěné od osobních dat aby umožnili jednoduchou kontrolu užívání těchto nových modulů ze strany i například kontrolních orgánů včetně oblasti kofinancování IROP.

2.7 Administrace

2.7.1 Po přihlášení do IDM bude administrátor IDM notifikován, že v systému došlo k některému z chybových stavů (např. synchronizovaný systém ve stavu chyba). Tato notifikace musí být zřetelná po přihlášení do systému a může být formou (barevného podbarvení části aplikace např. menu, pop-up okna oznamující, že je v IDM nějaký chybový stav, centrální dashboard aplikace apod.). Z notifikace musí být zřetelné, která část IDM je chybovém stavu.

2.7.2 IDM umožní definování různých úrovní oprávnění:

- možnost omezit oprávnění jenom na konkrétní organizační jednotky – uživateli to umožní spravovat identity pouze z daných organizačních jednotek např. vedoucí odboru spravuje oprávnění pro své podřízené (možnost omezit, zda může přiřazovat vybrané aplikační role, agendové role, skupiny, funkční místa, konkrétní uživatelské atributy apod.)
- možnost zadat oprávnění konkrétním uživatelům, skupinám, funkčním místům nebo organizačním jednotkám, aby mohli (pouze) spouštět vybraný synchronizační proces – např. personalistky si budou moci ručně pustit vstupní synchronizaci z personálního IS do IDM bez asistence administrátorů IDM.

2.7.3 IDM umožní nastavení prahových hodnot, které zabrání hromadným změnám např. z důvodu chybných dat na vstupu (např. z personálního systému), tak aby nedošlo k hromadným nežádoucím změnám (např. smazání objektů v Active Directory). Tato funkcionalita umožní při větším počtu změn zastavit frontu změn a upozornit administrátora IDM emailem a zapsat tuto informaci do logu IDM. Tato vlastnost je poplatná pro všechny vstupně/výstupní konektory.

2.7.4 IDM umožní notifikovat konfliktní stavy (např. synchronizovaný systém v chybě) v systému IDM pomocí emailu na administrátory IDM, případně na další osoby (včetně zápisu do logu IDM)

2.7.5 IDM umožní logování veškerých operací nad jednotlivými objekty (osoby, účty, funkce, synchronizované systémy, skupiny,...) i nad všemi spravovanými objekty a vlastní konfigurací.

2.7.6 IDM umožní sledovat jednotlivé stavy (počty objektů/identit) v průběhu synchronizace

2.7.7 IDM bude umožňovat databázovou historizaci (možnost dohledání změn v čase)

2.7.8 IDM umožní generování auditních reportů – přehled uživatelů a jejich aplikačních rolí, skupin definovaných v IDM včetně možnosti si zakázkově nechat vytvořit vlastní reporty.

2.7.9 Reporty lze vygenerovat i do CSV, aby šlo s případnými daty dále pracovat v programech typu MS Excel.

2.7.10 IDM umožní zobrazit kompletní popis napojených informačních systémů (vzájemných vazeb, typů synchronizací, ...) přímo u jednotlivých synchronizovaných IS z administrace IDM. Tyto popisy budou dodavatelem pravidelně udržovány a budou do nich zaznamenávané veškeré změny

3 Integrace IDM a migrace dat

3.1 Integrace IDM

3.1.1 V rámci implementace IDM do prostředí objednatele dojde k integraci na následující informační systémy způsobem, kdy IDM převezme správu veškerých identit a řízení veškerých uživatelských rolí v těchto informačních systémech za využití odpovídajících standardizovaných rozhraní těchto systémů:

- Microsoft Active Directory
- JIP/KAAS
- Emailový server IceWarp

3.1.2 Veškeré případné náklady spočívající v nezbytných úpravách informačních systémů uvedených výše a dodaných třetí stranou, které je potřeba provést za účelem integrace těchto systémů na nově dodané IDM ze strany dodavatelů těchto systémů ponese objednatel samostatně mimo plnění dodávky tohoto IDM.

3.2 Migrace dat

3.2.1 Pro úvodní naplnění dojde k převzetí konfigurací identity a uživatelských rolí ze současných informačních systémů, kdy dojde v rámci návrhu dokumentace skutečného provedení ke sjednocení těchto identit napříč pro napojené informační systémy v IDM a dále dojde k vytvoření dokumentace systematizovaných míst a organizační struktury identit a uživatelských rolí v organizaci objednatele, na jejímž základě bude provedena migrace a konfigurace nově dodaného řešení, která bude vycházet z již existujících konfigurací a dat.

4 Implementace IDM

4.1 Dokumentace skutečného provedení

4.1.1 Objednatel požaduje v rámci plnění zpracování tzv. dokumentace skutečného provedení (někdy také analogicky nazýváno jako cílový koncept nebo implementační analýza).

4.1.2 Zhotovitel zpracuje komplexní a detailní návrh nasazení IDM, a to ve vazbě na požadavky uvedené v této technické dokumentaci, jejích přílohách a smlouvě o dílo na dodávku IDM jako celek a na jeho hlavní funkcionality. Cílem je zpracování dokumentu v takové míře detailu jednotlivých postupů a prací zasazení do prostředí a jeho nastavení, která umožní dosažení zavedení IDM do rutinního provozu řízenou formou. Dokument proto bude jednoznačně a jasně konkretizovat jednotlivé kroky prací a to min. v rozsahu, které kroky a jakým způsobem budou řešeny, kým budou řešeny, za jaké součinnosti objednatele a v jakém čase. Taková konkretizace bude dále dodržovat časovou, věcnou a logickou souslednost a bude z ní tedy možné v každém okamžiku realizace díla určit co je právě realizováno a v jakém stavu a co bude následovat. Objednatel bude moci na základě takových podkladů alokovat své potřebné kapacity na součinnost a průběžnou kontrolu plnění díla. Dokument bude dále konkretizovat minimálně tyto oblasti

- návrh řešení instalace IDM (architektura technického řešení)
- detailní popis nastavení / konfigurace / parametrizace jednotlivých oblastí (společné registry, role a přístupová oprávnění, číselníky, reporty atd.)
- návrh technického řešení integračních vazeb (vazby mezi subsystémy, vazby s vybranými aplikacemi objednatele, vazby se spolupracujícími centrálními systémy)
- návrh řešení postupu a pořadí při nasazování jednotlivých oblastí – zohlednění v harmonogramu projektu

- popis případných organizačních opatření nutných pro implementaci (např. pracovní schůzky)
- upřesnění časového harmonogramu projektu
- rozsah součinnosti ze strany objednatele
- návrh průběhu testovacího provozu

4.1.3 Dokumentace skutečného provedení bude připomínkována objednatelem a připomínky budou ze strany zhotovitele vypořádány (tj. zapracovány, případně s jasným a konkrétním písemným zdůvodněním odmítnuty jako nevalidní). Ze strany objednatele nebude v rámci připomínkování v případě nepravdivých, nepřesných nebo věcně nejasných informací v této dokumentaci požadováno její opravování na správné znění, bude se pouze jednat o vyznačení výše uvedených nedokonalostí a bude na zhotoviteli jejich řádné zhojení.

4.2 Instalace IDM

4.2.1 Instalace IDM a jeho nastavení dle objednatelem odsouhlasené Dokumentace skutečného provedení bude provedena na hardware objednatele. Pro potřebu nasazení a provozu dodávaného řešení budou zhotoviteli poskytnuty systémové prostředky ze strany objednatele.

4.2.2 Veškeré softwarové komponenty a databáze poběží ve virtualizovaném prostředí objednatele. Licence virtualizace poskytne objednatel. Jedná se o jednotnou platformu virtualizace provozovanou objednatelem v jeho serverovém prostředí VMware. Dále objednatel poskytne pro provoz IDM licenci aktuální verze Windows serveru. V případě, že se zhotovitel rozhodne neužít nabízenou licenci operačního systému musí v rámci své dodávky dodat i odpovídající licence operačního systému, případně využít některou z nekomerčních distribucí OS Linux k provozu nad virtualizovanou platformou objednatele. Veškeré další potřebné licence software potřebného pro běh IDM musí v rámci své dodávky zajistit zhotovitel.

4.2.3 Pro provoz IDM budou v prostředí objednatele vyčleněny následující systémové prostředky, které budou pro provoz IDM alokovány po dobu min. 5 let. Zhotovitel v nabídce uvede, zda jsou pro něj tyto prostředky dostačující, či zda požaduje jejich navýšení. Zhotovitel musí garantovat, že takto stanovené prostředky budou po celou uvedenou dobu naprosto dostatečné, tedy, že za účelem optimálního běhu řešení IDM nebude minimálně po tuto dobu zhotovitel po objednateli požadovat navýšení takových systémových prostředků:

- 2 procesorová jádra,
- 12 GiB RAM,

4.2.4 Ze strany objednatele bude dále nasazeno zálohování na úrovni virtuálního stroje, ve kterém IDM poběží. Nastavení systémových záloh IDM bude součástí plnění zhotovitele, když objednatel umožní přístup na separátní úložiště pro odkládání takových záloh.

4.3 Konfigurace dodaného řešení pro potřeby objednatele

4.3.1 Konfigurace dodaného řešení dle zadání, požadavků a potřeb objednatele proběhne na základě odsouhlasené dokumentace skutečného provedení. Bude se jednat zejména o následující kroky a aktivity:

- provedení nastavení / konfigurace / parametrizace jednotlivých oblastí dle dokumentace skutečného provedení
- vytvoření reportů / výstupních sestav
- nastavení přístupových oprávnění do IDM pro administrátory

5 Dokumentace

5.1 Forma dokumentace

- 5.1.1 Objednatel požaduje dodávku dokumentace v rozsahu dle tohoto článku v elektronické podobě v českém jazyce, nejpozději do dne akceptace díla, není-li uvedeno nebo nevyplývá-li z jednotlivého typu dokumentace jinak.
- 5.1.2 Dokumentace musí být dodána v takové podobě a formátu, aby byla připravena bez potřeby jakýchkoliv dalších úprav k tisku.

5.2 Dokumentace skutečného provedení v prostředí objednatele

- 5.2.1 Bude sloužit jako podklad pro implementaci řešení do prostředí objednatele. Bude zpracována minimálně v rozsahu síťového schématu, datového schématu a aplikačního schématu včetně integrací, popis procesu nasazení informačního systému včetně zpřesněného harmonogramu, požadavků na součinnost ze strany zástupců objednatele. Bez předložení dokumentace skutečného provedení v prostředí objednatele nebude umožněno zhotoviteli instalovat a implementovat informační systém do určeného prostředí. Předložení dokumentace je povinností zhotovitele a v případě jejího nepředložení a z tohoto důvodu neumožnění implementace informačního systému do definovaného prostředí se bude jednat o prodlení na straně zhotovitele.
- 5.2.2 Na základě nasazení informačního systému bude dokumentace aktualizována na skutečně nasazené řešení a bude k ní zpracováno technologické schéma dodávaného řešení.

5.3 Uživatelská dokumentace

- 5.3.1 Zhotovitel dodá uživatelskou dokumentaci pro všechny aplikace a informační systémy, která bude obsahovat minimálně základní popis práce s jednotlivými aplikacemi/informačními systémy, postupy a bude popisovat jejich funkcionality pro potřebu řádné orientace uživatelů v systému/aplikaci a řádné práce uživatele v systému/aplikaci.

5.4 Administrátorská dokumentace

- 5.4.1 Zhotovitel dodá administrátorskou dokumentaci pro objednatele, která bude obsahovat detailní popis správy a údržby aplikací a informačních systémů na základě této smlouvy.

6 Harmonogram

6.1 Harmonogram s časovými požadavky objednatele

- 6.1.1 Objednatel požaduje realizaci předmětu plnění dle následujícího harmonogramu. Harmonogram je sestaven tak, aby jednotlivé práce na sebe logicky navazovaly a zároveň byl v souladu s požadavky výzvy číslo 28 IROP, ze které má být předmět plnění spolufinancován (s ohledem na termín dokončení předmětu plnění).
- 6.1.2 S ohledem na možnost kontroly realizace díla z pohledu času (tj. dílčí vyhodnocování dodržování harmonogramu realizace) je harmonogram doplněn milníky. Započetí každého milníku je možné pouze za předpokladu, že bude provedena akceptace všech milníků předcházejících.

Aktivita projektu	Termín nejpozději do:
Zpracování dokumentace skutečného provedení (cílový koncept), připomínkování ze strany objednatele, vypořádání připomínek, finalizace dokumentu	2 týdny
Milník číslo 1 – Předání dokumentace skutečného provedení	T + 2 týdny
Instalace systému	1 týden

Konfigurace dodaného řešení pro potřeby objednatele – nastavení / konfigurace / parametrizace jednotlivých oblastí, provedení integrací na spolupracující systémy, nastavení přístupových oprávnění Zpracování a dodávka dokumentace (uživatelská, administrátorská) Dodávka licencí (listinné potvrzení dodaných licencí co do jejich počtu a rozsahu)	2 týdny
Výzva zhotovitele objednateli k započetí akceptačního řízení pro Milník 1	1 týden
Akceptační řízení pro Milník 1	1 týden
Milník číslo 2 – Připravené prostředí pro testovací provoz	T + 7 týdnů
Výzva zhotovitele objednateli k započetí akceptačního řízení pro Milník 2	1 týden
Akceptační řízení pro Milník 2	1 týden
Milník číslo 3 – Předání do testovacího provozu	T + 9 týdnů
Testovací provoz s dohledem a podporou zhotovitele Oprava chyb a neshod, případná definice změnových požadavků Provedení doplňující migrace dat (počáteční stavy) Aktualizace dokumentace skutečného nasazení	1 týden
Akceptační řízení – porovnání skutečných vlastností se požadavky smlouvy	1 týden
Milník číslo 4 – Akceptace projektu, předání systému do rutinního provozu	T + 11 týdnů

Poznámka:

Ve sloupci „Termín nejpozději do:“ znak „T“ vyjadřuje datum uzavření smlouvy

6.2 Konkretizovaný harmonogram plnění ze strany zhotovitele

6.2.1 Zhotovitel blíže rozpracuje etapy a milníky minimálně v následující úrovni detailu (udávat v týdnech od uzavření smlouvy), které budou konkretizovat a dále rozpracovávat jednotlivé kroky a části harmonogramu stanoveného objednatelům:

- Zpracování specifických požadavků objednatele na konkrétní způsob nasazení IDM a zpracování implementačního plánu, tj. Dokumentace skutečného provedení a podrobného harmonogramu s uvedením potřebné součinnosti ze strany objednatele
- Implementace IS do prostředí objednatele
- Předání dokumentace a testovací provoz
- Akceptace, předání systému a následný pilotní a ostrý provoz

6.3 Testovací provoz

6.3.1 Testovací provoz proběhne po dobu uvedenou v harmonogramu realizace, a to se zvýšeným dohledem a podporou ze strany zhotovitele.

6.3.2 Cílem testovacího provozu je poskytnout metodické vedení a prostor uživatelům pro ověření funkcionalit a vlastní funkčnosti dodaného řešení, pro cvičnou práci se systémem a prostor pro zhotovitele pro identifikaci a opravu případných chyb a neshod. Dalším cílem testovacího provozu je možnost případné definice změnových požadavků ze strany objednatele.

6.3.3 V době testovacího provozu bude možné ze strany zhotovitele provedení případné nutné doplňující migrace dat (např. počáteční stavy) s ohledem na zahájení rutinního provozu.

6.3.4 Během testovacího provozu provede zhotovitel aktualizaci Dokumentace skutečného provedení.

- 6.3.5 Úspěšný průběh testovacího provozu, jehož výstupem bude faktické uživatelské ověření schopnosti nasazení nového IDM v prostředí objednatele na základě této technické dokumentace a jejich příloh, je jednou z nezbytných podmínek objednatele pro možnost akceptace plnění na základě této technické dokumentace a jejich příloh.

7 Projektové řízení

- 7.1.1 S ohledem na rozsah projektu a dopad jeho zavedení do produkčního provozu na výkon činnosti objednatele je v rámci dodávky předmětu plnění objednatelem požadováno aplikování základních principů projektového řízení ze strany zhotovitele.
- 7.1.2 Jedná se zejména řízení projektových prací v souladu s uzavřenou smlouvou s ohledem na věcné plnění dané smlouvou objednatele – rozsah, posloupnost a hloubku projektových prací, (tj. harmonogramu) – řízení postupu prací s ohledem na závazný harmonogram projektu – dodržování termínů a milníků harmonogramu, podchycení případných kolizí, zpoždění nebo vznikajících rizik a jejich reportování směrem k objednateli, aktivní řešení výše uvedených nestandardních situací
- 7.1.3 Zpracování pravdivých, úplných a věcně jasných a vypovídajících zápisů z konzultačních schůzek a pracovních jednání (s cílem zaznamenání klíčových rozhodnutí, ujednání, navržených nebo dohodnutých způsobů řešení dílčích částí projektu atd.)
- 7.1.4 Prezenční účast odpovědné osoby zhotovitele na kontrolních dnech v pravidelných min. měsíčních intervalech v sídle objednatele, případně se souhlasem obou smluvních stran formou videokonference nebo telekonference.
- 7.1.5 Reporting projektu na úrovni pravidelných dvoutýdenních písemných zpráv směrem k odpovědné osobě objednatele (seznam prací, které byly poskytovatelem vykonány pro danou část projektu, stav těchto prací (ukončeno, odloženo, v realizaci); popis vzniklých problémů a způsob jejich řešení).
- 7.1.6 Řízení rizik projektu, hodnocení pravděpodobnosti jejich výskytu a míry dopadu, návrh řešení k jejich eliminaci.
- 7.1.7 Řízení změn na projektu, v případě požadavků na změnu v projektu provedení konzultací k ověření nutnosti změny projektu; zjištění dopadu požadovaných změn směrem ke koncepci celkového řešení, harmonogramu, dotačnímu titulu, vytížení lidských zdrojů atd. V případě odsouhlasení změn spolupráce při implementaci změn do projektu, komunikace s poskytovateli a s realizačním týmem

8 Legislativa

- 8.1.1 Níže je obsažený obecný přehled legislativy, kterou je potřeba dodržet v souladu s realizací předmětu plnění této technické dokumentace. Tento výčet není konečný ani všeobjímající a má za cíl rámcově upozornit zhotovitele na rozsah problematiky, kterou se v návaznosti na jednotlivé požadované funkcionality zavazuje dodržet, a u níž se tedy zavazuje objednateli zajistit soulad s platnou legislativou. Dílčí legislativní požadavky a odkazy na právní akty jsou obsaženy i v dalších dílčích částech této dokumentace a jejich přílohách.
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů
 - Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů
 - Vyhláška NBÚ a Ministerstva vnitra ČR č. 317/2014 Sb., významných informačních systémech a jejich určujících kritérií, ve znění pozdějších předpisů

- Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů
- Zákon č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, v platném znění
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

9 Akceptace

9.1 Dílčí akceptační řízení

- 9.1.1 Dílčí akceptační řízení bude provedeno pro milník 1, 2 a 3 vyznačený v harmonogramu projektu dle této technické dokumentace. Dílčí akceptační řízení bude zahrnovat porovnání skutečného stavu vůči požadavkům této technické dokumentace a jejím přílohám (milník číslo 1, 2 a 3) a požadavků daných dokumentací skutečného provedení (milník 2 a 3).
- 9.1.2 Výsledkem dílčího akceptačního řízení je akceptační protokol s výsledkem Splněno nebo Nesplněno, podepsaný oprávněnými osobami smluvních stran.
- 9.1.3 Započítí dalších prací spadajících pod milník následující je možné pouze za předpokladu, že bude provedena akceptace s výsledkem Splněno všech milníků předcházejících.

9.2 Souhrnné akceptační řízení - akceptace díla

- 9.2.1 Souhrnné akceptační řízení bude zahrnovat:
- ověření splnění akceptace všech milníků, které akceptaci plnění předcházejí.
 - porovnání skutečného stavu vůči požadavkům smlouvy o dílo a této technické dokumentace, která je její přílohou, a jejích příloh, funkčního i nefunkčního charakteru – licence a příslušenství.
- 9.2.2 Výsledkem souhrnného akceptačního řízení je akceptační protokol s výsledkem Splněno / Splněno s výhradou / Nesplněno, podepsaný oprávněnými osobami smluvních stran. Klasifikace Splněno s výhradou umožní pokračování v realizaci díla v případě vad drobných, pro které může být opakování akceptačního řízení zbytečně nákladné.

9.3 Opakované akceptační řízení

- 9.3.1 Jestliže plnění nesplňuje podmínky stanovené pro akceptaci, bude obsahem akceptačního protokolu vyjádření Nesplněno spolu s popisem závad a uvedením termínů pro jejich nápravu. Zhotovitel napraví tyto nedostatky a akceptační řízení v odpovídajícím rozsahu bude provedeno znovu. Proces testování a následných oprav se bude opakovat, přičemž výše uvedená ustanovení se použijí obdobně. Proces testování a následných oprav lze opakovat, dokud zhotovitel nesplní požadavky pro akceptaci řádnou s výsledkem Splněno, nejvýše však 2× (dvakrát). V situaci, kdy by bylo nutné opakovat akceptační řízení více jak 2× (dvakrát) pro konkrétní milník projektu nebo celé plnění, bude takové opakování považováno za podstatné porušení smlouvy ze strany zhotovitele a objednatel bude oprávněn odstoupit od smlouvy o dílo. Prodlení vzniklé v souvislosti s potřebou opakování akceptačních řízení bude považováno vždy za prodlení vzniklé na straně zhotovitele se zachováním důsledků takového prodlení, tedy zejména smluvních pokut na základě uvažené smlouvy o dílo.