**Část I. – Identity Management**

Technická specifikace veřejné zakázky **Identity Management**

v rámci projektu **„Specifické informační a komunikační systémy a infrastruktura II. TC ORP Kutná Hora“**

(číslo projektu CZ.06.3.05/0.0/0.0/16\_044/0005060)

# Obsah

[1 Obsah 2](#_Toc493748345)

[2 Technická specifikace 3](#_Toc493748346)

[2.1 Požadavky na funkcionalitu řešení 3](#_Toc493748347)

[2.1.1 Požadavky na funkcionalitu řešení 3](#_Toc493748348)

[2.1.2 Požadavky na kontrolní reporty 5](#_Toc493748349)

[2.1.3 Požadavky na webové rozhraní 5](#_Toc493748350)

[2.1.4 Požadavky na webové služby 5](#_Toc493748351)

[2.2 Provedení integrační vazeb 5](#_Toc493748352)

[2.3 Požadavek na rozsah licenčních oprávnění 6](#_Toc493748353)

[2.4 Migrace dat 6](#_Toc493748354)

[2.5 Požadavky na implementaci 7](#_Toc493748355)

[2.6 Testovací provoz 7](#_Toc493748356)

[2.7 Záruka a podpora 7](#_Toc493748357)

# Technická specifikace

Předmětem plnění veřejné zakázky je zavedení systému Identity Management (IDM) do prostředí MěÚ Kutná Hora (a to včetně nedílně souvisejících požadavků typu provedení integračních prací, migrací dat, zaškolení, dodání licencí a zpracování dokumentace) a navazující technická podpora, jejíž podmínky jsou součástí samostatné smlouvy o Technické podpoře.

#### Zadavatel požaduje, aby dodavatelem nabízený systém splňoval veškeré níže uvedené minimální požadavky (funkcionality a parametry) a tyto byly zahrnuty v jeho nabídce a v celkové ceně.

#### Dodavatel jednoznačně deklaruje splnění, popřípadě absenci každého minimálního požadavku ve výše uvedených tabulkách, a to vyplněním příslušného pole Splněno jednou ze dvou nabízených možností:

* **ANO** - v případě, že dodávka dodavatele (Nabídka) minimální požadavek splňuje,

nebo

* **NE** - v případě, že dodávka dodavatele (Nabídka) minimální požadavek nesplňuje

Zadavatel požaduje uvést informaci o skutečné funkcionalitě nabízeného systému, kterou bude možné ověřit v nasazeném systému, a to již v testovacím provozu (testovacím prostředí, např. v rámci školení uživatelů).

Tabulky s vyplněním polí Splněno budou nedílnou součástí nabídky. V případě nevyplnění požadovaných údajů zadavatel vyloučí Dodavatele z účasti v zadávacím řízení.

#### V případě, že dodavatel v příslušné položce pole neoznačí nebo v položce budou označeny obě možnosti dle čl. 2., bude taková položka posuzována jako neoznačená a bude znamenat vyloučení dodavatele z důvodu nesplnění zadavatelem požadovaného minimálního plnění.

#### V případě, že dodavatel v příslušné položce pole označí NE, bude taková položka posuzována jako nesplnění minimálních požadavků zadavatele a bude znamenat vyloučení dodavatele z důvodu nesplnění zadavatelem požadovaného minimálního plnění.

#### Zadavatel si vyhrazuje právo ověřit splnění minimálních požadavků na funkcionality nabízeného systému přímou demonstrací příslušného produktu dodavatelem. V případě, že dodavatel nebude schopen splnění minimálních požadavků prokázat, bude vyloučen z důvodu nesplnění zadavatelem požadovaného minimálního plnění.

#### Dodavatel do sloupce „Popis jak“ výstižně doplní, jakým způsobem je požadovaná funkčnost splněna.

## Požadavky na funkcionalitu řešení

Pro jednotnou správu identit v napojených systémech vytvoří IDM centrální evidenci identit, uživatelů, rolí a oprávnění k integrovaným aplikacím. IDM umožní jednoduše a přehledně spravovat aplikace a aplikační role uživatelů v organizaci. Aplikační role bude možné přiřazovat na systemizovaná místa, IDM bude mít zavedenu vazbu na Jednotný identitní prostor (JIP) a Katalog autentizačních a autorizačních služeb (KAAS).

### Požadavky na funkcionalitu řešení

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Minimální požadavky** | **Splněno** | **Popis jak** |
| 1. | IDM musí udržovat a spravovat kompletní životní cyklus identity |  |  |
| 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. |  |  |
| 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 vztažené ke konkrétnímu systemizovanému místu. |  |  |
| 4. | IDM umožní přiřazení identit na takto vytvořená systematizovaná místa a to ve vazbě 1:N. Identita tedy může být v systému IDM evidována na více systematizovaných místech. Dále však na systematizovaném místě může být delegována další identita ve vztahu zastupitelnosti. |  |  |
| 5. | IDM musí umožňovat přidělení oprávnění nebo role konkrétní identitě, systemizovanému místu. |  |  |
| 6. | IDM musí umožnit správu uživatelských rolí, včetně zařazení uživatele do odpovídající role. |  |  |
| 7. | V IDM je možné aplikační role nastavovat dočasně. Po uplynutí nastaveného intervalu se role automaticky odebere. |  |  |
| 8. | IDM umožní registraci aplikací a jejich rolí. |  |  |
| 9. | 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. Delegace oprávnění bude dočasná, kdy se po nastaveném intervalu, nastavená delegace automaticky v IDM zruší. |  |  |
| 10. | IDM musí umožnit dodatečné přidávání vlastních atributů k identitám. |  |  |
| 11. | IDM musí umožňovat přesun identity v rámci organizační struktury i mezi jednotlivými organizačními strukturami. |  |  |
| 12. | IDM musí mít možnost detekovat situaci, kdy se ve zdrojovém systému vyskytne jako nový uživatel, který již dříve byl v IDM založen a přiřadit jej k existující identitě |  |  |
| 13. | IDM musí umožňovat kopírovat role mezi jednotlivými systematizovanými místy. |  |  |
| 14. | IDM musí obsahovat funkcionalitu kopírování veškerého nastavení oprávnění jedné identity na druhou. |  |  |
| 15. | 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. |  |  |
| 16. | IDM bude umožňovat přidělování agendových činnostních rolí z ISZR jak systematizovanému místu tak identitě. |  |  |
| 17. | IDM bude komunikovat v českém jazyce. |  |  |

### Požadavky na kontrolní reporty

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Minimální požadavky** | **Splněno** | **Popis jak** |
| 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 |  |  |

### Požadavky na webové rozhraní

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Minimální požadavky** | **Splněno** | **Popis jak** |
| 1. | IDM musí obsahovat webové rozhraní pro přístup administrátorů systému pro správu identit uživatelů a jejich možné založení, úpravu nebo zneplatnění. |  |  |

### Požadavky na webové služby

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Minimální požadavky** | **Splněno** | **Popis jak** |
| 1. | IDM musí poskytovat rozhraní webových služeb pro programové napojení dalších systémů města Kutná Hora na IDM |  |  |
| 2. | základní konfigurace přístupu k webovým službám musí být dostupná z webového rozhraní IDM |  |  |
| 3. | rozhraní 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 informaci o delegaci role, * zápis seznamu rolí uživatele do IDM |  |  |
| 4. | historie uživatele a jeho oprávnění k datu uvedeném v parametru |  |  |

## Provedení integrační vazeb

Za účelem efektivního využití komponenty IDM v organizaci bude v rámci předmětu plnění provedeno napojení na tyto systémy:

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Minimální požadavky** | **Splněno** | **Popis jak** |
| 1. | správní agendy (VITA, GEOVAP) |  |  |
| 2. | lokální registry – evidence obyvatel (GEOVAP) |  |  |
| 3. | elektronická spisová služba (GEOVAP) |  |  |
| 4. | Active Directory |  |  |
| 5. | Jednotný identitní prostor (JIP) / Katalog autentizačních a autorizačních služeb (KAAS). |  |  |
| 6. | Informační systém základních registrů (ISZR) |  |  |
| 7. | Databáze Microsoft SQL Server |  |  |

V rámci předmětu plnění veřejné zakázky není vznesen požadavek na integraci IDM na personální systém.

## Požadavek na rozsah licenčních oprávnění

Zadavatel požaduje licencování nabízeného softwarového řešení formou trvalé licence bez omezení na počet spravovaných identit, počet připojených informačních systémů a počet přistupujících uživatelů.

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Minimální požadavky** | **Splněno** | **Popis jak** |
| 1. | Zadavatel požaduje licencování nabízeného softwarového řešení formou trvalé licence bez omezení na počet spravovaných identit, počet připojených informačních systémů a počet přistupujících uživatelů. |  |  |

## Migrace dat

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Minimální požadavky** | **Splněno** | **Popis jak** |
| 1. | úvodní migrace dat z AD |  |  |
| 2. | úvodní migrace současného nastavení oprávnění do jednotlivých systémů uvedených v kapitole *2.2* *Provedení integrační vazeb* |  |  |

## Požadavky na implementaci

Zadavatel požaduje v rámci plnění realizaci následujících dodávek a služeb:

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Minimální požadavky** | **Splněno** | **Popis jak** |
| 1. | instalace do prostředí žadatele (řešení bude v rámci realizace nasazeno do clusterové architektury organizace do virtualizovaného prostředí, které umožní pružnou změnu přidělených systémových prostředků, stejně jako dostatečné zálohování a případnou bezvýpadkovou migraci v rámci virtualizovaných strojů.) |  |  |
| 2. | provedení integračních vazeb, migrace dat, konfigurace IDM, nastavení oprávnění do integrovaných systémů |  |  |
| 3. | zpracování a předání dokumentace skutečného provedení v prostředí žadatele |  |  |
| 4. | dodávka požadovaných SW licencí |  |  |
| 5. | zaškolení administrátorů na dodané řešení IDM v rozsahu do 8 hodin |  |  |

## Testovací provoz

Testovací provoz proběhne po dobu 2 týdnů, a to po provedení implementace. Zadavatel požaduje, aby v rámci testovacího provozu zajistil Dodavatel odborný dohled a podporu IT administrátorů Zadavatele a to formou (A) telefonické dostupnosti nebo (B) fyzické přítomnosti v místě plnění.

Cílem testovacího provozu je poskytnout metodické vedení a prostor administrátorům ze strany města pro ověření funkcionalit a vlastní funkčnosti dodaného řešení, pro cvičnou práci s IDM a prostor pro Dodavatele pro identifikaci a opravu případných chyb a neshod. Dalším cílem testovacího provozu je možnost případné definice změnových požadavků ze strany Zadavatele. Během testovacího provozu provede Dodavatel aktualizaci dokumentace skutečného provedení v prostředí žadatele.

Testovací provoz bude ukončen formální předáním implementovaného IDM systému do rutinního a podpisem Akceptačního protokolu.

## Záruka a podpora

IDM je požadováno se zárukou v délce trvání 2 let v místě jeho dodání. Po celou záruční dobu Dodavatel garantuje Zadavateli 24 hodin denně 7 dní v týdnu přijmout od něj nahlášení poruchy a do 72 hodin garantuje realizaci opravy technikem v místě poruchy.