Příloha č. 1 – Specifikace předmětu plnění

Název zakázky: Pořízení a implementace systému pro správu digitálních identit (IDM)
Číslo zakázky: P19V00000085
Zadavatel: Statutární město Frýdek-Místek, se sídlem Frýdek-Místek, Radniční 1148, PSČ 738 01

1. Cena dodávky

		ks	Jednotková cena bez DPH	DPH	Jednotková cena včetně DPH
I.	**IDM systém**	1	1837000	385770	2222770
II.	**Roční technická podpora (bod 2.i)**	1	331000	69510	400510
III.	**Technická podpora (dle bodu 2.j)**	1 hod.	2000	420	2420
IV.			**2170000**	**455700**	**2625700**

2. Technická specifikace předmětu plnění veřejné zakázky

Předmětem plnění veřejné zakázky je dodávka a implementace systému pro správu digitálních identit (dále jen identit), tzv. Identity management systém (dále jen IDM), který bude udržovat a spravovat identity (uživatele, uživatelské účty, oprávnění) a organizační strukturu Magistrátu města Frýdku-Místku a Městské policie Frýdek-Místek. Software musí být určen pro český trh a musí být kompletně v českém jazyce. Veřejná zakázka zahrnuje dodávku software a licencí, předprojektovou analýzu v místě plnění, instalaci a konfiguraci software včetně napojení systémů, dodání technické, administrátorské a uživatelské dokumentace, zkušební provoz, školení administrátorů, vedoucích pracovníků a uživatelů.

a) Požadavky na dodavatele

Zadavatel požaduje projektové vedení po celou dobu realizace zakázky certifikovanými specialisty.

b) Popis prostředí zadavatele

Stávající infrastruktura zadavatele obsahuje virtualizační prostředí, které je provozováno v režimu vysoké dostupnosti na platformě VMware vSphere 6.0 (do konce roku 2019 proběhne upgrade na vSphere 6.7). Virtualizační platforma je centrálně spravována přes vCenter 6.0 (do konce roku 2019 proběhne upgrade na vCenter 6.7). Součásti IT infrastruktury je centrální diskové pole s dostatečnou kapacitou. Datová struktura pro komunikaci mezi servery a diskovým polem je vybudovaná na technologii fiber channel s využitím SAN switchů a redundantních cest pro případ výpadku. Zadavatel disponuje licencí OS Windows Server 2016 Datacentrum. V případě distribucí Linux, musí být součástí dodávky licence pro OS pokud je vyžadována a OS musí být uveden na compatibility listu VMware (verzí 6.0, 6.7 a vyšší).

Zadavatel disponuje pracovními stanicemi uživatelů s OS Windows 7, 8.1 a 10 (32b/64b), kancelářským balíkem Office 2010, 2013, 2016 a 2019 a prohlížečem MS Internet Explorer (poslední dostupná verze), Firefox nebo Chrome v poslední dostupné verzi.

Zadavatel dále disponuje databází Oracle 12.2.0.1. s dostatečným výkonem. V případě, že je součástí dodávky provoz IDM na jiném databázovém systému, musí uchazeč zajistit dodávku a instalaci všech licencí potřebných pro provoz a pro cca 450 interních uživatelů a neomezený počet externích uživatelů (připojených z internetu). Dále uchazeč musí zajistit licenci databázového systému s neomezenou velikostí dodané databáze a servisní podporu databáze na 5 let.

c) Technické parametry

Obecné požadavky

- IDM systém bude udržovat a spravovat identity (uživatele, uživatelské účty, oprávnění) a organizační strukturu Magistrátu města Frýdku- Místku a Městské policie Frýdek-Místek
- spravované identity budou referenčními identitami pro interní i externí informační systémy
- pro správu identit musí být vytvořena jednotná centrální evidence uživatelů, uživatelských účtů a oprávnění k integrovaným i neintegrovaným informačním systémům
- identity a organizační struktura musí být ukládány a udržovány ve vnitřní databázi IDM
- IDM musí být uchazečem dodán jako jeden funkční celek
- s IDM systémem musí být dodány veškeré potřebné licence pro provoz v infrastruktuře zadavatele (možno využít stávající licence zadavatele, pokud jimi již disponuje viz. bod 2.b)
- IDM a dodané licence musí být trvalé a umožnit udržovat a spravovat neomezený počet uživatelů, identit, napojených i nenapojených systémů
- předpokládaný počet uživatelů zadavatele je cca 500
- dodané licence nesmí zadavatele omezovat v obvyklém provozu a nasazení (počet záznamů v databázi, velikost databáze atd.)
- IDM musí umožnit zvyšování výkonu rozložením na více serverů, a to minimálně oddělením rolí serverů (aplikační, databázový)
- IDM musí umožnit nasazení v režimu vysoké dostupnosti
- IDM musí obsahovat integrovaný registr informačních systémů a aplikací (dále jen IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby
- IDM musí obsahovat integrovanou správu uživatelských rolí, včetně zařazení uživatelů do odpovídající role v příslušných IS
- IDM musí obsahovat správu více organizačních struktur
- IDM musí umožnit přiřazení jedné identity do několika organizačních struktur najednou
- IDM musí umožnit spravovat organizační strukturu obsahující interní i externí identity jako samostatné větve struktury
- IDM musí umožnit dodatečné přidávání vlastních atributů k identitám a referenčním objektům (organizační jednotka, aplikační role, systematizované místo atd.), vyplňování jejich obsahu ze zdrojových systémů a jejich následnou publikaci přes rozhraní webových služeb

- IDM musí umožnit správu uživatelských rolí a zařazení uživatelů do odpovídajících rolí v daných IS
- IDM musí obsahovat modul pro registraci IS a aplikací a jejich rolí včetně importu rolí přes webové služby
- IDM musí umožňovat v intuitivním, přehledném grafickém rozhraní tvořit pravidla pro automatické vytváření uživatelských účtů, přiřazování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo atd.)
- IDM musí obsahovat princip systematizovaných míst na základě pracovních míst v souladu se strukturou organizace
- IDM musí umožnit spravovat jednotlivá systematizovaná místa a sadu oprávnění a rolí pro jednotlivé IS organizace vztažené ke konkrétnímu systematizovanému místu
- IDM musí umožnit grafické zobrazení identit ve stromové organizační struktuře. Součástí jednoho pohledu musí být zobrazení organizační struktury včetně systematizovaných míst až do úrovně jednotlivých uživatelských účtů. Musí být možno vyhledávat jednotlivé identity, systematizovaná místa, skupiny
- IDM musí obsahovat přehled uživatelů aktuálně pracujících s IDM systémem
- IDM musí být možno užívat a spravovat přes webovou konzoli přístupnou přes prohlížeče Internet Explorer 11 a vyšší, Google Chrome v poslední verzi, Mozilla Firefox v poslední verzi
- webová konzole bude hlavním rozhraním pro uživatele i administrátory pro přístup k datům, funkcím a administraci včetně integračních úloh IDM
- webová konzole bude přístupná výhradně přes https protokol
- webová konzole musí být implementována s responzivním designem
- IDM musí obsahovat autentizační rozhraní, které umožní systémům zprostředkovat autentizační úlohy min. přes následující standardy a protokoly:
    - LDAP (Active Directory)
    - Windows autentizace
    - Radius
    - pomocí certifikátu
    - OpenID
    - Oauth 2.0
    - SAML 2.0 s tím, že IDM musí umožnit plnit roli identity providera a současně roli service providera

- správa IDM musí obsahovat přehlednou správu samostatných identifikovatelných objektů - referenčních objektů, na které se identity mohou odkazovat: min. systematizované místo, organizační jednotka, skupina, agenda, agendová činnostní role, aplikace, skupina aplikací, aplikační role, certifikát v grafickém uživatelském rozhraní
- IDM musí umožnit přidávání a správu dalších typů referenčních objektů v grafickém uživatelském rozhraní
- IDM musí umožnit nastavit samostatné nezávislé administrátorské oprávnění pro správu jednotlivých referenčních objektů
- IDM musí umožnit vyhledávání i bez diakritiky
- IDM systém musí mít kompletní podporu českého jazyka
- IDM musí obsahovat 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 a o zrušení směrnice 1999/93/ES
- IDM musí obsahovat správu uživatelů (identit) a správu uživatelských digitálních certifikátů. Data o certifikátech musí být možno do IDM nahrávat přes webové služby. IDM musí obsahovat nastavení umožňující automatické zneplatnění certifikátů po uplynutí data platnosti.
- IDM musí umožnit přesun identit mezi jednotlivými organizačními jednotkami nebo jejími odděleními
- IDM musí umožnit kopírování aplikačních rolí, agendových činnostních rolí mezi jednotlivými systematizovanými místy
- IDM musí umožnit propojení více účtů v různých IS k jedné identitě
- IDM musí obsahovat mechanismus zabraňující hromadným změnám z důvodu případných chybných vstupních dat ze zdrojových systémů (nesmí dojít k hromadným nežádoucím změnám)
- IDM musí obsahovat editor filtrů pro vyhledávání identit a referenčních objektů. Filtrovat musí být možno dle libovolných atributů identit, včetně přidružených referenčních objektů. Filtry musí být možné ukládat za účelem znovupoužití
- IDM musí umožnit export zobrazených seznamů do CSV
- IDM musí obsahovat editor oprávnění, kde bude administrátor definovat různé úrovně oprávnění do IDM systému a tato oprávnění následně přiřazovat uživatelům. Tato oprávnění musí být definovatelná pro jednotlivé entity a moduly IDM systému (identity, referenční objekty, konfigurace notifikací, konfigurace synchronizací, workflow, správa webových služeb atd.). U jednotlivých konkrétních částí systému bude možnost definovat akce, které může uživatel s přidělenými oprávněními dělat.
- IDM musí umožnit identitám a referenčním objektům definovat konkrétní atributy včetně zobrazení daného atributu, možnost editace atributu uživatelem, povinnost atributu a pořadí atributu při zobrazení

- IDM musí obsahovat víceúrovňovou správu administrátorských oprávnění s možností nastavení oprávnění min. na úrovní organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, aplikační role, editace entity atd.)

- IDM musí umožnit zobrazení uživatelské karty, která musí obsahovat osobní údaje uživatele (jméno, příjemní, tituly, osobní číslo, funkční zařazení atd.), aktuální nastavení oprávnění k jednotlivým napojeným i nenapojeným systémům. U napojených IS musí být zobrazena informace, kdo a kdy o daná oprávnění žádal a kdo a kdy žádaná oprávnění povolil a schválil. Uživatelská karta musí být přehledná a exportovatelná do souboru ve formátu PDF.

- IDM musí obsahovat přiřazování rolí konkrétní identitě, systematizovanému místu, skupině a organizační jednotce včetně data a času konce platnosti přiřazení. Po vypršení data a času platnosti přiřazení bude role systémem IDM automaticky odebrána

- IDM musí umožnit spravovat licence pro jednotlivé napojené IS a přiřazovat je jednotlivým uživatelů (identitám). Pro schvalování přiřazování licencí bude IDM systém obsahovat workflow platformu s možností automatického přiřazování nebo vytváření víceúrovňových schvalovacích workflow

- IDM musí umožnit zobrazení přidělených rolí k jednotlivým identitám s rozdělením role navázané na systematizované místo, identitu, organizační jednotku, skupinu. U identity musí IDM systém evidovat souhrnné zobrazení seznamu všech rolí včetně informace o tom, odkud uživatele roli zdědil (skupina, organizační jednotka atd.)

- IDM musí umožňovat přiřadit identitu k systematizovaným místům ve vazbě M:N

- IDM musí umožnit správu skupin s možností začleňování více skupin do sebe, přiřazovat jednotlivé uživatele do skupin, přiřazovat systematizovaná místa do skupin

- IDM musí obsahovat správu vztahů zastupitelnosti mezi jednotlivými uživateli. IDM musí uživatelům umožnit ve vztahu k organizační struktuře delegovat v případě potřeby svoje role v IDM systému (nemoc, dovolená atd.) s tím, že různé části role mohou být delegovány na různé uživatele

- IDM musí umožnit delegování administrátorských práv

- IDM musí obsahovat rozhraní pro uživatele dostupné přes webové rozhraní, kde uživatel bude moct změnit samoobslužně heslo a požádat o přidělení jednotlivých aplikačních rolí a členství ve skupinách. Role a skupiny budou kategorizovány podle toho, jestli požadavek podléhá nějakému schvalovacímu workflow nebo zda dojde k přiřazení automaticky. Veškeré žádosti a jejich stav musí být evidovány v historii a musí být v IDM systému dohledatelné

- IDM musí obsahovat v rámci uživatelského rozhraní konfigurovatelné registrační formuláře pro registraci externích organizací, identit, žádostí o konkrétní aplikační role a skupiny. Seznamy rolí a skupin, o které mohou uživatele žádat, musí být v IDM systému možno specifikovat samostatně pro dané organizace a organizační jednotky

- IDM musí uživatelům umožnit individuální nastavení vlastního rozhraní (zobrazení/skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku pro všechny seznamy samostatně atd.)

- IDM musí umožnit správu osobních údajů, čili musí obsahovat správu evidence subjektů údajů a evidenci jejich osobních údajů včetně klasifikací a kategorií
- IDM musí obsahovat evidenci účelů pro nakládání s osobními údaji subjektu údajů
- IDM musí obsahovat workflow pro správu životního cyklu osobních údajů subjektu údajů

Požadavky na synchronizaci

- IDM musí umožnit synchronizaci s napojenými systémy spouštět automatizovaně, ručně a v simulačním režimu
- IDM musí umožnit zobrazení jednotlivých stavů průběhu synchronizace v přehledné grafické podobě
- v rámci napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM, musí IDM umožnit u každého systému následující režimy synchronizací (za předpokladu podpory na straně napojovaného systému):
    - Plná synchronizace - prochází všechny objekty v IDM a synchronizuje je s objekty daného systému
    - Změnová synchronizace - synchronizuje vždy jen změny od poslední spuštěné synchronizace
    - Okamžitá synchronizace - synchronizace vždy jen konkrétní identity na vyžádání, která se provede okamžitě
    - Ověřovací synchronizace - synchronizace vytvoří report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IDM vs. nastavení identit a oprávnění přímo v připojeném systému
    - Simulační synchronizace - synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace, report změn bude evidován jako pohled nebo přehledná souhrnná tabulka v IDM systému
- IDM musí obsahovat historii běhu všech synchronizací - jednotlivé běhy synchronizací musí být zaznamenány v historii dostupné v IDM systému. U plné synchronizace musí historie obsahovat odkazy na objekty v IDM, které byly synchronizované včetně logu, co bylo u těchto objektů synchronizací změněno. V případě změnové synchronizace musí být navíc v historii informace o události, která synchronizaci vyvolala
- IDM musí obsahovat správu jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možno zpracovat, nastavení časového intervalu spouštění a nastavení intervalu odstávky

Požadavky na workflow

- IDM musí podporovat kompletně elektronický schvalovací proces pro udělování přístupových oprávnění uživatelům a jejich následnou evidenci. Schvalovací workflow musí být založeno na funkcích elektronických formulářů s tím, že zadavatel preferuje podepisování s využitím kvalifikovaných el. podpisů.

- IDM musí obsahovat integrované workflow pro řízení životního cyklu změn identit a schvalování změn s min. následujícími funkcemi:
    - zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným, jak pro dotčeného uživatele, tak i pro podřízené pracovníky
    - sledování stavu vyřizování požadavků
    - možnost schválení i zamítnutí požadavků včetně možnosti uvedení odůvodnění formou komentáře u obou variant
    - odesílání schvalovateli upozornění formou emailové notifikace
    - schvalovatelé si mohou zobrazit přehled úloh čekajících na schválení
    - vícekrokové schvalovací workflow na základě podmínek
    - schvalovat může jednotlivec nebo více schvalovatelů (skupina schvalovatelů, která musí být definovatelná)
    - správce IDM je schopen pracovat se všemi úlohami workflow
    - řešení zastupitelnosti
    - upozornění schvalovatele při překročení termínu provedení schválení/zamítnutí
    - IDM musí být schopno zobrazit v grafické podobě workflow diagram včetně indikace stavu aktuálně běžícího workflow

Požadavky na historii, logování, audity a reporty

- IDM musí obsahovat detailní databázovou historizaci min. pro evidenci změn v identitách, referenčních objektech a jejich vzájemných vazbách
- IDM musí u historizace poskytovat data v libovolném časovém okamžiku (aktuální i zpětně v minulosti)
- IDM musí poskytovat auditní logy pro systémy typu SIEM a Log management
- IDM musí obsahovat min. následující typy logů:
    - aplikační log zaznamenávající události systému
    - auditní log zaznamenávající změny entit evidovaných v systému a změny konfigurace systému
    - synchronizační log zaznamenávající průběh synchronizací IDM s dalšími systémy
    - notifikační log zaznamenávající odeslané emailové notifikace a upozornění
- IDM musí obsahovat možnost exportu auditních reportů z údajů o identitě uložené v IDM systému včetně historických. Tyto reporty musí být min. ve formátech XML a CSV. Reporty musí obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM,

agendových rolí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti

- IDM musí všechny požadavky na změny, které provedou uživatelé provádět transakčně
- IDM musí logovat tak, aby bylo možno prokázat zpětně kdo a co v systému změnil v referenčních objektech, identitách, v administraci a konfiguraci
- IDM musí u identit pro generování auditního reportu umožnit filtrovat dle libovolných atributů identity včetně přidružených referenčních objektů
- IDM musí umožnit generovat report pro proces ohlašování působnosti v Registru práv a povinností. Report musí obsahovat počty úředníků agendových rolí a původní počet vzhledem k vybranému dříve vygenerovanému reportu. Report musí být exportovatelný ve formátu CSV
- IDM musí umožnit generovat reporty uživatelů přiřazených aplikačním rolím
- IDM musí umožnit automatizovaně zasílat reporty e-mailem na základě konfigurovatelných pravidel
- IDM musí umožnit automatické ukládání reportů v systému IDM pro možnost pozdějšího zobrazení nebo stažení
- IDM musí umožnit porovnání změn mezi vygenerovanými reporty stejného typu
- IDM musí veškeré požadavky na změny v IDM umožnit zadávat výhradně přes webové rozhraní, tak aby bylo zajištěno úplné logování všech změn jednotlivých parametrů. Není přípustné požadavky realizovat ručními úpravami textových souborů jakou jsou např. CSV, XML atd.

Požadavky na notifikace

- IDM musí umožnit notifikovat e-mailem o vytvoření a změně identity
- IDM musí umožnit notifikovat e-mailem o vytvoření a změně referenčních objektů jako jsou systematizované místo, organizační jednotka, agenda, skupina, agendová činnostní role, aplikace, skupina aplikací, aplikační role, dále o vypršení hesla v Active Directory a vypršení platnosti certifikátu (u vypršení musí být možnost definovat s jakým časovým předstihem bude notifikace zaslána)
- IDM musí umožnit notifikovat e-mailem o problémech či konfliktech při jednotlivých synchronizacích s napojenými systémy
- IDM musí umožnit správu notifikací včetně náhledu
- IDM musí umožnit v šabloně notifikací definovat příjemce, předmět a obsah upozornění. U notifikací vázaných k identitám musí IDM umožnit nastavit různé příjemce pro různé části organizační struktury

Požadavky na integraci IDM s jinými systémy

V případě, že u níže definovaných integrovaných systémů integrace vyžadují další licence na straně definovaných dodavatelů, musí být tyto náklady zahrnuty do nabídky uchazeče, a to včetně případné ceny za maintenance a technickou podporu

- Rozhraní webových služeb
    - IDM musí poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace přes webové rozhraní IDM
    - IDM musí umožnit řízení uživatelských účtů a rolí v jiných systémech na principu obecné webové služby (tzn. bude možné konfigurovat konektory pro tyto webové služby pro jakýkoliv jiný - podřízený - systém)
    - webové služby IDM musí být definované v rozšířeném standardu WSDL a podporovat protokol SOAP
    - konfigurace webových služeb musí umožnit konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet zvlášť
    - IDM musí volání webových služeb logovat a logy musí být zobrazitelné přímo ve webovém rozhraní IDM
    - rozhraní webových služeb musí poskytovat min. následující služby:
        - získání organizační struktury
        - získání hierarchie systematizovaných míst
        - získání seznamu identit
        - získání nadřízené osoby pro daného zaměstnance
        - získání seznamu aplikačních rolí
        - získání seznamu uživatelů dané aplikace
        - získání seznamu agend a agendových rolí přiřazených dané aplikaci
        - zápis seznamu aplikačních rolí do IDM
        - zápis certifikátů do IDM
        - zápis a změna identit
        - služba pro autorizaci pro ISZR - služba ověří validnost volání služby ISZR. Služba v IDM musí ověřovat:
            - zda je evidován uživatel v IDM, který je v požadavku na ISZR
            - zda je evidovaná aplikace v IDM, která je v požadavku na ISZR
            - zda má tento uživatel v IDM nastaven přístup do aplikace, která je v požadavku na ISZR
            - zda existuje v IDM v rámci evidence organizační struktury rovněž evidence pro dané OVM, které je uvedeno v požadavku na ISZR

- zda má aplikace, která je v požadavku na ISZR, v IDM povolenou agendovou činnostní roli a agendu, které jsou rovněž uvedeny v požadavku na ISZR

- Obecné konektory
    - IDM musí obsahovat min. tyto obecné konektory pro správu identit v napojených systémech a musí být možno je konfigurovat přímo z webového rozhraní IDM:
        - konektor pro spouštění CMD příkazů
        - konektor umožňující pracovat s CSV soubory
        - konektor umožňující správu identit v DB
        - konektor umožňující napojení na SOAP webové služby
        - konektor umožňující napojení na REST webové služby
        - konektor umožňující napojení na LDAPv3 (např. Active Directory)
    - IDM musí umožnit připojení libovolného množství dalších spravovaných systémů, a to bez dalších licenčních nákladů
- Napojení na Active Directory
    - IDM musí obsahovat min. tyto funkcionality:
        - komplexní správu účtů, certifikátů a skupin (založení, změnu atributů, zrušení, změnu hesla atd.)
        - podpora min. 6 vrstvé hierarchické struktury organizačních jednotek
        - založení domovského adresáře včetně nastavení oprávnění
        - správu účtů a jejich certifikátů včetně inicializačního načtení
        - správu skupin a členství ve skupinách včetně inicializačního načtení
        - správu organizačních jednotek včetně inicializačního načtení
- Napojení na Microsoft Exchange
    - IDM musí obsahovat min. tyto funkcionality:
        - správa emailových schránek na serveru Exchange 2016 (vytvoření, zrušení, zneplatnění)
        - řízení životního cyklu emailových schránek v IDM bude prostřednictvím správy odpovídajících aplikačních rolí uživatele
        - při změně role uživatele, na kterou je vázáno umístění schránky v datastore, bude při synchronizaci automaticky přemístěna schránka do odpovídajícího uložiště

- Napojení na RPP
    - IDM musí obsahovat evidenci matice práv a rolí dle informačního systému základních registrů (ISZR-RPP) matice RPP tak:
        - aby vedoucí pracovníci mohli zadávat k jednotlivým činnostem konkrétní uživatele
        - přidělování a odebírání agend/činností zaměstnancům vedoucími zaměstnanci s vazbou na systematizovaná místa
        - udržování a poskytování přehledu o oznámených působnostech, jejich stavech, kontrole registrace a změnách
        - evidence přehledu legislativy včetně vazby na jednotlivé činnosti/agendy
- Napojení na JIP
    - IDM musí obsahovat správu identit, rolí a systémů evidovaných v systému JIP (Jednotný identitní prostor) včetně:
        - obousměrné synchronizace s JIP
        - automatické pravidelné načítání aplikací a rolí z JIP do IDM
        - automatické předávání identity včetně vazby na jednotlivé aplikační a agendové činnostní role z IDM do JIP
        - možnosti změny hesla uživatele v JIP prostřednictvím webové konzole IDM
- Napojení na IS Ginis (mimo jiné obsahuje i spisovou službu)
    - IDM musí obsahovat min. tyto funkcionality:
        - Napojení na IS Ginis
            - Spárování identit mezi IDM a IS Ginis
        - Správu IS Ginis
            - Vytváření a rušení identit
            - Párování předdefinovaných funkčních míst na identity (včetně zastupujících identit)
            - Párování předdefinovaných konfiguračních skupin na funkční místa (musí být možno spárovat funkční místo s více konfiguračními skupinami)
            - Správa vazeb funkčního místa systému GINIS na agendy a role ISZR
    - Uchazeč si zajistí technické řešení a obchodní podmínky pro připojení IDM systému na IS u dodavatele GORDIC spol. s. r.o., kontaktní osoba: Ing. Tomáš Hubacz, email: [redacted] tel.: [redacted]
- Napojení na IS VERA Radnice

- IDM musí obsahovat min. tyto funkcionality:
  - Napojení na IS VERA Radnice
    - Spárování identit mezi IDM a IS VERA Radnice
  - Správu IS VERA Radnice
    - Vytváření a rušení identit
    - Vytváření multi vazeb identit na předdefinované role (jedna identita může mít více rolí)
- Uchazeč si zajistí technické řešení a obchodní podmínky pro připojení IDM systému na IS u dodavatele: VERA, spol. s r.o., kontaktní osoba: Mgr. Jan Hodač, email: [redacted]

- Napojení na IS VITA
  - IDM musí obsahovat min. tyto funkcionality:
    - Napojení na IS VITA
      - Spárování identit mezi IDM a IS VITA
    - Správu IS VITA
      - Vytváření a rušení identit
      - Správa oprávnění pro jednotlivé uživatele agend IS
  - Uchazeč si zajistí technické řešení a obchodní podmínky pro připojení IDM systému na IS u dodavatele: VITA software s.r.o., kontaktní osoba: Ing. Eva Sloupová, email: [redacted]

- Napojení na IS T-Mapy
  - IDM musí obsahovat min. tyto funkcionality:
    - inicializační načtení dat
    - spárování identit IDM a T-map skrze AD
    - na základě podnětu z IDM se vytvoří nebo zruší skupina oprávnění v AD, se kterou je svázáno CEU (role) v T-mapách
  - Uchazeč si zajistí technické řešení a obchodní podmínky pro připojení IDM systému na IS u dodavatele: T-MAPY spol. s r.o., kontaktní osoba: Ing. Milan Kollinger, email: [redacted] tel.: [redacted]

- Napojení na IS ADS RON
  - IDM musí obsahovat min. tyto funkcionality:
    - Napojení na IS ADS RON

        - Spárování identit mezi IDM a IS ADS RON
    - Správu IS ADS RON
        - Vytváření a rušení identit
        - Správa a přiřazení rolí jednotlivým uživatelským identitám
  - Uchazeč si zajistí technické řešení a obchodní podmínky pro připojení IDM systému na IS u dodavatele: RON Software, spol. s r.o., kontaktní osoba: Daniel Owczarzy, email: [redacted] tel.: [redacted]

- Napojení na IS Datacentrum 2
  - IDM musí obsahovat min. tyto funkcionality:
    - Napojení na IS Datacentrum 2
        - Spárování identit mezi IDM a IS Datacentrum 2
    - Správu IS Datacentrum 2
        - Správa lokálních identit
        - Správa oprávnění pro jednotlivé uživatele
        - Správa organizační struktury
        - Z tohoto personálního systému budou načítány údaje o hierarchii pracovních míst, osobách (zaměstnancích) a tyto údaje budou pro IDM systém sloužit jako zdrojové
  - Uchazeč si zajistí technické řešení a obchodní podmínky pro připojení IDM systému na IS u dodavatele: DataCentrum systems & consulting, a.s., kontaktní osoba: Václav Rusnok, email: [redacted] tel.: [redacted]

- Napojení na IS ServiceDesk
  - IDM musí obsahovat min. tyto funkcionality:
    - Napojení na IS ServiceDesk
        - Spárování identit mezi IDM a IS ServiceDesk
    - Správu IS ServiceDesk
        - Správa lokálních identit
        - Správa oprávnění pro jednotlivé uživatele (hlavně přiražení rolí)
  - Uchazeč si zajistí technické řešení a obchodní podmínky pro připojení IDM systému na IS u dodavatele: TruconneXion a.s., kontaktní osoba: Petr Bauer, email: [redacted] tel.: [redacted]

- IDM musí umožnit evidenci přístupových oprávnění a rolí v integrovaných systémech a jeho částech (modulech) u jednotlivých identit (uživatelů)
- IDM musí obsahovat informace o definovaných rolích identit (dle směrnic zadavatele)
- IDM musí umožnit zadavateli definovat jednotlivé role (min. 10 rolí v každém IS)
- Evidence integrovaných systémů musí vést pro každý integrovaný systém alespoň tyto údaje:
    - Název – označení integrovaného systému (povinná hodnota)
    - Kód ISVS – číselný kód přidělený Informačním systémem o informačních systémech veřejné správy (nepovinná hodnota)
    - Popis – slovní popis současného stavu a účelu provozování integrovaného systému
    - Koncepce – informace o způsobu využívání (koncepce rozvoje nebo ukončení životního cyklu)
    - Kategorie – zařazení integrovaného systému do kategorie výběrem z číselníku, kategorie mohou být uživatelsky definovatelné a upravovatelné
    - Stav integrovaného systému - evidence stavu životního cyklu nenapojeného systému („zkušební provoz", ostrý provoz", „ukončování provozu", provoz ukončen")
    - Využívané technické prostředky – evidence technických prostředků jako jsou servery, databáze, systémové prostředky výběrem z uživatelsky definovatelného číselníku
    - Zálohování – popis způsobu a frekvence zálohování, výběr z číselníku
    - Vazby na jiné IS a integrované systémy – označení jiných IS, na jejichž funkčnosti závisí provoz nenapojeného IS, výběr z číselníku

<u>Požadavky na evidenci v nenapojených (neintegrovaných) IS, aplikacích a systémech (dále jen NIS)</u>

- IDM musí umožnit evidenci přístupových oprávnění a rolí v NIS a jeho částech (modulech) u jednotlivých identit (uživatelů)
- IDM musí obsahovat informace o definovaných rolích identit (dle směrnic zadavatele)
- IDM musí umožnit zadavateli definovat jednotlivé role (min. 10 rolí v každém IS)
- IDM musí obsahovat informace o přidělených oprávněních a rolích identitám v IDM
- Evidence NIS musí vést pro každý NIS alespoň tyto údaje:
    - Název – označení NIS (povinná hodnota)
    - Popis – slovní popis současného stavu a účelu provozování NIS
    - Koncepce – informace o způsobu využívání (koncepce rozvoje nebo ukončení životního cyklu)
    - Kategorie – zařazení NIS do kategorie výběrem z číselníku, kategorie mohou být uživatelsky definovatelné a upravovatelné

- Stav NIS - evidence stavu životního cyklu nenapojeného systému („zkušební provoz", ostrý provoz", „ukončování provozu", provoz ukončen")
- Využívané technické prostředky – evidence technických prostředků jako jsou servery, databáze, systémové prostředky výběrem z uživatelsky definovatelného číselníku
- Zálohování – popis způsobu a frekvence zálohování, výběr z číselníku
- Vazby na jiné IS a NIS – označení jiných IS, na jejichž funkčnosti závisí provoz nenapojeného IS, výběr z číselníku

- U každého evidovaného NIS musí být možno přidávat vlastní atributy a podatributy ve formě stromové struktury reprezentující různé moduly a části NIS
- U každého atributu a podatributu musí být možné evidovat, jaké oprávnění (čtení/zápis) a roli v něm uživatel (identita) má
- IDM musí umožnit provádět evidenci oprávnění v NIS nadřízeným uživatelům (vedoucí odboru dle organizační struktury) a administrátorům NIS
- IDM musí umožnit evidenci oprávnění v NIS zobrazit v přehledné formě na kartě uživatele, pro dané uživatele (identity) a veškeré nadřízené uživatele dle organizační struktury
- IDM musí umožnit výstup přehledu z evidence NIS určeného k tisku a uchování
- IDM musí umožnit filtrování a třídění v evidenci NIS podle všech dostupných polí
- IDM musí umožnit definovat vlastní sestavy k tisku z evidence NIS
- IDM musí umožnit exportovat evidenci z NIS min. do formátu CSV

d) Implementace

Uchazeč musí dodat plně funkční systém, kompletně zprovozněný a nakonfigurovaný dle svých nejlepších znalostí a svědomí. Způsob implementace bude vycházet z projektové dokumentace implementace zpracované uchazečem v rámci předimplementační analýzy (náklady na provedení implementace musí být zahrnuty v nabídkové ceně).

- předimplementační analýza, která bude probíhat v místě plnění, u které budou přítomni jak zaměstnanci uchazeče z dotčených odborů, tak i zaměstnanci zadavatele
- předimplementační analýza bude mít jako výstup projektovou dokumentaci ve formátu DOCX, mimo jiné musí mapovat životní cyklus identit v jednotlivých napojených IS ve spolupráci s dodavateli v prostředí zadavatele, různé scénáře změn organizační struktury zadavatele
- projektová dokumentace musí být zpracována před zahájením realizace instalace a konfigurace IDM systému
- předimplementační analýza musí být předaná zadavateli a schválená zadavatelem
- instalace a konfigurace IDM bude realizována na zařízeních a programovém vybavení zadavatele (servery, stanice, operační systémy - definováno v bodě 2.b)

- napojení všech IS na IDM uvedených v bodě 2.c - Požadavky na integraci IDM s jinými systémy
- před napojením integrovaných systémů na IDM v produkčním prostředí musí dojít k otestování napojení v testovacím prostředí
- implementace musí probíhat prostřednictvím pracovníka uchazeče přímo v místě plnění, a to v pracovní době definované v bodě 2.g, nebo prostřednictvím pracovníka uchazeče vzdálenou správou nebo prostřednictvím pracovníka uchazeče formou vzdálené konzultace
- školení administrátorů, vedoucích pracovníků a uživatelů na začátku/v průběhu testovacího provozu v místě plnění v rozsahu specifikovaném v bodě 2. f tak, aby byli zaměstnanci zadavatele schopni obsluhovat a spravovat dodaný systém
- 30denní testovací provoz
- Vypracování a předání veškeré dokumentace specifikované v bodě 2. h
- předání díla po testovacím provozu za předpokladu odstranění veškerých nedostatků zjištěných během testovacího provozu

e) Akceptační testy a zkušební provoz

Součástí akceptačních testů a zkušebního provozu, které navrhne uchazeč, musí být minimálně:

- prokázání kompletnosti dodávky a splnění všech povinných požadavků
- prokázání aktivací aktivačními nebo jinými klíči či prostředky v případě, že je aktivace potřebná
- uchazečem vhodně navržené doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost
- před akceptací a předáním díla proběhne 30denní zkušební provoz. Pokud se vyskytnou během testování nebo zkušebního provozu závady, dodavatel je povinen závady odstranit nejpozději do 8 hodin od nahlášení v pracovní dny v době od 8 hod. do 17 hod.
- v průběhu zkušebního provozu může zadavatel průběžně posílat uchazeči požadavky na úpravy SW konfigurace, nejpozději však do konce 29. dne zkušebního provozu a uchazeč musí požadované změny realizovat (pokud to je technicky možné)
- dokončením díla se rozumí oboustranné odsouhlasení předávacího protokolu po dokončení testovacího provozu, akceptačních testech a úpravách v SW konfiguraci

f) Školení zaměstnanců zadavatele

Uchazeč zajistí školení zaměstnanců zadavatele v rozsahu minimálně dle následujících požadavků:

- první část školení v průběhu instalace a konfigurace před zahájením zkušebního provozu pro administrátory v rozsahu 24 hodin rozdělených do tří dnů v místě plnění v rozsahu potřebném pro provoz a údržbu systému (ukázka, popis a vysvětlení jednotlivých částí systému, vysvětlení stávající a tvorby/úpravy nové konfigurace atd.)

- druhá část školení v průběhu zkušebního provozu (v prvních 20 dnech) pro vedoucí pracovníky v rozsahu 4 hodin v místě plnění
- třetí část školení v průběhu zkušebního provozu (v prvních 20 dnech) pro uživatele v rozsahu 2 hod. Školení bude probíhat v 7 etapách po cca 50 uživatelích
- školení se dle předpokladu zúčastní průběžně všichni zaměstnanci MMFM (k dispozici je školící místnost s prezentační technikou v místě plnění)
- náklady na školení musí být zahrnuty v nabídkové ceně

g) Harmonogram, plán implementace a odstávek

Zadavatel vyžaduje dodržení následujícího harmonogramu plnění, jenž začíná v čase T a, v němž jsou uvedeny maximální možné lhůty pro jednotlivé významné milníky této veřejné zakázky.
Uchazeč připraví podrobný harmonogram prací před započetím realizace veřejné zakázky v čase T, který musí schválit obě strany.
Uchazeč je povinen nejpozději první pracovní den následující po uplynutí lhůty v 3. bodě harmonogramu vyzvat zadavatele k převzetí díla do zkušebního provozu.

1.	Předimplementační analýza v místě plnění za přítomnosti zaměstnanců zadavatele z dotčených odborů a zhotovení projektové dokumentace	T + 20 dní (20 dní)
2.	Předání projektové dokumentace zadavateli a připomínkování	T + 5 dní (25 dní)
3.	Zapracování připomínek a předání finální verze projektové dokumentace zadavateli, akceptace zadavatelem	T + 5 dní (30 dní)
4.	Implementace + školení administrátorů	T + 120 dní (150 dní)
5.	Zkušební provoz + školení vedoucích pracovníků a uživatelů + vypracování a předání dokumentace	T + 30 dní (180 dní)
6.	Předání díla	T + 1 den (181 dní)

Bez odstávkové práce mohou probíhat za provozu. Práce, jež omezují provoz nebo vyžadují odstávku, musí být provádět mimo pracovní dobu po předchozí domluvě.

Pracovní doba, po kterou je možno pracovat v místě plnění:
- pondělí až pátek od 8:00, dle individuální domluvy je možné od 6:00
- pondělí a středa do 17:00
- úterý a pátek do 13:30
- čtvrtek do 15:00

Odstávky a práce omezující provoz je možno provádět v těchto časech po předchozí domluvě:
- pondělí a středa od 17:30 do 19:00
- úterý a pátek od 14:00 do 19:00
- čtvrtek od 15:30 do 19:00
- odstávky po 19 hod. a o víkendu je možno realizovat dle individuální domluvy

h) Provozní a technická dokumentace

Uchazeč po úspěšné instalaci, konfiguraci a zkušebním provozu vypracuje a dodá zadavateli v písemné podobě podrobné dokumentace (ve formátu DOCX) k IDM systému.

- Provozní dokumentace musí minimálně obsahovat popis a postupy vedoucí k nastavení systému do takového stavu, aby jej bylo možno po instalaci provozovat na základní úrovni. Cílem dokumentu je popsat a zdokumentovat provozní postupy pro zajištění správného, bezchybného a bezpečného provozování IDM systému. Rozsah dokumentu bude min. 5 stran. Dokument bude mít formu textového popisu (může být i např. formou okomentovaného config souboru) a bude min. obsahovat:
    - konfiguraci sítě (IPv4, IPv6), nastavení připojení a komunikace na další systémy (např. DB, web server,...),
    - nastavení portů na kterých služba naslouchá, kam odesílá data...,
    - spuštění potřebných modulů, registrování knihoven, úprava registrů OS Windows, atd.,
    - nastavení automatických úloh, nastavení systémových účtů atd.
- Technická dokumentace musí obsahovat popis technické specifikace všech klíčových částí/komponent systému, jejich úkol, význam a účel (jakou platformou jsou jednotlivé komponenty zajištěny – software, agenti, typy použitých serverů, moduly, zdroje atd). Dále popis schéma systému, popis kompletní aktuální konfigurace, parametrů a nastavení jednotlivých částí systému, tak aby IDM systém bylo možno nadále provozovat a spravovat. Cílem dokumentu je popsat a zdokumentovat technickou stránku a aktuální konfiguraci IDM systému. Rozsah dokumentu bude min. 10 stran. Dokument bude mít formu textového popisu a může být doplněn obrazovým návodem schématu.
- Dokumentace popisující restart a obnovu musí min. obsahovat posloupnost všech kroků (co, kde a jak udělat), aby bylo možné provést bezpečný restart (např. informování uživatelů, ověření odhlášení uživatelů, provedení zálohy, samotný restart systému, kontrola funkčnosti). Dále posloupnost všech kroků (co, kde a jak udělat), aby bylo možné systém obnovit do jeho plně funkčního stavu po jeho selhání (např. obnova ze zálohy). Cílem dokumentu je popsat a zdokumentovat postupy a konkrétní kroky, které povedou k bezpečnému restartu nebo obnově systému. Rozsah dokumentu bude min. 2 strany. Dokument bude mít formu textového popisu a může být doplněn obrazovým návodem.
- Dokumentace popisující monitoring musí obsahovat výčet logovaných událostí (např. přihlášení/odhlášení, přidělení/odebrání oprávnění, synchronizace atd.) Dále popis práce s logovanými událostmi (umístění souboru, doba uložení, vzdálený server atd.) a logovací protokol (syslog, snmp atd.). Cílem dokumentu je popsat a zdokumentovat monitoring události. Rozsah dokumentu bude min. 2 strany. Dokument bude mít formu textového popisu.
- Uživatelská příručka, která musí po prostudování umožniti uživatelům využívat dodaný IDM systém. Cílem dokumentu je popsat, vysvětlit a naučit uživatele používat IDM systém. Rozsah dokumentu bude min. 5 strana. Dokument bude mít formu textového popisu a měl by být doplněn obrazovým návodem.

Veškeré dokumentace a příručky se po předání zadavateli stává jeho majetkem a může s nimi nakládat dle svých potřeb.

i) Technická podpora za roční paušální poplatek

Uchazeč musí od doby předání díla za roční paušální poplatek zajišťovat podporu k předmětu dodávky – tj. k systému IDM v minimálním rozsahu:

- poskytování pravidelných aktualizací formou upgrade, update, patch včetně legislativních aktualizací (aktualizace vyvolaná vývojem operačních systémů, změnou nebo vydáním nových nařízení EU, zákonů, vyhlášek, nařízení vlády, metodických pokynů atd.)
- zajištění kompletní instalace a úplné zprovoznění každé aktualizace
- zajištění funkčního stavu IDM systému (řešení závad, anomálií, vad vzniklých bez zjevného zapříčinění nebo důvodu na straně zadavatele atd.)
- řešení problémů komunikace a spolupráce s napojenými IS třetích stran po nasazení aktualizací
- zajištění zachování funkčního propojení se všemi napojenými IS třetích stran (i v případě, že dojde ke změně v připojených IS formou aktualizací)
- poskytování rad ke správnému a efektivnímu provozování a užití IDM systému formou telefonických nebo emailových konzultací nebo vzdáleným přístupem, a to nejpozději do 5 dní od doručení žádosti zadavatele v pracovní době od 8:00 do 18:00 hod. (pokud není dohodnuto jinak).

j) Technická podpora mimo roční paušální poplatek

Technická podpora mimo roční paušální poplatek bude poskytována na základě dílčích objednávek dle předem odsouhlasené nabídky uchazeče. Nejmenší účtovatelný interval této podpory činí 0,5 hod.

- odstraňování vad IDM systému vzniklých na straně zadavatele
- provádění úprav komunikačního rozhraní IDM systému, pokud dojde ke změně rozhraní u kterékoliv z připojených IS třetích stran
- provádění úprav nebo vytváření nových komunikačních rozhraní pro nově připojované IS třetích stran a realizace těchto propojení
- provádět školení zaměstnanců po předešlé objednávce zadavatele