



EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program



MINISTERSTVO
PRO MÍSTNÍ
ROZVOJ ČR

1. **Město Nové Město na Moravě**

se sídlem Vratislavovo náměstí 103, 592 31 Nové Město na Moravě

zastoupené **Michalem Šmardou**, starostou města

IČ: 00294900

DIČ: CZ00294900

bankovní spojení: Komerční banka, a.s.

č.ú.: 1224751/0100

(dále jen „objednatel“)

a

2. **AUTOCONT a.s.**

se sídlem: Hornoplní 3322/34, 702 00 Ostrava

IČ: 04308697

DIČ: CZ04308697

zastoupená: Ing. Jaroslavem Dvořákem, ředitel RC na základě plné moci

bankovní spojení: ČS

č.ú.: 6563752/0800

zapsaná v obchodním rejstříku vedeném Krajským soudem v Ostravě pod spis. zn.:oddíl B, vložka 11012.

(dále jen „zhotovitel“)

uzavírají níže uvedeného dne, měsíce a roku v souladu s ust. § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“) tuto :

Smlouvu o dílo č. RCV-220154

Čl. I

Předmět smlouvy

1. Zhotovitel bere na vědomí, že objednatel je nositelem projektu reg. číslo CZ.06.3.05/0.0/0.0/16_034/0006428, „Harmonizace prostorových dat a řízení identit pro Nové Město na Moravě“, u kterého je předpokládáno financování z prostředků Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného regionálního operačního programu (dále jen „IROP“) a státního rozpočtu ČR, v rámci kterého bude předmět smlouvy realizován.



EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program



MINISTERSTVO
PRO MÍSTNÍ
ROZVOJ ČR

2. Zhotovitel se touto smlouvou zavazuje, že pro objednatele na vlastní náklady a na vlastní nebezpečí ve sjednané době a za sjednaných podmínek provede **dodávku, implementaci Identity management systému do prostředí města Nové Město na Moravě**, a to včetně nedílně souvisejících požadavků typu zaškolení, dodání licencí, zpracování dokumentace (dále jen „dílo“) a předá jej objednateli v dohodnutém termínu. Objednatel se zavazuje řádně a včas dokončené dílo převzít a zaplatit za něj zhotoviteli dohodnutou cenu dle čl. IV této smlouvy.
3. Závazným podkladem, kterým se sjednává obsah, rozsah, způsob a podmínky provedení díla je:
 - a) zadávací dokumentace veřejné zakázky „**Harmonizace prostorových dat a IDM pro Nové Město na Moravě**“ předaná uchazeči(ům) objednatelem jako zadavatelem v rámci zadávacího řízení (dále také jen „zadávací dokumentace“).
 - b) nabídka zhotovitele
4. Bližší specifikace díla je obsahem přílohy č. 1, která je nedílnou součástí této smlouvy.

Čl. II

Doba plnění

1. K provedení díla dojde jeho řádným a včasným dokončením a předáním objednateli nejpozději do 20.12.2022. Dílo je dokončeno, je-li předvedena jeho způsobilost sloužit svému účelu.
2. Realizace díla bude zahájena ihned po uzavření této smlouvy.
3. Dojde-li při realizaci díla k prodloužení z důvodů na straně objednatele, je zhotovitel oprávněn požadovat na objednateli prodloužení dohodnutého termínu předání díla dle čl. II odst. 1 této smlouvy přímo úměrné délce prodloužení.
4. Pokud bude v průběhu realizace díla zjištěna skutečnost, o níž zhotovitel nevěděl a vědět nemohl, a která ztíží nebo znemožní provedení díla ve sjednaném rozsahu, sdělí tuto skutečnost zhotovitel neprodleně objednateli a projedná s ním další postup.
5. Místem plnění a předání díla je Vratislavovo náměstí 103, Nové Město na Moravě

Čl. III

Předání a převzetí díla

1. Zhotovitel je povinen provést realizaci díla podle této smlouvy a předat jej objednateli ve lhůtě uvedené v čl. II odst. 1 této smlouvy.



- Objednatel převezme dokončené dílo s výhradami, nebo bez výhrad. Převezme-li objednatel dílo bez výhrad, nepřizná mu soud právo ze zjevné vady díla, namítne-li zhotovitel, že právo nebylo uplatněno včas.
- O předání díla zhotovitelem a jeho převzetí objednatelem bude sepsán předávací protokol. K převzetí díla a podpisu protokolu je za objednatele oprávněn Zbyněk Grepl, vedoucí oddělení informatiky, Městského úřadu Nové Město na Moravě, k předání díla a podepsání protokolu je za zhotovitele oprávněn Ing. Miroslav Veselý, ředitel OZ.
- Objednatel je povinen řádně a včas zhotovené dílo od zhotovitele za podmínek stanovených touto smlouvou převzít. Pokud objednatel bezdůvodně odepře řádně a včas zhotovené dílo převzít nebo požádá o změnu termínu převzetí díla, není zhotovitel v prodlení.
- Objednatel není povinen převzít dílo v případě, že dílo má vady nebo nebylo dodáno ve lhůtě dle čl. II odst. 1 této smlouvy. V případě, že objednatel převezme od zhotovitele dílo, které má vady, ačkoli k tomu není povinen, je zhotovitel povinen při předání a převzetí díla dohodnout s objednatelem opatření a termín k odstranění zjištěných vad.

Čl. IV

Cena a platební podmínky

- Smluvní strany se dohodly, že celková a nejvýše přípustná cena díla vč. DPH činí **820380,- Kč**, slovy: osmsetdvacetisícetřistaosmdesát korun českých (dále jen „cena“). Cena zahrnuje veškeré náklady zhotovitele vynaložené při realizaci díla.
- Smluvní strany sjednávají možnost jednostranného zvýšení ceny díla ze strany zhotovitele v průběhu provádění díla, a to v případě zvýšení zákonné sazby DPH. Navýšení sjednané ceny musí odpovídat zvýšení hodnoty DPH v závislosti na zvýšení zákonné sazby DPH. Smluvní strany sjednávají dále možnost jednostranného snížení ceny díla ze strany objednatele v průběhu provádění díla, a to v případě snížení zákonné sazby DPH. Snížení sjednané ceny musí odpovídat snížení hodnoty DPH v závislosti na snížení zákonné sazby DPH.
- Cenu uhradí objednatel na základě faktury vystavené zhotovitelem po řádném a včasném předání a převzetí díla. Splatnost faktury je dohodou smluvních stran stanovena na 14 dnů ode dne jejího prokazatelného doručení objednateli. Zaplacením se pro účely této smlouvy rozumí odepsání příslušné částky z účtu objednatele.
- Faktura musí obsahovat veškeré náležitosti účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a daňového dokladu podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.



5. Vzhledem k tomu, že je toto dílo součástí projektu financovaného z prostředků Evropského fondu pro regionální rozvoj prostřednictvím IROP a státního rozpočtu ČR, se zhotovitel zavazuje předkládat k proplacení pouze faktury, které budou obsahovat **název a číslo projektu, v rámci kterého je zakázka zadávána, tedy „reg. číslo CZ.06.3.05/0.0/0.0/16_034/0006428, „Harmonizace prostorových dat a řízení identit pro Nové Město na Moravě“.**
6. Objednatel si vyhrazuje právo před uplynutím lhůty splatnosti vrátit fakturu, pokud neobsahuje požadované náležitosti nebo obsahuje nesprávné cenové údaje. Oprávněným vrácením faktury přestává běžet původní lhůta splatnosti. Opravená nebo přepracovaná faktura bude opatřena novou lhůtou splatnosti.

Čl. V

Práva a povinnosti smluvních stran

1. Zhotovitel je povinen provést realizaci díla podle této smlouvy a podle pokynů a podkladů předaných mu objednatelem na vlastní náklady a na vlastní odpovědnost, a v dohodnuté lhůtě je objednateli předat.
2. Při realizaci díla je zhotovitel povinen dodržovat obecně závazné předpisy, které se vztahují k realizaci díla a postupovat s odbornou péčí v zájmu objednatele, v případě financování projektu dle platných právních předpisů a podmínek IROP (více na www.irop.mmr.cz , záložka IROP2014-2020).
3. Objednatel je povinen řádně a včas zhotovené dílo převzít a zaplatit za něj zhotoviteli dohodnutou cenu dle čl. IV odst. 1 této smlouvy.
4. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškerou součinnost a informace potřebné pro řádné plnění svých závazků vyplývajících z této smlouvy. Smluvní strany jsou povinny informovat se navzájem o všech jim známých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této smlouvy.
5. Zhotovitel je povinen za účelem ověření plnění povinností vyplývajících z této smlouvy vytvořit podmínky k provedení kontroly vztahující se k realizaci projektu tím, že poskytne minimálně do konce roku 2028 požadované informace a dokumentaci související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.
6. Zhotovitel má povinnost uchovávat veškerou dokumentaci související s plněním předmětu této smlouvy včetně účetních dokladů do 31.12. 2028.



ČI. VI

Sankční ujednání

1. V případě prodlení zhotovitele s provedením díla v termínu uvedeném v čl. II odst. 1 této smlouvy je objednatel oprávněn účtovat zhotoviteli smluvní pokutu ve výši 0,01% z ceny, a to za každý i započatý den prodlení.
2. V případě prodlení objednatele se zaplacením faktury vystavené zhotovitelem v souladu s čl. IV odst. 3 a 4 této smlouvy je zhotovitel oprávněn účtovat objednateli smluvní pokutu ve výši 0,01% z nezaplacené částky, a to za každý i započatý den prodlení.

ČI. VII

Ukončení smlouvy

1. Tato smlouva se uzavírá na dobu určitou, a to do ukončení realizace díla.
2. Tuto smlouvu lze ukončit písemnou dohodou smluvních stran.
3. Objednatel může od této smlouvy odstoupit, pokud zhotovitel neprovede dílo v termínu sjednaném v čl. II odst. 1 této smlouvy nebo v kvalitě dle této smlouvy. Zhotovitel může od této smlouvy odstoupit, pokud objednatel nezaplatí cenu stanovenou v čl. IV odst. 1 této smlouvy za řádně a včas provedené dílo. Odstoupení nabývá účinnosti dnem následujícím po dni prokazatelného doručení jeho písemného vyhotovení druhé smluvní straně.
4. Smluvní strany výslovně sjednávají, že pokud veškeré závazky z této smlouvy vyplývající nebudou zcela splněny či vypořádány do uplynutí doby trvání této smlouvy podle čl. IX odst. 2, resp. čl. II odst. 1 této smlouvy, platnost této smlouvy se automaticky prodlužuje do doby úplného vypořádání veškerých závazků z ní vyplývajících.

ČI. VIII

Závěrečná ustanovení

1. Tato smlouva byla projednána na schůzi Rady města Nové Město na Moravě č 67 konané dne 19.9.2022 a schválena usnesením přijatým pod č. 3/67/RM/2022 programem.
2. Zhotovitel podpisem této smlouvy souhlasí s jejím uveřejněním v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv ("zákon o registru smluv"). Zhotovitel výslovně souhlasí se zveřejněním celého textu smlouvy v informačním systému veřejné správy – Registru smluv.
3. Smluvní strany se dohodly, že stranou povinnou k uveřejnění této smlouvy v centrálním registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv ("zákon o registru smluv") je město Nové Město na Moravě, které je povinno tuto smlouvu bez zbytečného odkladu, nejpozději však do 30 dnů od uzavření smlouvy odeslat k uveřejnění v registru smluv.
4. Smluvní strany shodně prohlašují, že žádné ustanovení v této smlouvě nemá charakter obchodního tajemství, jež by požívalo zvláštní ochrany.



EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program



MINISTERSTVO
PRO MÍSTNÍ
ROZVOJ ČR

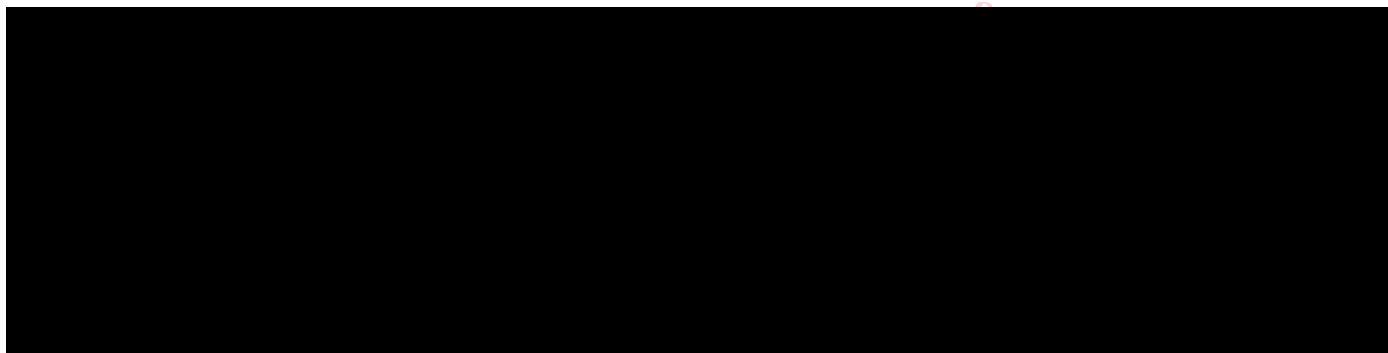
5. Objednateli svědčí zákonné zmocnění (zák. č. 89/2012 Sb., občanský zákoník, zák. č. 128/2000 Sb., o obcích) ke shromažďování, nakládání a zpracovávání osobních údajů v souvislosti s uzavřením této smlouvy.
6. Tuto smlouvu lze měnit pouze formou písemných, vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran.
7. Tato smlouva byla sepsána ve třech vyhotoveních s platností originálu, objednatel obdrží dvě vyhotovení a zhotovitel jedno vyhotovení této smlouvy.
8. Vztahy smluvních stran touto smlouvou neupravené se řídí příslušnými ustanoveními občanského zákoníku.
9. Nedílnou součástí této smlouvy je příloha č. 1 - specifikace díla.
10. Smluvní strany prohlašují, že si tuto smlouvu přečetly, že tato byla sepsána na základě jejich pravé a svobodné vůle, nikoli v tísní ani za nápadně nevýhodných podmínek, a na důkaz toho připojují své podpisy.
11. Tato smlouva nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem jejího uveřejnění v Centrálním registru smluv.

V Novém Městě na Moravě dne 14.11.2022

V Jihlavě

Objednatel:

Zhotovitel:





„Veřejná zakázka Harmonizace prostorových dat.“

Specifikace nabízeného zboží:

Jako účastník o předmětnou veřejnou zakázku - část 5 navrhuji níže uvedené požadavky řešit dodávkou a implementací systému pro správu a řízení elektronických identit na platformě IDM -AC Identita autorem tohoto systému je: CES EA s.r.o., IČ:08028656

Základní požadavky na IDM:

- Předmětem dodávky je nasazení sjednocujícího řešení pro správu identit (dále jen IDM nebo Systém) v prostředí města Nové Město na Moravě. Systém bude udržovat a spravovat identity a organizační strukturu organizace. Spravované identity budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy. Identity budou ukládány v databázi.
- Poskytnutá licence umožní nasazení a provoz IDM bez omezení počtu uživatelů, spravovaných identit a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází, atd.)
- Systém musí umožnit zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů - minimálně oddělení rolí (serverů) uživatelského rozhraní od výkonu integračních a provozních úloh
- 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) ve vybraných hlavních systémech organizace, a to zejména v návaznosti na personální systém a adresářové služby.
- Integrovaný registr aplikací a informačních systémů (souhrnně IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby.
- Integrovaná správa uživatelských rolí, včetně zařazení uživatele do odpovídající role v příslušných IS.
- Vestavěná detailní databázová historizace pro evidenci změn identit včetně referenčních objektů a vazeb mezi nimi. Historizace poskytne data v libovolném časovém okamžiku - aktuálním nebo zpětně v minulosti.
- IDM bude spravovat a řídit identity (uživatele, jejich uživatelské účty) v rámci připojených systémů.

- 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.
- Součástí nasazení takového řešení bude i vytvoření systematizovaných pracovních míst, jím 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.
- 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.
- 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.
- IDM bude dále realizováno při naplňování legislativních požadavků 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.

Minimálně zajistí:

- auditní záznamy oprávnění uživatelů a poskytuje reporty o stavu
- IDM a jeho funkcionality musí respektovat standardní architekturu IS v prostředí objednatele a pro svou integraci využít standardizovaná rozhraní a existující prostředky IS.
- 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 a o zrušení směrnice 1999/93/ES.

Funkcionality IDM

- 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)
- 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.
 - 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 vztahované ke konkrétnímu systemizovanému místu.
 - 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.
 - IDM musí umožňovat přidělení role konkrétní identitě, systemizovanému místu, skupině nebo organizační jednotce
 - IDM musí umožnit správu uživatelských rolí, včetně zařazení uživatele do odpovídající role.
 - V IDM je možné aplikační role nastavovat dočasně. Po uplynutí nastaveného intervalu se role automaticky odebere.
 - IDM umožní registraci aplikací a jejich rolí a dále také import rolí přes webové služby do IDM.
 - IDM musí umožnit nastavení schvalovacího workflow (při přidělení práva, role atd.), včetně emailových notifikací a potvrzování.
 - IDM musí umožnit definovat vztahy zastupitelnosti mezi uživateli – musí umožnit uživatelům, aby v souladu se strukturou nemocnice 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.
 - IDM musí umožnit dodatečné přidávání vlastních atributů k identitám.
 - IDM musí umožňovat přesun identity v rámci organizační struktury i mezi jednotlivými organizačními strukturami.
 - 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.
 - IDM musí umožňovat kopírovat role mezi jednotlivými systematizovanými místy.
 - IDM musí obsahovat funkcionalitu kopírování veškerého nastavení oprávnění z jednoho uživatele na druhého.
 - 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.
 - IDM musí umožňovat generování minimálně 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.
 - IDM bude komunikovat v českém jazyce.

Požadavky na grafické rozhraní IDM

- IDM musí obsahovat grafické uživatelské rozhraní pro přístup administrátorů systému pro správu identit uživatelů a jejich možné založení, úpravu nebo zneplatnění.
- Správa systému IDM musí být implementována jako webová konzole/aplikace přístupná přes běžné prohlížeče Edge, Chrome, FireFox v aktuálních verzích. Tato webová konzole musí být přístupná výhradně protokolem https.

- Portál bude umožňovat přehlednou správu samostatných identifikovatelných objektů - referenčních objektů, na které se identity mohou odkazovat: min. systematizované místo, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role, certifikát.
- Systém umožní přidávání a správu dalších typů referenčních objektů a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity. IDM bude v modulu správy identit u scénáře správy konkrétní identity implementovat v grafickém rozhraní přímý odkaz (proklik) na referenční objekty, na která se daná identita odkazuje včetně toho, aby administrátor mohl po přechodu na tento odkaz vytvářet a editovat další referenční objekty a následně po vrácení zpět na detail identity je v tomto scénáři přiřadil dané spravované identitě.
- Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů.
- Systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM.
- IDM bude obsahovat grafické zobrazení identit (uživatelských účtů) ve stromové organizační struktuře. Součástí jednoho pohledu v IDM bude zobrazení organizační struktury včetně systematizovaných míst organizace až do úrovně jednotlivých uživatelských účtů (identit). V grafickém zobrazení stromové struktury bude možné vyhledávat jednotlivé identity, systematizovaná místa, organizační jednotky.
- Portál bude umožňovat vyhledávat i bez diakritiky (např. zadání Zbynek vyhledává i Zbyněk apod.)
- Správa uživatelů (identit) bude umožňovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím rozhraní webových služeb. Systém umožní automatické zneplatnění uložených certifikátů po vypršení data platnosti.
- Systém umožní k jednotlivým účtům (identitám) přikládat obrázky – fotografie.
- Systém umožní přesun identit mezi jednotlivými organizacemi či jejich odděleními.
- Systém umožní kopírování aplikačních rolí, mezi jednotlivými systematizovanými místy.
- Systém bude obsahovat mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (např. z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory apod).
- Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem
- Systém umožní sjednocení více uživatelů (identit) do jedné, a odpovídající sjednocení spravovaných účtů.
- Vestavěný export přehledů a seznamů zobrazených na portále do souborů CSV nebo obdobného strojově zpracovatelného a současně běžně čitelného formátu.
- Vestavěný editor filtrů pro vyhledávání identit a referenčních identit. Možnost filtrování libovolných atributů identity včetně přidružených referenčních objektů. Možnost uložení filtrů pro opakované použití.
- Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity apod.).
- IDM bude obsahovat editor oprávnění. V rámci editoru bude administrátor definovat oprávnění do IDM a následně tato oprávnění přiřazovat konkrétním uživatelům. Oprávnění bude definováno pro

jednotlivé entity a moduly systému (identity, referenční objekty, konfigurace notifikací, konfigurace synchronizací, konfigurace systému IDM, reporty, workflow, správa webových služeb IDM atd.) Dále bude oprávnění u entit (identit a referenčních objektů) definováno až na jejich konkrétní atributy včetně zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti atributu, pořadí zobrazení atributů ve formuláři. U jednotlivých entit a modulů bude možnost definovat akce, které může uživatel s entitami a v rámci IDM provádět.

- Na úrovni organizační jednotky bude možné pro výběr a přiřazování rolí nastavit sady povolených aplikačních rolí, skupiny, systematizovaných míst dostupných pro identity z dané organizační jednotky.
- IDM bude umožňovat přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení IDM rolí přiřazenému objektu automaticky odebere.
- Možnost přiřazení identit k systematizovaným místům ve vazbě M:N. Identita může být v IDM evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit.
- IDM bude zajišťovat zobrazení přidělených rolí k jednotlivým identitám s rozdělením na role navázané na systemizované místo, role navázané na identitu, role navázané na organizační jednotku, role navázané na skupinu. U identity musí být evidován a v IDM souhrnně zobrazen seznam všech rolí včetně informace o tom, odkud uživatel roli zdědil nebo mu byla delegována (z organizační jednotky, systematizovaného místa, skupiny apod.).
- IDM bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa.
- IDM bude obsahovat správu vztahů zastupitelnosti mezi uživateli. Musí umožnit uživatelům, aby v souladu se strukturou organizace mohli uživatelé delegovat v případě potřeby (dovolená, služební cesta) svoje role, nebo jejich část na jiné pověřené osoby a to i v režimu, kdy jeden uživatel může mít pro každou svou činnost nastaveného jiného uživatele jako zástupce.
- Možnost delegování administrátorských práv.
- IDM umožní správu evidence osobních údajů - bude obsahovat správu evidence subjektů údajů a evidenci jejich osobních údajů včetně jejich kategorií a klasifikací.
- IDM bude obsahovat evidenci účelů pro nakládání s osobními údaji subjektů údajů. V rámci daného účelu budou definována oprávnění, aplikační role pro přístup k osobním údajům.
- IDM bude obsahovat workflow pro správu životního cyklu osobních údajů subjektu údajů.
- IDM bude obsahovat samoobslužné uživatelské rozhraní pro zadávání žádostí o přidělení jednotlivých aplikačních rolí a členství ve skupinách. Role a skupiny budou kategorizovány a kategoriím bude možné přidělit schvalovací workflow nebo může žádost vyřízena automaticky bez schválení.
- Samoobslužné rozhraní umožní na úrovni organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat.
- IDM umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní - min. zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku - vždy pro každý seznam samostatně.

- Integrované workflow pro řízení životního cyklu změn identit a schvalování změn. Funkční požadavky:
 - zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřazeným,
 - možnost sledování stavu svých požadavků uživateli,
 - e-mailové upozornění schvalovatele na požadavek ke schválení,
 - přehled úloh ke schválení pro každého schvalovatele,
 - schvalování či zamítnutí požadavků včetně uvedení zdůvodnění,
 - podpora vícekrokového schvalování,
 - podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů),
 - správce IDM může pracovat se všemi úlohami,
 - možnost větvení pro ošetření výjimek vzniklých při schvalování,
 - řešení zastupitelnosti,
 - eskalace - upozornění při překročení termínu splnění,
 - možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů.
- Průběh workflow bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram bude ve obvyklém formátu pro zobrazení workflow např. aktivity diagram, BPMN nebo Archimate.
- IDM zajistí zasílání konfigurovatelných emailových upozornění min. pro následující události: vytvoření a změna identity, referenčního objektu (systematizované místo organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu. Mechanismus správy notifikací včetně náhledu na odeslané notifikace musí být spravován přímo v IDM.
- IDM bude obsahovat notifikační šablony a notifikace pro upozornění na vypršení hesla v Active Directory a vypršení platnosti certifikátů. Notifikaci lze nastavit na několik dní dopředu před vlastním vypršením hesla nebo certifikátu.
- Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám musí být možné nastavovat různé příjemce pro různé části organizační struktury (např. odbor, oddělení) apod. Šablony musí umožnit vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu.
- U notifikací ve vazbě na identity a referenční objekty musí být možné konfigurovat nastavení na úroveň jednotlivých atributů. V šabloně musí být možné vybrat libovolné atributy identity a referenčních objektů a následně je vložit a použít v definici textu pro emailové zprávy. Dále musí být možné u notifikací konfigurovat podmínky pro provedení notifikace na základě hodnot jednotlivých libovolných atributů identity a referenčních objektů. (například notifikace je generována pouze pro identitu v konkrétních uvedených skupinách, která má uvedenu konkrétní aplikační roli, systematizované místo, atd.). V IDM musí být možné notifikace aktivovat pro jednotlivé zdrojové systémy, které v IDM změnu identity nebo referenčního objektu provedly.
- Veškeré změny vyvolané požadavky uživatele a administrátorů/správčů IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy změnil v identitách a

referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu.

- Veškeré požadavky na změny v IDM bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových souborů jako XML, CSV, atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM.
- IDM umožní export auditního reportu z údajů o identitách uložených v IDM a to i historických. Auditní reporty budou minimálně ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti.
- IDM bude obsahovat editor pro vyhledávání identit a referenčních objektů v systému IDM pro vytvoření reportu. Do filtru musí být možné zadat libovolné atributy identity, které jsou v systému IDM evidovány včetně přidružených referenčních objektů.
- Vestavěné reporty obsahující uživatele s přímo přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od jiných uživatelů. Reporty budou exportovatelné do CSV souboru.
- IDM bude obsahovat možnost generovat do CSV souboru report uživatelů přiřazených aplikačním rolím a možnost nastavení pravidel pro automatické zasílání reportu emailem
- IDM bude obsahovat report, který do formátu PDF vygeneruje kartu uživatele obsahující informace o uživateli včetně seznamu rolí, které uživatel má, skupin, certifikátů, atd.
- Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení.
- Snadné porovnání změn mezi vygenerovanými reporty stejného typu v prostředí Portálu.
- IDM bude obsahovat centrální dashboard, který bude obsahovat následující údaje:
 - synchronizační úlohy v chybě,
 - chyby běhu synchronizací,
 - chyby při generování a odesílání notifikací,
 - chyby volání metod rozhraní webových služeb IMD (např. pokus o přístup k metodě, na kterou nemám oprávnění),
 - chyby plánovaných úloh (agentů),
 - nově vytvořené poznámky,
 - workflow v chybě,
 - neúspěšné akce systému v systému IDM.
- IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu.

Požadavky na webové služby

- 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 objednatel, 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.

- Základní konfigurace přístupu k webovým službám musí být dostupná z grafického rozhraní IDM.
- 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.
- IDM umožní vstupně/výstupní synchronizace do připojených informačních systémů. Typy synchronizací:
 - plná
 - 1 identita (možnost prosynchronizovat pouze 1 identitu bez nutnosti pouštět plnou nebo změnovou synchronizaci)
 - změnová (pokud to napojený IS umožní)

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.
- IDM umožní publikaci objektů (osob, účtů, skupin, funkcí, org. jednot,...) 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. 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, včetně možnosti omezit dané API IDM pro jednotlivé aplikace (pouze vydefinované metody API IDM pro potřeby dané aplikace).
- Webové služby IDM budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP.
- Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně.
- Volání webových služeb bude logováno a bude možné je zobrazit v prostředí Portálu.
- Rozhraní bude poskytovat minimálně 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,
 - zápis seznamu aplikačních rolí do IDM,
 - zápis certifikátů do IDM,
 - zápis a změna identit.
- Ruční i automatické spuštění synchronizací s propojenými systémy.
- Spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy budou zobrazitelné v Portálu.
- Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v přehledné grafické podobě.

- Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM u každého systému využít více režimů synchronizací (za předpokladu podpory 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 konkrétní identity na vyžádání – synchronizuje okamžitě pouze vybranou identitu,
 - simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka,
 - historie běhu synchronizací – jednotlivé běhy synchronizací budou zaznamenány v historii dostupné v Portálu. Historie plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii dále informace o události, která změnovou synchronizaci vyvolala.
- Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, nastavení časového intervalu spouštění, nastavení intervalu odstávky. U jednotlivých synchronizací je rovněž požadováno, aby bylo možné vybírat organizace, které se mají z IDM synchronizovat s danými systémy. Správa bude součástí Portálu.
- IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. V těchto systémech bude IDM vytvářet, aktualizovat, vytvářet uživatele a nastavovat jim oprávnění k rolím:
- Registr práv a povinností (RPP),
- Jednotný identitní prostor (JIP).
- Microsoft Active Directory, a dále
 - IS GINIS
 - IS VITA
 - IS TESS (spisová služba fy T-MAPY)
 - Geografický informační systém T-Mapy
 - IS VERA e-Jednání
- IDM bude napojeno na personální systém MAGMA HCM od fy ID.EST. Z personálního systému budou načítány údaje o organizační struktuře, hierarchii pracovních míst, osobách a tyto údaje budou pro IDM sloužit jako zdrojové.

Implementace:

Proces implementace Systému bude obsahovat zpracování předimplementační analýzy, implementačního projektu, vlastní implementaci a následné zpracování dokumentace a zaškolení administrátorů.

- Předimplementační analýza bude obsahovat následující oblasti specifické pro komoditu:
 - analýzu procesů a aplikací se zaměřením na oblast správy uživatelských účtů, přidělování oprávnění a rolí,
 - analýzu požadavků zasílaných centrálním informačním systémům, základním registrům a dalších informačních systémů s požadavkem na autorizaci a autentizaci,
 - technologický popis stávajících technologií s vazbou na systém správy identit
 - analýzu možností správy výstupních struktur,
 - analýzu evidenčních údajů a logů,

- návrh životního cyklu identity uživatelů,
 - model organizační struktury,
 - seznam systemizovaných pracovních pozic,
 - přiřazení pracovníků k pracovním pozicím.
- Implementační projekt musí obsahovat minimálně:
 - manažerský souhrn,
 - detailní popis řešení včetně integrace na systémy, které budou IDM využívat,
 - harmonogram implementace řešení,
 - požadavky na součinnost zadavatele,
 - návrh akceptačních testů a akceptačního protokolu,
 - návrh harmonogramu nasazování systému.

Implementační projekt je Zhotovitel povinen dodat v písemné podobě. Před jeho předáním je Zhotovitel povinen podrobit jej připomínkovému řízení ze strany Objednatele.

- Instalace a implementace

Instalaci a implementaci je Zhotovitel povinen provádět v souladu se schváleným implementačním projektem. Nebude-li předávané dílo prosto vad či nedodělků, Objednatel uvede zjištěné vady či nedodělky do předávacího protokolu a zároveň stanoví Zhotoviteli lhůtu k jejich odstranění.