Smlouva č.: 2024/0376

SMLOUVA O DÍLO

Identity Management pro město Neratovice

uzavřená níže uvedeného dne, měsíce a roku podle § 2586 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů a podle zákona č. 121/2000 Sb. (autorský zákon), ve znění pozdějších předpisů

Čl. 1. Smluvní strany

1.1. Město Neratovice

se sídlem: Kojetická 1028, 277 11 Neratovice
IČO: 00237108
DIČ: CZ00237108
zastoupené: Ing. Romanem Kroužeckým, starostou
bankovní spojen[redacted]
číslo účtu[redacted]
kontaktní osob[redacted]
telefon:
e-mail:
(dále jen „objednatel", „zadavatel")

a

1.2. Obchodní jméno: Aricoma Systems a.s.

se sídlem / místem podnikání: Hornopolní 3322/34, Moravská Ostrava, 702 00 Ostrava
IČO: 04308697
DIČ: CZ04308697
zastoupený/jednající: [redacted]
bankovní spojení: [redacted]
číslo účtu: [redacted]
zapsán v obchodním rejstříku, vedeném u Krajského soudu v Ostravě, sp. zn. B 11012
zhotovitel je plátce DPH: Ano
kontaktní osoba[redacted]
telefon:
e-mail:
(dále jen „zhotovitel", „uchazeč", „účastník zadávacího řízení")

Tato smlouva je uzavírána v návaznosti na veřejnou zakázku s názvem „Identity Management pro město Neratovice“, zadávanou objednatelem jakožto zadavatelem.

Čl. 2. Předmět smlouvy

2.1.1. Předmětem plnění této smlouvy je dodávka a implementace identity management systému do prostředí objednatele, včetně příslušenství, a poskytování technické podpory k tomuto systému.

2.2. Předmětem díla jsou následující činnosti zhotovitele

2.2.1. Dodávka licencí, implementace Identity management systému (dále jen jako „IDM“), testovací provoz a předání do řádného užívání.

2.2.2. Pro výše uvedený rozsah plnění:

- provedení integrací na další systémy v prostředí objednatele i mimo něj,
- úprava dodaného řešení dle potřeb a požadavků dle pokynů objednatele,
- zaškolení odborného personálu objednatele.

2.2.3. Dále je předmětem plnění dodávka

- dokumentace k dodanému plnění v požadovaném rozsahu,
- dalších licencí potřebných pro provoz IDM,
- listinného potvrzení dodaných licencí co do jejich počtu a rozsahu.

2.2.4. Detailní předmět plnění je uveden v příloze č. 1 této smlouvy – Technické dokumentaci.

2.2.5. Předmět smlouvy rovněž obsahuje plnění, které není uvedeno v příloze č. 1 této smlouvy - Technické dokumentaci, ale jehož realizace je nezbytná pro provedení díla, tj. pro řádné a včasné dokončení díla v souladu s touto smlouvou. Zahrnuje veškerá plnění včetně software pro zajištění 100% funkčnosti a provozuschopnosti nových elektronizovaných agend a dalších komponent na základě této smlouvy o dílo.

2.3. Vzdálený přístup do prostředí objednatele

2.3.1. Předmětem této smlouvy je dále i zajištění a sjednání podmínek vzdáleného přístupu zhotovitele bez aktivní účasti objednatele do prostředí objednatele za účelem plnění této smlouvy.

2.3.2. Objednatel se zavazuje, že umožní zhotoviteli vzdálený přístup k informačním systémům a aplikacím uvedeným v předmětu plnění této smlouvy nejpozději do 10 pracovních dnů ode dne uzavření této smlouvy.

Čl. 3. Doba a místo plnění

3.1.1. Plnění díla bude zahájeno ihned po nabytí účinnosti této smlouvy.

3.1.2. Plnění předmětu díla této smlouvy bude dokončeno jeho řádným zhotovením ze strany zhotovitele a řádnou a bezvýhradnou akceptací se strany objednatele. S výjimkou ustanovení týkajících se vzdáleného přístupu, který je předmětem této smlouvy.

3.2. Místo plnění

3.2.1. Místem plnění díla je sídlo objednatele na adrese Kojetická 1028, 277 11 Neratovice.

3.3. Doba dokončení díla

3.3.1. Řádně zhotovené a dokončené dílo bude předáno objednateli nejpozději do 20 týdnů od uzavření smlouvy.

3.3.2. Detailní závazný harmonogram plnění včetně dílčích milníků, na jejichž splnění v daném pořadí a čase objednatel bude trvat, je obsažen v příloze č. 1 této smlouvy o dílo – Technické dokumentaci.

Čl. 4. Práva a povinnosti smluvních stran

4.1.1. Zhotovitel se zavazuje za podmínek stanovených touto smlouvou na svůj náklad a na své nebezpečí ve sjednaném termínu splnit celý předmět smlouvy. Zhotovitel se dále zavazuje dodat řádně a včas plnění podle této smlouvy bez právních a faktických vad.

4.1.2. Při zhotovování díla se zhotovitel zavazuje počínat si s odbornou péčí tak, aby byl zcela naplněn předmět a účel smlouvy.

4.1.3. Zhotovitel je povinen vynaložit maximální úsilí, aby docílil nejlepšího možného výsledku při plnění předmětu této smlouvy prostřednictvím využití svých znalostí a zkušeností.

4.1.4. Při provádění díla postupuje zhotovitel samostatně, je však vázán zejména písemnými pokyny objednatele. Zhotovitel je povinen bez zbytečného odkladu písemně upozornit objednatele na nevhodnost jeho pokynů k provedení díla. Pokud nevhodné pokyny brání v řádném provádění díla, je zhotovitel povinen v nezbytně nutném rozsahu přerušit provádění díla do doby změny pokynů objednatele nebo písemného sdělení, že objednatel trvá na provádění díla dle svých pokynů. V souvislosti s realizací díla po dobu takového přerušení má zhotovitel nárok na prokazatelně vynaložené náklady.

4.1.5. Zhotovitel je povinen v průběhu provádění díla dodržovat obecně závazné předpisy a normy, postupovat s náležitou odbornou péčí, podle nejlepších znalostí a schopností, sledovat a chránit oprávněné zájmy objednatele.

4.1.6. Zhotovitel je povinen v průběhu provádění díla neprodleně informovat objednatele o všech skutečnostech, které mají nebo mohou mít vliv na provedení díla.

4.1.7. Pokud objednatel zjistí, že zhotovitel provádí dílo v rozporu se svými povinnostmi, je oprávněn požadovat, aby zhotovitel odstranil v objednatelem stanovené lhůtě vzniklé vady a dílo prováděl řádným způsobem.

4.1.8. Zhotovitel se zavazuje v průběhu provádění díla postupovat v souladu se zásadami projektového řízení a zejména jejich jednotlivými konkrétními pokyny zanesenými objednatelem v příloze č. 1 této smlouvy – Technické dokumentaci v kapitole s názvem Projektové řízení.

4.1.9. Objednatel se zavazuje řádně a včas dokončený předmět smlouvy od zhotovitele protokolárně převzít a zaplatit zhotoviteli sjednanou cenu.

4.2. Součinnost

4.2.1. Objednatel požaduje, aby maximum práce odvedl zhotovitel samostatně, bez zatěžování pracovníků objednatele. Součinnost objednatele bude omezena na nezbytnou míru a bude se vztahovat především na schvalování výstupů zhotovitele v předem definovaných kontrolních dnech a na nezbytnou IT podporu nutnou k nasazení řešení a realizaci vazeb.

4.2.2. Rozsah součinnosti bude odsouhlasen při zahájení realizace jako součást Dokumentace skutečného provedení (v detailu viz. příloha č. 1 této smlouvy – Technická dokumentace), včetně termínů jejího poskytování.

4.2.3. V případě následného požadavku zhotovitele na součinnost nad dohodnutý rámec má objednatel právo součinnost odmítnout, případně ji poskytnout v termínu a rozsahu dle svých možností, a to bez dopadu na harmonogram realizace a z něj vyplývající sankce za nedodržení termínů.

4.2.4. Neposkytnutí součinnosti jako důvod pro posun smluvních termínů bude akceptován pouze tam, kde byla součinnost objednatelem přislíbena při zahájení realizace.

Čl. 5. Cena díla

5.1.1. Cena za zhotovení díla představuje objednatelem /jakožto zadavatelem/ akceptovanou nabídkovou cenu, předloženou zhotovitelem /jakožto uchazečem/ v nabídce na veřejnou zakázku „Identity Management pro město Neratovice".

5.1.2. Zhotovitel výslovně prohlašuje, že nabídková cena a cena díla obsahuje veškeré práce a dodávky, poplatky a jiné náklady nezbytné pro řádnou a úplnou realizaci sjednaného předmětu plnění a veškeré náklady včetně všech rizik a vlivů souvisejících s plněním předmětu smlouvy.

5.1.3. Objednatel a zhotovitel se dohodli, že cena za řádné a včasné provedení celého díla specifikovaného v čl. 2 této smlouvy činí celkem částku:

1 556 060,00 Kč včetně DPH, přičemž

cena bez DPH činí 1 286 000 Kč,

sazba DPH činí 21 %,

výše DPH činí 270 060,00 Kč.

5.1.4. Tato cena je stanovena jako cena konečná a úplná.

5.1.5. Zhotovitel není oprávněn požadovat po objednateli poskytnutí zálohy.

5.1.6. Zhotovitel na sebe výslovně bere odpovědnost za to, že sazba a výše daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy.

5.1.7. Daň z přidané hodnoty bude připočtena k ceně díla ve výši dle právní úpravy platné ke dni uskutečnění zdanitelného plnění.

5.1.8. Sjednaná celková cena díla dle této smlouvy je cenou nejvýše přípustnou, kterou je možné překročit pouze v případě zvýšení sazby DPH, a to tak, že zhotovitel ke sjednané ceně bez DPH připočítá DPH v procentní sazbě odpovídající zákonné úpravě účinné k datu uskutečnitelného zdanitelného plnění.

Čl. 6. Platební podmínky

6.1.1. Cena díla bude objednatelem uhrazena jednorázovou platbou na základě zhotovitelem vystavené faktury.

6.1.2. Fakturu je zhotovitel oprávněn vystavit nejdříve následující den po dni uskutečnění zdanitelného plnění, jímž se pro účely této smlouvy rozumí řádná realizace předmětu díla definovaného v čl. 2 této smlouvy.

6.1.3. Podkladem pro vystavení faktury je podepsaný protokol o předání a převzetí předmětu díla.

6.1.4. Všechny faktury dle této smlouvy musí obsahovat název a registrační číslo projektu **Rozvoj eGovernmentu města Neratovice**, číslo projektu **CZ.06.01.01/00/22_009/0002331**.

6.1.5. Splatnost faktury činí 30 dnů ode dne jejího prokazatelného doručení na adresu sídla objednatele.

6.1.6. Faktura bude mít náležitosti daňového dokladu dle platných právních předpisů (zákona č. 563/1991 Sb., o účetnictví, v platném znění a zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění).

6.1.7. Faktury musí obsahovat označení smlouvy, číslo účtu zhotovitele a všechny údaje uvedené v § 28 odst. 2 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

6.1.8. Součástí faktury bude specifikace dodaného plnění tak, aby byla v souladu s platnými účetními a daňovými předpisy, a to za účelem řádného vedení evidence majetku objednatele v souladu s těmito právními předpisy.

6.1.9. V případě, že faktura – daňový doklad nebude obsahovat stanovené náležitosti nebo v něm nebudou správně uvedené údaje, je objednatel oprávněn ji vrátit ve lhůtě splatnosti zpět zhotoviteli s uvedením chybějících náležitostí nebo nesprávných údajů. V takovém případě se přeruší běh lhůty splatnosti a nová lhůta splatnosti počne běžet doručením opravené faktury – daňového dokladu.

6.1.10. Po vzniku práva fakturovat je zhotovitel povinen vystavit a objednateli předat fakturu.

6.1.11. Cena bude zhotoviteli zaplacena bezhotovostní formou převodem na jeho bankovní účet. Faktura je považována za proplacenou okamžikem odepsání příslušné částky z účtu objednatele ve prospěch zhotovitele.

6.1.12. Zhotovitel souhlasí s tím, aby subjekty oprávněné dle zák. č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, provedly finanční kontrolu závazkového vztahu vyplývajícího ze smlouvy s tím, že se zhotovitel podrobí této kontrole, a bude spolupůsobit jako osoba povinná ve smyslu ust. § 2 písm. e) uvedeného zákona při výkonu finanční kontroly prováděné v souvislosti s úhradou služeb z veřejných výdajů.

6.1.13. Pro případ, že zhotovitel je, nebo se od data uzavření smlouvy do dne uskutečnění zdanitelného plnění stane na základě rozhodnutí správce daně „nespolehlivým plátcem“ ve smyslu ustanovení § 106a zákona č. 235/2004 Sb., o DPH, ve znění pozdějších předpisů, souhlasí zhotovitel s tím, že mu objednatel uhradí cenu plnění bez DPH a DPH v příslušné výši odvede za nespolehlivého plátce přímo příslušnému správci daně. V souvislosti s tímto ujednáním nebude zhotovitel vymáhat od objednatele část z ceny plnění rovnající se výši odvedeného DPH a souhlasí s tím, že tímto bude uhrazena část jeho pohledávky, kterou má vůči objednateli, a to ve výši rovnající se výši odvedené DPH.

6.1.14. Zhotovitel je povinen uchovávat veškerou dokumentaci související s realizací projektu (předmětu plnění této smlouvy) včetně účetních dokladů minimálně do konce roku 2040.

6.1.15. Zhotovitel je poskytovat požadované informace a dokumentaci související s realizací projektu (předmětu plnění této smlouvy) 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 (předmětu plnění této smlouvy) a poskytnout jim při provádění kontroly součinnost.

Čl. 7. Předání díla

7.1.1. Zhotovitel splní svoji povinnost zhotovit dílo jeho řádným a včasným dokončením v souladu s podmínkami této smlouvy a předáním hotového díla objednateli.

7.1.2. Předání a převzetí díla je rozděleno do několika částí označených jako „milníky" podle harmonogramu obsaženého v příloze č. 1 této smlouvy – Technické dokumentaci. Akceptace díla jako celku je podmíněna dílčími akceptacemi jednotlivých milníků harmonogramu s výsledkem „Splněno".

7.1.3. Specifické podmínky stanovené pro akceptační řízení jsou dále detailně rozpracovány v příloze č. 1 této smlouvy – Technické dokumentaci v kapitole s názvem Akceptace.

7.1.4. Objednatel prohlašuje, že převezme pouze dokončené dílo bez zjevných vad, nedodělků a podstatných vad bránících funkcionalitě předávaného díla. V opačném případě si objednatel vyhrazuje právo převzetí díla odmítnout, bez nároku na navýšení ceny díla.

7.1.5. Předání a převzetí díla proběhne na základě porovnání skutečných vlastností díla dle specifikace díla uvedené v čl. 2. této smlouvy. Plnění bude potvrzeno podpisem protokolu o předání a převzetí díla Objednatelem. Součástí protokolu o předání je jednoznačná identifikace předávaného díla.

7.1.6. Zjistí-li objednatel nedostatky, nedodělky, či vady, oznámí to písemnou formou bez zbytečného odkladu zhotoviteli.

7.1.7. Místem předání díla je sídlo objednatele.

7.1.8. Za objednatele je oprávněn jednotlivé milníky dle harmonogramu díla a hotové dílo převzít a protokol o předání a převzetí díla podepsat [redacted]

7.1.9. Vlastnické právo k dílu přechází na objednatele okamžikem předání díla objednateli. Práva z poskytnuté licence objednatel nabývá okamžikem převzetí díla od zhotovitele.

Čl. 8. Záruka za dílo

8.1.1. Zhotovitel poskytuje objednateli záruku v délce trvání 2 let. Dílo dle této smlouvy bude ke dni předání a převzetí objednatelem způsobilé k řádnému užití a bude mít vlastnosti stanovené touto smlouvou.

8.1.2. Zhotovitelem poskytovaná záruka se vztahuje na kompletní funkčnost díla, jakož i na jeho vlastnosti požadované objednatelem.

8.1.3. Záruční doba začíná běžet ode dne převzetí díla objednatelem. Záruční doba se prodlužuje o dobu, po kterou mělo dílo vadu bránící jeho řádnému užívání objednatelem, nebo po kterou bylo plnění mimo provoz z důvodu vady, na kterou se vztahuje záruka.

8.1.4. Veškeré zjištěné nedostatky, nedodělky a vady díla, které se vyskytnou v záruční době, je objednatel povinen bez zbytečného odkladu písemně oznámit zhotoviteli.

8.1.5. Vadou díla se pro účely této smlouvy rozumí rozpor mezi sjednanými podmínkami provedení díla, jeho parametry a skutečným stavem díla.

8.1.6. Objednatel má vůči zhotoviteli tato práva z odpovědnosti za vady:

- právo na bezplatné odstranění reklamovaných vad, a to bezprostředně po oznámení vady objednatelem, nejpozději ve lhůtě 15 dnů od oznámení vady objednatelem,
- právo na poskytnutí přiměřené slevy z ceny odpovídající rozsahu reklamovaných vad či nedodělků,
- právo na odstoupení od smlouvy, kdy vady či nedodělky jsou takového charakteru, že ztěžují či dokonce brání v užívání díla, nebo
- právo na zaplacení nákladů na odstranění vad v případě, kdy si objednatel vadu či nedodělek odstraní sám nebo použije třetí osoby k jejich odstranění.

8.1.7. Uplatněním nároků z odpovědnosti za vady není dotčeno právo na náhradu škody. Zhotovitel odpovídá objednateli za případnou škodu, která mu vznikne z titulu neodstranění vady díla zhotovitelem ve stanoveném termínu.

8.1.8. Záruka je poskytována v souladu s ustanovením § 2113 a násl. zákona č. 89/2012 Sb., občanského zákoníku, v platném znění.

Čl. 9. Licenční ujednání

9.1.1. Zhotovitel v rámci plnění předmětu této smlouvy vytvoří dílo podléhající ochraně podle zákona č. 121/2000 Sb., o právu autorském (autorský zákon), a zákona č. 89/2012 Sb., občanského zákoníku, a tak poskytuje objednateli licenci - tj. oprávnění k výkonu práva užívat jím vytvořené autorské dílo.

9.2. Zhotovitel poskytuje licenci jako:

- nevýhradní licenci k veškerým známým způsobům užití takového díla, zejména, nikoliv však výlučně k účelu, ke kterému bylo takové dílo zhotovitelem vytvořeno v souladu se smlouvou a to v rozsahu minimálně nezbytném pro řádné užívání díla objednatelem,
- licenci neomezenou územím výkonu působnosti objednatele,
- licenci co do rozsahu oprávněného počtu uživatelů k užívání informačního systému a jeho jednotlivých oblastí neomezenou;
- neomezenou způsobem nebo rozsahem užití;
- licenci udělenou na dobu určitou, a to po celou dobu trvání majetkových práv k dílu;
- licenci, kterou není objednatel povinen využít.

9.2.1. Povinnost týkající se licence platí pro zhotovitele i v případě zhotovení části díla poddodavatelem.

9.2.2. Licence je poskytnutá v maximálním rozsahu povoleném platnými právními předpisy.

9.2.3. Zhotovitel je povinen zajistit, aby výsledkem jeho plnění nebo jakékoliv jeho části nebyla porušena práva třetích osob. Pro případ, že užíváním předmětu plnění nebo jeho dílčí části nebo prostou existencí předmětu plnění nebo jeho dílčí části budou v důsledku porušení povinností zhotovitele dotčena práva třetích osob, nese zhotovitel vedle odpovědnosti za takovéto vady plnění i odpovědnost za veškeré škody, které tím objednateli vzniknou.

9.3. Zhotovitel uděluje objednateli

- oprávnění dílo (nebo jeho dílčí část), které podléhá ochraně podle zákona č. 121/2000 Sb. (autorský zákon) a zákona č. 89/2012 Sb., občanského zákoníku, upravovat, zpracovávat, měnit jeho název,
- a oprávnění dílo spojit s dílem jiným a s dílem dále pracovat za účelem jeho dalšího rozvoje a používání.

9.3.1. Objednatel a zhotovitel se výslovně dohodli, že odměna za veškerá licenční oprávnění poskytnutá objednateli je již zahrnuta v ceně za poskytnuté plnění dle této smlouvy, tj. cena za poskytnutí licence, včetně nákladů souvisejících s případnou aktualizací licence.

9.4. Licence k datům

9.4.1. Veškerá data zpracovávaná nejen objednatelem v informačním systému jsou daty objednatele a o nakládání s nimi rozhoduje výhradně objednatel.

Čl. 10. Odpovědnost za škodu

10.1.1. Smluvní strany nesou odpovědnost za způsobenou škodu v rámci platných právních předpisů a této smlouvy.

10.1.2. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

Čl. 11. Podmínky pro vzdálený přístup do prostředí objednatele

11.1.1. Vzdálený přístup je poskytován výhradně zhotoviteli a nelze ho dále převádět na jinou osobu nebo osoby. Porušení této povinnosti bude považováno za podstatné porušení této smlouvy.

11.1.2. Zhotovitel se zavazuje, že vzdálený přístup k informačním systémům a aplikacím v prostředí počítačové sítě objednatele na základě této smlouvy bude využívat jen za účelem dodávky těchto informačních systémů a aplikací a poskytování služeb uvedených v této smlouvě a samostatné smlouvě o technické podpoře a rozvoji k předmětnému informačnímu systému. Porušení této povinnosti bude považováno za podstatné porušení smlouvy.

11.1.3. Zhotovitel se zavazuje postupovat při realizaci svých práv a povinností vyplývajících z této smlouvy tak, aby v počítačové síti objednatele nezpůsobil poškození, ztrátu nebo odcizení dat. Pokud by se tak stalo, zavazuje se na vlastní náklady takto vzniklé závady odstranit v co nejkratším termínu, nejpozději však do 5 pracovních dnů.

Čl. 12. Sankční ujednání

12.1.1. Dojde-li k prodlení s úhradou daňového dokladu - faktury, je zhotovitel oprávněn účtovat objednateli úrok z prodlení ve výši 0,05 % z dlužné částky za každý započatý den prodlení po termínu splatnosti až do doby zaplacení dlužné částky.

12.1.2. Nesplní-li zhotovitel svůj závazek vycházející z každého z dílčích termínů milníků harmonogramu, který je součástí přílohy č. 1 této smlouvy - Technické dokumentace, je oprávněn objednatel požadovat po zhotoviteli zaplacení jednorázové smluvní pokuty ve výši 2.000,- Kč za nedodržení termínu plnění každého z těchto milníků.

12.1.3. Nesplní-li zhotovitel svůj závazek v rozsahu a čase plnění sjednaném touto smlouvou, je oprávněn objednatel požadovat po zhotoviteli nad rámec nedodržení plnění dle milníků harmonogramu zaplacení jednorázové smluvní pokuty ve výši 20.000,- Kč za nedodržení termínu plnění a dále smluvní pokuty ve výši 0,2 % ze sjednané ceny plnění dle této smlouvy za každý započatý den prodlení, až do řádného dokončení a předání celého předmětu plnění a zhotovitel je povinen takto požadovanou smluvní pokutu zaplatit.

12.1.4. Nesplní-li zhotovitel v dohodnutém termínu svůj závazek odstranit vady a nedodělky vytknuté při převzetí díla nebo v průběhu záruční doby, je objednatel oprávněn požadovat na zhotoviteli zaplacení smluvní pokuty ve výši 0,05 % ze sjednané ceny předmětu plnění za každý započatý den prodlení až do jejich úplného odstranění a zhotovitel se zavazuje takto požadovanou smluvní pokutu objednateli zaplatit.

12.1.5. Nesplní-li zhotovitel řádně podmínky projektového řízení dle přílohy č. 1 této smlouvy – Technické dokumentace zejména v případě zápisů ze schůzek a pracovních jednání, v případě účasti odpovědné osoby zhotovitele na kontrolních dnech a v případě pravidelného reportingu, je objednatel oprávněn požadovat po zhotoviteli smluvní pokutu ve výši 500,- Kč za každý případ takového pochybení, a to i opakovaně.

12.1.6. Pokud zhotovitel nesplní svůj závazek vyplývající ze vzdáleného přístupu na základě této smlouvy, zejména v oblasti odstranění vzniklých závad v souvislosti s jeho vzdáleným přístupem do počítačové sítě objednatele, zavazuje se uhradit objednateli nutné náklady spojené s uvedením počítačové sítě do původního stavu a navíc se zavazuje zaplatit smluvní pokutu ve výši 10.000,- Kč za každý zjištěný a prokázaný případ porušení povinnosti spojené se vzdáleným přístupem do počítačové sítě objednatele.

12.1.7. Zaplacením smluvní pokuty není dotčeno právo poškozené strany na náhradu vzniklé škody. Výši smluvních pokut považují obě smluvní strany shodně za přiměřené.

12.1.8. Základem pro výpočet smluvní pokuty je na základě dohody smluvních stran cena v Kč včetně DPH.

12.1.9. Smluvní pokuty a úroky z prodlení podle tohoto článku jsou splatné do 30 dnů ode dne doručení jejich vyúčtování.

Čl. 13. Ukončení smlouvy

13.1.1. Tuto smlouvu lze ukončit dohodou smluvních stran. Dohoda o ukončení smluvního vztahu musí být písemná, jinak je neplatná.

13.1.2. Od této smlouvy lze odstoupit v případě podstatného porušení povinností jednou smluvní stranou, jestliže je takové porušení povinnosti označeno za podstatné touto smlouvou nebo zákonem. Odstoupení od smlouvy je účinné dnem doručení písemného oznámení o odstoupení druhé smluvní straně.

13.1.3. Smluvní strany se dohodly, že za podstatné porušení této smlouvy ze strany zhotovitele považují:

- dodání nebo zhotovení vadného předmětu plnění,
- prodlení s plněním závazku vyplývajícího z této smlouvy po dobu delší než třicet (30) dní a nezjednání nápravy ani do patnácti (15) dní od doručení oznámení objednatele o prodlení s plněním závazku,
- další dílčí konkretizovaná porušení označená za podstatná uvedená v příloze č. 1 této smlouvy – Technické dokumentaci.

13.1.4. Smluvní strany se dohodly, že za podstatné porušení této smlouvy ze strany objednatele považují:

- prodlení se zaplacením vyfakturované ceny díla (jeho části) delší než třicet (30) kalendářních dnů.

13.1.5. Porušení jakékoliv jiné povinnosti objednatele nebo zhotovitele, vyplývající z této smlouvy, je třeba zhojit v dodatečné přiměřené lhůtě k tomu poskytnuté.

13.1.6. Odstoupením od této smlouvy nejsou dotčena ustanovení týkající se smluvních pokut a úroků z prodlení a stejně tak práva a povinnosti smluvních stran vzniklá do okamžiku účinnosti odstoupení od smlouvy.

Čl. 14. Závěrečná ustanovení

14.1.1. Práva a povinnosti smluvních stran v této smlouvě výslovně neupravené a z ní vyplývající nebo s ní související se řídí zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů a zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

14.1.2. V případě rozporu technické dokumentace objednatele (zadavatele) a technické nabídky (technického řešení) zhotovitele platí, není-li uvedeno v této smlouvě jinak, technická dokumentace objednatele tj. příloha č. 1 – Technická dokumentace.

14.1.3. Pokud jakýkoli závazek dle smlouvy nebo kterékoli ustanovení smlouvy je nebo se stane neplatným či nevymahatelným, nebude to mít vliv na platnost a vymahatelnost ostatních závazků a ustanovení dle smlouvy a smluvní strany se zavazují takovýto neplatný nebo nevymahatelný závazek či ustanovení nahradit novým, platným a vymahatelným závazkem, nebo ustanovením, jehož předmět bude nejlépe odpovídat předmětu a ekonomickému účelu původního závazku či ustanovení.

14.1.4. V případě, že po podpisu této smlouvy na zhotovitele anebo jeho poddodavatele budou dopadat mezinárodní sankce podle zákona upravujícího provádění mezinárodních sankcí č. 69/2006 Sb. ve smyslu zákona č. 240/2022 Sb. účinného od 1. 9. 2022, je povinen to zhotovitel písemně oznámit objednateli. V případě, že oznámení neprovede a objednatel zjistí, že na zhotovitele anebo jeho poddodavatele mezinárodní sankce dopadají, vyzve dodavatele k vysvětlení nebo nápravě formou vyjmutí osoby ze sankčního seznamu. V případě že náprava není možná, odstoupí objednatel od této smlouvy, přičemž účinnost odstoupení nastává doručením odstoupení zhotoviteli.

14.1.5. Vzhledem k charakteru objednatele zhotovitel výslovně souhlasí se zveřejněním smluvních podmínek obsažených v této smlouvě v rozsahu a za podmínek vyplývajících z příslušných právních předpisů. A to včetně uveřejnění kompletního znění smlouvy na základě zákonné povinnosti objednatele jako veřejnoprávního subjektu.

14.1.6. Tato smlouva je vyhotovena v elektronickém originále, který po podpisu oběma smluvními stranami obdrží obě smluvní strany.

14.1.7. Tuto smlouvu je možno platně měnit pouze na základě dohody smluvních stran, formou písemných a vzestupně číslovaných dodatků, podepsaných oběma smluvními stranami.

14.1.8. Tato smlouva nabývá platnosti dnem podpisu druhou ze smluvních stran a účinnosti uveřejněním v registru smluv. Uveřejnění v registru smluv zajistí objednatel.

14.1.9. Zhotovitel se zavazuje zajistit dodržování pracovněprávních předpisů, zejména zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (se zvláštním zřetelem na regulaci odměňování, pracovní doby, doby odpočinku mezi směnami atp.), zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů (se zvláštním zřetelem na regulaci zaměstnávání cizinců), a to vůči všem osobám, které se na plnění zakázky podílejí a bez ohledu na to, zda jsou práce na předmětu plnění prováděny bezprostředně zhotovitelem či jeho poddodavateli.

14.1.10. Zhotovitel je povinen zajistit řádné a včasné plnění finančních závazků svým poddodavatelům, kdy za řádné a včasné plnění se považuje plné uhrazení poddodavatelem vystavených faktur za plnění poskytnutá k plnění veřejné zakázky v termínu splatnosti, nejpozději však do 30 dnů od obdržení platby ze strany objednatele za konkrétní plnění. Zhotovitel se zavazuje přenést totožnou povinnost do dalších úrovní dodavatelského řetězce.

14.1.11. Tato smlouva je schválena usnesením rady města č. RM/23/40/24 dne 20.11.2024

14.2. Nedílnou součástí této smlouvy jsou její přílohy:

- příloha č.1 Technická dokumentace objednatele
- příloha č.2 Technická dokumentace zhotovitele (technické řešení z nabídky účastníka)

14.2.1. Smluvní strany prohlašují, že tuto smlouvu před jejím podpisem přečetly, zcela rozumí jejímu obsahu a s celým jejím obsahem souhlasí. Dále prohlašují, že tato smlouva vyjadřuje jejich pravou a svobodnou vůli. Na důkaz toho připojují vlastnoruční podpisy svých oprávněných zástupců.

V Karlových Varech dne dle elektr. podpisu

Za zhotovitele

[redacted]ng.

Zdeněk Chobot, na základě plné moci

V Neratovicích dne dle elektr. podpisu

Za objednatele

[redacted]

Ing. Roman Kroužecký, starosta

Příloha č. 1 smlouvy o dílo – Technická dokumentace objednatele

(Pro potřebu podání nabídky na veřejnou zakázku nebude uchazeč kompletovat nabídku v tom smyslu, že jako součást návrhu smlouvy na předmět plnění nemusí být přiložena přílohy smlouvy. Tyto budou zkompletovány až při podpisu smlouvy s vítězným uchazečem.)

Příloha č. 2 smlouvy o dílo – Technická dokumentace zhotovitele

(Pro potřebu podání nabídky na veřejnou zakázku nebude uchazeč kompletovat nabídku v tom smyslu, že jako součást návrhu smlouvy na předmět plnění nemusí být přiložena přílohy smlouvy. Tyto budou zkompletovány až při podpisu smlouvy s vítězným uchazečem.

Příloha č. 1 Zadávací dokumentace – Technická dokumentace zadavatele

Příloha č. 1 Smlouvy o dílo – Technická dokumentace

Technická dokumentace

Identity Management pro město Neratovice

verze 05 z 31.07.2024

Obsah

1 Úvod

1.1.1 Tento dokument je určen k popisu a definici rozsahu díla, dodávek a služeb, které objednatel poptává jako předmět plnění ve veřejné zakázce s názvem „Identity Management pro město Neratovice“.

1.1.2 Předmětem této dokumentace je popis a stanovení požadavků objednatele na dodávku a implementaci identity managementu a zpracování dokumentace.

1.2 Popis plnění podle této technické dokumentace

1.2.1 Předmětem plnění této technické dokumentace je dodávka a implementace identity managementu pro Město Neratovice, a to včetně nedílně souvisejících požadavků typu dodání licencí a zpracování dokumentace.

1.2.2 Předmětem díla jsou následující činnosti zhotovitele:

- dodávka licencí, implementace identity managementu, testovací provoz a předání do řádného užívání.

1.2.3 Pro výše uvedený rozsah plnění:

- provedení integrací na další systémy v prostředí objednatele i mimo něj,
- úprava dodaného řešení dle potřeb a požadavků dle pokynů objednatele.

1.2.4 Dále je předmětem plnění dodávka

- dokumentace k dodanému plnění v požadovaném rozsahu,
- dalších licencí potřebných pro provoz identity managementu,
- listinného potvrzení dodaných licencí co do jejich počtu a rozsahu.

2 Základní požadavky na IDM

2.1.1 Předmětem dodávky je nasazení sjednocujícího řešení pro správu identit, uživatelských rolí a případně i oprávnění uživatelů, včetně jejich evidence, v prostředí objednatele.

2.1.2 IDM zajistí centrální a jednoduchou správu identity, uživatelských rolí a případně i oprávnění uživatelů v aplikacích a informačních systémech, u kterých bude provedena integrace na takové IDM.

2.1.3 Cílem je zefektivnit a automatizovat proces řízení identit v organizaci a zavést centrální platformu pro řízení identit v organizaci – IDM (Identity Management Systém). IDM umožní automatizovaně spravovat identity (osoby, uživatelské role a oprávnění) ve vybraných hlavních systémech organizace, a to zejména v návaznosti na personální systém a adresářové služby. Cílem je rovněž zavést samoobslužné procesy pro zadávání žádostí o oprávnění a přístupů samostatnými koncovými uživateli organizace. V rozšířeném IDM, na rozdíl od řešení stávajícího, bude následně možné takovéto požadavky schválit a změny nastavení u identit automatizovaně předat (vypublikovat) do připojených systémů (integrovaných aplikací).

2.1.4 Systém Identity management bude spravovat a řídit identity (uživatele, jejich uživatelské účty a oprávnění) v rámci připojených systémů. Pro unifikovanou správu identit v systémech organizace je nutné vybudování jednotné centrální evidence uživatelů, uživatelských účtů a oprávnění uživatelů k integrovaným aplikacím. Tato evidence je spravována centrálně v systému IDM v návaznosti na centrální službu JIP/KAAS.

2.1.5 Současně s nasazením IDM bude potřeba konsolidovat a standardizovat procesy související s personálními obměnami v organizaci (nový zaměstnanec, odchod zaměstnance, zařazení zaměstnance na pozici, změna pozice zaměstnance a další) v této souvislosti s vývojem jejich identity (zejména nabývání a ztráta oprávnění do vybraných aplikací a informačních systémů), případně procesy existující v IDM zohlednit. Na základě takových procesů ze zdrojových systémů (personální systém) vstupují do IDM údaje o osobách, uživatelských účtech, zařazení v organizační struktuře, přiřazení pracovního místa, přiřazení do skupin atd.

2.1.6 Součástí nasazení takového řešení bude i vytvoření systematizovaných pracovních míst, 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.

2.1.7 Součástí nasazovaného řešení bude nástroj správy identifikačních prostředků, který rozšíří autentizační systém a zajistí řízené a evidované vystavení a přidělení identifikačního prostředku uživatelům včetně odpovídajících certifikátů. Nástroj zajistí podporu a evidenci operací spojených s užíváním identifikačního prostředku a uložených certifikátů (odvolání certifikátu, obnova certifikátu atd.) a s ukončením jejich užívání (odstranění certifikátů, reinicializace prostředku atd.). Součástí bude automatické hlídání platnosti certifikátů, upozornění uživatelů na vypršení platnosti a průvodce uživatele pro jednoduché samostatné prodloužení certifikátu (resp. vystavení a uložení nového), pokud bude mít uživatel přidělena odpovídající oprávnění.

2.1.8 IDM bude mít provedenou vazbu na Jednotný identitní prostor (JIP) a Katalog autentizačních a autorizačních služeb (KAAS) se kterými bude spolupracovat, a to do plného rozsahu těchto IS ve vztahu k povaze objednatele jako orgánu vykonávajícímu přenesenou i samostatnou působnost pro územní samosprávný celek.

2.1.9 Systém IDM bude reflektovat veškeré potřebné změny související s životním cyklem identity v prostředí objednatele a ve vazbě na všechny na IDM napojené informační systémy, ve kterých bude mít daná identita uživatelské role a oprávnění. Takové změny budou reflektovány ve všech aktuálně napojených informačních systémech vždy v konkrétní rozhodné době.

2.1.10 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 rolí. IDM bude provádět správu automaticky, tak aby byly spravované systémy vždy aktuální.

2.1.11 IDM bude dále realizováno při naplňování nových legislativních požadavků. V případě tohoto plnění zejména s dopady Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Minimálně zajistí:

- zajišťuje auditní záznamy oprávnění uživatelů a poskytuje reporty o stavu

2.1.12 IDM a jeho funkcionality musí respektovat standardní architekturu IS v prostředí objednatele a pro svou integraci využít standardizovaná rozhraní a existující prostředky IS.

2.1.13 Součástí plnění bude dále i navržení metodiky pro správu identit

- jmenné konvence uživatelských jmen a zajištění jejich unikátnosti (sjednocení loginů),
- mechanismu práce s hesly (přidělení, změna, samoobslužný reset apod.),
- postupy správy uživatelů (zavádění, změny, rušení, nastavování oprávnění apod.),
- návrh členění objektů v rámci IDM (osoby, účty, funkce, organizační jednotky, skupiny),
- definice bezpečnostních zásad a pravidel pro práci s IDM.

2.2 Funkcionality IDM

Parametr	Popis parametru
	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 rolí a oprávnění. IDM bude provádět správu automaticky, tak aby byly spravované systémy vždy aktuální.

Parametr	Popis parametru
	IDM bude dále realizováno při naplňování nových legislativních požadavků. V případě tohoto plnění zejména s dopady Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), tj. IDM zajistí auditní záznamy oprávnění uživatelů a umožní reporting stavu těchto oprávnění.
	IDM a jeho funkcionality musí respektovat standardní architekturu IS v prostředí objednatele a pro svou integraci využít standardizovaná rozhraní a existující prostředky IS.
	IDM bude ukládat data do databáze Microsoft SQL.
	IDM bude komunikovat v českém jazyce.
	Součástí plnění bude dále i navržení či úprava metodiky pro správu identit - jmenné konvence uživatelských jmen a zajištění jejich unikátnosti (sjednocení loginů), - mechanismu práce s hesly (přidělení, změna, samoobslužný reset), - postupy správy uživatelů (zavádění, změny, rušení, nastavování oprávnění), - návrh členění objektů v rámci IDM (osoby, účty, funkce, organizační jednotky, skupiny), - definice bezpečnostních zásad a pravidel pro práci s IDM.
Funkční požadavky	IDM musí udržovat a spravovat kompletní životní cyklus identity. Tedy v typovém případě příchod zaměstnance, jeho založení, přidělení rolí v informačních systémem 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 ((musí být možno kombinovat). Minimálně se jedná o 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)
	Poskytnutá licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit či napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Objednatele (počet záznamů, velikost databází atd.).
	Předpokládaný počet spravovaných identit je až 150.
	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.
	Systém musí být možno nasadit na více serverů v režimu vysoké dostupnosti.
	Integrovaný registr aplikací a agendových/informačních systémů (souhrnně IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby.

Parametr	Popis parametru
	IDM musí udržovat identity, skupiny identit a organizační struktury v databázi. Identity v databázi budou sloužit jako referenční identity pro ostatní informační systémy. Preferováno je využití stávajícího databázového serveru Microsoft SQL Server.
	Integrovaná správa uživatelských rolí, včetně zařazení uživatele do odpovídající role v příslušných IS.
	Integrovaná podpora automatizace – intuitivní tvorba pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo atd.).
	Integrovaná automatizace pro řízení životního cyklu změn identit a schvalování změn musí umožnit minimálně - zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným, - možnost sledování stavu svých požadavků uživateli, - emailové upozornění schvalovatele na požadavek ke schválen, - přehled úloh ke schválení pro každého schvalovatel, - 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 automatizovaných procesů bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý jejich stav. Diagram bude v obvyklém formátu pro zobrazení automatizovaných postupů (workflow) např. aktivity diagram, BPMN nebo Archimate.
	Integrovaná podpora eIDAS 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.
	Správa organizační struktury obsahující interní a externí identity jako samostatných větví struktury.
	Systém umožní přidávání a správu dalších typů referenčních objektů (min. min. systematizované místo, organizační jednotka, skupina, pracovní pozice, funkce, aplikace, skupina aplikací, aplikační role, certifikát) a to i v průběhu zakládání či úpravy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity
	Systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci i těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM.
	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.

Parametr	Popis parametru
	Systém umožní přesun identit mezi jednotlivými organizacemi či jejich odděleními.
	Systém umožní kopírovaní aplikačních rolí, pracovních pozic mezi jednotlivými systematizovanými místy.
	Systém umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů.
	Integrovaná přehledá správa samostatných identifikovatelných objektů – referenčních objektů, na které se identity mohou odkazovat: min. systematizované místo, organizační jednotka, skupina, pracovní pozice, funkce, aplikace, skupina aplikací, aplikační role, certifikát.
	IDM bude obsahovat správu licencí, tj. umožní spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám). Pro schvalování přiřazování licencí bude IDM obsahovat automatizační (workflow) platformu s možností vytvářeni víceúrovňových schvalovacích postupů (workflow).
	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.
	Možnost zobrazení přidělených rolí k jednotlivým identitám s přehledným rozlišením rolí navázaných na systemizované místo, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných na skupinu a delegovaných role.
	IDM musí umožňovat přidělení oprávnění nebo 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 musí umožnit definovat vztahy zastupitelnosti mezi uživateli – musí umožnit uživatelům, aby v souladu se strukturou organizace 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 moc být dočasná, kdy se po nastaveném intervalu nastavená delegace automaticky v IDM zruší.
	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 jednoho uživatele na druhého.

Parametr	Popis parametru
	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 automatizaci (workflow) pro správu životního cyklu osobních údajů subjektu údajů.
	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 umožní autonomní správu hesel (samoobsluha)., tj. bude obsahovat uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele musí být možno provádět pomocí SMS (tj. IDM musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu).
	IDM bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa.
	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.
	IDM bude obsahovat samoobslužné uživatelské rozhraní s konfigurovatelnými registračními formuláři pro registraci externích organizací a jejich identit včetně žádostí o konkrétní aplikační role nebo přiřazení do skupin.
	Samoobslužné rozhraní umožní na úrovní 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.
	Vestavěné obecné komunikační moduly (konektory) pro správu identit v napojených systémech: - konektor pro spouštění CMD příkazů - konektor pro práci s CSV soubory, - konektor pro práci s databází Microsoft SQL, - konektor pro napojení na SOAP webové služby, - konektor pro napojení na REST webové služby, - konektor pro napojení na LDAP server s podporou LDAP v3.
Správa identifikačních prostředků	Automatické hlídání expirace uživatelských doménových, kvalifikovaných a komerčních certifikátů a vyvolání uživatelského průvodce pro jeho jednoduchou automatizovanou uživatelskou obnovu podle nastavených politik.
	Autentizace uživatele v operačních systémech Windows včetně RDS (Remote Desktop Services) všech verzích aktuálně podporovaných výrobcem Microsoft.
	Uživatelská správa uložených certifikátů a bezpečnostních údajů (PIN, QPIN, PUK atd.).
	Export / import certifikátů/klíčů, z/na identifikační prostředek, smazání certifikátů nebo privátního klíče, od/registrace certifikátu ve Windows, testování integrity a použitelnosti.
	Automatizované předávání veřejných klíčů doménových certifikátů do stávajícího systému Microsoft Active Directory.

Parametr	Popis parametru
	Podpora kontaktních, bezkontaktních i hybridních identifikačních prostředků.
	Evidence zejména: - typ prostředku (kontaktní, bezkontaktní, hybridní), - druh prostředku (uživatelský, administrační, operátorský), - stav prostředku (používaný, k recyklaci, skartovaný), - historii prostředku (datum zavedení do evidence, vydání uživateli, recyklace), - držitele prostředku (aktuálního držitele i všechny předchozí držitele), - data uložená v prostředku (certifikáty a další data, včetně historie dat).
	Napojení na Active Directory (zdroj dat o uživatelích, autentizace uživatelů, řízení rolí podle členství ve skupinách) a interní certifikační autoritu (certifikáty).
	Správa certifikátů (doménových i kvalifikovaných) ve webovém prostředí systému: - vydávání (ukládání) certifikátů na identifikační prostředek, vytvoření a tisk protokolu o vystavení, - odvolání certifikátu, - vydávání "v zastoupení" - např. personalista vydá novému zaměstnanci identifikační prostředek včetně certifikátu zaměstnance, - včasné (konfigurovatelné) e-mailové upozornění na vypršení platnosti certifikátu.
	Systém musí umožnit použití jakékoliv certifikačních autority od kvalifikovaných poskytovatelů certifikačních služeb (https://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx).
	Recyklace identifikačních prostředků s pevným i náhodným PIN/PUK, změna uživatele, odblokování PIN (i vzdálené), tisk protokolů.
	Integrované aktivní aplikační rozhraní (API) pro bezpečné (autorizované) poskytování veřejných informací o uložených prostředcích, certifikátech a kvalifikovaných elektronických pečetí pro systémy třetích stran včetně dokumentace.
Požadavky na reporty a přehledy	Zobrazení rolí přidělených k jednotlivým identitám s přehledným rozlišením rolí navázaných na systemizované místo, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných na skupinu a delegovaných role.
	IDM umožní evidenci a přehledné souhrnné zobrazení všech rolí včetně informace, odkud uživatel roli zdědil (z organizační jednotky, systematizovaného místa, skupiny) nebo zda a odkud má nějakou roli od někoho delegovánu.
	Vestavěná detailní databázové 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 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, pracovních pozic / funkcí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti. Identity pro generování auditního reporty musí být možné vybrat (filtrovat) dle libovolných atributů identity včetně přidružených referenčních objektů.
	IDM umožní sledovat jednotlivé stavy (počty objektů/identit) v průběhu synchronizace.
	IDM bude obsahovat přehled uživatelů aktuálně pracujících se systémem.

Parametr	Popis parametru
	Vestavěný export zobrazených přehledů a seznamů do souborů CSV nebo obdobného strojově zpracovatelného a současně běžně čitelného formátu.
	Reporty bude možné zasílat automaticky e-mailem na základě konfigurovatelných pravidel.
	Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení.
	Snadné porovnání změn mezi vygenerovanými reporty stejného typu přímo v uživatelském/administrátorském rozhraní
	IDM umožní zobrazit kompletní popis napojených informačních systémů (vzájemných vazeb, typů synchronizací apod.). přímo u jednotlivých synchronizovaných IS z administrace IDM.
	Kumulovaný online přehled o aktuálním stavu hlavních částí systému a případných chybách – min. chyby běhu synchronizací, generování a odesílání notifikací, volání webových služeb, plánovaných úloh a běhu automatizovaných úloh.
Upozornění	IDM zajistí zasílání konfigurovatelných e-mailových upozornění min. pro následující události: vytvoření a změna identity, referenčního objektu (systematizované místo, organizační jednotka, skupina, pracovní pozice / funkce, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu.
	Upozornění na vypršení časových termínů musí být možno zasílat v předstihu. Velikost předstihu (např. počet dnů) musí být možno konfigurovat pro každý typ upozornění samostatně.
	Systém upozornění bude obsahovat správu šablon. 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.
	Pro zasílání jednotlivých typů upozornění bude možno konfigurovat kontext, resp. podmínky, za jakých bude upozornění zasláno. V konfiguraci bude možné využít atributů identit a referenčních objektů. Např. notifikace budou generovány pouze pro identity v konkrétních uvedených skupinách, které mají uvedenu konkrétní aplikační role a konkrétní atribut atd.
Rozhraní	IDM musí obsahovat grafické uživatelské rozhraní portálového typu funkční v obvyklých webových prohlížečích (Edge, Chrome, Firefox, Safari) bez potřeby instalace doplňku do prohlížeče, které bude sloužit uživatelům pro využívání systému i administrátorů pro jeho správu.
	Rozhraní bude implementováno s responzivním designem – přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno (stolní počítač, notebook, tablet, smart telefon).
	Zobrazení organizační struktury je požadováno v přehledné stromové struktuře, s možností vyhledávání identit / uživatelských účtů a seskupování / rozklikávání struktury až do úrovně jednotlivých uživatelských účtů (identit). Musí být možné oddělit jednotlivé stromy identity, např. interní / externí.
	Vyhledávání i bez diakritiky (např. zadání Parizek vyhledává i Pařízek apod.)
	Integrovaný filtrovací nástroj pro vyhledávání identit a referenčních identit. Možnost filtrování libovolných atributů identity včetně přidružených referenčních objektů. Možnost uložení filtrů pro opakované použití.

Parametr	Popis parametru
Logy	Řešení musí umožňovat publikovat kopie logů do externího systému určeného pro sběr logů typu SIEM (Security Information and Event Management), log manažer apod.
	Systém bude obsahovat logování min. následujících typů událostí: - události systému (aplikační log), - změny entit evidovaných systémem a změny konfigurace systému (auditní log), - synchronizace s napojenými systémy (synchronizační log) včetně volání webových služeb, - odeslané notifikace a upozornění (notifikační log).
	Veškeré změny vyvolané požadavky uživatelů a administrátorů/správců IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu.
	Pro zajištění důvěryhodnosti logů bude možné veškeré požadavky na změny v IDM zadávat výhradně prostřednictvím uživatelského či administrátorského rozhraní. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV atd. – z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM.
Administrace	Došlo-li v systému k některému z chybových stavů (např. synchronizovaný systém ve stavu chyba), bude po přihlášení do IDM administrátor na tuto skutečnost upozorněn. Toto upozornění musí být zřetelné a výrazné (např. barevné podbarvení části aplikace (např. menu), pop-up okno oznamující chybový stav, centrální dashboard aplikace apod.). Z notifikace musí být zřetelné, která část IDM je chybovém stavu.
	Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (lépe hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity apod.)
	Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů
	Možnost delegování administrátorských práv.
	Oprávnění přidělovaná uživatelům a správcům bude možné definovat a přidělovat pro jednotlivé části systému (identity, referenční objekty, notifikace, synchronizace, konfigurace systému, reporty, automatizace, webové služby atd.). U jednotlivých částí bude možnost definovat akce, které může uživatel s přidělenými oprávnění v konkrétní části IDM provádět.
	Pro identity a referenční objekty bude možné definovat oprávnění k jejich atributům včetně možností zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti nastavení/vyplnění atributu, pořadí zobrazení atributů.
	Na úrovní organizační jednotky bude možné pro výběr a přiřazování rolí nastavit sady povolených aplikační rolí, skupiny, pracovních pozic, systematizovaných míst dostupných pro identity z dané organizační jednotky.
	Integrovaný ochranný mechanismus zabránění hromadným změnám např. z důvodu chybných dat na vstupu, aby nedošlo k hromadným nežádoucím změnám (např. smazání objektů v Active Directory). Tato funkcionalita umožní při větším počtu změn zastavit frontu změn a upozornit administrátora IDM emailem a zapsat tuto informaci do logu IDM. Tato vlastnost je požadována pro všechny vstupně/výstupní integrační rozhraní.

Parametr	Popis parametru
	Integrovaná správa 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 požadována možnost výběru organizace, které se mají z IDM synchronizovat s danými systémy.
Webové služby	IDM musí poskytovat rozhraní webových služeb pro programové napojení dalších systémů. Toto rozhraní bude dodáno včetně jeho dokumentace, která bude určena k přímému poskytnutí dalším dodavatelům IT technologií do prostředí objednatele za účelem napojení se na takové rozhraní.
	Webové služby budou definované v rozšířeném standardu WSDL a podporovat SOAP protokol. Součástí dokumentace bude proto i popis řešení webových služeb v podobě XSD. Rozhraní webových služeb a jeho konfigurace musí být součástí plnění na takové úrovni, že napojení nového informačního systému bude možné jen se zapojením administrátora objednatele, který provede konfiguraci rozhraní na straně IDM a dodavatele nového IS, který provede konfiguraci dle dodané dokumentace na straně nového IS (tedy bez nutného zapojení nebo součinnosti dodavatele IDM). Zadavatel připouští možnost výše uvedené služby zajistit i formou ekvivalentního rozsahu realizovaného na bázi http REST služeb definovaných podle OpenAPI standardu (Swagger specifikace), včetně specifikace datových vět pomocí JSON Schema.
	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 informaci o delegaci role, - získání seznamu uživatelů dané aplikace, - získání seznamu pracovních pozic / funkcí přiřazených dané aplikaci, - zápis seznamu rolí uživatele do IDM, - zápis certifikátů do IDM, - zápis a změna identit.
	Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně.
Synchronizace	IDM umožní vstupně/výstupní synchronizace s připojenými informačními systémy. Podporované typy synchronizací (pokud je umožní připojený systém): - plná – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému - jedna identita – synchronizace vybrané identity bez nutnosti pouštět plnou nebo změnovou synchronizaci - změnová – synchronizuje vždy jen změny od poslední spuštěné synchronizace - simulační, který vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn k dispozici jako pohled nebo přehledná souhrnná tabulka - porovnávací – vytvoří porovnávací report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IDM versus nastavení identit a oprávnění přímo v připojeném systému.

Parametr	Popis parametru
	Jednotlivé běhy synchronizací budou logovány. Log plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a informace, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v logu dále informace o události, která změnovou synchronizaci vyvolala.
Integrace	IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. Systémům Microsoft bude IDM vytvářet a spravovat uživatelské účty a jejich oprávnění včetně provádění souvisejících operací potřebných pro automatizaci správy identit v daném systému (zejména. vytváření mailových schránek, úpravy metadat): - Microsoft Active Directory IDM bude integrováno (přímo propojeno) s následujícími systémy, ve který bude přímo řídit vznik/úpravy/zánik identit a jejich oprávnění: - Personální a mzdový IS – FLUX, spol. s r.o., - Docházkový IS – TETRONIK – výrobní družstvo Terezín, družstvo, - Elektronická spisová služba – GEOVAP, spol. s r.o., - Ekonomický IS Proxio (MARBES CONSULTING s.r.o.), - Portál občana – DATRON, a.s., - Vyvolávací systém – Kadlec – elektronika, s.r.o. - Příslušná rozhraní (konektory) na straně IDM budou součástí dodávky.

3 Integrace IDM a migrace dat

3.1 Integrace IDM

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

3.1.2 Příslušná rozhraní (konektory) na straně IDM budou součástí dodávky.

3.1.3 **Personální a mzdový IS (FLUX, spol. s r.o.)** – IDM bude z personálního informačního systému čerpat informace o uživatelích a jejích roli v organizaci. Popis komunikačního rozhraní systému je uveden viz příloha č. 2 této technické dokumentace.

3.1.4 **Docházkový IS (TETRONIK – výrobní družstvo Terezín)** – je požadována integrace za účelem řízení a správy uživatelských účtů v tomto systému, popis komunikačního rozhraní systému je uveden viz příloha č. 2 této technické dokumentace.

3.1.5 **Elektronická spisová služba (GEOVAP, spol. s r.o.)** – je požadována integrace za účelem řízení a správy uživatelských účtů v tomto systému, popis komunikačního rozhraní systému je uveden viz příloha č. 3 této technické dokumentace.

3.1.6 **Ekonomika – Proxio (MARBES CONSULTING s.r.o.)** – je požadována integrace za účelem řízení a správy uživatelských účtů v tomto systému, popis komunikačního rozhraní systému je uveden viz příloha č. 4 této technické dokumentace.

3.1.7 **Vyvolávací systém (Kadlec – elektronika, s.r.o.)** – je požadována integrace za účelem řízení a správy účtů v tomto systému (zaměstnanci MěÚ), popis komunikačního rozhraní systému je uveden viz příloha č. 5 této technické dokumentace.

3.1.8 **Portál občana (DATRON, a.s.)** – je požadována integrace za účelem řízení a správy uživatelských účtů v tomto systému (administrátoři MěÚ), popis komunikačního rozhraní systému je uveden viz příloha č. 4 této technické dokumentace.

3.1.9 **Microsoft Active Directory** – dle specifikace společnosti Microsoft. V prostředí objednatele bude v době dodávky IDM provozováno doménové prostředí Windows Server 2012, v blízké budoucnosti bude prostředí AD migrováno na Windows Server 2019.

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

3.2 Migrace dat

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

4 Implementace IDM

4.1 Dokumentace skutečného provedení

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

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

- návrh řešení instalace IDM (architektura technického řešení),
- detailní popis nastavení / konfigurace / parametrizace jednotlivých oblastí (společné registry, role a přístupová oprávnění, číselníky, reporty atd.),
- návrh technického řešení integračních vazeb (vazby mezi subsystémy, vazby s vybranými aplikacemi objednatele, vazby se spolupracujícími centrálními systémy),
- návrh řešení postupu a pořadí při nasazování jednotlivých oblastí – zohlednění v harmonogramu projektu,
- popis případných organizačních opatření nutných pro implementaci (např. pracovní schůzky),
- upřesnění časového harmonogramu projektu,
- forma a místo zaškolení IT administrátorů systému na dodané řešení v prostorách MěÚ,
- rozsah součinnosti ze strany objednatele,
- návrh průběhu testovacího provozu.

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

4.1.4 Bez předložení dokumentace skutečného provedení v prostředí objednatele nebude umožněno zhotoviteli instalovat a implementovat informační systém do určeného prostředí. Předložení dokumentace je povinností zhotovitele a v případě jejího nepředložení a z tohoto důvodu neumožnění implementace informačního systému do definovaného prostředí se bude jednat o prodlení na straně zhotovitele.

4.1.5 Na základě nasazení informačního systému bude dokumentace aktualizována na skutečně nasazené řešení a bude k ní zpracováno technologické schéma dodávaného řešení.

4.2 Instalace IDM

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

4.2.2 Veškeré softwarové komponenty a databáze poběží ve virtualizovaném prostředí objednatele. Licence virtualizace poskytne objednatel. Jedná se o jednotnou platformu virtualizace provozovanou objednatelem v jeho serverovém prostředí Hyper-V. Dále objednatel poskytne pro provoz IDM licenci Windows Server 2019 Datacenter. V případě, že se zhotovitel rozhodne neužít nabízenou licenci operačního systému musí v rámci své dodávky dodat i odpovídají licence operačního systému k provozu nad virtualizovanou platformou objednatele. Veškeré další potřebné licence software potřebného pro běh IDM musí v rámci své dodávky zajistit zhotovitel.

4.2.3 Pro provoz IDM budou v prostředí objednatele vyčleněny tyto systémové prostředky, které budou pro provoz IDM alokovány po dobu min. 5 let a které musí zhotovitel garantovat, že budou po celou uvedenou dobu naprosto dostatečné, tedy, že za účelem optimálního běhu řešení IDM nebude minimálně po tuto dobu zhotovitel po objednateli požadovat navýšení takových systémových prostředků:

- 2 procesorová jádra,
- 12 GB RAM,
- 500 GB diskového prostoru,
- 1 Gbit síťová karta.

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

4.3 Konfigurace dodaného řešení pro potřeby objednatele

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

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

5 Dokumentace

5.1 Forma dokumentace

5.1.1 Objednatel požaduje dodávku dokumentace v rozsahu dle tohoto článku v elektronické podobě v českém jazyce, nejpozději do dne akceptace díla, není-li uvedeno nebo nevyplývá-li z jednotlivého typu dokumentace jinak.

5.1.2 Dokumentace musí být dodána v takové podobě a formátu, aby byla připravena bez potřeby jakýchkoliv dalších úprav k tisku.

5.2 Dokumentace skutečného provedení v prostředí objednatele

5.2.1 Bude sloužit jako podklad pro implementaci řešení do prostředí objednatele. Bude zpracována minimálně v rozsahu dle kap. 4.1 tohoto dokumentu.

5.3 Uživatelská dokumentace

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

5.4 Administrátorská dokumentace

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

6 Harmonogram

6.1 Harmonogram s časovými požadavky objednatele

6.1.1 Objednatel požaduje realizaci předmětu plnění dle následujícího harmonogramu. Harmonogram je sestaven tak, aby jednotlivé práce na sebe logicky navazovaly a zároveň byl v souladu s požadavky dotační žádosti objednatele do IROP.

6.1.2 S ohledem na možnost kontroly realizace díla z pohledu času (tj. dílčí vyhodnocování dodržování harmonogramu realizace) je harmonogram doplněn milníky. Započetí každého milníku je možné pouze za předpokladu, že bude provedena akceptace všech milníků předcházejících.

Aktivita projektu	Doba trvání
Zpracování dokumentace skutečného provedení.	2 týdny
Připomínkování dokumentace skutečného provedení ze strany objednatele.	1 týden
Vypořádání připomínek a finalizace dokumentace skutečného provedení.	1 týden
Milník číslo 1 – Finální návrh Dokumentace skutečného provedení.	Nejpozději do T + 4 týdny
Instalace systému.	2 týdny
Provedení integračních vazeb.	8 týdny
Nastavení, konfigurace a parametrizace jednotlivých oblastí SW, včetně nastavení přístupových oprávnění.	
Milník číslo 2 – Připravené prostředí pro testovací provoz	Nejpozději do T + 14 týdnů
Dodávka dokumentace.	1 týden
Prezenční zaškolení IT administrátorů systému na dodané řešení	2 týdny
Testovací provoz se zvýšeným dohledem a podporou ze strany dodavatele s možností identifikace a opravy případných chyb a neshod.	3 týdny
Akceptační řízení.	
Milník číslo 3 – Akceptace projektu, předání systému do rutinního provozu.	Nejpozději do T + 20 týdnů

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

6.2 Konkretizovaný harmonogram plnění ze strany zhotovitele

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

- zpracování specifických požadavků objednatele na konkrétní způsob nasazení IDM a zpracování implementačního plánu, tj. Dokumentace skutečného provedení a podrobného harmonogramu s uvedením potřebné součinnosti ze strany objednatele,

- implementace IS do prostředí objednatele,
- předání dokumentace a testovací provoz,
- akceptace, předání systému a následný pilotní a ostrý provoz.

6.3 Testovací provoz

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

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

6.3.3 Během testovacího provozu provede zhotovitel aktualizaci Dokumentace skutečného provedení.

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

6.3.5 Testovacímu provozu bude předcházet zaškolení IT administrátorů systému na dodané řešení v prostorách MěÚ v rozsahu do 6 hodin.

7 Projektové řízení

7.1.1 S ohledem na rozsah projektu a dopad jeho zavedení do produkčního provozu na výkon činnosti objednatele je v rámci dodávky předmětu plnění objednatelem požadováno aplikování základních principů projektového řízení ze strany zhotovitele.

7.1.2 Jedná se zejména řízení projektových prací v souladu s uzavřenou smlouvu s ohledem na věcné plnění dané smlouvou objednatele – rozsah, posloupnost a hloubku projektových prací, (tj. harmonogramu) – řízení postupu prací s ohledem na závazný harmonogram projektu – dodržování termínů a milníků harmonogramu, podchycení případných kolizí, zpoždění nebo vznikajících rizik a jejich reportování směrem k objednateli, aktivní řešení výše uvedených nestandardních situací

7.1.3 Zpracování pravdivých, úplných a věcně jasných a vypovídajících zápisů z konzultačních schůzek a pracovních jednání (s cílem zaznamenání klíčových rozhodnutí, ujednání, navržených nebo dohodnutých způsobů řešení dílčích částí projektu atd.)

7.1.4 Prezenční účast odpovědné osoby zhotovitele na kontrolních dnech v pravidelných min. měsíčních intervalech v sídle objednatele, případně se souhlasem obou smluvních stran formou videokonference nebo telekonference.

7.1.5 Reporting projektu na úrovni pravidelných dvoutýdenních písemných zpráv směrem k odpovědné osobě objednatele (seznam prací, které byly poskytovatelem vykonány pro danou část projektu, stav těchto prací (ukončeno, odloženo, v realizaci); popis vzniklých problémů a způsob jejich řešení).

7.1.6 Řízení rizik projektu, hodnocení pravděpodobnosti jejich výskytu a míry dopadu, návrh řešení k jejich eliminaci.

7.1.7 Řízení změn na projektu, v případě požadavků na změnu v projektu provedení konzultací k ověření nutnosti změny projektu; zjištění dopadu požadovaných změn směrem ke koncepci celkového řešení, harmonogramu, dotačnímu titulu, vytížení lidských zdrojů atd. V případě odsouhlasení změn spolupráce při implementaci změn do projektu, komunikace s poskytovateli a s realizačním týmem.

8 Legislativa

Níže je obsažený obecný přehled legislativy, kterou je potřeba dodržet v souladu s realizací předmětu plnění této technické dokumentace. Tento výčet není konečný ani všeobjímající a má za cíl rámcově upozornit zhotovitele na rozsah problematiky, kterou se v návaznosti na jednotlivé požadované funkcionality zavazuje dodržet, a u níž se tedy zavazuje objednateli zajistit soulad s platnou legislativou. Dílčí legislativní požadavky a odkazy na právní akty jsou obsaženy i v dalších dílčích částech této dokumentace a jejích přílohách.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.
Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.
Vyhláška NBÚ a Ministerstva vnitra ČR č. 317/2014 Sb., významných informačních systémech a jejich určujících kritérií, ve znění pozdějších předpisů.
Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů.
Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, v platném znění.
Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27.dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

9 Akceptace

9.1 Dílčí akceptační řízení

9.1.1 Dílčí akceptační řízení bude provedeno pro milník 1 a 2 vyznačený v harmonogramu projektu dle této technické dokumentace. Dílčí akceptační řízení bude zahrnovat porovnání skutečného stavu vůči požadavkům této technické dokumentace a jejím přílohám (milník číslo 1 a 2) a požadavků daných dokumentací skutečného provedení (milník 2).

9.1.2 Výsledkem dílčího akceptačního řízení je akceptační protokol s výsledkem Splněno nebo Nesplněno, podepsaný oprávněnými osobami smluvních stran.

9.1.3 Započetí dalších prací spadajících pod milník následující je možné pouze za předpokladu, že bude provedena akceptace s výsledkem Splněno všech milníků předcházejících.

9.2 Souhrnné akceptační řízení – akceptace díla

9.2.1 Souhrnné akceptační řízení bude zahrnovat:

- ověření splnění akceptace všech milníků, které akceptaci plnění předcházeli.
- porovnání skutečného stavu vůči požadavkům smlouvy o dílo a této technické dokumentace, která je její přílohou, a jejích příloh, funkčního i nefunkčního charakteru – licence a příslušenství.

9.2.2 Výsledkem souhrnného akceptačního řízení je akceptační protokol s výsledkem Splněno / Splněno s výhradou / Nesplněno, podepsaný oprávněnými osobami smluvních stran.

9.3 Opakované akceptační řízení

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

Seznam zkratek

Zkratka	Význam
BPMN	Business Process Modelling Notation
CMD	Command
CSV	Comma Separated Value
ČR	Česká republika
ES	Evropská společenství
EU	Evropská unie
GB	Gigabyte
IDM	Identity Management
IROP	Integrovaný regionální operační program
IS	Informační systém
IT	Informační technologie
JIP	Jednotný identitní prostor
KAAS	Katalog autentizačních a autorizačních služeb
LDAP	Lightweight Directory Access Protocol
NBÚ	Národní bezpečnostní úřad
RAM	Random Access Memory
REST	Representational State Transfer
SIEM	Security Information and Event Management
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
WSDL	Web Services Description Language
XML	Extensible Markup Language
XMS	XML Message Server
XSD	XML Schema

Přílohy

Příloha 1 – Popis rozhraní na personální a mzdový IS (FLUX, spol. s r.o.)

*Příloha je tvořena samostatným souborem **Popis-rozhrani-PAM.PDF***

Příloha 2 – Popis rozhraní na docházkový IS (TETRONIK – výrobní družstvo Terezín)

*Příloha je tvořena samostatným souborem **Popis-rozhrani-DOCHAZKA.PDF***

Příloha 3 – Popis rozhraní na elektronickou spisovou službu (GEOVAP, spol. s r.o.)

*Příloha je tvořena samostatným souborem **Popis-rozhrani-eSSL.PDF***

Příloha 4 – Popis rozhraní na ekonomický IS Proxio (MARBES CONSULTING s.r.o.)

*Příloha je tvořena samostatným souborem **Popis-rozhrani-Proxio.ZIP***

Příloha 5 – Popis rozhraní na portál občana (DATRON, a.s.)

*Příloha je tvořena samostatným souborem **Popis-rozhrani-Portal.PDF***

Příloha 6 – Popis rozhraní na vyvolávací systém (Kadlec – elektronika, s.r.o.)

*Příloha je tvořena samostatným souborem **Popis-rozhrani-VYVOLAVACI.PDF***

Příloha č. 1 Zadávací dokumentace – Technická dokumentace zadavatele

Příloha č. 1 Smlouvy o dílo – Technická dokumentace

Technická dokumentace

Identity Management pro město Neratovice

verze 05 z 31.07.2024

Obsah

1 Úvod

1.1.1 **Tento dokument je určen k popisu a definici rozsahu díla, dodávek a služeb, které objednatel poptává jako předmět plnění ve veřejné zakázce** s **názvem „Identity Management pro město** Neratovice**".**

1.1.2 **Předmětem této dokumentace je popis a stanovení požadavků objednatele na** dodávku a implementaci identity managementu a zpracování dokumentace.

1.2 Popis plnění podle této technické dokumentace

1.2.1 **Předmětem plnění této** technické dokumentace je dodávka a implementace identity managementu pro **Město** Neratovice**, a to včetně nedílně souvisejících požadavků typu** dodání licencí a zpracování dokumentace.

1.2.2 **Předmětem díla jsou následující činnosti zhotovitele:**

- dodávka licencí, implementace identity managementu**, testovací provoz a předání** do **řádného užívání.**

1.2.3 **Pro výše uvedený rozsah plnění**:

- **provedení integrací na další systémy v prostředí objednatele i mimo něj**,
- **úprava dodaného řešení dle potřeb a požadavků dle pokynů objednatele**.

1.2.4 **Dále je předmětem plnění dodávka**

- dokumentace k **dodanému plnění v požadovaném rozsahu**,
- **dalších licencí potřebných pro provoz** identity managementu,
- **listinného potvrzení dodaných licencí co do jejich počtu a rozsahu**.

2 Základní požadavky na IDM

2.1.1 Předmětem dodávky je nasazení sjednocujícího řešení pro správu identit, uživatelských rolí a případně i oprávnění uživatelů, včetně jejich evidence, v prostředí objednatele.

2.1.2 IDM zajistí centrální a jednoduchou správu identity, uživatelských rolí a případně i oprávnění uživatelů v aplikacích a informačních systémech, u kterých bude provedena integrace na takové IDM.

2.1.3 Cílem je zefektivnit a automatizovat proces řízení identit v organizaci a zavést centrální platformu pro řízení identit v organizaci – IDM (Identity Management Systém). IDM umožní automatizovaně spravovat identity (osoby, uživatelské role a oprávnění) ve vybraných hlavních systémech organizace, a to zejména v návaznosti na personální systém a adresářové služby. Cílem je rovněž zavést samoobslužné procesy pro zadávání žádostí o oprávnění a přístupů samostatnými koncovými uživateli organizace. V rozšířeném IDM, na rozdíl od řešení stávajícího, bude následně možné takovéto požadavky schválit a změny nastavení u identit automatizovaně předat (vypublikovat) do připojených systémů (integrovaných aplikací).

2.1.4 Systém Identity management bude spravovat a řídit identity (uživatele, jejich uživatelské účty a oprávnění) v rámci připojených systémů. Pro unifikovanou správu identit v systémech organizace je nutné vybudování jednotné centrální evidence uživatelů, uživatelských účtů a oprávnění uživatelů k integrovaným aplikacím. Tato evidence je spravována centrálně v systému IDM v návaznosti na centrální službu JIP/KAAS.

2.1.5 Současně s nasazením IDM bude potřeba konsolidovat a standardizovat procesy související s personálními obměnami v organizaci (nový zaměstnanec, odchod zaměstnance, zařazení zaměstnance na pozici, změna pozice zaměstnance a další) v této souvislosti s vývojem jejich identity (zejména nabývání a ztráta oprávnění do vybraných aplikací a informačních systémů), případně procesy existující v IDM zohlednit. Na základě takových procesů ze zdrojových systémů (personální systém) vstupují do IDM údaje o osobách, uživatelských účtech, zařazení v organizační struktuře, přiřazení pracovního místa, přiřazení do skupin atd.

2.1.6 Součástí nasazení takového řešení bude i vytvoření systematizovaných pracovních míst, 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.

2.1.7 Součástí nasazovaného řešení bude nástroj správy identifikačních prostředků, který rozšíří autentizační systém a zajistí řízené a evidované vystavení a přidělení identifikačního prostředku uživatelům včetně odpovídajících certifikátů. Nástroj zajistí podporu a evidenci operací spojených s užíváním identifikačního prostředku a uložených certifikátů (odvolání certifikátu, obnova certifikátu atd.) a s ukončením jejich užívání (odstranění certifikátů, reinicializace prostředku atd.). Součástí bude automatické hlídání platnosti certifikátů, upozornění uživatelů na vypršení platnosti a průvodce uživatele pro jednoduché samostatné prodloužení certifikátu (resp. vystavení a uložení nového), pokud bude mít uživatel přidělena odpovídající oprávnění.

2.1.8 IDM bude mít provedenou vazbu na Jednotný identitní prostor (JIP) a Katalog autentizačních a autorizačních služeb (KAAS) se kterými bude spolupracovat, a to do plného rozsahu těchto IS ve vztahu k povaze objednatele jako orgánu vykonávajícímu přenesenou i samostatnou působnost pro územní samosprávný celek.

2.1.9 Systém IDM bude reflektovat veškeré potřebné změny související s životním cyklem identity v prostředí objednatele a ve vazbě na všechny na IDM napojené informační systémy, ve kterých bude mít daná identita uživatelské role a oprávnění. Takové změny budou reflektovány ve všech aktuálně napojených informačních systémech vždy v konkrétní rozhodné době.

2.1.10 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 rolí. IDM bude provádět správu automaticky, tak aby byly spravované systémy vždy aktuální.

2.1.11 IDM bude dále realizováno při naplňování nových legislativních požadavků. V případě tohoto plnění zejména s dopady Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Minimálně zajistí:

- zajišťuje auditní záznamy oprávnění uživatelů a poskytuje reporty o stavu

2.1.12 IDM a jeho funkcionality musí respektovat standardní architekturu IS v prostředí objednatele a pro svou integraci využít standardizovaná rozhraní a existující prostředky IS.

2.1.13 Součástí plnění bude dále i navržení metodiky pro správu identit

- jmenné konvence uživatelských jmen a zajištění jejich unikátnosti (sjednocení loginů),
- mechanismu práce s hesly (přidělení, změna, samoobslužný reset apod.),
- postupy správy uživatelů (zavádění, změny, rušení, nastavování oprávnění apod.),
- návrh členění objektů v rámci IDM (osoby, účty, funkce, organizační jednotky, skupiny),
- definice bezpečnostních zásad a pravidel pro práci s IDM.

2.2 Funkcionality IDM

Uchazeč nabízí následující softwarové produkty včetně veškerých požadovaných služeb:

- ProID moduly pro plnění požadavku *Správa identifikačních prostředků*:
  - Card Management System (max. 250 uživatelů)
  - Kartové centrum - 1 instance
  - ACEx (max. 250 uživatelů)
- IDM systém AC Identita s požadovanými konektory pro plnění všech ostatních požadavků (bez omezení počtu uživatelů)

Parametr	Popis parametru
	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.

Parametr	Popis parametru
	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 rolí a oprávnění. IDM bude provádět správu automaticky, tak aby byly spravované systémy vždy aktuální.
	IDM bude dále realizováno při naplňování nových legislativních požadavků. V případě tohoto plnění zejména s dopady Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), tj. IDM zajistí auditní záznamy oprávnění uživatelů a umožní reporting stavu těchto oprávnění.
	IDM a jeho funkcionality musí respektovat standardní architekturu IS v prostředí objednatele a pro svou integraci využít standardizovaná rozhraní a existující prostředky IS.
	IDM bude ukládat data do databáze Microsoft SQL.
	IDM bude komunikovat v českém jazyce.
	Součástí plnění bude dále i navržení či úprava metodiky pro správu identit - jmenné konvence uživatelských jmen a zajištění jejich unikátnosti (sjednocení loginů), - mechanismu práce s hesly (přidělení, změna, samoobslužný reset), - postupy správy uživatelů (zavádění, změny, rušení, nastavování oprávnění), - návrh členění objektů v rámci IDM (osoby, účty, funkce, organizační jednotky, skupiny), - definice bezpečnostních zásad a pravidel pro práci s IDM.
Funkční požadavky	IDM musí udržovat a spravovat kompletní životní cyklus identity. Tedy v typovém případě příchod zaměstnance, jeho založení, přidělení rolí v informačních systémem 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 ((musí být možno kombinovat). Minimálně se jedná o 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)
	Poskytnutá licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit či napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Objednatele (počet záznamů, velikost databází atd.).
	Předpokládaný počet spravovaných identit je až 150.

Parametr	Popis parametru
	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.
	Systém musí být možno nasadit na více serverů v režimu vysoké dostupnosti.
	Integrovaný registr aplikací a agendových/informačních systémů (souhrnně IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby.
	IDM musí udržovat identity, skupiny identit a organizační struktury v databázi. Identity v databázi budou sloužit jako referenční identity pro ostatní informační systémy. Preferováno je využití stávajícího databázového serveru Microsoft SQL Server.
	Integrovaná správa uživatelských rolí, včetně zařazení uživatele do odpovídající role v příslušných IS.
	Integrovaná podpora automatizace – intuitivní tvorba pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo atd.).
	Integrovaná automatizace pro řízení životního cyklu změn identit a schvalování změn musí umožnit minimálně - zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným, - možnost sledování stavu svých požadavků uživateli, - emailové upozornění schvalovatele na požadavek ke schválen, - přehled úloh ke schválení pro každého schvalovatel, - 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 automatizovaných procesů bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý jejich stav. Diagram bude v obvyklém formátu pro zobrazení automatizovaných postupů (workflow) např. aktivity diagram, BPMN nebo Archimate.
	Integrovaná podpora eIDAS 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.
	Správa organizační struktury obsahující interní a externí identity jako samostatných větví struktury.
	Systém umožní přidávání a správu dalších typů referenčních objektů (min. min. systematizované místo, organizační jednotka, skupina, pracovní pozice, funkce, aplikace, skupina aplikací, aplikační role, certifikát) a to i v průběhu zakládání či úpravy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity

Parametr	Popis parametru
	Systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci i těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM.
	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 kopírovaní aplikačních rolí, pracovních pozic mezi jednotlivými systematizovanými místy.
	Systém umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů.
	Integrovaná přehledá správa samostatných identifikovatelných objektů – referenčních objektů, na které se identity mohou odkazovat: min. systematizované místo, organizační jednotka, skupina, pracovní pozice, funkce, aplikace, skupina aplikací, aplikační role, certifikát.
	IDM bude obsahovat správu licencí, tj. umožní spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám). Pro schvalování přiřazování licencí bude IDM obsahovat automatizační (workflow) platformu s možností vytvářeni víceúrovňových schvalovacích postupů (workflow).
	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.
	Možnost zobrazení přidělených rolí k jednotlivým identitám s přehledným rozlišením rolí navázaných na systemizované místo, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných na skupinu a delegovaných role.
	IDM musí umožňovat přidělení oprávnění nebo 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 musí umožnit definovat vztahy zastupitelnosti mezi uživateli – musí umožnit uživatelům, aby v souladu se strukturou organizace 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 moc být dočasná, kdy se po nastaveném intervalu nastavená delegace automaticky v IDM zruší.

Parametr	Popis parametru
	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 jednoho uživatele na druhého.
	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 automatizaci (workflow) pro správu životního cyklu osobních údajů subjektu údajů.
	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 umožní autonomní správu hesel (samoobsluha)., tj. bude obsahovat uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele musí být možno provádět pomocí SMS (tj. IDM musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu).
	IDM bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa.
	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.
	IDM bude obsahovat samoobslužné uživatelské rozhraní s konfigurovatelnými registračními formuláři pro registraci externích organizací a jejich identit včetně žádostí o konkrétní aplikační role nebo přiřazení do skupin.
	Samoobslužné rozhraní umožní na úrovní 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.
	Vestavěné obecné komunikační moduly (konektory) pro správu identit v napojených systémech: - konektor pro spouštění CMD příkazů - konektor pro práci s CSV soubory, - konektor pro práci s databází Microsoft SQL, - konektor pro napojení na SOAP webové služby, - konektor pro napojení na REST webové služby, - konektor pro napojení na LDAP server s podporou LDAP v3.
Správa identifikačních prostředků	Automatické hlídání expirace uživatelských doménových, kvalifikovaných a komerčních certifikátů a vyvolání uživatelského průvodce pro jeho jednoduchou automatizovanou uživatelskou obnovu podle nastavených politik.

Parametr	Popis parametru
	Autentizace uživatele v operačních systémech Windows včetně RDS (Remote Desktop Services) všech verzích aktuálně podporovaných výrobcem Microsoft.
	Uživatelská správa uložených certifikátů a bezpečnostních údajů (PIN, QPIN, PUK atd.).
	Export / import certifikátů/klíčů, z/na identifikační prostředek, smazání certifikátů nebo privátního klíče, od/registrace certifikátu ve Windows, testování integrity a použitelnosti.
	Automatizované předávání veřejných klíčů doménových certifikátů do stávajícího systému Microsoft Active Directory.
	Podpora kontaktních, bezkontaktních i hybridních identifikačních prostředků.
	Evidence zejména: - typ prostředku (kontaktní, bezkontaktní, hybridní), - druh prostředku (uživatelský, administrační, operátorský), - stav prostředku (používaný, k recyklaci, skartovaný), - historii prostředku (datum zavedení do evidence, vydání uživateli, recyklace), - držitele prostředku (aktuálního držitele i všechny předchozí držitele), - data uložená v prostředku (certifikáty a další data, včetně historie dat).
	Napojení na Active Directory (zdroj dat o uživatelích, autentizace uživatelů, řízení rolí podle členství ve skupinách) a interní certifikační autoritu (certifikáty).
	Správa certifikátů (doménových i kvalifikovaných) ve webovém prostředí systému: - vydávání (ukládání) certifikátů na identifikační prostředek, vytvoření a tisk protokolu o vystavení, - odvolání certifikátu, - vydávání "v zastoupení" - např. personalista vydá novému zaměstnanci identifikační prostředek včetně certifikátu zaměstnance, - včasné (konfigurovatelné) e-mailové upozornění na vypršení platnosti certifikátu.
	Systém musí umožnit použití jakékoliv certifikačních autority od kvalifikovaných poskytovatelů certifikačních služeb (https://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx).
	Recyklace identifikačních prostředků s pevným i náhodným PIN/PUK, změna uživatele, odblokování PIN (i vzdálené), tisk protokolů.
	Integrované aktivní aplikační rozhraní (API) pro bezpečné (autorizované) poskytování veřejných informací o uložených prostředcích, certifikátech a kvalifikovaných elektronických pečetí pro systémy třetích stran včetně dokumentace.
Požadavky na reporty a přehledy	Zobrazení rolí přidělených k jednotlivým identitám s přehledným rozlišením rolí navázaných na systemizované místo, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných na skupinu a delegovaných role.
	IDM umožní evidenci a přehledné souhrnné zobrazení všech rolí včetně informace, odkud uživatel roli zdědil (z organizační jednotky, systematizovaného místa, skupiny) nebo zda a odkud má nějakou roli od někoho delegovánu.
	Vestavěná detailní databázové historizace pro evidenci změn identit včetně referenčních objektů a vazeb mezi nimi. Historizace poskytne data v libovolném časovém okamžiku – aktuálním nebo zpětně v minulosti.

Parametr	Popis parametru
	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, pracovních pozic / funkcí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti. Identity pro generování auditního reporty musí být možné vybrat (filtrovat) dle libovolných atributů identity včetně přidružených referenčních objektů.
	IDM umožní sledovat jednotlivé stavy (počty objektů/identit) v průběhu synchronizace.
	IDM bude obsahovat přehled uživatelů aktuálně pracujících se systémem.
	Vestavěný export zobrazených přehledů a seznamů do souborů CSV nebo obdobného strojově zpracovatelného a současně běžně čitelného formátu.
	Reporty bude možné zasílat automaticky e-mailem na základě konfigurovatelných pravidel.
	Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení.
	Snadné porovnání změn mezi vygenerovanými reporty stejného typu přímo v uživatelském/administrátorském rozhraní
	IDM umožní zobrazit kompletní popis napojených informačních systémů (vzájemných vazeb, typů synchronizací apod.). přímo u jednotlivých synchronizovaných IS z administrace IDM.
	Kumulovaný online přehled o aktuálním stavu hlavních částí systému a případných chybách – min. chyby běhu synchronizací, generování a odesílání notifikací, volání webových služeb, plánovaných úloh a běhu automatizovaných úloh.
Upozornění	IDM zajistí zasílání konfigurovatelných e-mailových upozornění min. pro následující události: vytvoření a změna identity, referenčního objektu (systematizované místo, organizační jednotka, skupina, pracovní pozice / funkce, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu.
	Upozornění na vypršení časových termínů musí být možno zasílat v předstihu. Velikost předstihu (např. počet dnů) musí být možno konfigurovat pro každý typ upozornění samostatně.
	Systém upozornění bude obsahovat správu šablon. 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.
	Pro zasílání jednotlivých typů upozornění bude možno konfigurovat kontext, resp. podmínky, za jakých bude upozornění zasláno. V konfiguraci bude možné využít atributů identit a referenčních objektů. Např. notifikace budou generovány pouze pro identity v konkrétních uvedených skupinách, které mají uvedenu konkrétní aplikační role a konkrétní atribut atd.
Rozhraní	IDM musí obsahovat grafické uživatelské rozhraní portálového typu funkční v obvyklých webových prohlížečích (Edge, Chrome, Firefox, Safari) bez potřeby instalace doplňku do prohlížeče, které bude sloužit uživatelům pro využívání systému i administrátorů pro jeho správu.
	Rozhraní bude implementováno s responzivním designem – přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno (stolní počítač, notebook, tablet, smart telefon).

Parametr	Popis parametru
	Zobrazení organizační struktury je požadováno v přehledné stromové struktuře, s možností vyhledávání identit / uživatelských účtů a seskupování / rozklikávání struktury až do úrovně jednotlivých uživatelských účtů (identit). Musí být možné oddělit jednotlivé stromy identity, např. interní / externí.
	Vyhledávání i bez diakritiky (např. zadání Parizek vyhledává i Pařízek apod.)
	Integrovaný filtrovací nástroj pro vyhledávání identit a referenčních identit. Možnost filtrování libovolných atributů identity včetně přidružených referenčních objektů. Možnost uložení filtrů pro opakované použití.
Logy	Řešení musí umožňovat publikovat kopie logů do externího systému určeného pro sběr logů typu SIEM (Security Information and Event Management), log manažer apod.
	Systém bude obsahovat logování min. následujících typů událostí: - události systému (aplikační log), - změny entit evidovaných systémem a změny konfigurace systému (auditní log), - synchronizace s napojenými systémy (synchronizační log) včetně volání webových služeb, - odeslané notifikace a upozornění (notifikační log).
	Veškeré změny vyvolané požadavky uživatelů a administrátorů/správců IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu.
	Pro zajištění důvěryhodnosti logů bude možné veškeré požadavky na změny v IDM zadávat výhradně prostřednictvím uživatelského či administrátorského rozhraní. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV atd. – z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM.
Administrace	Došlo-li v systému k některému z chybových stavů (např. synchronizovaný systém ve stavu chyba), bude po přihlášení do IDM administrátor na tuto skutečnost upozorněn. Toto upozornění musí být zřetelné a výrazné (např. barevné podbarvení části aplikace (např. menu), pop-up okno oznamující chybový stav, centrální dashboard aplikace apod.). Z notifikace musí být zřetelné, která část IDM je chybovém stavu.
	Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (lépe hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity apod.)
	Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů
	Možnost delegování administrátorských práv.
	Oprávnění přidělovaná uživatelům a správcům bude možné definovat a přidělovat pro jednotlivé části systému (identity, referenční objekty, notifikace, synchronizace, konfigurace systému, reporty, automatizace, webové služby atd.). U jednotlivých částí bude možnost definovat akce, které může uživatel s přidělenými oprávnění v konkrétní části IDM provádět.
	Pro identity a referenční objekty bude možné definovat oprávnění k jejich atributům včetně možností zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti nastavení/vyplnění atributu, pořadí zobrazení atributů.

Parametr	Popis parametru
	Na úrovní organizační jednotky bude možné pro výběr a přiřazování rolí nastavit sady povolených aplikační rolí, skupiny, pracovních pozic, systematizovaných míst dostupných pro identity z dané organizační jednotky.
	Integrovaný ochranný mechanismus zabránění hromadným změnám např. z důvodu chybných dat na vstupu, aby nedošlo k hromadným nežádoucím změnám (např. smazání objektů v Active Directory). Tato funkcionalita umožní při větším počtu změn zastavit frontu změn a upozornit administrátora IDM emailem a zapsat tuto informaci do logu IDM. Tato vlastnost je požadována pro všechny vstupně/výstupní integrační rozhraní.
	Integrovaná správa 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 požadována možnost výběru organizace, které se mají z IDM synchronizovat s danými systémy.
Webové služby	IDM musí poskytovat rozhraní webových služeb pro programové napojení dalších systémů. Toto rozhraní bude dodáno včetně jeho dokumentace, která bude určena k přímému poskytnutí dalším dodavatelům IT technologií do prostředí objednatele za účelem napojení se na takové rozhraní.
	Webové služby budou definované v rozšířeném standardu WSDL a podporovat SOAP protokol. Součástí dokumentace bude proto i popis řešení webových služeb v podobě XSD. Rozhraní webových služeb a jeho konfigurace musí být součástí plnění na takové úrovni, že napojení nového informačního systému bude možné jen se zapojením administrátora objednatele, který provede konfiguraci rozhraní na straně IDM a dodavatele nového IS, který provede konfiguraci dle dodané dokumentace na straně nového IS (tedy bez nutného zapojení nebo součinnosti dodavatele IDM). Zadavatel připouští možnost výše uvedené služby zajistit i formou ekvivalentního rozsahu realizovaného na bázi http REST služeb definovaných podle OpenAPI standardu (Swagger specifikace), včetně specifikace datových vět pomocí JSON Schema.
	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 informaci o delegaci role, - získání seznamu uživatelů dané aplikace, - získání seznamu pracovních pozic / funkcí přiřazených dané aplikaci, - zápis seznamu rolí uživatele do IDM, - zápis certifikátů do IDM, - zápis a změna identit.
	Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně.

Parametr	Popis parametru
Synchronizace	IDM umožní vstupně/výstupní synchronizace s připojenými informačními systémy. Podporované typy synchronizací (pokud je umožní připojený systém): - plná – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému - jedna identita – synchronizace vybrané identity bez nutnosti pouštět plnou nebo změnovou synchronizaci - změnová – synchronizuje vždy jen změny od poslední spuštěné synchronizace - simulační, který vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn k dispozici jako pohled nebo přehledná souhrnná tabulka - porovnávací – vytvoří porovnávací report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IDM versus nastavení identit a oprávnění přímo v připojeném systému.
	Jednotlivé běhy synchronizací budou logovány. Log plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a informace, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v logu dále informace o události, která změnovou synchronizaci vyvolala.
Integrace	IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. Systémům Microsoft bude IDM vytvářet a spravovat uživatelské účty a jejich oprávnění včetně provádění souvisejících operací potřebných pro automatizaci správy identit v daném systému (zejména. vytváření mailových schránek, úpravy metadat): - Microsoft Active Directory IDM bude integrováno (přímo propojeno) s následujícími systémy, ve který bude přímo řídit vznik/úpravy/zánik identit a jejich oprávnění: - Personální a mzdový IS – FLUX, spol. s r.o., - Docházkový IS – TETRONIK – výrobní družstvo Terezín, družstvo, - Elektronická spisová služba – GEOVAP, spol. s r.o., - Ekonomický IS Proxio (MARBES CONSULTING s.r.o.), - Portál občana – DATRON, a.s., - Vyvolávací systém – Kadlec – elektronika, s.r.o. - Příslušná rozhraní (konektory) na straně IDM budou součástí dodávky.

3 Integrace IDM a migrace dat

3.1 Integrace IDM

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

3.1.2 Příslušná rozhraní (konektory) na straně IDM budou součástí dodávky.

3.1.3 **Personální a mzdový IS (FLUX, spol. s r.o.)** – IDM bude z personálního informačního systému čerpat informace o uživatelích a jejích roli v organizaci. Popis komunikačního rozhraní systému je uveden viz příloha č. 2 této technické dokumentace.

3.1.4 **Docházkový IS (TETRONIK – výrobní družstvo Terezín)** – je požadována integrace za účelem řízení a správy uživatelských účtů v tomto systému, popis komunikačního rozhraní systému je uveden viz příloha č. 2 této technické dokumentace.

3.1.5 **Elektronická spisová služba (GEOVAP, spol. s r.o.)** – je požadována integrace za účelem řízení a správy uživatelských účtů v tomto systému, popis komunikačního rozhraní systému je uveden viz příloha č. 3 této technické dokumentace.

3.1.6 **Ekonomika – Proxio (MARBES CONSULTING s.r.o.)** – je požadována integrace za účelem řízení a správy uživatelských účtů v tomto systému, popis komunikačního rozhraní systému je uveden viz příloha č. 4 této technické dokumentace.

3.1.7 **Vyvolávací systém (Kadlec – elektronika, s.r.o.)** – je požadována integrace za účelem řízení a správy účtů v tomto systému (zaměstnanci MěÚ), popis komunikačního rozhraní systému je uveden viz příloha č. 5 této technické dokumentace.

3.1.8 **Portál občana (DATRON, a.s.)** – je požadována integrace za účelem řízení a správy uživatelských účtů v tomto systému (administrátoři MěÚ), popis komunikačního rozhraní systému je uveden viz příloha č. 4 této technické dokumentace.

3.1.9 **Microsoft Active Directory** – dle specifikace společnosti Microsoft. V prostředí objednatele bude v době dodávky IDM provozováno doménové prostředí Windows Server 2012, v blízké budoucnosti bude prostředí AD migrováno na Windows Server 2019.

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

3.2 Migrace dat

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

4 Implementace IDM

4.1 Dokumentace skutečného provedení

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

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

- **návrh řešení instalace** IDM **(architektura technického řešení)**,
- **detailní popis nastavení / konfigurace / parametrizace jednotlivých oblastí (společné registry, role a přístupová oprávnění, číselníky, reporty atd.)**,
- **návrh technického řešení integračních vazeb (vazby mezi subsystémy, vazby** s vybranými aplikacemi objednatele, vazby se spolupracujícími centrálními systémy),
- **návrh řešení postupu a pořadí při nasazování jednotlivých oblastí – zohlednění** v harmonogramu projektu,
- **popis případných organizačních opatření nutných pro implementaci (např. pracovní schůzky)**,
- **upřesnění časového harmonogramu projektu**,
- forma a místo **zaškolení IT administrátorů systému na dodané řešení v prostorách MěÚ**,
- **rozsah součinnosti ze strany objednatele**,
- **návrh průběhu testovacího provozu**.

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

4.1.4 **Bez předložení dokumentace skutečného provedení v prostředí objednatele nebude umožněno zhotoviteli instalovat a implementovat informační systém do určeného prostředí. Předložení dokumentace je povinností zhotovitele a v případě jejího nepředložení a z tohoto důvodu neumožnění implementace informačního systému do definovaného prostředí se bude jednat o prodlení na straně zhotovitele.**

4.1.5 Na základě nasazení informačního systému bude dokumentace aktualizována na skutečně nasazené řešení a bude k ní zpracováno technologické schéma dodávaného řešení.

4.2 Instalace IDM

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

4.2.2 Veškeré softwarové komponenty a databáze poběží ve virtualizovaném prostředí objednatele. Licence virtualizace poskytne objednatel. Jedná se o jednotnou platformu virtualizace provozovanou objednatelem v jeho serverovém prostředí Hyper-V. Dále objednatel poskytne pro provoz IDM licenci Windows Server 2019 Datacenter. V případě, že se zhotovitel rozhodne neužít nabízenou licenci operačního systému musí v rámci své dodávky dodat i odpovídají licence operačního systému k provozu nad virtualizovanou platformou objednatele. Veškeré další potřebné licence software potřebného pro běh IDM musí v rámci své dodávky zajistit zhotovitel.

4.2.3 Pro provoz IDM budou v prostředí objednatele vyčleněny tyto systémové prostředky, které budou pro provoz IDM alokovány po dobu min. 5 let a které musí zhotovitel garantovat, že budou po celou uvedenou dobu naprosto dostatečné, tedy, že za účelem optimálního běhu řešení IDM nebude minimálně po tuto dobu zhotovitel po objednateli požadovat navýšení takových systémových prostředků:

- 2 procesorová jádra,
- 12 GB RAM,
- 500 GB diskového prostoru,
- 1 Gbit síťová karta.

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

4.3 Konfigurace dodaného řešení pro potřeby objednatele

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

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

5 Dokumentace

5.1 Forma dokumentace

5.1.1 **Objednatel požaduje dodávku dokumentace v rozsahu dle tohoto článku v elektronické podobě** v **českém jazyce, nejpozději do** dne akceptace díla, není-li uvedeno nebo nevyplývá-li z jednotlivého typu dokumentace jinak.

5.1.2 Dokumentace musí být dodána v **takové podobě a formátu, aby byla připravena bez potřeby jakýchkoliv dalších úprav k** tisku.

5.2 Dokumentace skutečného provedení v prostředí objednatele

5.2.1 **Bude sloužit jako podklad pro implementaci řešení do prostředí** objednatele. Bude zpracována **minimálně v** rozsahu dle kap. 4.1 tohoto dokumentu.

5.3 Uživatelská dokumentace

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

5.4 Administrátorská dokumentace

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

6 Harmonogram

6.1 Harmonogram s časovými požadavky objednatele

6.1.1 **Objednatel požaduje realizaci předmětu plnění dle následujícího harmonogramu. Harmonogram je sestaven tak, aby jednotlivé práce na sebe logicky navazovaly a zároveň byl v souladu s požadavky dotační žádosti** objednatele do IROP.

6.1.2 **S ohledem na možnost kontroly realizace díla z pohledu času (tj. dílčí vyhodnocování dodržování harmonogramu realizace) je harmonogram doplněn milníky. Započetí každého milníku je možné pouze za předpokladu, že bude provedena akceptace všech milníků předch**ázejících.

Aktivita projektu	Doba trvání
Zpracování **dokumentace skutečného provedení.**	2 týdny
Připomínkování dokumentace skutečného provedení ze strany objednatele.	1 týden
Vypořádání připomínek a finalizace dokumentace skutečného provedení.	1 týden
Milník číslo 1 – Finální návrh Dokumentace **skutečného provedení.**	**Nejpozději do** T + 4 týdny
Instalace systému.	2 týdny
Provedení integračních vazeb.	8 týdny
Nastavení, konfigurace a parametrizace jednotlivých oblastí SW, **včetně** nastavení **přístupových oprávnění.**	
Milník číslo 2 – Připravené prostředí pro testovací provoz	**Nejpozději do** T + 14 **týdnů**
Dodávka dokumentace.	1 týden
Prezenční zaškolení IT administrátorů systému na dodané řešení	2 týdny
Testovací provoz se zvýšeným dohledem a podporou ze strany dodavatele s možností identifikace a opravy případných chyb a neshod.	3 týdny
Akceptační řízení.	
Milník číslo 3 – Akceptace projektu, předání systému do rutinního provozu.	**Nejpozději do** T + 20 **týdnů**

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

6.2 Konkretizovaný harmonogram plnění ze strany zhotovitele

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

- **z**pracování specifických požadavků objednatele na konkrétní způsob nasazení IDM a zpracování implementačního plánu, tj. Dokumentace skutečného provedení a podrobného harmonogramu s uvedením potřebné součinnosti ze strany objednatele,

- implementace IS do prostředí objednatele,
- předání dokumentace a testovací provoz,
- akceptace, předání systému a následný pilotní a ostrý provoz.

6.3 Testovací provoz

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

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

6.3.3 Během testovacího provozu provede zhotovitel aktualizaci Dokumentace skutečného provedení.

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

6.3.5 Testovacímu provozu bude předcházet zaškolení IT administrátorů systému na dodané řešení v prostorách MěÚ v rozsahu do 6 hodin.

7 Projektové řízení

7.1.1 S ohledem na **rozsah projektu a dopad jeho zavedení do produkčního provozu na výkon činnosti objednatele je v rámci dodávky předmětu plnění objednatelem požadováno aplikování základních principů projektového řízení ze strany zhotovitele.**

7.1.2 **Jedná se zejména řízení projektových prací v souladu s uzavřenou smlouvu s ohledem na věcné plnění dané smlouvou objednatele** – rozsah, posloupnost a hloubku projektových prací, (tj. harmonogramu) **– řízení postupu prací s ohledem na závazný harmonogram projektu – dodržování termínů a milníků harmonogramu, podchycení případných kolizí, zpoždění nebo vznikajících rizik a jejich reportování směrem k objednateli, aktivní řešení výše uvedených** nestandardních situací

7.1.3 **Zpracování pravdivých, úplných a věcně jasných a vypovídajících zápisů z konzultačních schůzek a pracovních jednání (s cílem zaznamenání klíčových rozhodnutí, ujednání, navržených nebo dohodnutých způsobů řešení dílčích částí projektu atd.)**

7.1.4 **Prezenční účast odpovědné osoby zhotovitele na kontrolních dnech v pravidelných min. měsíčních intervalech v sídle objednatele, případně se souhlasem obou smluvních stran** formou videokonference nebo telekonference.

7.1.5 **Reporting projektu na úrovni pravidelných dvoutýdenních písemných zpráv směrem k odpovědné osobě objednatele (seznam prací, které byly poskytovatelem vykonány pro danou část projektu, stav těchto prací (ukončeno, odloženo, v realizaci); popis vzniklých problémů a způsob jejich řešení).**

7.1.6 **Řízení rizik projektu, hodnocení pravděpodobnosti jejich výskytu a míry dopadu, návrh řešení** k jejich eliminaci.

7.1.7 **Řízení změn na projektu, v případě požadavků na změnu v projektu provedení konzultací k ověření nutnosti změny projektu; zjištění dopadu požadovaných změn směrem ke koncepci celkového řešení, harmonogramu, dotačnímu titulu, vytížení lidských zdrojů atd. V případě odsouhlasení změn spolupráce při implementaci změn do projektu, komunikace s poskytovateli a s realizačním týmem.**

8 Legislativa

Níže je obsažený obecný přehled legislativy, kterou je potřeba dodržet v souladu s realizací předmětu plnění této technické dokumentace. Tento výčet není konečný ani všeobjímající a má za cíl rámcově upozornit zhotovitele na rozsah problematiky, kterou se v návaznosti na jednotlivé požadované funkcionality zavazuje dodržet, a u níž se tedy zavazuje objednateli zajistit soulad s platnou legislativou. Dílčí legislativní požadavky a odkazy na právní akty jsou obsaženy i v dalších dílčích částech této dokumentace a jejích přílohách.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.
Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.
Vyhláška NBÚ a Ministerstva vnitra ČR č. 317/2014 Sb., významných informačních systémech a jejich určujících kritérií, ve znění pozdějších předpisů.
Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů.
Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, v platném znění.
Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27.dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

9 Akceptace

9.1 Dílčí akceptační řízení

9.1.1 Dílčí akceptační řízení bude provedeno pro milník 1 a 2 vyznačený v harmonogramu projektu dle této technické dokumentace. Dílčí akceptační řízení bude zahrnovat porovnání skutečného stavu vůči požadavkům této technické dokumentace a jejím přílohám (milník číslo 1 a 2) a požadavků daných dokumentací skutečného provedení (milník 2).

9.1.2 Výsledkem dílčího akceptačního řízení je akceptační protokol s výsledkem Splněno nebo Nesplněno, podepsaný oprávněnými osobami smluvních stran.

9.1.3 Započetí dalších prací spadajících pod milník následující je možné pouze za předpokladu, že bude provedena akceptace s výsledkem Splněno všech milníků předcházejících.

9.2 Souhrnné akceptační řízení – akceptace díla

9.2.1 Souhrnné akceptační řízení bude zahrnovat:

- ověření splnění akceptace všech milníků, které akceptaci plnění předcházeli.
- porovnání skutečného stavu vůči požadavkům smlouvy o dílo a této technické dokumentace, která je její přílohou, a jejích příloh, funkčního i nefunkčního charakteru – licence a příslušenství.

9.2.2 Výsledkem souhrnného akceptačního řízení je akceptační protokol s výsledkem Splněno / Splněno s výhradou / Nesplněno, podepsaný oprávněnými osobami smluvních stran.

9.3 Opakované akceptační řízení

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

Seznam zkratek

Zkratka	Význam
BPMN	Business Process Modelling Notation
CMD	Command
CSV	Comma Separated Value
ČR	**Česká republika**
ES	**Evropská společenství**
EU	Evropská unie
GB	Gigabyte
IDM	Identity Management
IROP	**Integrovaný regionální operační program**
IS	**Informační systém**
IT	**Informační technologie**
JIP	Jednotný identitní prostor
KAAS	**Katalog autentizačních a autorizačních služeb**
LDAP	Lightweight Directory Access Protocol
NBÚ	**Národní bezpečnostní úřad**
RAM	Random Access Memory
REST	Representational State Transfer
SIEM	Security Information and Event Management
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
WSDL	Web Services Description Language
XML	Extensible Markup Language
XMS	XML Message Server
XSD	XML Schema

Přílohy

Příloha 1 – Popis rozhraní na personální a mzdový IS (FLUX, spol. s r.o.)

*Příloha je tvořena samostatným souborem **Popis-rozhrani-PAM.PDF***

Příloha 2 – Popis rozhraní na docházkový IS (TETRONIK – výrobní družstvo Terezín)

*Příloha je tvořena samostatným souborem **Popis-rozhrani-DOCHAZKA.PDF***

Příloha 3 – Popis rozhraní na elektronickou spisovou službu (GEOVAP, spol. s r.o.)

*Příloha je tvořena samostatným souborem **Popis-rozhrani-eSSL.PDF***

Příloha 4 – Popis rozhraní na ekonomický IS Proxio (MARBES CONSULTING s.r.o.)

*Příloha je tvořena samostatným souborem **Popis-rozhrani-Proxio.ZIP***

Příloha 5 – Popis rozhraní na portál občana (DATRON, a.s.)

*Příloha je tvořena samostatným souborem **Popis-rozhrani-Portal.PDF***

Příloha 6 – Popis rozhraní na vyvolávací systém (Kadlec – elektronika, s.r.o.)

*Příloha je tvořena samostatným souborem **Popis-rozhrani-VYVOLAVACI.PDF***

Digitálně podepsal
Ing. Zdeněk Chobot
Datum: 2024.10.08
09:35:16 +02'00'