**TECHNICKÁ SPECIFIKACE**

pro veřejnou zakázku na dodávky v otevřeném nadlimitním řízení

**Pořízení aplikace Identity management**

**Preambule:** Tato technická specifikace je vypracována ve formě stanovení minimálních požadavků na množství, funkce, vlastnosti, jakost a výkonnostní nebo jiné parametry předmětu plnění veřejné zakázky. Technická specifikace je také součástí obchodních podmínek, ve kterých uchazeči doplní požadované údaje a stávají se tak součástí smlouvy, která bude uzavřena s vítězným dodavatelem.

**Systém správy identit (Identity Management System)**

Předmětem dodávky je informační systém správy identit (dále jen „IDM“) pro statutární město Karviná (dále jen „SMK“). IDM bude sloužit správcům informačních systémů k řízení životního cyklu identit uživatelů v datové síti SMK a evidenci informačních aktiv.

# Požadované minimální technické parametry a funkcionality

### Evidence informačních aktiv

IDM bude plnit funkci **evidence informačních aktiv.** Za informační aktiva jsou považovány veškeré ucelené soubory informací, ukládané a zpracovávané  v digitální formě prostřednictvím agendových informačních systémů (AIS) nebo jiným způsobem. Evidence informačních aktiv je primárním zdrojem informací pro:

1. Informační koncepci (dle zákona č. 365/2000 Sb.)
   1. Informace o způsobu využívání a životním cyklu aktiva (koncepce dalšího rozvoje nebo postupy pro ukončení životního cyklu)
   2. Informace o odpovědnostech za provoz aktiva
2. Bezpečnostní politiku informací SMK
   1. Informace o hodnocení aktiva
   2. Informace o zajištění bezpečnosti dat
   3. Informace o plánech obnovy aktiva a náhradních postupech
   4. technické Informace o způsobech provozu aktiva
   5. informace o rozsahu přístupů oprávněných osob k aktivu
3. Evidenci práv a rolí v IDM
   1. Informace o definovaných rolích v aktivu (role určuje rozsah oprávnění pro autorizaci uživatele)
   2. Informace o přidělených oprávněních identitám v IDM ve vazbě na role
4. Evidenci zpracování osobních údajů

#### Rozsah a obsah evidovaných údajů

Evidence informačních aktiv bude vést pro každé aktivum alespoň následující údaje:

1. Základní údaje
   * 1. ***Název*** – označení aktiva; textové pole
     2. ***Organizace*** *–* označení organizace, ve které je aktivum provozováno; výběr z číselníku
     3. ***Kategorie*** – zařazení aktiva do tematické kategorie; výběr z číselníku; kategorie mohou být uživatelsky definovány/upravovány
     4. ***Stav aktiva*** – označení stavu aktiva v životním cyklu („ověřovací provoz“, „ostrý provoz“, „ukončování provozu“, „provoz ukončen“); výběr z číselníku
     5. ***Kód ISVS*** – číselný kód přidělený aktivu Informačním systémem o informačních systémech veřejné správy; hodnota je nepovinná
2. Ochrana informací a osobních údajů
3. ***Klasifikace***– klasifikace informací dle bezpečnostní politiky informací SMK; výběr z číselníku
4. ***Zdroj dat*** – popis způsobu získávání dat v aktivu; textový popis
5. ***Aktualizace*** *–* popis způsobu aktualizace informací; textový popis
6. ***Skartace*** *–* popis doby uložení a způsobu skartace informací; textový popis
7. ***Osobní údaje*** *–* určení způsobu zpracování osobních údajů v aktivu („nejsou“, „z úřední činnosti“, „z vlastní činnosti“); výběr z číselníku
8. ***Registr OÚ*** *–* popis registrace zpracování osobních údajů na Úřadu pro ochranu osobních údajů; textový popis
9. ***Kategorie OÚ*** – popis kategorií osobních údajů, které jsou zpracovávány; textový popis
10. ***Účel zpracování OÚ*** – popis účelu zpracování osobních údajů; textový popis
11. ***Zpracovatel OÚ*** – identifikace zpracovatele osobních údajů (je-li odlišný od správce) a číslo smlouvy se zpracovatelem; textový popis
12. ***Příjemce OÚ*** – identifikace příjemce osobních údajů, pokud jsou předávány; textový popis
13. ***Legislativa*** – seznam zákonů vztahujících se k provozu aktiva; textový popis
14. Odpovědné osoby
15. ***Vlastník*** – vlastník aktiva dle definice uvedené v bezpečnostní politice informací SMK; výběr vlastníka bude vázán na seznam identit (vlastníkem může být pouze osoba vedená v IDM)
16. ***Správce*** – správce aplikace dle definice uvedené v bezpečnostní politice informací SMK; výběr správce bude vázán na seznam identit (vlastníkem může být pouze osoba vedená v IDM)
17. ***Zástupce***– zástupce správce aplikace dle definice uvedené v bezpečnostní politice informací SMK; výběr zástupce bude vázán na seznam identit (vlastníkem může být pouze osoba vedená v IDM)
18. ***Uživatelé*** – seznam uživatelů, kteří mají v informačním aktivu přidělenu jakoukoliv roli (oprávnění); může být ve formě rolovacího seznamu nebo odkazu na seznam uživatelů; tyto údaje jsou získávány z vazby IDM na evidenci aktiv
19. Analýza rizik
20. ***Zabezpečení***– popis způsobu zabezpečení aktiva (přihlášení do aplikace nebo vazba na metody jednotného přihlášení apod.); textové pole
21. ***Frekvence přístupu*** – hodnocení frekvence používání aktiva garantem; textový popis
22. ***Maximální nedostupnost*** – hodnocení maximální doby nedostupnosti aktiva garantem; textový popis
23. ***Hodnocení***– číselné hodnocení aktiva dle atributů definovaných v bezpečnostní politice: *Důvěrnost / Dostupnost / Integrita;* výběr z číselníku
24. ***Náhradní postupy*** – slovní popis náhradních postupů pro případ nedostupnosti aktiva; textový popis
25. Technické údaje
26. ***Technické prostředky (servery, databáze)*** – označení technických prostředků (serverů a databází), jehož služeb aktivum využívá; vícenásobný výběr z číselníku (pole hodnot)
27. ***Zálohování*** – popis způsobu a frekvence zálohování, přiřazení do plánu zálohování; vícenásobný výběr z číselníku (pole hodnot)
28. ***Vazby na jiná aktiva*** – označení jiných informačních aktiv, na jejichž funkčnosti závisí provoz aktiva; vícenásobný výběr z číselníku (pole hodnot)
29. Informační koncepce
30. ***Popis*** – slovní popis současného stavu aktiva a účelu jeho provozování; textový popis
31. ***Koncepce*** – slovní popis koncepce vztahující se k tomuto aktivu; textový popis
32. IDM
33. ***Role*** – přístupové role definované pro aktivum; tvorba číselníku (v záznamu aktiva bude možné vytvářet definici přístupových rolí)

#### Poža**dova**ný minimální rozsah a obsah výstupů z evidence informačních aktiv

Z evidence informačních aktiv bude možné provádět minimálně tyto výstupy:

1. Přehledy aktiv určené k tisku a uchování pro účely informační koncepce a plánů kontinuity (evidenční karty se všemi údaji o aktivech).
2. Přehledy aktiv s možností filtrování a třídění podle všech dostupných polí.
3. Rychlé vyhledávání aktiv podle názvu, garanta, správce a zástupce.
4. Zobrazení vazeb mezi aktivy a technickými prostředky (dotčená aktiva) – bude možné zobrazit dopady na funkčnost aktiv při omezení provozu serverů a databází nebo mezi aktivy.
5. Zobrazení matice oprávnění pro vybrané aktivum nebo vybraného uživatele.
6. Možnost definice vlastních výstupů (definice výběrových kritérií a třídění).
7. Možnost definice vlastních sestav (definice tiskových sestav).

### Evidence digitálních identit

IDM bude plnit funkci **evidence digitálních identit** (dále jen identit)Magistrátu města Karviné, Městské policie Karviná a 15 příspěvkových organizacích města. Za digitální identitu jsou považovány údaje o fyzické osobě v postavení uživatele dle Bezpečnostní politiky informací SMK. Evidence digitálních identit je primárním zdrojem informací pro:

1. Evidenci informačních aktiv
   * Informace o osobách podílejících se na odpovědnostech za provoz aktiva
   * Informace o přiřazení rolí v aktivech
2. Schvalovací workflow
   * Informace o osobách vstupujících do schvalování přístupů k informačnímu aktivu
3. Integrované systémy
   * Informace o digitální identitě s přístupem do integrovaného systému na základě matice oprávnění

#### Stavy identity včetně historie

1. Vytvoření identity – manuální vytvoření nové identity v IDM, automatické vygenerování přístupových údajů dle šablony (musí být zajištěna jedinečnost uživatelského jména), IDM automaticky vytvoří účty v defaultních systémech – dle nastavených pravidel.
2. Zrušení identity – na základě manuální ukončení platnosti identity, IDM okamžitě zneplatní účty ve všech napojených systémech, zároveň IDM uloží aktuální časovou značku, po uplynutí 30 dní identitu fyzicky smaže, případně přesune do archívu.
3. Změna identity – na základě provedených změn u identity musí IDM automaticky aktualizovat popisné atributy uživatele v napojených systémech (stejně tak přejmenování).
4. Změna hesla identity - změnu hesla bude moci provést jak administrátor IDM, tak i uživatelé s konkrétním oprávněním. V IDM bude zavedena politika na komplexitu hesla. IDM pak propaguje změnu hesla do všech napojených systémů.
5. Řízení rolí - v IDM budou založeny role, které budou odpovídat oprávnění v koncových systémech. Tyto role pak bude možné centrálně přidělovat/odebírat uživatelům. Současně bude možné na role aplikovat automatická časová omezení.
6. Žádosti o přidělení rolí - IDM bude umožňovat prostřednictvím grafického uživatelského rozhraní tvorbu žádosti o přiřazení nové role (žádat může sám zaměstnanec/externista nebo nadřízený pracovník). Taková žádost v IDM spustí předdefinované jedno či více úrovňové workflow, po jehož proběhnutí bude automaticky role přidělena nebo žádost zamítnuta.
7. Notifikace - IDM bude umožnovat zasílat notifikace pro různé typy událostí (blížící se exspirace hesla, nová žádost o schválení, vyřízená žádost apod.).
8. Audit - IDM umožní na jedné obrazovce zjistit, na jakých koncových systémech má uživatel aktuálně účty, dále umožní reportovat účty na koncových systémech, které nemají v IDM žádného majitele. IDM poskytne report z auditního logu, ve kterém jsou zaznamenány všechny akce a změny provedené prostřednictvím IDM.

#### Obecné funkce IDM

1. Celý systém musí být dodán jako jeden celek, včetně všech licencí potřebných pro jeho provoz v infrastruktuře zadavatele. V případě, že zadavatel potřebnou licencí již disponuje, může být tato využita pro IDM viz „Popis prostředí zadavatele“ níže v tomto dokumentu.
2. IDM musí udržovat identity a organizační struktury ve své vnitřní databázi. Identity ve vnitřní databázi budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy.
3. IDM musí umožnit udržovat a spravovat kompletní životní cyklus identity v počtu minimálně 2000 identit.
4. IDM musí umožňovat správu více organizačních struktur (větví) s možnosti přiřazení jedné identity do více struktur najednou.
5. IDM bude spravovat a administrovat organizační strukturu obsahující interní a externí identity jako samostatné větve struktury pro každou organizaci.
6. IDM musí umožnit pro každou organizaci definovat vlastní konektory k IS, pravidla a šablony pro vytváření účtů, politiky apod.
7. IDM musí umožnit dodatečné přidávání vlastních atributů k identitám a referenčním objektům, naplňování jejich obsahu ze zdrojových systémů a jejich publikaci externím aplikacím přes rozhraní webových služeb.
8. IDM musí umožnit napojení na více nezávislých domén Active directory (každá organizace má svou vlastní doménu AD) pro vytváření doménových účtu.
9. Zadavatel požaduje licencování formou trvalé multilicence bez jakéhokoliv omezení (počtu uživatelů, počtu připojených IS, velikosti DB apod.).
10. IDM musí být možné spravovat přes webovou konzoli pro správu a výkon jednotlivých administračních, integračních a provozních úloh.
11. IDM musí obsahovat modul pro registraci aplikací a jejich rolí. Dále pak import rolí přes webové služby do IDM.
12. IDM musí obsahovat správu uživatelských rolí, včetně zařazení uživatele do odpovídající role v daném IS.
13. IDM musí implementovat databázovou historizaci zejména pro evidenci změn na identitách a referenčních objektech, na které se identita odkazuje. Historizace bude i na vazbách mezi identitami a referenčními objekty. Historizace bude poskytovat data poplatné stavu identity a referenčních objektů a vazeb v libovolném časovém okamžiku ať aktuálním nebo zpětně v minulosti.
14. V IDM musí umožnit dynamicky konfigurovat pravidla pro automatické začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě atributů identity a přidružených referenčních objektů. (organizační jednotka, aplikační role, systematizované místo atd.). Stejným mechanismem pravidel bude IDM moct automaticky vytvářet další účty uživatele. Pravidla budou spravována v grafickém editoru prostřednictvím webového prohlížeče.
15. IDM bude poskytovat auditní logy pro monitorovací systém typu Log management nebo SIEM.
16. Součástí dodávky IDM bude implementační dokumentace, administrátorská a uživatelská příručka v českém jazyce.
17. IDM musí umožnit 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.
18. IDM musí obsahovat minimálně následující logy:
    1. Aplikační log – zaznamenává události systému
    2. Auditní log – zaznamenává změnu entit evidovaných v systému a změny konfigurace nastavení systému IDM.
    3. Synchronizační log – zaznamenává průběh synchronizací IDM s dalšími systémy
    4. Notifikační log – zaznamenává log odeslaných emailových notifikací
19. IDM musí obsahovat autentizační rozhraní, které bude umožňovat zprostředkovávat systémům autentizační úlohy přes následující protokoly/standardy:
    1. LDAP (Active Directory)
    2. Windows autentizaci
    3. Radius
    4. Ověření pomocí certifikátu
    5. OpenID
    6. OAuth2.0
    7. SAML 2.0. V rámci SAML protokolu bude IDM naplňovat roli identity providera a bude umožňovat pro jednotlivé aplikace doplňovat do SAML tokenu autorizační data ve vazbě na to, jaké má uživatel v IDM role a skupiny. Současně bude IDM umožňovat naplňovat roli service providera a uživatel se bude moct do něj autentizovat protokoly/standardy uvedenými výše kromě Radius protokolu.
    8. Podpora vícefaktorové autentizace
20. Správa systému IDM musí být implementována jako webová konzole/aplikace přístupná přes prohlížeče Internet Explorer verze 10 a vyšší, a poslední verze prohlížečů Firefox, Chrom a bude implementována s responzivním designem. Tato webová konzole musí být přístupná výhradně protokolem https, wildcard certifikát dodá zadavatel.
21. Správa IDM musí obsahovat přehlednou a oddělenou správu samostatných identifikovatelných objektů - referenčních objektů, na které se identita odkazuje: systematizované místo, organizační jednotka, skupina, agenda, agendová činnostní role, aplikace, skupina aplikací, aplikační role, certifikát atd. Webová konzole IDM bude pro tyto objekty obsahovat prostředí, kde bude možné tyto objekty v grafickém uživatelském rozhraní samostatně spravovat. Webová konzole IDM musí umožnovat přidávání nových a dalších typů takovýchto referenčních objektů a zajišťovat jejich správu v grafickém uživatelském rozhraní. IDM bude v modulu správy identit u scénáře správy konkrétní identity implementovat v grafickém rozhraní přímý odkaz (proklik) na referenční objekty, na která se daná identita odkazuje včetně toho, aby administrátor mohl po přechodu na tento odkaz vytvářet a editovat další referenční objekty a následně po vrácení zpět na detail identity je v tomto scénáři přiřadil dané spravované identitě.
22. IDM musí obsahovat funkcionalitu pro dodatečné rozšiřování identit a referenčních objektů o další atributy a publikaci těchto nových atributů externím aplikacím přes rozhraní webových služeb IDM.
23. IDM musí obsahovat evidenci matice práv a rolí dle Informačního systému základních registrů (ISZR-RPP) matice RPP tak, aby vedoucí pracovníci měli možnost zadávat k jednotlivým činnostem konkrétní uživatele
24. IDM musí obsahovat evidenci přehledu legislativy včetně vazby na jednotlivé činnosti/agendy.
25. IDM musí obsahovat správu identit, rolí a systémů evidovaných v systému JIP.
26. IDM musí obsahovat grafické zobrazení identit (uživatelských účtů) ve stromové organizační struktuře. Součástí jednoho pohledu v IDM bude zobrazení organizační struktury včetně systematizovaných míst organizace až do úrovně jednotlivých uživatelských účtů (identit). V grafickém zobrazení stromové struktury bude možné vyhledávat jednotlivé identity, systematizovaná místa, organizační jednotky, skupiny.
27. IDM musí umožnit vyhledávat bez diakritiky.
28. IDM musí obsahovat správu uživatelů a údajů o jejich certifikátech. Data o certifikátech uživatelů bude navíc možné nahrávat do IDM přes webové služby IDM. IDM musí obsahovat nastavení, které zajistí automatické zneplatnění certifikátů v IDM, které jsou po vypršení data platnosti.
29. IDM musí umožnit k jednotlivým účtům (identitám) přikládat fotografie, tyto pak musí být možné publikovat do dalších napojených systémů.
30. IDM musí umožnit přesun identity mezi jednotlivými strukturami jedné organizace a kopírovaní aplikačních rolí, agendových činnostních rolí mezi jednotlivými systematizovanými místy.
31. Systém pro správu IDM musí obsahovat správu parametrů, konfigurace systému IDM.
32. IDM musí obsahovat funkcionalitu pro sjednocení více osob do jedné a jejich sjednocení účtů.
33. IDM musí umožnit propojit k jedné identitě více účtů v různých informačních systémech
34. IDM musí obsahovat funkcionalitu pro export zobrazených seznamů minimálně do CSV, ideálně i do XML a PDF.
35. IDM musí obsahovat editor filtrů pro vyhledávání identit, referenčních objektů, rolí apod. v systému IDM. Do filtru musí být možné zadat libovolné atributy identity, které jsou v systému IDM evidovány včetně přidružených referenčních objektů. Výsledné filtry musí být možné uložit pro pozdější použití.
36. IDM musí mít kompletní podporu českého jazyka
37. IDM musí umožnit zobrazení „karty uživatele“, která bude obsahovat jeho osobní údaje (jméno, příjmení, tituly, osobní číslo, funkční zařazení, role atd.) včetně aktuálně nastavených oprávnění k informačním systémům včetně informace, kdo a kdy daná oprávnění žádal, povolil, schválil. Tato „karta uživatele“ musí být graficky přehledná a dostupná pro export do souboru PDF.
38. IDM musí obsahovat správu jednotlivých úrovní administrátorských oprávnění k identitám a stromové struktuře. V IDM musí být zejména možnost vytvářet administrátorská oprávnění na úrovni jednotlivých organizačních jednotek jako například přiřazovatel vybraných aplikačních rolí (pro organizační jednotku), vybraných činnostních agendových rolí a správce identit.
39. IDM musí obsahovat editor oprávnění. V rámci editoru bude administrátor definovat oprávnění do IDM a následně tato oprávnění přiřazovat konkrétním uživatelům. Oprávnění bude definováno pro jednotlivé entity a moduly systému (identity, referenční objekty, konfigurace notifikací, konfigurace synchronizací, konfigurace systému IDM, reporty, workflow, správa webových služeb IDM atd.) Dále bude oprávnění u entit (identit a referenčních objektů) definováno až na jejich konkrétní atributy včetně zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti atributu, pořadí zobrazení atributů ve formuláři. U jednotlivých entit a modulů bude možnost definovat akce, které může uživatel s entitami a v rámci IDM provádět.
40. V definici oprávnění musí být možné nastavit vlastníka vybraných aplikačních rolí, skupin, agendových rolí, administrátora vybrané konfigurace synchronizačních úloh pro napojené systémy.
41. IDM musí obsahovat správu rolí / přístupů k osobním údajům uchovávaných v rámci systémů organizace.
42. IDM musí obsahovat správu přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce. U přiřazování jednotlivých rolí musí být možné nastavit datum a čas počátku a konce platnosti přiřazení. Role bude přiřazena objektu jen v období platnosti.
43. IDM musí zajišťovat zobrazení přidělených rolí k jednotlivým identitám s rozdělením na role navázané na systemizované místo, role navázané na identitu, role navázané na organizační jednotku, role navázané na skupinu. U identity musí být evidován a v IDM souhrnně zobrazen seznam všech rolí včetně informace o tom, odkud uživatel roli zdědil (z organizační jednotky, systematizovaného místa, skupiny apod.).
44. IDM musí obsahovat správu skupin, kde je možné začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele, přiřazovat do skupin systematizovaná místa.
45. IDM musí umožňovat dědění rolí z nadřazené větve struktury organizace.
46. IDM musí obsahovat rozhraní pro uživatele, kde musí být umožněno uživateli změnit heslo, požádat o přidělení jednotlivých aplikačních rolí a skupin. Role a skupiny budou kategorizovány podle toho, zda požadavek na přidělení podléhá nějakému konkrétnímu schvalovacímu workflow nebo zda dojde k přiřazení bez schválení. Veškeré žádosti a jejich stav musí být evidován v historii a bude dohledatelný v IDM.
47. rozhraní pro uživatele IDM musí obsahovat konfigurovatelné registrační formuláře pro registraci externích organizací, identit, žádostí o konkrétní aplikační role nebo skupiny. Výběr seznamu rolí, skupin, o které mohou uživatelé požádat, bude možné v IDM specifikovat pro dané organizace a organizační jednotky samostatně.
48. rozhraní pro uživatele IDM musí umožnit individuální nastavení pohledů (zobrazení/skrytí sloupců, počet záznamů apod.)

#### Správa synchronizací

1. IDM musí umožnit jednotlivé synchronizace – napojení na systémy spouštět ručně i automaticky. Synchronizace musí být možné spouštět i v simulačním režimu, tak aby bylo možné si ověřit stav dopadu reálného spuštění předem. Simulační logy budou zobrazeny v IDM.
2. IDM musí zobrazovat jednotlivé stavy v průběhu synchronizace v grafické podobě.
3. V rámci napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM, musí být implementovány u každého systému následující režimy synchronizací (za předpokladu, že jejich implementaci napojovaný systém umožňuje):
   1. Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému
   2. Změnová synchronizace – synchronizuje vždy jen změny od poslední spuštěné synchronizace.
   3. Okamžitá synchronizace konkrétní identity na vyžádání – synchronizuje okamžitě pouze vybranou identitu.
   4. Rekonciliační synchronizace – synchronizace vytvoří rekonciliační report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IDM vs. nastavení identit a oprávnění přímo v připojeném systému.
   5. Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka přímo v Portálu IDM.
   6. Historie běhu synchronizací – jednotlivé běhy synchronizací budou zaznamenány v historii dostupné v IDM. Historie v případě plné synchronizace bude obsahovat odkazy na objekty v IDM, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii navíc informace o události, která změnovou synchronizaci vyvolala.
4. Systém pro správu IDM musí obsahovat správu jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, nastavení časového intervalu spouštění, nastavení intervalu odstávky. U jednotlivých synchronizací je rovněž požadováno, aby bylo možné v IDM vybírat organizace, které se mají z IDM synchronizovat s danými systémy.

#### Notifikace

1. IDM umožní notifikovat emailovou zprávou vytvoření a změny identity.
2. IDM umožní notifikovat emailovou zprávou vytvoření a změny referenčních objektů jako systematizované místo, organizační jednotka, skupina, agenda, agendová činnostní role, aplikace, skupina aplikací, aplikační role atd.
3. IDM umožní notifikovat emailovou zprávou konflikt, problém při jednotlivých synchronizacích probíhajících se systémy, na které je IDM napojeno.
4. Mechanismus správy notifikací včetně náhledu na odeslané notifikace musí být spravováno přímo v IDM.
5. V  IDM je požadováno v šabloně notifikace definovat příjemce, předmět a obsah dané notifikace. U notifikací vázané k identitám je dále požadována možnost nastavovat pro odesílání notifikací samostatné příjemce pro různé části organizační struktury (oddělení, atd.).
6. U notifikací ve vazbě na identity a referenční objekty musí být možné konfigurovat nastavení na úroveň jednotlivých atributů. V šabloně musí být možné vybrat libovolné atributy identity a referenčních objektů a následně je vložit a použít v definici textu pro emailové zprávy. Dále musí být možné u notifikací konfigurovat podmínky pro provedení notifikace na základě hodnot jednotlivých libovolných atributu identity a referenčních objektů. (například notifikace je generována pouze pro identitu v konkrétních uvedených skupinách, která má uvedenu konkrétní aplikační roli, systematizované místo, atd.)
7. IDM musí obsahovat notifikační šablony a notifikace pro upozornění na vypršení hesla v Active Directory a vypršení platnosti certifikátů. Notifikaci lze nastavit na několik dní dopředu před vlastním vypršením hesla nebo certifikátu.
8. V IDM musí být možné notifikace aktivovat pro jednotlivé zdrojové systémy, které v IDM změnu identity nebo referenčního objektu provedly.

#### Workflow

1. IDM musí podporovat plně elektronický schvalovací proces pro udělování přístupových práv uživateli a jejich následnou evidenci. Zadavatel preferuje schvalovací workflow s podepisováním s využití kvalifikovaného elektronického podpisu a může být založeno na funkcích elektronických formulářů a 602FormFlow Serveru, který má zadavatel k dispozici. Proces schvalování, evidence a nastavení přístupových práv by měl odpovídat schématu uvedenému v kapitole V. této přílohy.
2. schvalovací workflow IDM musí umožnit řízení životního cyklu změn identit a schvalování změn. Workflow musí splňovat následující požadavky:
   1. Možnost vložit pro nadřízené pracovníky požadavky na změny v přiřazení rolí, skupin pro podřízené pracovníky a sledovat stav vyřizování jejich žádostí.
   2. Možnost schválení či zamítnutí požadavků.
   3. Odeslání schvalovateli upozornění ve formě emailové notifikace
   4. Schvalovatelé si mohou zobrazit přehled úloh ke schválení
   5. Požadavky je možné schválit či zamítnout včetně uvedení zdůvodnění
   6. vícekrokové schvalování workflow na základě podmínek
   7. Schvalovat může jednotlivec nebo skupina schvalovatelů
   8. Správce IDM je schopen pracovat se všemi úlohami workflow
   9. Workflow musí obsahovat možnost větvení pro ošetření výjimek vzniklých při schvalování, upozorňování prostřednictvím mailu, řešení zastupitelnosti a eskalaci upozornění při nedodržení termínu splnění.
   10. V konzoli IDM je možné v grafické podobě zobrazení diagramu workflow, který obsahuje indikaci stavu aktuálně běžícího workflow.
3. IDM bude obsahovat mechanismus recertifikace rolí, kde bude možné opakovaně spustit úlohu z Portálu IDM, která zajistí schvalování pro všechny role přidělené identitám.
4. V IDM je možné definovat různě složitá workflow a do workflow je možné vkládat systémové kroky pro volání webových služeb a skriptovatelnou aplikační logiku.

#### Reporty a audit

1. IDM musí obsahovat funkcionalitu pro export auditního reportu z údajů o identitě uložené v IDM a to i historické. Auditní reporty budou minimálně ve formátu XML a CSV a budou obsahovat souhrnné zobrazení daného uživatele a jeho rolí v IS napojených na IDM, agendových rolí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti.
2. Veškeré požadavky změn, které provedou uživatelé v IDM se provádějí transakčně. Musí být historizovány a logovány tak, aby bylo možné zpětně prokázat kdo, kdy a co změnil v IDM identitách, referenčních objektech, ale i v administraci a konfiguraci IDM. Záznam v historii bude obsahovat původní i novou hodnotu.
3. IDM musí obsahovat editor pro vyhledávání identit a referenčních objektů v systému IDM pro vytvoření reportu. Do filtru musí být možné zadat libovolné atributy identity, které jsou v systému IDM evidovány včetně přidružených referenčních objektů.
4. IDM musí umožnit generovat report pro proces ohlašování působnosti v Registru práv a povinností. Report bude obsahovat počty úředníků na agendových rolích a původní počet (vzhledem k vybranému dříve vygenerovanému reportu). Výstupem reportu bude CSV soubor.
5. IDM musí obsahovat možnost generovat do CSV souboru report uživatelů přiřazených aplikačním rolím a možnost nastavení pravidel pro automatického zasílání reportu emailem.
6. Vygenerované report zůstávají v systému IDM a je možné je zobrazit/stáhnout i později.
7. IDM musí obsahovat funkcionalitu na porovnání změn mezi vygenerovanými reporty stejného typu.

### Rozhraní a integrace IDM s jinými systémy

#### Rozhraní webových služeb

1. IDM musí poskytovat rozhraní webových služeb pro napojení dalších systémů. Základní konfigurace přístupu k webovým službám bude přístupná ve webové aplikaci/konzoli IDM.
2. IDM musí umožnit řízení uživatelských účtů a rolí v jiných systémech na principu obecné webové služby (tzn. bude možné konfigurovat konektory pro tyto webové služby pro jakýkoliv jiný – podřízený - systém).
3. Webové služby IDM musí být definované v rozšířeném standardu WSDL a podporovat protokol SOAP.
4. Konfigurace webových služeb v konzoli IDM musí umožnit nastavovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet zvlášť.
5. Volání webových služeb musí být logováno a zobrazeno přímo v IDM.
6. Rozhraní musí poskytovat minimálně následující služby
   1. Získání organizační struktury
   2. Získání hierarchie systematizovaných míst
   3. Získání seznamu identit
   4. Získání nadřízené osoby pro daného zaměstnance
   5. Získání seznamu aplikační rolí
   6. Získání seznamu uživatelů dané aplikace
   7. Získání seznamu agend a agendových rolí přiřazených dané aplikaci
   8. Zápis seznamu aplikačních rolí do IDM
   9. Zápis certifikátů do IDM
   10. Zápis a změna identit
   11. Služba pro autorizaci pro ISZR – služba ověří validnost volání služby ISZR. Služba bude ověřovat v IDM:
   * Zda je evidován uživatel v IDM, který je v požadavku na ISZR
   * Zda je evidována aplikace v IDM, která je v požadavku na ISZR
   * Zda má tento uživatel v IDM nastaven přístup do aplikace, která je v požadavku na ISZR
   * Zda existuje v IDM v rámci evidence organizační struktury rovněž evidence pro dané OVM, které je uvedeno v požadavku na ISZR
   * Zda má aplikace, která je v požadavku na IZSR, v IDM povolenou agendovou činnostní roli a agendu, které jsou rovněž uvedeny v požadavku na ISZR.

#### Obecné konektory

1. IDM musí obsahovat obecné konektory pro správu identit v napojených systémech:
   1. CMD – konektor umožňuje spouštět CMD příkazy
   2. CSV – konektor umožňuje generovat CSV soubory
   3. Databáze – konektor umožnuje spravovat identity v DB
   4. SOAP– konektor umožňuje se napojit na SOAP webové služby (WS-SOAP)
   5. REST – konektor umožňuje se napojit na restové webové služby (WS-REST)
   6. LDAP - konektor umožňuje se napojit na LDAPv3 server (např. Active Directory)
2. Všechny výše uvedené konektory musí být konfigurovatelné přímo z konzole IDM
3. IDM musí umožnit připojení libovolného množství dalších spravovaných systémů a to bez dalších licenčních nákladů

#### Napojení na Active Directory

1. IDM musí umožnit komplexní správu účtů, certifikátů, skupin a členství ve skupinách v systému MS Active Directory, zejména musí umožnit založení uživatele, změnu atributů u uživatele, zrušení uživatele, změny zařazení uživatele do skupin a správu skupin, změnu hesla atd. IDM musí dále umožnit založení domovského adresáře uživatele včetně nastavení oprávnění. IDM dále nesmí v AD přepisovat další nastavené atributy, které nejsou řízeny IDM.
2. IDM umožní správu účtu a jejich certifikátů v Active Directory včetně iniciačního načtení účtů z AD.
3. IDM umožní správu skupin a členství ve skupinách v Active Directory, včetně iniciačního načtení z AD.
4. IDM umožní správu organizačních jednotek v Active Directory včetně iniciačního načtení z AD.

#### Napojení na Exchange

1. IDM musí umožňovat správu emailové schránky na serveru MS Exchange 2016, zejména musí umožnit vytvoření schránky, zrušení schránky a zneplatnění schránky. Řízení životního cyklu emailových schránek v IDM bude prostřednictvím správy odpovídajících aplikačních rolí uživatele. Při změně role uživatele, na kterou je vázáno umístění schránky v datastore, bude při synchronizaci automaticky přemístěna schránka do odpovídajícího úložiště.
2. IDM musí dále umožnit při dlouhodobé nepřítomnosti uživatele automatické nastavení automatické odpovědi na straně Exchange.
3. IDM musí umožnit správu distribučních seznamů.

#### Napojení na DB Oracle verze 12.1.0.1

1. Inicializační načtení dat ze systému
2. Správu lokálních identit (uživatelů, účtů)
3. správu rolí
4. správu systémových oprávnění
5. správu objektových oprávnění

#### Napojení na RPP

1. IDM musí obsahovat evidenci matice práv a rolí dle Informačního systému základních registrů (ISZR-RPP) matice RPP tak, aby vedoucí pracovníci měli možnost zadávat k jednotlivým činnostem konkrétní uživatele (systemizovaná místa) a tyto změny po odsouhlasení odeslat do ISZR-RPP.
2. IDM musí umožnit přidělování/odebírání agend/činností zaměstnancům vedoucími zaměstnanci s vazbou na systemizovaná místa.
3. V IDM musí být udržován přehled o oznámené působnosti, jejich stavů, kontrola přeregistrace a změn.
4. IDM musí obsahovat evidenci přehledu legislativy včetně vazby na jednotlivé činnosti/agendy. Automatická synchronizace všech požadovaných dat mezi RPP, JIP, IDM.

#### Napojení na JIP

1. IDM musí umožnit obousměrnou synchronizaci s JIP.
2. Z JIP budou do IDM pravidelně načítány jednotlivé aplikace a role.
3. Ze strany IDM budou do JIP předávány identity včetně vazby na jednotlivé aplikační a agendové činnostní role.
4. V IDM musí být možné měnit heslo uživatele v JIP.

#### Napojení na IS fy Geovap

1. Napojení na spisovou službu
   1. Inicializační načtení dat ze systému
   2. Správu lokálních identit (uživatelů)
   3. Správu oprávnění pro jednotlivé uživatele spisové služby
   4. Správu funkčních míst a organizačních jednotek
2. Napojení na IS Cityware
   1. Inicializační načtení dat ze systému
   2. Správu lokálních identit (uživatelů)
   3. Správu oprávnění pro jednotlivé uživatele na moduly Cityware
3. Dodavatel si zjistí technické řešení a obchodní podmínky pro připojení IDM na IS u dodavatele: Geovap, s.r.o., Kontaktní osoba: Ing. Alena Drábková, tel: 466 024 130, e-mail: alena.drabkova@geovap.cz

#### Napojení na IS VITA

1. Inicializační načtení dat ze systému
2. Správu lokálních identit (uživatelů)
3. Správu oprávnění pro jednotlivé uživatele na moduly VITA
4. Dodavatel si zjistí technické řešení a obchodní podmínky pro připojení IDM na IS u dodavatele: VITA software, s.r.o, kontaktní osoba: RNDr. Ivana Havlíková, tel. 604 245 991, e-mail: vita@vitasw.cz

#### Napojení na IS Fenix

1. Inicializační načtení dat ze systému
2. Správu lokálních identit (uživatelů)
3. Správu oprávnění pro jednotlivé uživatele na moduly Fenix
4. Dodavatel si zjistí technické řešení a obchodní podmínky pro připojení IDM na IS u dodavatele: Asseco Solutions, a. s., kontaktní osoba: Petra Zárubová, tel. 731 425 367, e-mail: petra.zarubova@assecosol.com

#### Napojení na IS 602 FormFlow Server

1. Inicializační načtení dat ze systému
2. Správu lokálních identit (uživatelů)
3. Správu oprávnění pro jednotlivé uživatele
4. Dodavatel si zjistí technické řešení a obchodní podmínky pro připojení IDM na IS u dodavatele: Software 602, a. s., kontaktní osoba: Michal Vejvoda, tel. 725 326 994, e-mail: vejvoda@602.cz

#### Napojení na IS ADS RON

1. Inicializační načtení dat ze systému
2. Správu lokálních identit (uživatelů)
3. Správu oprávnění pro jednotlivé uživatele
4. Dodavatel si zjistí technické řešení a obchodní podmínky pro připojení IDM na IS u dodavatele: RON Software, spol. s r.o., kontaktní osoba: Daniel Owczarzy, tel. 596 312 827, e-mail: daniel.owczarzy@ron.cz

#### Napojení na IS FLUX

1. Inicializační načtení dat ze systému
2. Správu lokálních identit (uživatelů)
3. Správu oprávnění pro jednotlivé uživatele na moduly FLUX
4. Správu organizační struktury
5. Dodavatel si zjistí technické řešení a obchodní podmínky pro připojení IDM na IS u dodavatele: FLUX, spol. s r.o., kontaktní osoba: Petr Kuchař, tel. 257 221 700, e-mail: petr.kuchar@flux.cz

#### Napojení na IS MPK

1. Nastavení konektoru v IDM pomocí webových služeb
2. Inicializační načtení dat ze systému
3. Správu lokálních identit (uživatelů)
4. Správu rolí/oprávnění pro jednotlivé uživatele na moduly IS MPK

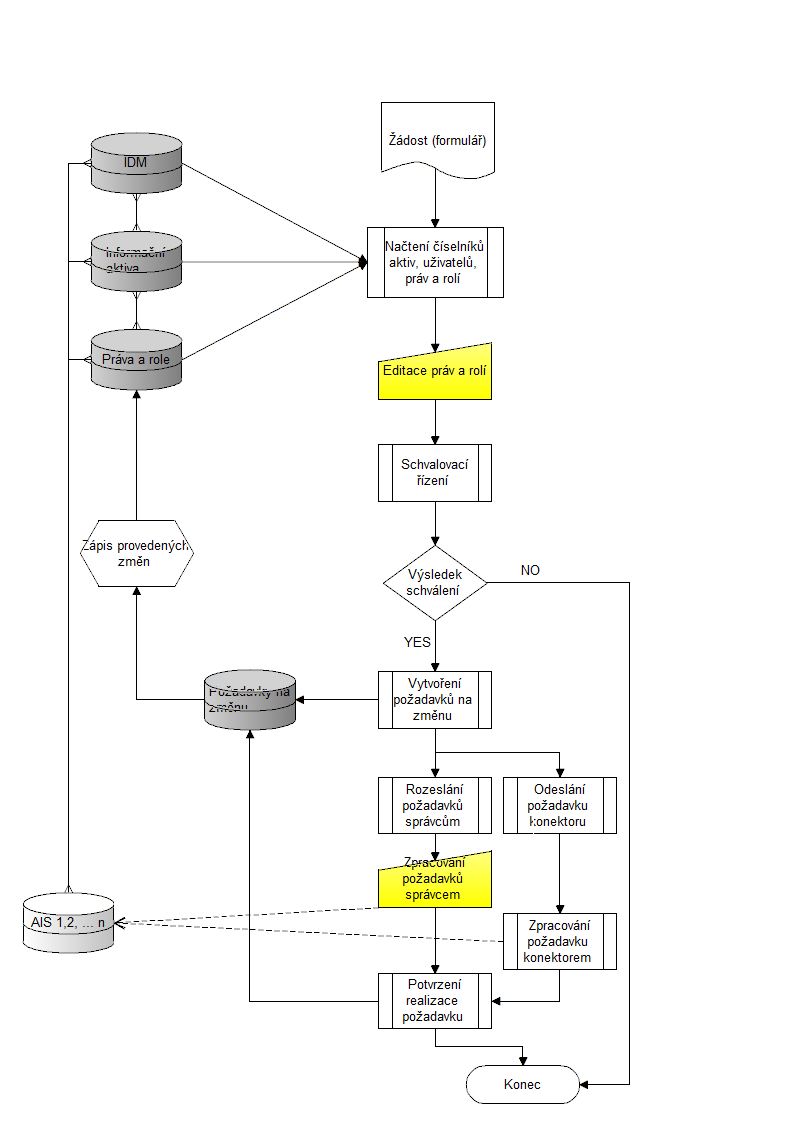
#### Napojení na PCO MPK

1. Správu lokálních identit (uživatelů)
2. Správu rolí/oprávnění pro jednotlivé uživatele na moduly IS MPK
3. Dodavatel si zjistí technické řešení a obchodní podmínky pro připojení IDM na IS u dodavatele: ECHO alarm, s. r.o., kontaktní osoba: Lukáš Barvík, tel. 603 556 561, e-mail: barvik@echoalarm.cz

### Implementace a harmonogram nasazení

1. Způsob implementace bude vycházet z projektové dokumentace implementace zpracované dodavatelem v rámci předimplementační analýzy a schválené zadavatelem.
2. Instalace a konfigurace bude provedena na zařízení a programovém vybavení zadavatele (servery, pracovní stanice a operační systémy dle uvedené specifikace v bodě VI.).
3. Napojení na IS všech organizací dle požadavků výše bude součástí implementace.
4. Školení uživatelů bude provedeno v odpovídajícím rozsahu s ohledem na organizaci práce pracovníků, a to na počátku testovacího provozu.
5. K software bude průběžně dodávána aktuální dokumentace ve shodě s aktuálním nastavením.
6. Dokumentace bude předána v elektronické podobě a bude respektovat požadavky specifikované zákonem č. 365/2000 Sb., O informačních systémech veřejné správy a o změně některých dalších zákonů, a vyhláškou č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy).
7. Předimplementační analýza bude provedena v termínu do 1 měsíce od podpisu smlouvy.
8. Implementace a zkušební provoz bude probíhat 2 měsíce od ukončení předimplementační analýzy.
9. Ukončením zkušebního provozu a odsouhlasením všech implementací zadavatelem bude projekt předán zadavateli do ostrého provozu.

### Schéma workflow



### Popis prostředí zadavatele

**Servery:**

1. Datové centrum zadavatele disponuje virtualizačním řešením VMWare v režimu vysoké dostupnosti, verze 6.0,
2. Podporované verze OS serverů jsou Microsoft Windows 2012R2 a vyšší,
3. V případě distribucí Linux, musí být součástí dodávky licence pro OS pokud je vyžadována a OS musí být uveden na compatibility listu VMware,
4. Přidělené systémové prostředky (procesor, RAM, diskový prostor) je možné upravovat ve virtuálním prostředí a jsou k dispozici v přiměřené kapacitě (procesor 6x 2,8 GHz, 8 GB RAM, 100 GB diskového prostoru),
5. Zálohovacím SW je Tivoli Storage Manager (TSM) – denní zálohování.

**Pracovní stanice:**

1. Virtuální PC (VMware Horizon View), fyzická PC a notebooky
2. Operační systémy Windows 7 a 10 (32/64 bit)
3. Kancelářské aplikace MS Office 2016 Standard
4. Prohlížeč MS Explorer (poslední dostupná verze), MS Edge (poslední dostupná verze), Firefox (poslední dostupná verze), Chrome (poslední dostupná verze)

**Databáze:**

1. Zadavatel disponuje databází Oracle 12.0.1., s dostatečným výkonem a nastaveným systémem zálohování (TSM)
2. Pokud je součástí dodávky provoz na jiné databázi, musí dodavatel zajistit:
   * dodávku databáze, včetně instalace a všech licencí potřebných pro provoz a pro 420 interních uživatelů a neomezený počet externích uživatelů (připojovaných z Internetu);
   * neomezenou velikost dodané databáze;
   * servisní podporu databáze na dobu 5 let;
   * integraci databáze do systému zálohování MMK a úpravy zálohovacích plánů a dokumentace.