1.3 Příloha č. 3 – navrhované Technické řešení

1.3.1 Naplnění požadavků zadavatele

Popis povinného parametru	ANO / NE	Popis naplnení
2.2.1 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. Minimálně se jedná o následující procesy: • vznik nové identity • nový pracovněprávní vztah • úprava identity a pracovněprávního vztahu • úpravy popisných atributů, např. jméno • úpravy organizačního zařazení • změny platnosti • automatická změna rolí na základě změny stavu / typu identity, případně jiného příznaku identity • změna evidenčního stavu identity • ukončení pracovněprávního vztahu • aktivace/deaktivace (ruční, automatická)	ANO	Více v kapitole Procesy správy identit. CzechIdM obsahuje ve standardní konfiguraci parametrizovatelné procesy pokrývající všechny požadavky zadavatele.
2.2.2 IDM musí udržovat identity, skupiny identit a organizační struktury ve své vnitřní databázi. Identity ve vnitřní databázi budou sloužit jako referenční identity pro ostatní informační systémy.	ANO	CzechIdM používá pro persistenci dat relační databázi.
2.2.3 IDM musí implementovat princip založený na systemizovaných místech. IDM musí umožnit systemizaci pracovních míst v souladu se strukturou organizace, definovat jednotlivá systematizovaná místa a jejich činnosti a sadu oprávnění a rolí pro jednotlivé informační systémy organizace vztažené ke konkrétnímu systemizovanému místu.	ANO	Přidělování role v CzechIdM má vlastnost automatického přidělení na základě organizačního zařazení či libovolných atributů identity. To znamená, že u role lze nakonfigurovat podmínku, za které je uživateli automaticky role přidána. Například

		• Role reprezentující skupinu v AD bude přidělena všem uživatelům, kteří mají atribut „funkce“ vyplněn hodnotou „sekretářka“ • Role prezentující skupinu v AD bude přidělena všem, kteří pracující na pediatrické klinice . CzechIdM navíc umožňuje konfiguračně nastavit, zda takto přidělované role dostanou uživatelé • posazeni přímo na konkrétní místo ve stromě • všichni posazeni na konkrétní místo ve stromě a také všichni posazení na podřazená místa ve stromě • všichni posazeni na konkrétní místo ve stromě a také všichni posazení na nadřazená místa ve stromě Přidělením role v CzechIdM, která reprezentuje skupinu v AD je automaticky vyvolán provisioning (propis dat do napojených systémů) a tím pádem je uživatel zařazen do konkrétní skupiny v AD.
2.2.4 IDM umožní přiřazení identit na takto vytvořená systematizovaná místa a to i ve vazbě M:N. Identita tedy může být v systému IDM evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit.	ANO	Standardní funkce produktu CzechIdM.
IDM musí umožňovat přidělení oprávnění nebo role konkrétní identitě, systemizovanému místu, skupině nebo organizační jednotce.	ANO	Ano, přidělení role identitě je standardní funkce produktu. Přidělení role organizačním jednotkám viz kapitola „Aplikační role“.
IDM musí umožnit správu uživatelských rolí, včetně zařazení uživatele do odpovídající role.	ANO	Standardní funkce IdM
V IDM je možné aplikační role nastavovat dočasně. Po uplynutí nastaveného intervalu se role automaticky odebere.	ANO	Standardní funkce CzechIdM – role na dobu určitou.
IDM umožní registraci aplikací a jejich rolí a dále také import rolí přes webové služby do IDM.	ANO	Veškeré operace CzechIdM IdM jsou dostupné i aplikacím přes univerzální služby RESTful rozhraní.
IDM musí umožnit definovat vztahy zastupitelnosti mezi uživateli – musí umožnit	ANO	Zastupitelnost je v CzechIdM řešena ve více režimech.

uživatelům, aby v souladu se strukturou úřadu mohli delegovat v případě potřeby (nemoc, dovolená atd.) svoje role, nebo jejich část na jiné pověřené osoby, a to i tak, že jeden uživatel může mít pro každou svou činnost nastaveného jako zástupce jiného různého uživatele. Delegace oprávnění bude dočasná, kdy se po nastaveném intervalu, nastavená delegace automaticky v IDM zruší.		1. zastupitelnost ve schvalování/výkonu práv v identity manageru – toto je řešeno nativními funkcemi, kdy pro každé schvalování je určeno jeden nebo více schvalovatelů, kteří se mohou zastupovat. Schvalovatelé jsou určeni buď jmenovitě nebo rolí. Pokud jsou určení rolí, tak zastupujícím se stává každý kdo tuto roli dostane. 2. zastupitelnost na pracovní pozici - zastupování se řeší novým vztahem/zástupem, který umožní po dobu zastupování posadit na místo zastupovaného nového uživatele, ale zároveň nejsou v kolizi s jeho dalšími vztahy. V závislosti na konfiguraci rolí podléhá zastupování standardnímu schvalování přidělení role.
IDM musí umožnit dodatečné přidávání vlastních atributů k identitám.	ANO	CzechIdM implementuje mechanismus tzn. „Extended atributů“ (EAV). Tyto atributy lze definovat a upravovat v GUI CzechIdM pro všechny základní objekty jako je: Identita, Role, TreeNode, Vztah a další.
IDM musí umožňovat přesun identity v rámci organizační struktury i mezi jednotlivými organizačními strukturami.	ANO	Standardní funkce produktu CzechIdM.
IDM musí mít možnost detekovat situaci, kdy se ve zdrojovém systému vyskytne nový uživatel, který již dříve byl v IDM založen a přiřadit jej k existující identitě.	ANO	Standardní funkce produktu CzechIdM. Kapitola Synchronizace
IDM musí umožňovat kopírovat role mezi jednotlivými systematizovanými místy.	ANO	Funkcionalita bude konfigurována v rámci zákaznického modulu.
IDM musí obsahovat funkcionalitu kopírování veškerého nastavení oprávnění jednoho uživatele na druhého.	ANO	Funkcionalita bude konfigurována v rámci zákaznického modulu. Nicméně její použití je sporné z bezpečnostních důvodů. Způsob použití a jeho rizika bude řešen v rámci analýzy prostředí.
Veškeré požadavky, které provedou uživatelé na IDM, musí být provedeny transakčně, musí být historizovány a logovány tak, aby bylo možné zpětně prokázat kdo, kdy a co změnil v IDM identitách, referenčních objektech, ale i v administraci. Záznam v historii musí obsahovat původní i novou hodnotu.	ANO	Důležitou součástí správy identit je prokazování zpětně v čase změn v identitách a jejich oprávněních. CzechIdM zavádí tzv. stroj času - každá změna nad libovolným objektem (identita, role, spravovaný systém…) je auditována ve formě snímku staré verze.

		Kdykoliv tak lze procházet a porovnávat revize změn.
IDM umožní autonomní správu hesel (samoobsluha).	ANO	Standardní funkce produktu CzechIdM.
IDM bude komunikovat v českém jazyce.	ANO	Standardní funkce produktu CzechIdM. Produkt je vyvíjen v České republice.
IDM musí umožňovat generování min. těchto kontrolních reportů:	ANO	Viz níže.
přehled uživatele (uživatelů) a jejich rolí v systémech spravovaných IDM v době generování reportu,	ANO	Report bude prostředí Zadavatele zpřístupněn v požadované formě.
report historie delegování práv uživatele/uživatelů v definovaném časovém období.	ANO	Report bude prostředí Zadavatele zpřístupněn v požadované formě.
IDM musí umožnit generování těchto reportů ve strojově čitelném formátu (např. v XML).	ANO	Viz kapitola modul Reportů
IDM musí obsahovat grafické uživatelské rozhraní pro přístup administrátorů systému pro správu identit uživatelů a jejich možné založení, úpravu nebo zneplatnění.	ANO	Kapitola uživatelské rozhraní
IDM musí obsahovat grafické uživatelské rozhraní sloužící jako obsluha pro uživatele, ve kterém uživatelé mohou měnit/resetovat heslo, žádat o přidělení rolí pro sebe nebo své podřízené, schvalovat nebo zamítat žádost a provádět další činnosti, na které mají oprávnění.	ANO	Kapitola uživatelské rozhraní
IDM musí poskytovat rozhraní webových služeb pro programové napojení dalších systémů města. Toto rozhraní bude dodáno včetně jeho dokumentace, která bude určena k přímému poskytnutí dalším dodavatelům v prostředí města za účelem napojení se na takové rozhraní. Webové služby budou dostupné jako SOAP nebo REST rozhraní. Součástí takové dokumentace bude proto i popis řešení webových služeb v podobě XSD. Rozhraní a jeho konfigurace musí být součástí plnění na takové úrovni, že napojení nového informačního systému bude možné pouze za zapojení pracovníka objednatele, který provede konfiguraci rozhraní na straně IDM a dodavatele nového IS, který provede konfiguraci dle dodané dokumentace na straně nového IS, tedy vše bude možné bez aktivního zapojení dodavatele IDM.	ANO	Webové služby jsou v CzechIdM dostupné formátu REST. Webové služby pokrývají 100% funkčnosti CzechIdM. Kompletní dokumentace API je distribuována spolu s produktem nejen jako výčet možných metod, ale i jako interaktivní nástroj pro manuální volání těchto metod. Implementátor napojení přes REST tak může online zkoušet napojení svého systému oproti všem funkcím IdM bez nutnosti cokoli upravovat na CzechIdM.
Základní konfigurace přístupu k webovým službám musí být dostupná z grafického rozhraní IDM.	ANO	Webové služby jsou v CzechIdM dostupné formátu REST. Webové služby pokrývají 100% funkčnosti CzechIdM.
Rozhraní IDM musí poskytovat minimálně následující služby: • získání organizační struktury,	ANO	Webové služby jsou v CzechIdM dostupné formátu REST. Webové služby pokrývají 100% funkčnosti CzechIdM.

• získání hierarchie systematizovaných míst, • získání seznamu identit, • získání nadřízené osoby pro daného zaměstnance, • získání seznamu rolí pro daného zaměstnance, včetně případné informaci o delegaci role, • zápis seznamu rolí uživatele do IDM, • historie uživatele a jeho oprávnění k datu uvedeném v parametru.		
IDM umožní vstupně/výstupní synchronizace do připojených informačních systémů. Typy synchronizací: • plná • 1 identita (možnost prosynchronizovat pouze 1 identitu bez nutnosti pouštět plnou nebo změnovou synchronizaci) • změnová (pokud to napojený IS umožní)	ANO	Standardní funkčnost produktu. Více v kapitole synchronizace.
Plná a změnová synchronizace musí umožňovat naplánované i ruční spuštění synchronizace, synchronizace 1 identity musí umožňovat pouze ruční spuštění. Dále musí existovat možnost (trvale nebo dočasně) vyřadit identitu ze synchronizace s daným IS.	ANO	Standardní funkčnost produktu. Více v kapitole synchronizace, Provisioning. Dostupné pro uživatele s příslušným oprávněním.
IDM umožní publikaci objektů (osob, účtů, skupin, funkcí, org. jednotek...) informačním systémům přes datové rozhraní (API IDM) na principu webových služeb (SOAP). Toto API IDM musí tedy mít čtecí metody a ideálně by mělo mít i zápisové metody (součást kvalitativního hodnocení). V rámci čtecích metod musí mít dané API IDM i autentizační metody, umožňující ověřit identitu (její login/heslo) i třetím aplikacím. IDM by mělo mít historii volání API IDM z důvodu auditu (součást kvalitativního hodnocení), včetně možnosti omezit dané API IDM pro jednotlivé aplikace (pouze vydefinované metody API IDM pro potřeby dané aplikace).	ANO	Webové služby jsou v CzechIdM dostupné formátu REST. Webové služby pokrývají 100% funkčnosti CzechIdM.
IDM musí umožňovat publikovat kopie logů do externího systému určeného pro sběr logů např. syslog, DB apod.	ANO	Logy jsou poskytovány prostřednictvím univerzálního rozhraní aplikace (REST).
Veškeré nové moduly IDM musí vést a umožňovat jednoduchý export anonymizovaných logů o počtu užití těchto jednotlivých modulů.	ANO	Veškeré logy jsou přehledně dostupné v GUI

Tyto logy musejí být natolik přehledné a oproštěné od osobních dat aby umožnili jednoduchou kontrolu užívání těchto nových modulů ze strany i například kontrolních orgánů včetně oblasti kofinancování IROP.	ANO	Veškeré logy jsou přehledně dostupné v GUI
Po přihlášení do IDM bude administrátor IDM notifikován, že v systému došlo k některému z chybových stavů (např. synchronizovaný systém ve stavu chyba). Tato notifikace musí být zřetelná po přihlášení do systému a může být formou (barevného podbarvení části aplikace např. menu, pop-up okna oznamující, že je v IDM nějaký chybový stav, centrální dashboard aplikace apod.). Z notifikace musí být zřetelné, která část IDM je chybovém stavu.	ANO	CzechIdM obsahuje na úvodní obrazovce tzv. dashboard, kde se nacházejí informace z jednotlivých modulů CzechIdM relevantní pro přihlášeného uživatele. Jedním z modulů je modul pro výpis chybových stavů pravidelných akcí – naplánované úlohy, sychronizace dat..
IDM umožní definování různých úrovní oprávnění:	ANO	
možnost omezit oprávnění jenom na konkrétní organizační jednotky – uživateli to umožní spravovat identity pouze z daných organizačních jednotek např. vedoucí odboru spravuje oprávnění pro své podřízené (možnost omezit, zda může přiřazovat vybrané aplikační role, agendové role, skupiny, funkční místa, konkrétní uživatelské atributy apod.)	ANO	CzechIdM obsahuje sadu oprávnění pro práci s objekty v aplikaci. Oprávnění lze přidělovat i omezovat také na konkrétní data – například vedoucí spravuje podřízené, garant role spravuje své role. Omezení, jaká data uživatel může spravovat, je v CzechIdM reprezentováno tzn. Evaluátory. Například evaluátor „SubordinatesEvaluator“ umožní všem nadřízeným spravovat identity, které jsou z organizačního postavení podřízené. CzechIdM obsahuje sadu takovýchto evaluátorů, která umožňuje omezit práci na organizační zařazení uživatelů, konkrétní katalog rolí (např. pouze pro určité aplikace) nebo na konfiguraci konkrétního systému (spuštění synchronizace HR). CzechIdM je od základu samo řízeno skrz Role a jejich oprávnění a evaluátory a umožňuje tedy omezit práva na vybrané části aplikace přesně dle požadavků konkrétního objednatele.
možnost zadat oprávnění konkrétním uživatelům, skupinám, funkčním místům nebo organizačním jednotkám, aby mohli (pouze) spouštět vybraný synchronizační proces –	ANO	Viz předchozí bod

např. personalistky si budou moci ručně pustit vstupní synchronizaci z personálního IS do IDM bez asistence administrátorů IDM.		
IDM umožní nastavení prahových hodnot, které zabrání hromadným změnám např. z důvodu chybných dat na vstupu (např. z personálního systému), tak 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 poplatná pro všechny vstupně/výstupní konektory.	ANO	CzechIdM zařazuje požadavky na provisioning dat (propis dat do spravovaného systému) do fronty provisionigu. Z této fronty jsou data odesílána na systém. CzechIdM obsahuje mechanismus pozastavení odesílání neboli přepnutí systému do ReadOnly stavu. Dále obsahuje tzv. brzdu provisioningu. V CzechIdM je možné konfiguračně nastavit limity pro jednotlivé operace na koncový systém (CREATE/UPDATE/DELETE) nezávisle na použitém konektoru. Při blížícím se dosažení limitu je notifikován administrátor. Při dosažení limitu jsou všechny další požadavky tohoto typu pozastaveny a opět je notifikován administrátor. Zastavené požadavky jsou drženy ve frontě pro kontrolu administrátorem a je možné je manuálně provést nebo odstranit.
IDM umožní notifikovat konfliktní stavy (např. synchronizovaný systém v chybě) v systému IDM pomocí emailu na administrátory IDM, případně na další osoby (včetně zápisu do logu IDM)	ANO	CzechIdM obsahuje širokou paletu předdefinovaných upozornění a zároveň umožňuje definici vlastních přes webové rozhraní. Upozornění lze navázat prakticky na libovolnou událost v systému formou tzv. processoru, který událost zpracovává.
IDM umožní logování veškerých operací nad jednotlivými objekty (osoby, účty, funkce, synchronizované systémy, skupiny,....) i nad všemi spravovanými objekty a vlastní konfigurací.	ANO	CzechIdM obsahuje persistentní auditní log všech objektů v CzechIdM. Auditní log je tvořen formou tzn. „Time Machine“. Neboli libovolná změna na objektu v CzechIdM vyvolá zápis otisku tohoto objektu do auditního logu. V GUI CzechIdM má administrátor možnost zvolit si libovolný otisk z historie objektu – například jak vypadala identita „jnovak“ při založení. Tento otisk si může porovnat s libovolným jiným otiskem, například jak vypadá identita „jnovak“ teď.

		Dalším místem, kde lze nalézt veškeré volání operací na objektech v CzechIdM je logu rozhraní: • Veškeré změnové požadavky (UPDATE, CREATE, DELETE operace) na datech jsou auditovány ve standardním auditním logu aplikace CzechIdM. • Veškeré volání REST API je logováno předřazeným webserverem do tzv. access logu.
IDM umožní sledovat jednotlivé stavy (počty objektů/identit) v průběhu synchronizace	ANO	Standardní funkce produktu CzechIdM. Kapitola Synchronizizace
IDM bude umožňovat databázovou historizaci (možnost dohledání změn v čase)	ANO	Standardní funkce produktu CzechIdM. Viz výše
IDM umožní generování auditních reportů – přehled uživatelů a jejich aplikačních rolí, skupin definovaných v IDM včetně možnosti si zakázkově nechat vytvořit vlastní reporty.	ANO	S využitím modulu reportů. Více v kapitole popisují funkčnost tohoto modulu.
Reporty lze vygenerovat i do CSV, aby šlo s případnými daty dále pracovat v programech typu MS Excel.	ANO	Standardní funkce modulu
IDM umožní zobrazit kompletní popis napojených informačních systémů (vzájemných vazeb, typů synchronizací, ...) přímo u jednotlivých synchronizovaných IS z administrace IDM. Tyto popisy budou dodavatelem pravidelně udržovány a budou do nich zaznamenávané veškeré změny	ANO	CzechIdM udržuje informace o systému v konfiguraci daného systému: • Základní konfigurace spojení • Mapování spravovaných atributů • výčet sychronizací a historie jednotlivých běhů Jakékoli změny jsou předmětem automatického záznamu do auditního systému CzechIdM a jsou standardně rekostruovatelné pomocí mechanismu „time-machine“ viz. výše
V rámci implementace IDM do prostředí objednatele dojde k integraci na následující informační systémy způsobem, kdy IDM převezme správu veškerých identit a řízení veškerých uživatelských rolí v těchto informačních systémech za využití odpovídajících standardizovaných rozhraní těchto systémů:	ANO	Viz. níže
Microsoft Active Directory	ANO	Bude využit standardní konektor CzechIdM
JIP/KAAS	ANO	Bude využit specializovaný modul (konektor) CzechIdM
Emailový server IceWarp	ANO	Bude využit standardní konektor CzechIdM

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.	ANO	U uvedených systémů není předpoklad pro využití součinnosti třetích stran. Je možné že bude řešeno v rámci očekávaného rozvoje prostředí.
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.	ANO	Standardní součástí CzechIdM je synchronizace dat z napojených systémů, která je prováděna buď opakovaně (zdroj dat) nebo jednorázově – migrace dat ze spravovaných systémů. Standardní synchronizace v CzechIdM dokáže načítat jak základní objekty (identity, role, struktury atd.), tak jejich aktuální vzájemný vztah (jednorázová migrace stavu v napojovaných systémech) – tzn. například identita a její role/skupiny v MS AD, nebo identita a její zařazení na systemizované místo

1.3.2 Popis řešení

Centralizované řešení správy identit a jejich uživatelských účtů a oprávnění v koncových systémech bude v města Klatovy implementováno pomocí software CzechIdM, edice Enterprise.

Identity manager umožňuje z jednoho místa zjištění aktuálního stavu rolí, identit a uživatelských účtů, všechny prováděné operace jsou auditovány a dohledatelné přes webové rozhraní aplikace.

Nasazení tohoto systému umožní automatizaci správy životního cyklu identit. Zamezí akumulaci práv – umožní automatické přidělování práv na určitou dobu „od-do“ a tím zmenšuje prostor pro lidskou chybu nebo opomenutí. Zároveň také zavede centrální webové rozhraní pro uživatele s možností žádosti o přidělení rolí a změny hesla.

Implementovaný identity manager bude spravovat identity následujícího typu:

- interní zaměstnanci

Správa životního cyklu identit, kterou bude identity manager provádět automaticky na základě informací z personálního systému nebo ručně zadaných informací o identitě, bude řešit následující procesy. Uvádíme seznam řešených procesů a rámcový rozsah implementace:

- Nástup nového zaměstnance
  - Nově vzniklý záznam o zaměstnanci v personálním systému bude identity manager automaticky přebírat, vygeneruje unikátní uživatelské jméno dle politiky definované v rámci úvodní analýzy projektu. Identity manager automaticky založí do Active Directory, případně do jiných koncových systémů uživatelský účet.
- Výmaz zaměstnance
  - Na základě informace z personálního systému identity manager provede okamžité zneplatnění identity a tím i zneplatnění uživatelských účtů ve koncových systémech. Identita bude po 30 dnech od tohoto zneplatnění smazána.
- Úprava identity
  - Identity manager automaticky provádí aktualizaci popisných atributů a přejmenování na koncových systémech, které tuto operaci podporují. Aktualizace bude iniciována změnou atributu v personálním systému a realizována v rámci automatické synchronizace.
- Změna hesla
  - Změna hesla bude realizována z webového rozhraní identity manageru na systém Active Directory. Změnu hesla bude moci provádět uživatel s přiděleným potřebným oprávněním. Změna hesla bude podřízena politice pro hesla. Exspirace hesla bude řízena koncovým systémem (tj. Active Directory).
- Žádosti o přidělení rolí
  - Přes webové rozhraní identity manageru bude možné požádat o přidělení role pro sebe nebo svého podřízeného. Žádost pro kohokoliv bude moci podat uživatel s potřebným oprávněním.
  - Žádost o role vyvolá schvalovací workflow, toto workflow je konfigurovatelné a umožňuje jedno či více kolové schvalování. Po zpracování schvalovacího workflow schvalovatelem (případně více schvalovateli) bude výsledek ihned zpracován. Jestliže byla žádost schválena, role jsou automaticky přiděleny uživateli.

- Žádost o role bude využita standardní produktová, která splňuje požadavky kladené v zadávací dokumentaci.

1.3.3 Úvodní analýza projektu

Pro realizaci projektu bude vytvořena úvodní analýza projektu. V rámci těchto činností budou získány od pracovníků zadavatele informace potřebné pro implementaci identity manageru.

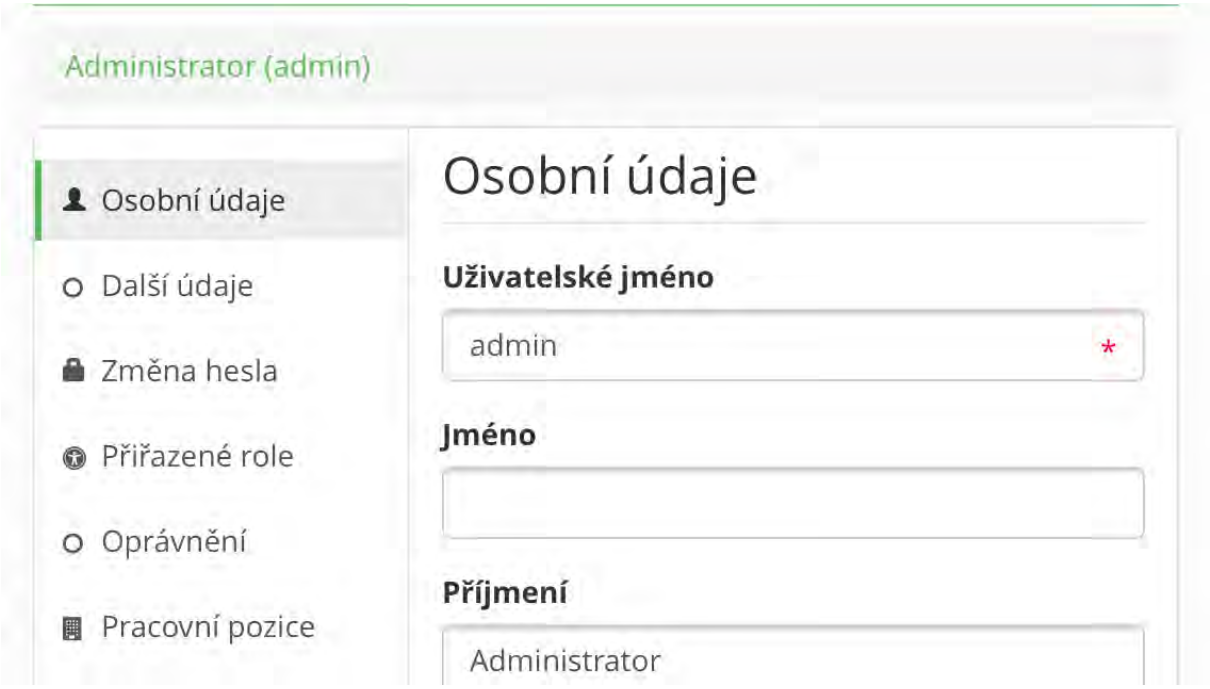
Zejména se jedná o:

- Získání informací o aktuálních procesech správy životního cyklu identit
- Tvorba loginu uživatele
- Politika hesel
- Předání informací o konektorech pro správu napojovaných systémů a potřebném aplikačním rozhraní (API) těchto systémů, získání informací o přístupu k API
- Získání informací o schvalování oprávnění a notifikacích
- Získání informací o konfiguraci sítě a prostředí pro instalaci CzechIdM do prostředí sítě města Klatovy.

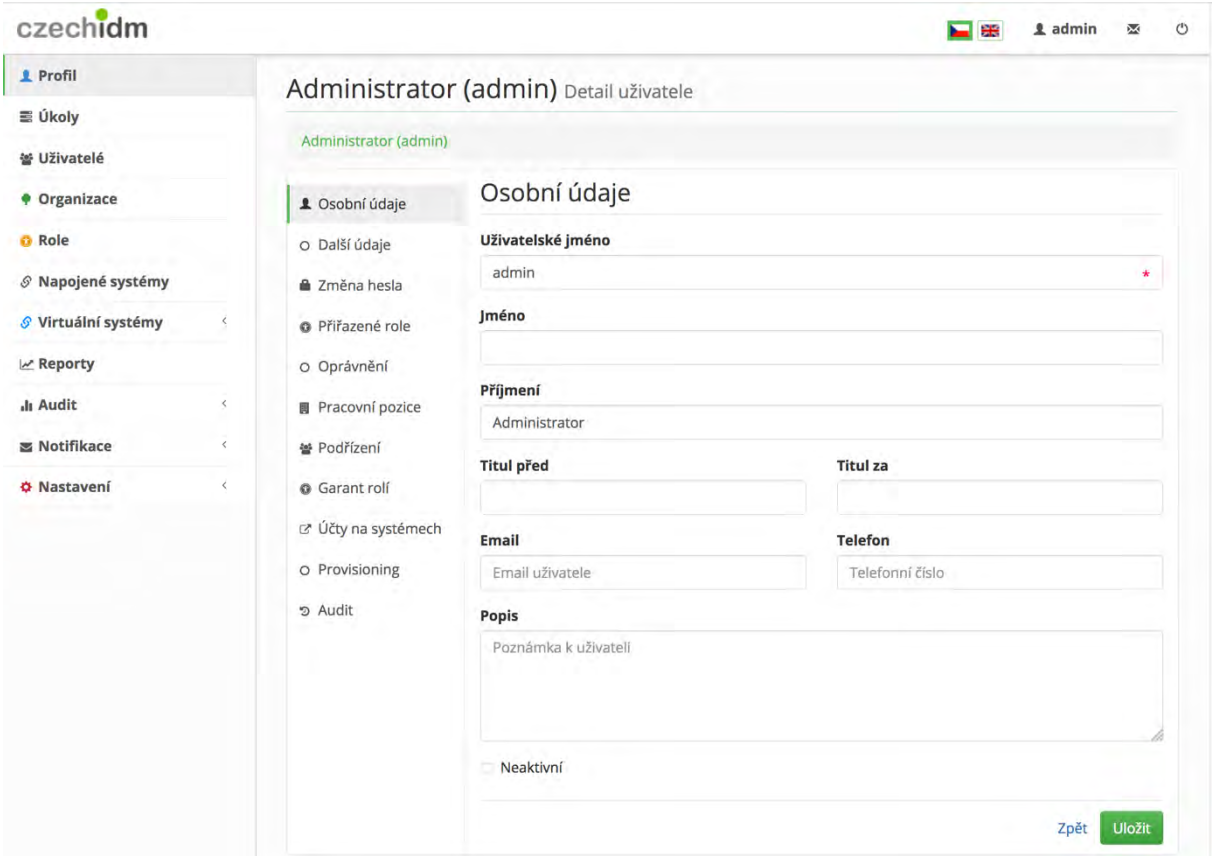
1.3.4 Obecné požadavky na uživatelské rozhraní

Uživatelské rozhraní CzechIdM je řešeno jako webová aplikace přístupná z aktuálních běžně používaných webových prohlížečů s podporou javascriptu. Aplikace podporuje zobrazení na různých typech zařízení od osobních počítačů až po mobilní zařízení. Rozhraní je lokalizováno do českého a anglického jazyka s možností lokalizace do dalších jazyků.

Uživatelé mají v závislosti na svých oprávněních dostupné jednotlivé funkce správy identit. Všichni uživatelé včetně administrátorů tak používají jednotné rozhraní jak pro běžné činnosti typu schvalování a žádosti o role, tak i pro administraci CzechIdM (v závislosti na oprávnění).



Obrázek 1 - Snímek obrazovky z mobilního telefonu



Obrázek 2- Snímek obrazovky z počítače

1.3.5 Autoritativní zdroj dat

Zdrojem identit/uživatelů bude personální systém, který je bude standardním připojen univerzálním konfigurovaným konektorem. Zdrojů může být více, v CzechIdM není na zdroj dat jiný požadavek než podpora čtení informací v konektoru KONCOVÝ SYSTÉM. Zdrojem dat o identitě může být také ruční zadání přes webové rozhraní, případně zadání informací z externího systému přes REST rozhraní do CzechIdM.

Identity manager umožní spravovat identity různého typu:

- Interní uživatelé

Typ identit není omezen, lze evidovat identity různého typu a rozdělit je do samostatných komunit, na které je možné aplikovat různá oprávnění a pravidla (např. pro každou komunitu jiná organizační struktura apod., jiný delegovaný správce).

1.3.6 Firemní pravidla a byznys logika v CzechIdM

Identity manager CzechIdM je modulární aplikace, která je uzpůsobena pro striktní oddělení produktu a zákaznické implementace. Implementace u zákazníka je vedena v samostatném modulu, který je na produktu nezávislý, resp. má požadavky na minimální kompatibilitu API.

Proto je velmi snadné aktualizovat produkt na novější verzi – zákaznické úpravy se nemusí složitě přenášet a aktualizaci zvládne snadno i správce se základním zaškolením.

Úpravy fungování CzechIdM je možné provádět na různých úrovních:

- přes webové rozhraní lze změnou konfigurace ovlivnit chování standardních funkcí produktu a výchozích workflow,
- složitější úpravy chování – různé transformace a úpravy dat lze vynutit pomocí groovy skriptů, které se aplikují při přidělování rolí uživateli, načítání dat z KONCOVÝ SYSTÉM a zápisu do KONCOVÝ SYSTÉM, aplikace skriptů se provádí přes webové rozhraní
- výchozí produktová workflow lze při upravit nebo nahradit vlastními workflow, nová workflow se zavádí přes webové rozhraní.
- rozšíření fungování identity manageru tzv. procesory, které lze navázat na události v systému (například „uložení identity“, „změna přidělených rolí“ apod.), procesor je implementován v Javě v zákaznickém modulu.

Politiky pro validaci a generování hesla

CzechIdM obsahuje politiky hesel pro validaci a generování. Pravidla odpovídají nárokům MS AD a dalších podobných systémů. Kromě výchozí politiky lze mít na konkrétní

systémy přiřazenou jinou politiku. Stejně tak lze generovat hesla tak aby byla pro uživatele lépe použitelná (např. vynechat il1 při zasílání SMS, vygenerovat přístupovou frázi místo hesla apod.) a přesto splňovala bezpečnostní politiky.

Pravidla tvorby názvu účtu

Loginy, emailové adresy, emailové aliasy a další podobné řetězce se v CzechIdM vytváří pravidly podle zákaznicky dodaného algoritmu. Nastavení pravidel pro tvorbu řetězců je plně konfigurovatelné administrátorem přes webové rozhraní a zapisuje se ve formě groovy skriptu.

1.3.7 Možnosti integrace s dalšími systémy

Rozhraní pro integraci

CzechIdM obsahuje různá rozhraní pro integraci:

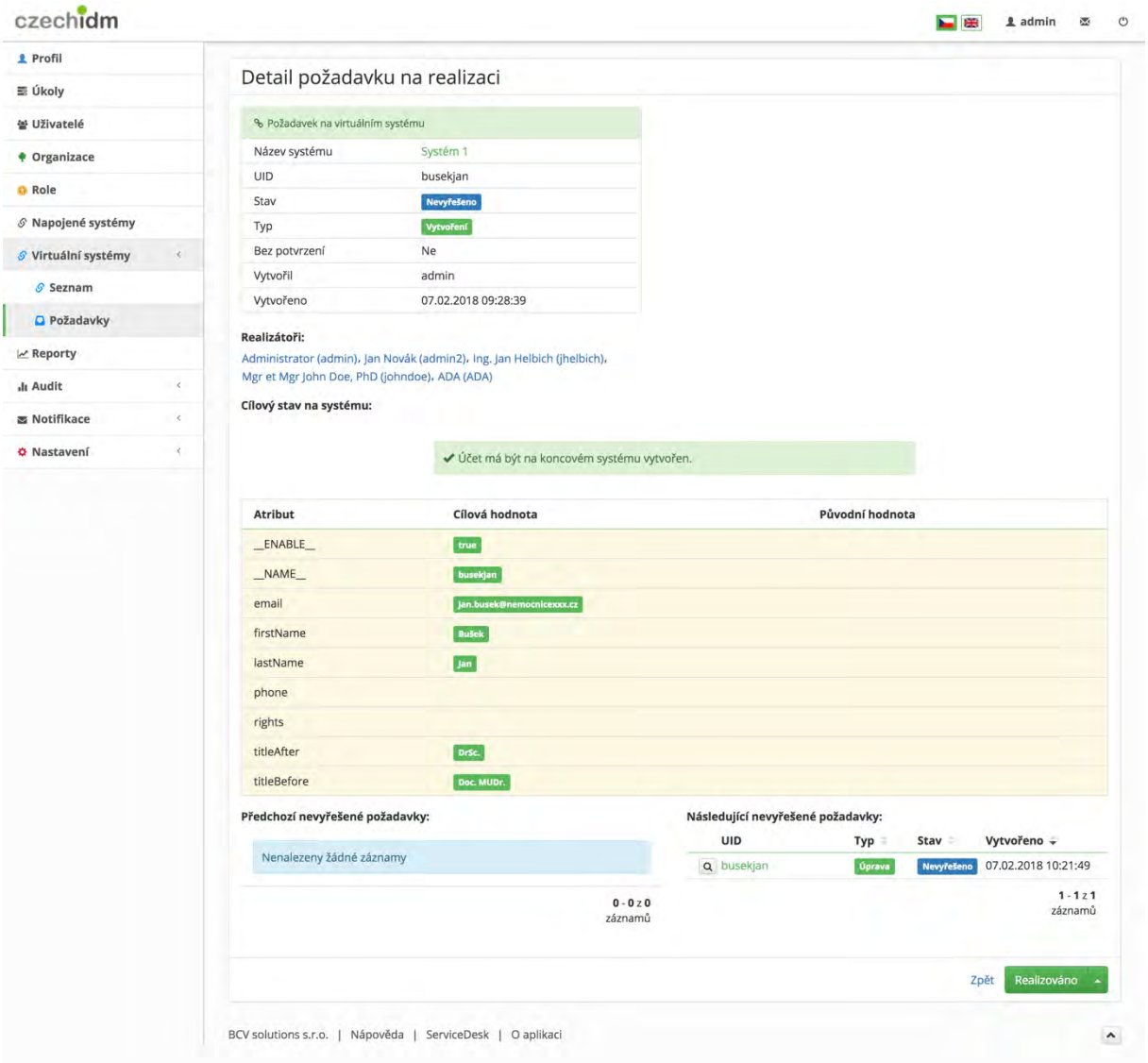
- REST api – zpřístupňuje všechny funkce identity manageru
- Konektory – slouží pro napojení na KONCOVÝ SYSTÉM
- Notifikace – SMTP, SMS brána, vlastní transport

REST API

REST API zpřístupňuje všechny funkce identity manageru, které jsou dostupné z webového rozhraní. Standardně je dostupné přes https.

Konektory pro napojení na koncové systémy

Definice koncového systému v identity manageru obsahuje konfiguraci konektoru, konektor je knihovna, která slouží pro napojení IdM na KONCOVÝ SYSTÉM. V základu provádí tzv. „CRUD“ operace nad identitami, ale podle konektoru také někdy nad rolemi, skupinami nebo například organizační strukturou.



Obrázek 3-Offline napojený systém - detail požadavku na realizaci

Účty na koncových systémech jsou řízeny buď automatickými procesy nebo na základě pokynů z webového rozhraní administrátorem (tedy přes REST API).

Pro napojení identity manageru na koncový systém jsou dostupné minimálně následující konektory:

- MS AD konektor – připojení k MS Active Directory (LDAP, Powershell)
- LDAP konektor – LDAPv3 konektor
- CSV konektor – konektor pro připojení CSV souboru

Dále jsou dostupné univerzální konektory, kterými lze připojit velké množství aplikací:

- skriptovatelný konektor pro MS Windows (Powershell)
- skriptovatelný konektor pro unixové OS (SSH, shell)
- skriptovatelný konektor pro připojení k DB přes JDBC (groovy skripty)

Pro CzechIdM je dostupné velké množství dalších hotových konektorů, které jsou uvedené v dokumentaci produktu na webu.
Pokud není pro některou aplikaci konektor dostupný, je možné snadno vytvořit vlastní konektor.

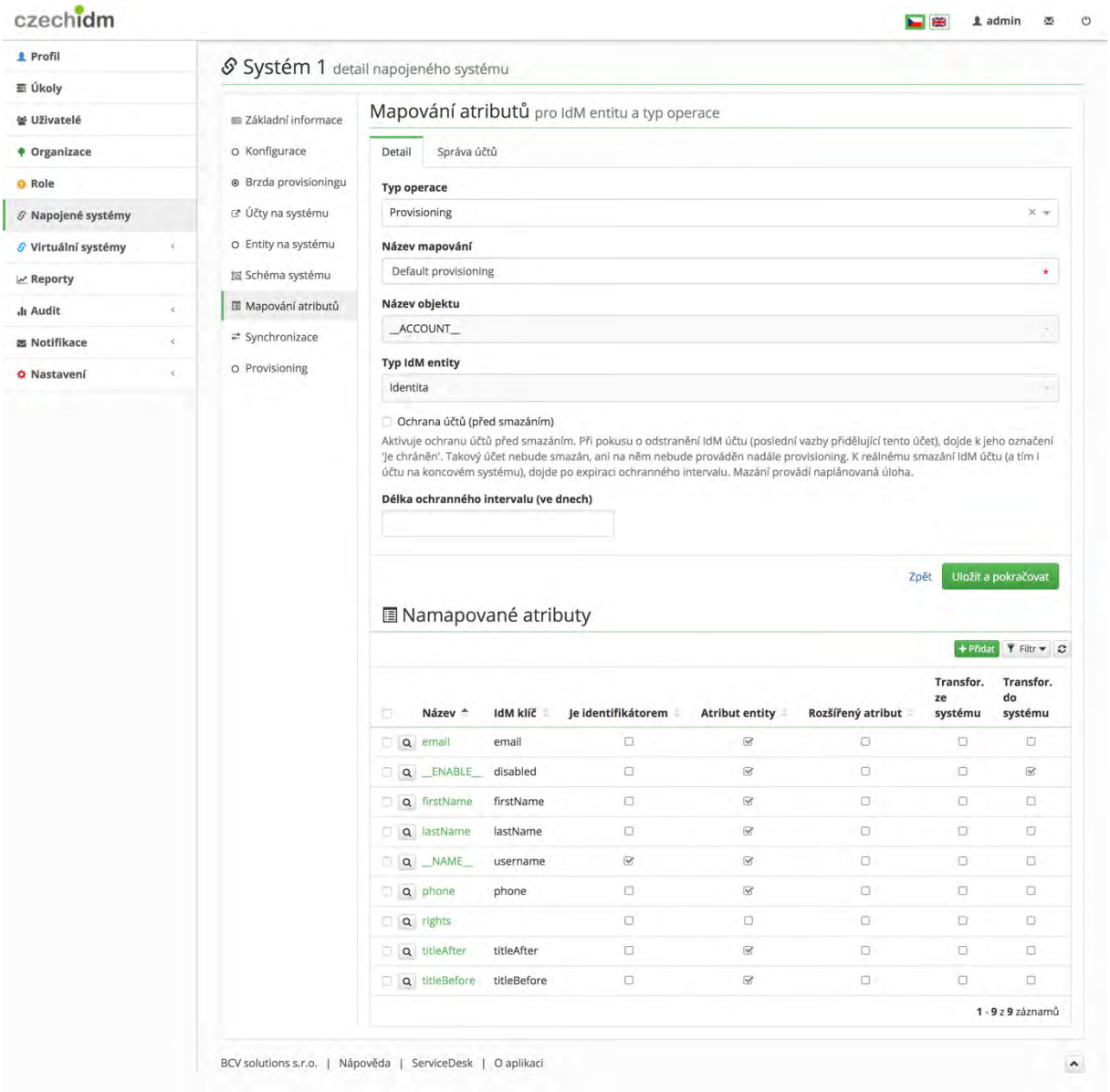
Aplikace spravované ručně se připojují jako tzv. virtuální systémy. Z pohledu uživatele se jedná o běžný systém, ale z pohledu správce IdM je to systém spravovaný pomocí výzev k ruční realizaci. Každý virtuální systém má plnou funkčnost (tj. lze nad ním spouštět rekoncilace, mít odpovídající mapování atributů apod.), jen modifikační požadavky jsou předávány k realizaci administrátorovi tohoto systému.

Mapování atributů mezi IdM a KONCOVÝM SYSTÉMEM

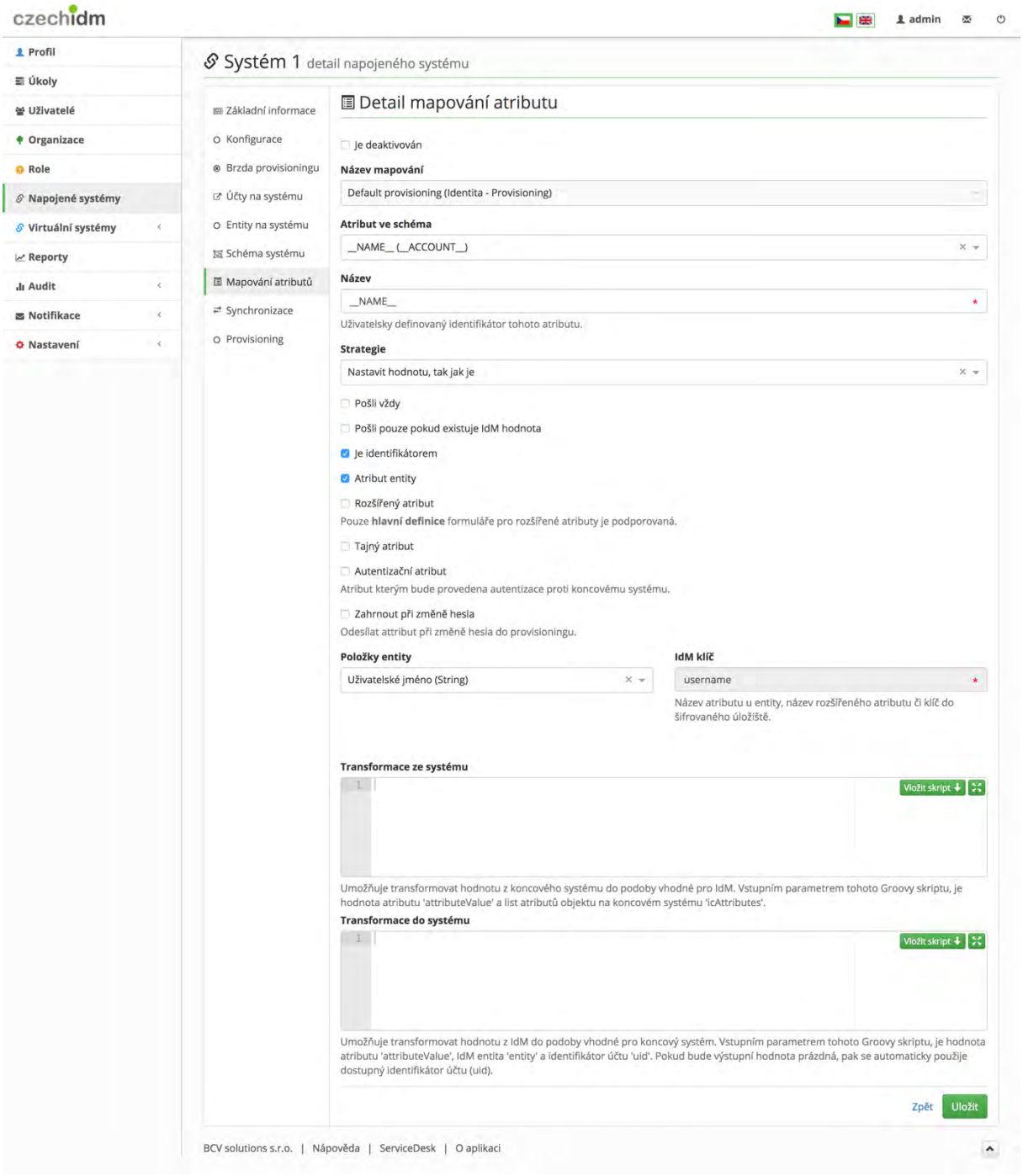
Při napojení identity manageru na koncový systém je možné nakonfigurovat pro každý systém samostatné mapování atributů (tj. jméno v IdM je „firstname“ v KONCOVÉM SYSTÉMU), jejich transformace při zápisu/čtení, určit který atribut je unikátní identifikátor, proti kterému se případně provádí autentizace apod.

Pro jednotlivé atributy jsou podporovány různé datové typy a lze běžně spravovat i data typu certifikáty, uživatelská fotografie atd.

Také podporovány atributy s citlivými informacemi jako je PIN, heslo apod. Tyto atributy (jejich hodnoty) jsou automaticky všude v GUI zobrazovány pomocí zástupných znaků, a pokud je to z nějakého důvodu třeba, tak jsou ukládány v IdM šifrovaně a nepřenáší se v procesech nechráněné.



Obrázek 4-Koncový systém - mapování atributů mezi IdM a KONCOVÝM SYSTÉMEM



Obrázek 5-Koncový systém – detail mapování jednoho atributu

1.3.8 Provisioning

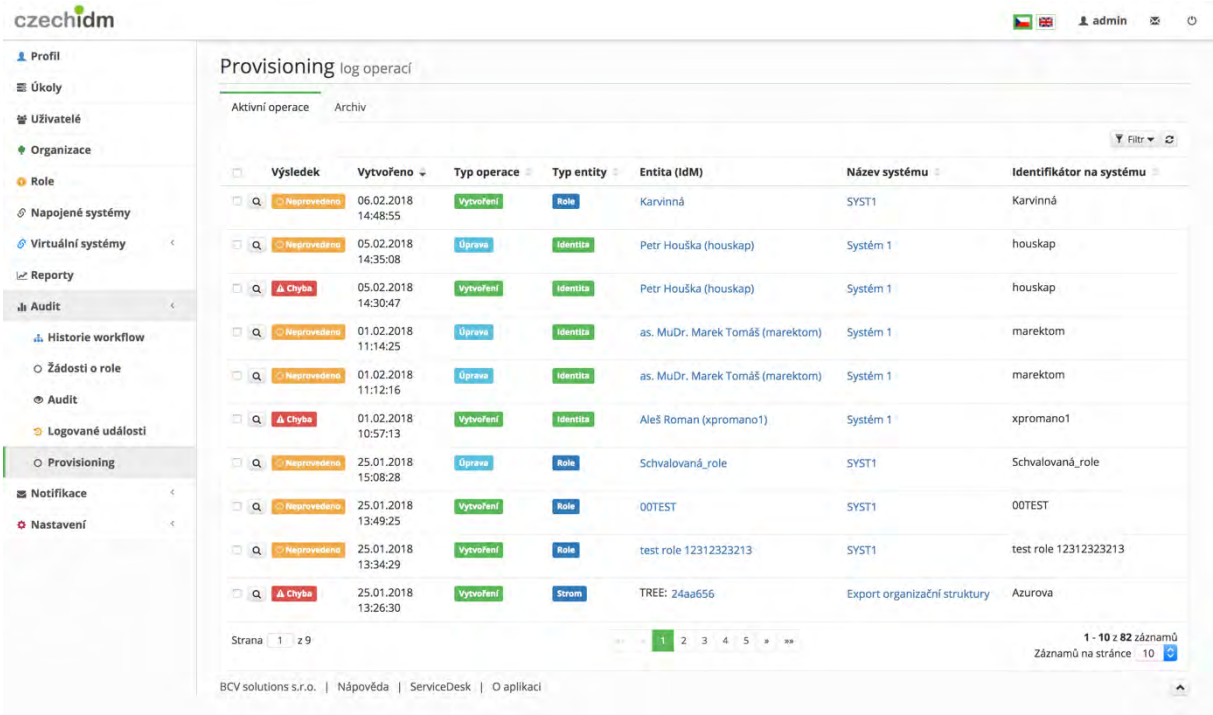
Zápis změn z IdM na koncový systém je prováděn v rámci operace „provisioning“. Provisioning v závislosti na podporovaných funkcích konektoru připojujícímu konkrétní koncový systém provádí:

- čtení informací o účtu
- vypsání všech účtů
- vytvoření
- úprava popisných atributů
- změna přiřazení rolí
- nastavení/změna hesla
- enable
- disable
- autentizace uživatele proti systému
- seznam skupin/rolí na koncovém systému
- vytvoření, úprava a smazání skupiny/role na koncovém systému
- seznam prvků organizační struktury na koncovém systému
- vytvoření, úprava a smazání prvků organizační struktury na koncovém systému

Pro všechny výstupní operace z IdM směrem ke KONCOVÝ SYSTÉM je implementována řada funkcí, které slouží pro podporu běžného provozu:

- ošetření chyb v komunikaci s KONCOVÝM SYSTÉMEM, možnost vynutit opakování
- „brzda“ na operace – např. povolení pouze 2 operací delete na systému za hodinu, pokud by bylo operací víc, tak jsou zablokovány a čekají na administrátorovo potvrzení. Administrátor je notifikován.
- archiv provedených operací včetně zaslaných hodnot na koncový systém
- požadavky na realizaci mohou být řešeny synchronně (proces čeká na výsledek – např. změna hesla a nahlášení úspěšného provedení uživateli v GUI) nebo asynchronně (dlouhotrvající proces se spustí na pozadí a v GUI umožní uživateli pokračovat v činnosti)
- Agenda je dostupná administrátorovi přes webové rozhraní jak pro každý systém zvlášť, tak souhrnně pro všechny koncové systémy.

Proces provisioningu lze ovlivnit pomocí vlastního procesoru a lze tak vynutit např. částečný provisionig v závislosti na stavu účtu na koncovém systému apod. (lze tak kontrolovat splnění podmínek pro provisioning a přidělení oprávnění).



Obrázek 6- Provisioning - fronta nedokončených operací

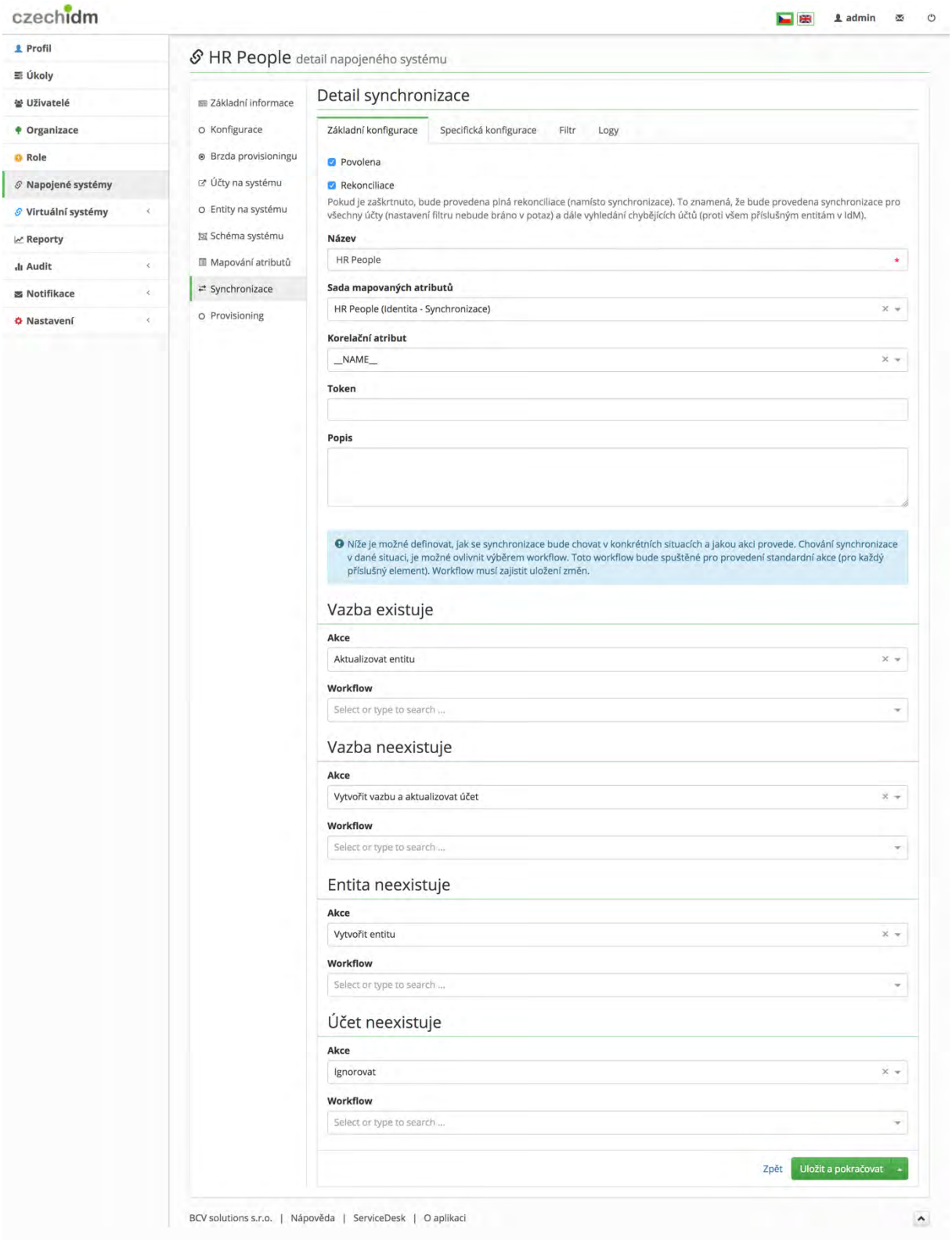
1.3.9 Synchronizace, rekonciliace

Podpora pro synchronizace a rekoncilace je standardní součástí všech spravovaných systémů (i virtuálních – tedy „offline“ systémů) závislá pouze na podpoře konkrétního použitého konektoru.

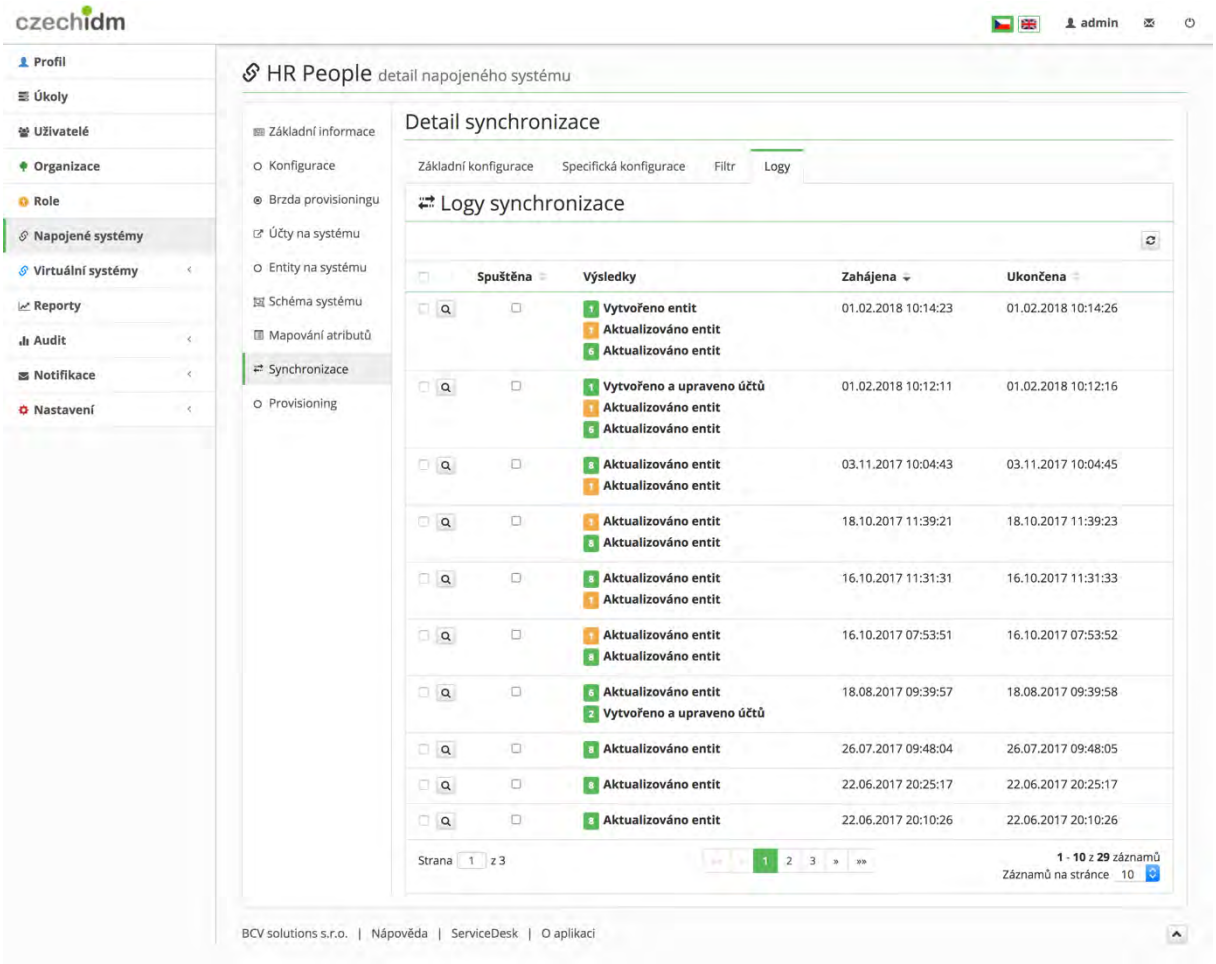
Jak synchornizace tak i rekoncilace mají stejné konfigurační možnosti, liší se jen schopností pracovat nad změnami (synchronizace) nebo celou sadou dat (rekoncilace). Synchronizace a rekonciliace jsou podporovány pro různé objekty (identita, vztah, role, org. struktura), které se definují v konfiguraci. Stejně tak je možné definovat filtry omezující seznam zpracovávaných objektů.

Pro každou synchronizaci/rekoncilaci je možné nastavit vlastní korelační pravidla. CzechIdM podporuje více různě nastavených synchronizací/rekonciliací pro každý spravovaný systém. Synchronizace i rekoncilace mohou být spouštěné ručně na vyžádání administrátorem nebo automaticky v závislosti na naplánování.

Pro každý stav synchronizované/rekonciliované entity je možné nadefinovat konkrétní akci včetně vlastního workflow. Všechny prováděné operace jsou podrobně auditovány. V průběhu, ale i po dokončení synchronizace lze na jednotlivé události reagovat dalšími (i vlastními) akcemi.



Obrázek 7- Synchronizace - detail konfigurace



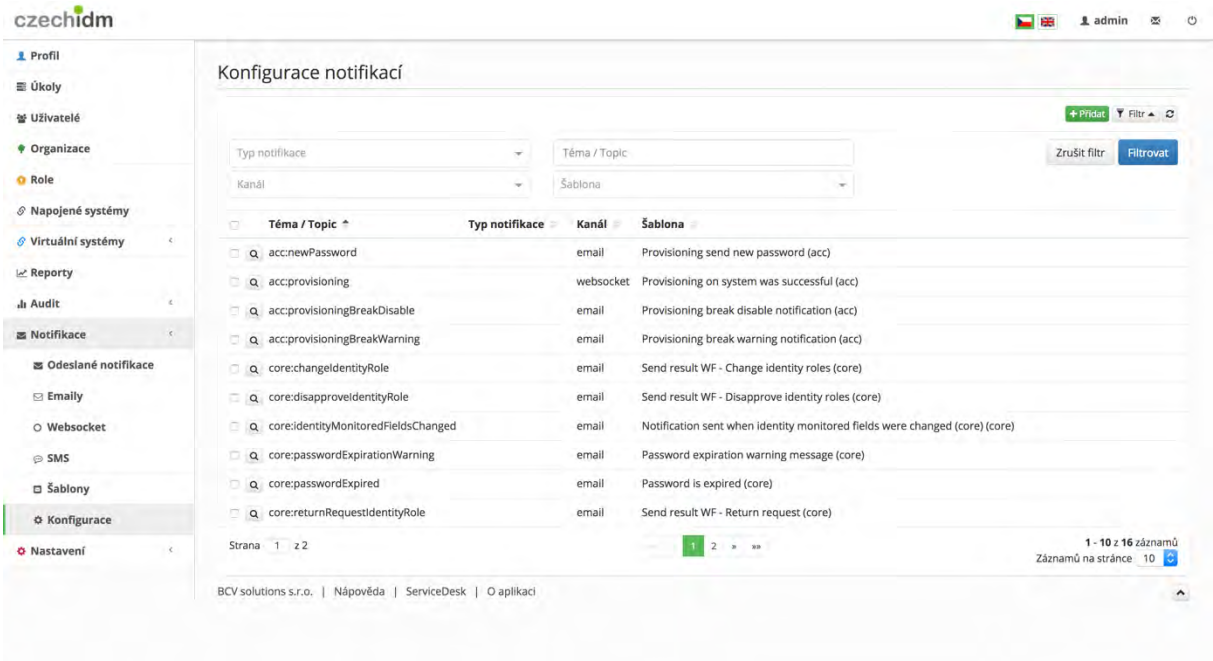
Obrázek 8- Synchronizace - logy proběhlé synchronizace

1.3.10 Notifikace

Identity manager CzechIdM disponuje systémem notifikací, který má dostupnou samostatnou agendu pro konfiguraci notifikací a kompletní historii zaslaných notifikací.

Konfigurace notifikací umožňuje nastavit směrování zpráv – například po dokončení synchronizace zaslat informaci emailem. Dále obsahují šablony jednotlivých zpráv, které může administrátor upravovat nebo přidávat. Zasílání notifikací je standardně podporováno na email, SMS (pokud je připojena SMS brána), websocket (uživateli do webového prohlížeče). Další kanály pro notifikace je možné přidat v zákaznickém modulu.

Notifikované akce
Notifikace je možné zařadit do různých částí identity manageru – ať už do workflow, tak i do jednotlivých dílčích procesů v rámci zpracování události vlastním procesorem.



Obrázek 9-Notifikace - konfigurace směrování zpráv

1.3.11 Operace spojené s připojením do koncových systémů

Identity manager podporuje operace vypsané v Technické specifikaci Zadavatele dle požadavků.

Podporované operace:

- Vytvoření účtu
- Aktivace a deaktivace účtu
- Čtení informací o účtu
- Update informací účtu
- Přiřazení aplikačních rolí
- Odebrání aplikačních rolí
- Odebrání všech aplikačních rolí
- Seznam přiřazených aplikačních rolí
- Seznam aplikačních rolí
- Seznam uživatelů koncového systému
- a další, viz dokumentace produktu na https://wiki.czechidm.com/

1.3.12 Role management

Správa rolí je neoddělitelnou součástí správy identit. Role udělují uživateli různá práva do spravovaných aplikací nebo do identity manageru.

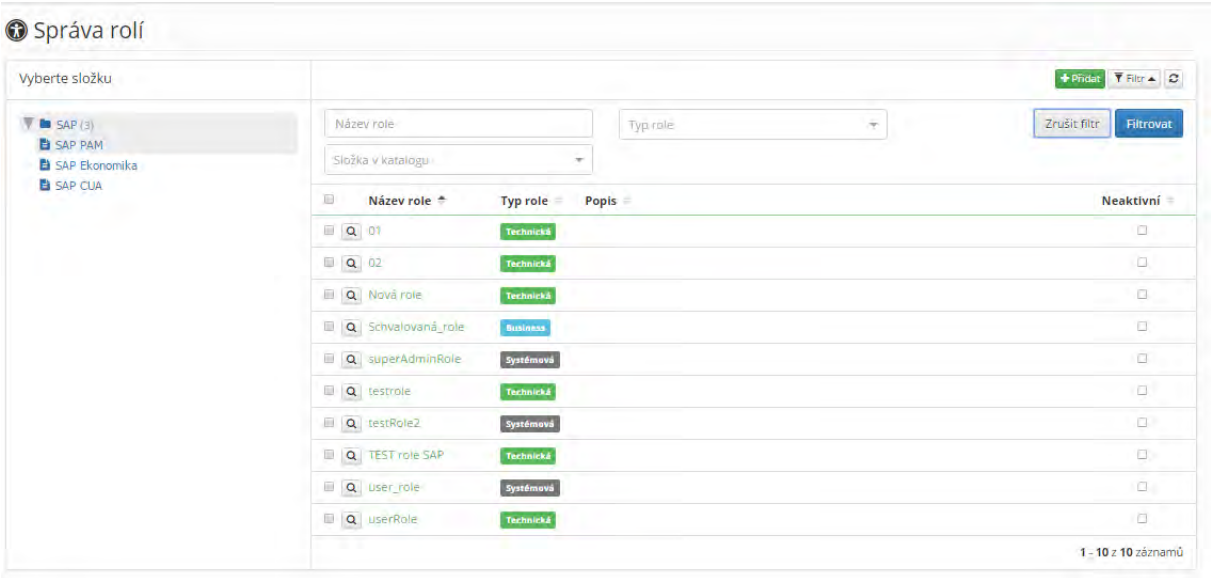
Definice rolí v CzechIdM je prováděna administrátorem přes webové rozhraní. Přiřazování rolí uživatelům může být realizováno automatickými procesy nebo ručně přes webové rozhraní v rámci různých procesů nebo na základě žádosti oprávněné osoby. Přidělení rolí uživateli je kontrolováno schvalovacím procesem.

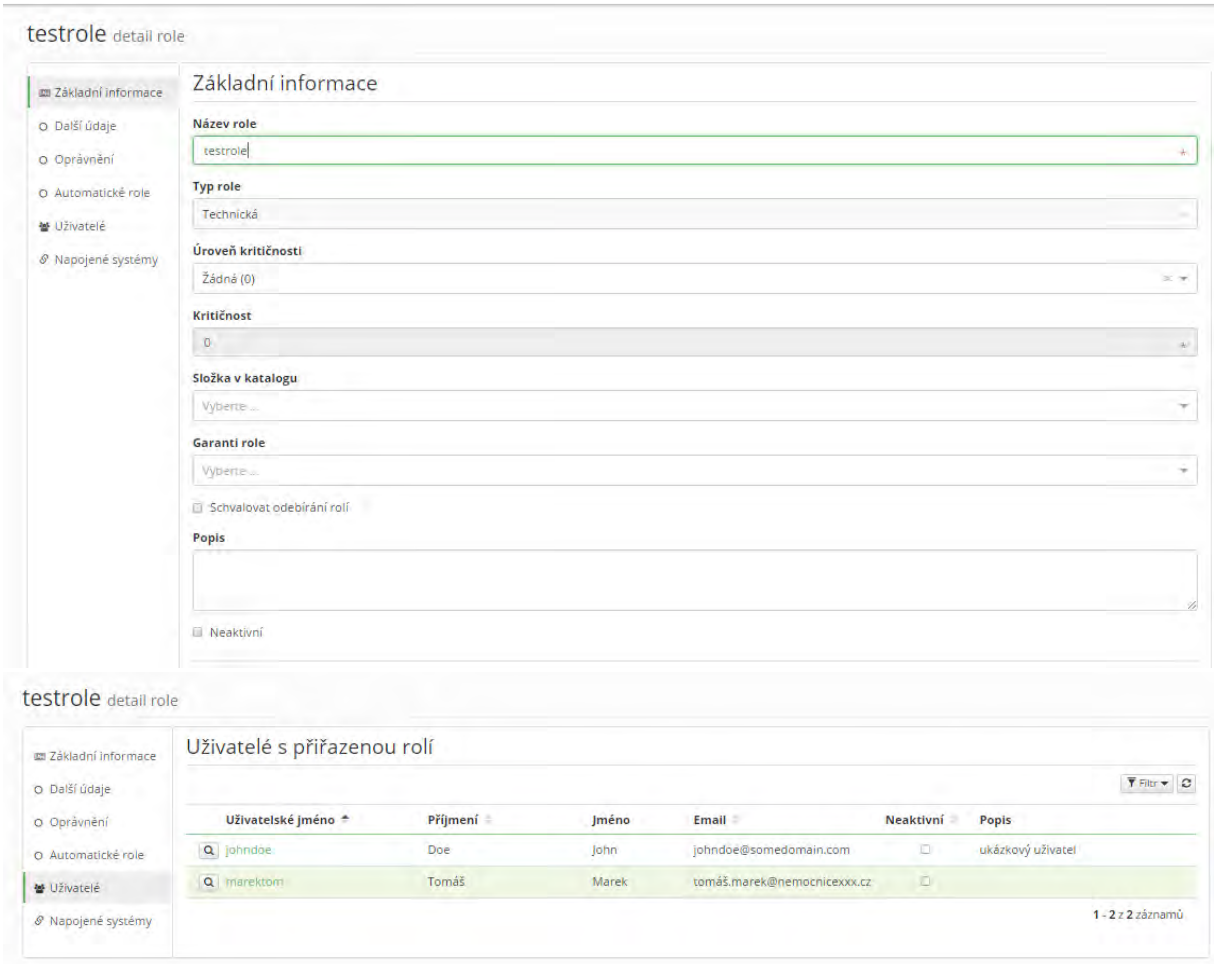
CzechIdM v rámci svého grafického rozhraní nabízí možnost žádat o role, které přiřazují oprávnění ve spravovaných systémech.

Zajímavé vlastnosti rolí:

- Garanti role
- Různá schvalovací workflow pro role
- Platnost přidělení od-do
- Kritičnost rolí
- Sloučení rolí
- Automaticky přidělované role dle pravidel
- Synchronizace rolí z externího zdroje
- Export rolí do spravovaného systému

Správa rolí v CzechIdM



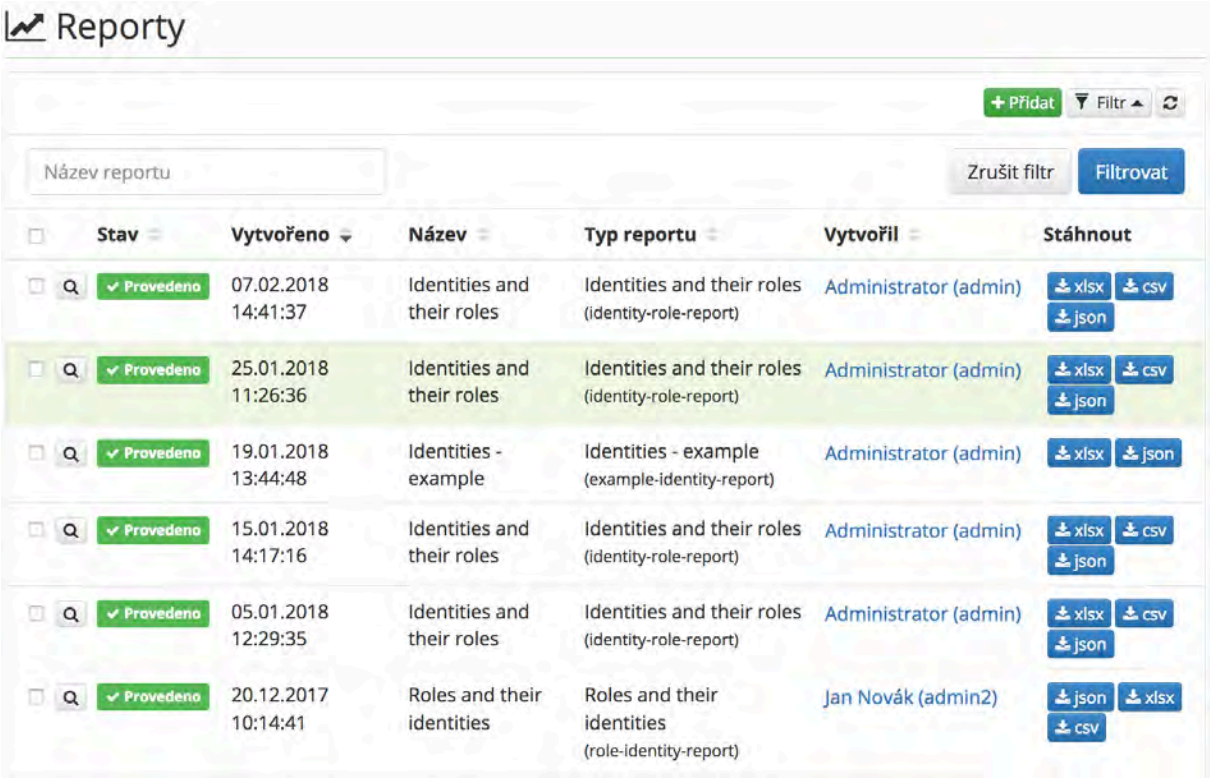


1.3.13 Reporting

Identity manager uchovává a zpřístupňuje logy aplikace, auditní informace o změnách entit a výsledky rekoncilace, synchronizace, provisioningu.

Reportování je v CzechIdM řešeno samostatným modulem Reporty. který slouží pro správu a spouštění samotných reportů.

Jednotlivé reporty jsou samostatné objekty importované z modulů, lze tedy i v budoucnu přidávat další reporty. Při spouštění je možné report parametrizovat. Výsledky spuštěného reportu se ukládají a je možné je stáhnout přes web.



Obrázek 10 - Reporty - uložené výsledky ke stažení

1.3.14 Modul připravených reportů

Reporty mají vypovídající hodnotu při užití na reálných případech a dle reálných potřeb zákazníka. Nové druhy reportů jsou do tohoto modulu pravidelně přidávány, případně konfigurovány dle potřeb projektu .

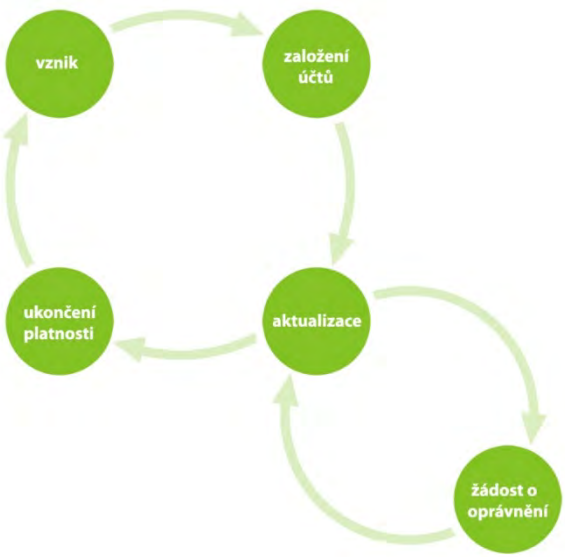
Modul obsahuje sadu reportů:

- Identity a jejich role - podporované formáty: CSV, XLSX, JSON
- Seznam rolí a identity, které danou roli mají - podporované formáty: CSV, XLSX, JSON
- Provisioning operace - přehled čekajících (aktivních) operací ve frontě provisioningu a atributů, které budou zapsány na koncový systém. Podporovaný formát: XLSX

1.3.15 Procesy správy identit

CzechIdM nabízí následující procesy uživatelské identity

- Nová identita – na základě synchronizace ze zdroje dat založí novou identitu pro zaměstnance v CzechIdM, pokud nebyla načtena již dříve
- Nový vztah – identity mají v CzechIdM jeden a více vztahů (u zaměstnanců odpovídá počtu úvazků). Při zavedení vztahu do zdroje dat, je tento vztah přenesen k identitě v CzechIdM. Vztah může být zařazen do organizační struktury – například na určité funkční místo. Dle zařazení vztahu do struktury může identita automaticky získat role.



- Konec vztahu – CzechIdM automaticky kontroluje konec vztahu identity a odebírá či blokuje přístupy do IT systémů. Tím zajišťuje, že ve spravovaných systémech nezůstávají tzv. mrtvé duše.
- Vynětí z evidenčního počtu – při nástupu identity na mateřskou/rodičovskou dovolenou CzechIdM automaticky blokuje úvazek uživatele a může také blokovat jeho přístupy do IT systémů.

Data potřebná pro start každého procesu jsou dostupná v zdrojovém systému a budou pravidelně synchronizována do CzechIdM. Zavedením automatický procesů uživatelské identity budou nahrazeny manuální procesy. Tím se značně zjednoduší a zrychlí správa uživatelů a jejich oprávnění v IT systémech.


Správa workflow definic
Přetáhněte soubory na tuto plochu a nebo na ní klikněte pro výběr souborů.
Klíč
Název
Název zdroje
Popis
Verze
approve-delete-automatic-role
Approve delete automatic role by role guarantee
approveDeleteAutomaticRole.bpmn20.xml
Workflow for approving delete automatic role by guarantee Input variables: - entityEvent: event with roleTreeNode:
1
approve-create-automatic-role
Approve new automatic role by role guarantee
approveCreateAutomaticRole.bpmn20.xml
Workflow for approving new automatic role by guarantee Input variables: - entityEvent: event with roleTreeNode:
1
approve-role-by-guarantee
Assign role idenity. Approvers are all guarantees for given role.
approveRoleByAuthorizer.bpmn20.xml
Approval workflow for assign new role to identity or change validity dates on assigned role. Approvers are all guarantees for given role. Input variables: - applicantIdentifier - applicantUsername - operationType (add/change/remove) - conceptRole (IdmConceptRoleRequestDto) - applicantDescription
3
approve-role-by-manager
Assign role idenity. Approvers are all managers for given applicant.
approveRoleByManager.bpmn20.xml
Approval workflow for assign new role to identity or change validity dates on assigned role. Approvers are all managers for given applicant. Input variables: - applicantIdentifier - applicantUsername - operationType (add/change/remove) - conceptRole (IdmConceptRoleRequestDto) - applicantDescription
3
approve-role-by-guarantee-security
Assign role to idenity. Approvers are all guarantees for given role and all with security role.
approveRoleByAuthorizerAndSecurity.bpmn20.xml
Approval workflow for assign new role to identity or change validity dates on assigned role. Approvers are all guarantees for given role and all
3

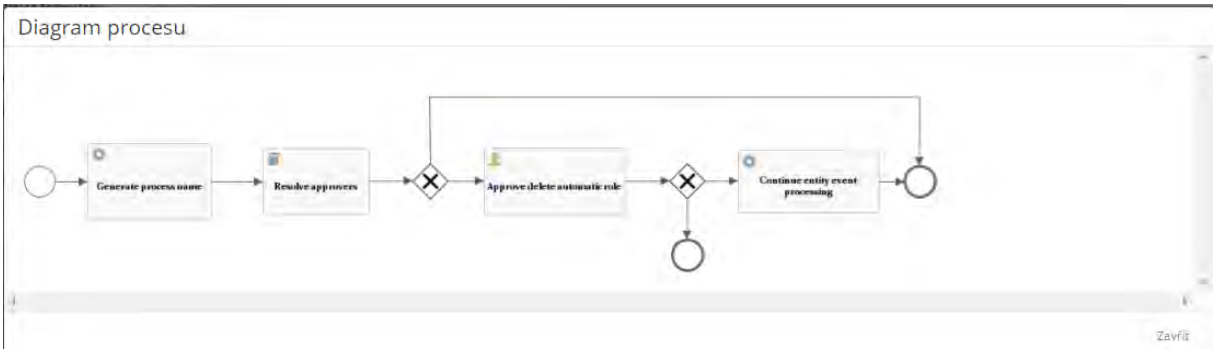


Diagram procesu
Generate process name
Resolve approvers
Approve delete automatic role
Continue entity event processing
Zavřít

1.3.16 Doporučená konfigurace HW

Doporučená konfigurace HW:

Účel serverů	Doporučená konfigurace HW	Počet serverů
Testovací prostředí		
Identity Manager, Databáze pro IdM	2 jádra CPU, 10 GiB RAM	1
Produkční prostředí		
Identity Manager, Databáze pro IdM	2 jádra CPU, 12 GiB RAM	1

1.4 Příloha č. 4 – Technické podmínky

Tento dokument je určen k popisu a definici rozsahu díla, dodávek a služeb, které objednatel poptává jako předmět plnění ve veřejné zakázce s názvem „IDM pro město Klatovy“.
Předmětem této dokumentace je popis a stanovení požadavků objednatele na dodávku a implementaci identity managementu a zpracování dokumentace.
Popis plnění podle této technické dokumentace
Předmětem plnění této technické dokumentace je dodávka a implementace identity managementu pro město Klatovy, a to včetně nedílně souvisejících požadavků typu dodání licencí a zpracování dokumentace.
Předmětem díla jsou následující činnosti zhotovitele:

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

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

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

Seznam zkratek
AIFO Agendový identifikátor fyzické osoby
Autentizace proces ověření proklamované identity subjektu
Autorizace proces získávání souhlasu s provedením nějaké operace nebo povolení přístupu
Citlivá data osobní údaje a další data, která za citlivá považuje tato Technická dokumentace a její přílohy
DB databáze
IDM Identity management system
IS Informační systém
MěÚ Městský úřad
Nařízení eIDAS 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
Nařízení GDPR 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) (Text s významem pro EHP)

Základní požadavky na IDM
Předmětem dodávky je nasazení sjednocujícího řešení pro správu identit, uživatelských rolí a oprávnění uživatelů, včetně jejich evidence, v prostředí MěÚ Klatovy (cca.200 uživatelů úřadu s možností rozšířit o další 200 externích).

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

bude následně možné takovéto požadavky schválit a změny nastavení u identit automatizovaně předat (vypublikovat) do připojených systémů (integrovaných aplikací).

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.

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

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

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.

Systém IDM bude reflektovat veškeré potřebné změny související s životním cyklem identity v prostředí objednatele a ve vazbě na všechny na IDM napojené informační systémy, ve kterých bude mít daná identita uživatelské role a oprávnění. Takové změny budou reflektovány ve všech aktuálně napojených informačních systémech vždy v konkrétní rozhodné době.
Ve vztahu k napojeným systémům musí IDM zajistit samostatnou a úplnou správu v oblasti identity a uživatelských rolí ve vztahu k těmto systémům, včetně skupin uživatelů a systematizovaných míst. Ze strany objednatele není rozhodné o kolik politik a konfiguračních operací se na straně informačních systémů jedná, ale je pro něj důležitý výsledek, tedy například správné nastavení uživatelských rolí, zařazení do skupiny a konfigurace oprávnění pro všechny funkcionality Microsoft Active Directory užívané v prostředí objednatele. IDM bude autoritativním zdrojem informací o identitách a jejich účtech a přidělených rolích. IDM bude provádět správu automaticky, tak aby byly spravované systémy vždy aktuální.

IDM bude dále realizováno při naplňování 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 auditní záznamy o prováděných změnách a poskytne reporty o stavuIDM a jeho funkcionality musí respektovat standardní architekturu I S v prostředí objednatele a pro svou integraci využít standardizovaná rozhraní a existující prostředky IS.

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...)

- postupy správy uživatelů (zavádění, změny, rušení, nastavování oprávnění...)
- návrh členění objektů v rámci IDM (osoby, účty, funkce, org. jednotky, skupiny...)
- definice bezpečnostních zásad a pravidel pro práci s IDM

Funkcionality IDM

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. Minimálně se jedná o následující procesy:

vznik nové identity

- nový pracovněprávní vztah
- úprava identity a pracovněprávního vztahu
- úpravy popisných atributů, např. jméno
- úpravy organizačního zařazení
- změny platnosti
- automatická změna rolí na základě změny stavu / typu identity, případně jiného příznaku identity
- změna evidenčního stavu identity
- ukončení pracovněprávního vztahu
- aktivace/deaktivace (ruční, automatická)

IDM musí udržovat identity, skupiny identit a organizační struktury ve své vnitřní databázi. Identity ve vnitřní databázi budou sloužit jako referenční identity pro ostatní informační systémy.

IDM musí implementovat princip založený na systemizovaných místech. IDM musí umožnit systemizaci pracovních míst v souladu se strukturou organizace, definovat jednotlivá systematizovaná místa a jejich činnosti a sadu oprávnění a rolí pro jednotlivé informační systémy organizace vztažené ke konkrétnímu systemizovanému místu.

IDM umožní přiřazení identit na takto vytvořená systematizovaná místa a to i ve vazbě M:N. Identita tedy může být v systému IDM evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit.

IDM musí umožňovat přidělení 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 umožní registraci aplikací a jejich rolí a dále také import rolí přes webové služby do IDM.

IDM musí umožnit nastavení schvalovacího workflow (při přidělení práva, role atd.), včetně emailových notifikací a potvrzování.

IDM musí umožnit definovat vztahy zastupitelnosti mezi uživateli – musí umožnit uživatelům, aby v souladu se strukturou úřadu mohli delegovat v případě potřeby (nemoc, dovolená atd.) svoje role, nebo jejich část na jiné pověřené osoby, a to i tak, že jeden uživatel může mít pro každou svou činnost nastaveného jako zástupce jiného různého uživatele. Delegace oprávnění bude dočasná, kdy se po nastaveném intervalu, nastavená delegace automaticky v IDM zruší.

IDM musí umožnit dodatečné přidávání vlastních atributů k identitám.

IDM musí umožňovat přesun identity v rámci organizační struktury i mezi jednotlivými organizačními strukturami.

IDM musí mít možnost detekovat situaci, kdy se ve zdrojovém systému vyskytne 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.

Veškeré požadavky, které provedou uživatelé na IDM, musí být provedeny transakčně, musí být historizovány a logovány tak, aby bylo možné zpětně prokázat kdo, kdy a co změnil v IDM identitách, referenčních objektech, ale i v administraci. Záznam v historii musí obsahovat původní i novou hodnotu.

IDM umožní autonomní správu hesel (samoobsluha).

IDM bude komunikovat v českém jazyce.

Požadavky na kontrolní reporty
IDM musí umožňovat generování min. těchto kontrolních reportů:
- přehled uživatele (uživatelů) a jejich rolí v systémech spravovaných IDM v době generování reportu,
- report historie delegování práv uživatele/uživatelů v definovaném časovém období.

IDM musí umožnit generování těchto reportů ve strojově čitelném formátu (např. v XML).
Požadavky na grafické rozhraní IDM

IDM musí obsahovat grafické uživatelské rozhraní pro přístup administrátorů systému pro správu identit uživatelů a jejich možné založení, úpravu nebo zneplatnění.
IDM musí obsahovat grafické uživatelské rozhraní sloužící jako obsluha pro uživatele, ve kterém uživatelé mohou měnit/resetovat heslo, žádat o přidělení rolí pro sebe nebo své podřízené, schvalovat nebo zamítat žádost a provádět další činnosti, na které mají oprávnění.

Požadavky na webové služby

IDM musí poskytovat rozhraní webových služeb pro programové napojení dalších systémů města. Toto rozhraní bude dodáno včetně jeho dokumentace, která bude určena k přímému poskytnutí dalším dodavatelům v prostředí města za účelem napojení se na takové rozhraní. Webové služby budou dostupné jako SOAP nebo REST rozhraní. Součástí takové dokumentace bude proto i popis řešení webových služeb v podobě XSD. Rozhraní a jeho konfigurace musí být součástí plnění na takové úrovni, že napojení nového informačního systému bude možné pouze za zapojení pracovníka objednatele, který provede konfiguraci rozhraní na straně IDM a dodavatele nového IS, který provede konfiguraci dle dodané dokumentace na straně nového IS, tedy vše bude možné bez aktivního zapojení dodavatele IDM.

Základní konfigurace přístupu k webovým službám musí být dostupná z grafického rozhraní IDM.

Rozhraní IDM musí poskytovat minimálně následující služby:
- získání organizační struktury,

- získání hierarchie systematizovaných míst,
- získání seznamu identit,
- získání nadřízené osoby pro daného zaměstnance,
- získání seznamu rolí pro daného zaměstnance, včetně případné informaci o delegaci role,
- zápis seznamu rolí uživatele do IDM,
- historie uživatele a jeho oprávnění k datu uvedeném v parametru.

IDM umožní vstupně/výstupní synchronizace do připojených informačních systémů. Typy synchronizací:

- plná
- 1 identita (možnost prosynchronizovat pouze 1 identitu bez nutnosti pouštět plnou nebo změnovou synchronizaci)
- změnová (pokud to napojený IS umožní)

Plná a změnová synchronizace musí umožňovat naplánované i ruční spuštění synchronizace, synchronizace 1 identity musí umožňovat pouze ruční spuštění. Dále musí existovat možnost (trvale nebo dočasně) vyřadit identitu ze synchronizace s daným IS
IDM umožní publikaci objektů (osob, účtů, skupin, funkcí, org. jednotek...) informačním systémům přes datové rozhraní (API IDM) na principu webových služeb (SOAP). Toto API IDM musí tedy mít čtecí metody a ideálně by mělo mít i zápisové metody (součást kvalitativního hodnocení). V rámci čtecích metod musí mít dané API IDM i autentizační metody, umožňující ověřit identitu (její login/heslo) i třetím aplikacím. IDM by mělo mít historii volání API IDM z důvodu auditu (součást kvalitativního hodnocení), včetně možnosti omezit dané API IDM pro jednotlivé aplikace (pouze vydefinované metody API IDM pro potřeby dané aplikace).

Logy IDM
IDM musí umožňovat publikovat kopie logů do externího systému určeného pro sběr logů např. syslog, DB apod.

Veškeré nové moduly IDM musí vést a umožňovat jednoduchý export anonymizovaných logů o počtu užití těchto jednotlivých modulů.

Tyto logy musejí být natolik přehledné a oproštěné od osobních dat aby umožnili jednoduchou kontrolu užívání těchto nových modulů ze strany i například kontrolních orgánů včetně oblasti kofinancování IROP.

Administrace
Po přihlášení do IDM bude administrátor IDM notifikován, že v systému došlo k některému z chybových stavů (např. synchronizovaný systém ve stavu chyba). Tato notifikace musí být zřetelná po přihlášení do systému a může být formou (barevného podbarvení části aplikace např. menu, pop-up okna oznamující, že je v IDM nějaký chybový stav, centrální dashboard aplikace apod.). Z notifikace musí být zřetelné, která část IDM je chybovém stavu.
IDM umožní definování různých úrovní oprávnění:

- možnost omezit oprávnění jenom na konkrétní organizační jednotky – uživateli to umožní spravovat identity pouze z daných organizačních jednotek např. vedoucí odboru spravuje oprávnění pro své podřízené (možnost omezit, zda může přiřazovat vybrané aplikační role, agendové role, skupiny, funkční místa, konkrétní uživatelské atributy apod.)
- možnost zadat oprávnění konkrétním uživatelům, skupinám, funkčním místům nebo organizačním jednotkám, aby mohli (pouze) spouštět vybraný synchronizační proces – např. personalistky si budou moci ručně pustit vstupní synchronizaci z personálního IS do IDM bez asistence administrátorů IDM.

IDM umožní nastavení prahových hodnot, které zabrání hromadným změnám např. z důvodu chybných dat na vstupu (např. z personálního systému), tak 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 poplatná pro všechny vstupně/výstupní konektory.

IDM umožní notifikovat konfliktní stavy (např. synchronizovaný systém v chybě) v systému IDM pomocí emailu na administrátory IDM, případně na další osoby (včetně zápisu do logu IDM)

IDM umožní logování veškerých operací nad jednotlivými objekty (osoby, účty, funkce, synchronizované systémy, skupiny,....) i nad všemi spravovanými objekty a vlastní konfigurací.

IDM umožní sledovat jednotlivé stavy (počty objektů/identit) v průběhu synchronizace IDM bude umožňovat databázovou historizaci (možnost dohledání změn v čase)

IDM umožní generování auditních reportů – přehled uživatelů a jejich aplikačních rolí, skupin definovaných v IDM včetně možnosti si zakázkově nechat vytvořit vlastní reporty. Reporty lze vygenerovat i do CSV, aby šlo s případnými daty dále pracovat v programech typu MS Excel.

IDM umožní zobrazit kompletní popis napojených informačních systémů (vzájemných vazeb, typů synchronizací, ...) přímo u jednotlivých synchronizovaných IS z administrace IDM. Tyto popisy budou dodavatelem pravidelně udržovány a budou do nich zaznamenávané veškeré změny

Integrace IDM a migrace dat

Integrace IDM

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

- Microsoft Active Directory
- JIP/KAAS
- Emailový server IceWarp

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.

Migrace dat

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.

Implementace IDM

Dokumentace skutečného provedení

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

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
- rozsah součinnosti ze strany objednatele
- návrh průběhu testovacího provozu

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.

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

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 VMware. Dále objednatel poskytne pro provoz IDM licenci aktuální verze Windows serveru. V případě, že se zhotovitel rozhodne neužít nabízenou licenci operačního systému musí v rámci své dodávky dodat i odpovídají licence operačního systému, případně využít některou z nekomerčních distribucí OS Linux k provozu nad virtualizovanou platformou objednatele. Veškeré další potřebné licence software potřebného pro běh IDM musí v rámci své dodávky zajistit zhotovitel.

Pro provoz IDM budou v prostředí objednatele vyčleněny následující systémové prostředky, které budou pro provoz IDM alokovány po dobu min. 5 let. Zhotovitel v nabídce uvede, zda jsou pro něj tyto prostředky dostačující, či zda požaduje jejich navýšení. Zhotovitel musí garantovat, že takto stanovené prostředky 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 GiB RAM,

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.

Konfigurace dodaného řešení pro potřeby objednatele
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 / parametrizace jednotlivých oblastí dle dokumentace skutečného provedení
- vytvoření reportů / výstupních sestav
- nastavení přístupových oprávnění do IDM pro administrátory

Dokumentace
Forma dokumentace
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.

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

Dokumentace skutečného provedení v prostředí objednatele
Bude sloužit jako podklad pro implementaci řešení do prostředí objednatele. Bude zpracována minimálně v rozsahu síťového schématu, datového schématu a aplikačního schématu včetně integrací, popis procesu nasazení informačního systému včetně zpřesněného harmonogramu, požadavků na součinnost ze strany zástupců objednatele. 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.

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

Uživatelská dokumentace
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.
Administrátorská dokumentace
Zhotovitel dodá administrátorskou dokumentaci pro objednatele, která bude obsahovat detailní popis správy a údržby aplikací a informačních systémů na základě této smlouvy.
Harmonogram
Harmonogram s časovými požadavky objednatele
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 výzvy číslo 28 IROP, ze které má být předmět plnění spolufinancován (s ohledem na termín dokončení předmětu plnění).

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	Termín nejpozději do:
Zpracování dokumentace skutečného provedení (cílový koncept), připomínkování ze strany objednatele, vypořádání připomínek, finalizace dokumentu	2 týdny
Milník **č**íslo 1 – Předání dokumentace skutečného provedení	T + 2 týdny
Instalace systému	1 týden
Konfigurace dodaného řešení pro potřeby objednatele – nastavení / konfigurace / parametrizace jednotlivých oblastí, provedení integrací na spolupracující systémy, nastavení přístupových oprávnění Zpracování a dodávka dokumentace (uživatelská, administrátorská) Dodávka licencí (listinné potvrzení dodaných licencí co do jejich počtu a rozsahu)	2 týdny
Výzva zhotovitele objednateli k započetí akceptačního řízení pro Milník 1	1 týden
Akceptační řízení pro Milník 1	1 týden
Milník **č**íslo 2 – Připravené prostředí pro testovací provoz	T + 7 týdnů
Výzva zhotovitele objednateli k započetí akceptačního řízení pro Milník 2	1 týden
Akceptační řízení pro Milník 2	1 týden
Milník **č**íslo 3 – Předání do testovací provozu	T + 9 týdnů
Testovací provoz s dohledem a podporou zhotovitele Oprava chyb a neshod, případná definice změnových požadavků Provedení doplňující migrace dat (počáteční stavy) Aktualizace dokumentace skutečného nasazení	1 týdny
Akceptační řízení – porovnání skutečných vlastností se požadavky smlouvy	1 týden
Milník **č**íslo 4 – Akceptace projektu, předání systému do rutinního provozu	T + 11 týdnů

Poznámka:
Ve sloupci „Termín nejpozději do:“ znak „T“ vyjadřuje datum uzavření smlouvy
Konkretizovaný harmonogram plnění ze strany zhotovitele
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

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

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.

V době testovacího provozu bude možné ze strany zhotovitele provedení případné nutné doplňující migrace dat (např. počáteční stavy) s ohledem na zahájení rutinního provozu.

Během testovacího provozu provede zhotovitel aktualizaci Dokumentace skutečného provedení.

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.
Projektové řízení
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.

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

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.)

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.

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).

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

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
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. 128/2000 Sb., o obcích (obecní zřízení), 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)
Akceptace
Dílčí akceptační řízení
Dílčí akceptační řízení bude provedeno pro milník 1, 2 a 3 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, 2 a 3) a požadavků daných dokumentací skutečného provedení (milník 2 a 3).
Výsledkem dílčího akceptačního řízení je akceptační protokol s výsledkem Splněno nebo Nesplněno, podepsaný oprávněnými osobami smluvních stran.
Započetí dalších prací spadajících pod milník následující je možné pouze za předpokladu, že bude provedena akceptace s výsledkem Splněno všech milníků předcházejících.

Souhrnné akceptační řízení - akceptace díla
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.

Výsledkem souhrnného akceptačního řízení je akceptační protokol s výsledkem Splněno / Splněno s výhradou / Nesplněno, podepsaný oprávněnými osobami smluvních stran. Klasifikace Splněno s výhradou umožní pokračování v realizaci díla v případě vad drobných, pro které může být opakování akceptačního řízení zbytečně nákladné.

Opakované akceptační řízení

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

1.5 Příloha č. 5 – Podmínky provádění technické podpory a rozvoje souvisejícího s produktivním provozem IDM pro město Klatovy

Čl. 1. Rozsah podpory
Technická podpora bude dodavatelem k aplikacím a informačním systémům poskytována průběžně v následujícím rozsahu:
1.1. Služba „Help-line“

1.1.1. Dodavatel zajistí help-line a bude ji udržovat dostupnou v pracovní dny a časy. V rámci poskytování služby „Help-line“ získává objednatel nárok na garantovanou pomoc při řešení technických problémů objednatele souvisejících s provozem aplikace. Jedná se o vzdálené konzultace a řešení po telefonu, emailu nebo přednostně s využitím aplikace HelpDesk. Služba je poskytována v pracovní dny v době mezi 8:00 a 16:00.
1.1.2. V případě zjištění, že se jedná o chybu na straně objednatele, poskytne dodavatel jako součást této služby objednateli správný postup řešení problematiky.
1.1.3. V případě, že bude potřeba věc řešit jako potřebnou úpravu, jako novou funkcionalitu, a nikoliv jako problém se stávajícím řešením, zpracuje dodavatel v rámci této služby popis rozsahu takové úpravy, a to včetně její funkcionality a rozsahu pracnosti, a odešle kontaktní osobě objednatele k uvážení, zda jako rozvoj objedná či nikoliv.
1.2. Služba „Upgrade a update“
1.2.1. V rámci poskytování této služby objednatel získává nárok na poskytnutí zlepšení a dodatků k poskytnuté aplikaci (upgrade a update stávajícího modulu) vydaných dodavatelem během příslušného ročního období a zároveň licence na tyto produkty. Součástí poskytnutí těchto upgrade a update není jejich instalace a implementace u objednatele.
1.2.2. Před provedením jednotlivých upgrade či update ze strany dodavatele musí vždy proběhnout odsouhlasení ze strany objednatele (kontaktní osoby) a to minimálně v rozsahu prováděné úpravy (upgrade, update) a času, ve kterém taková činnost bude provedena.
1.2.3. Dodavatel v souvislosti s poskytováním služby upgrade a update zodpovídá za funkčnost svých aplikací, kdy se v případě, že takto nasazené řešení nebude funkční, uplatní řádné obecné SLA na funkčnost aplikace na základě této smlouvy.
1.3. Služba „Legislativní podpora“
1.3.1. V rámci poskytování této služby objednatel získává nárok na to, že aplikace bude uvedena v soulad s aktuálním stavem právního řádu ČR (tj. v soulad s platnými obecně závaznými právními předpisy ČR), a to nejpozději ke dni, kdy nabyla nová právní úprava účinnosti. Aktualizace bude zajišťována prostřednictvím upgrade nebo update aplikace. Součástí legislativní podpory je instalace a implementace těchto upgrade a update.
1.3.2. Instalace a implementace těchto upgrade a update bude provedena v termínech navržených dodavatelem po odsouhlasení objednatelem (termín uvolnění nové verze či opravného balíčku aktuální verze software) nejpozději však k datu nabytí účinnosti nové právní úpravy. Pokud je implementace nové právní úpravy odvislá od vydání příslušných prováděcích předpisů zavazuje se dodavatel provést instalaci a implementaci legislativního update v co nejkratším termínu a nejpozději do 60 kalendářních dnů od vydání příslušných prováděcích předpisů k právní úpravě. Dodavatel se v tomto případě zavazuje vyvinout maximální úsilí v co nejkratším možném termínu provést implementaci legislativního update.
1.3.3. Smluvní strany se dohodly, že nedodržení této legislativní podpory dle článku 1.3 této přílohy bude vždy kvalifikováno jako kritická závada, na kterou se vztahují termíny a smluvní pokuta dle bodu 3.1.3 přílohy č. 1 této smlouvy.
1.4. Služba „Odstraňování závad aplikace“
1.4.1. V rámci poskytování této služby získává objednatel nárok na odstraňování závad aplikace, pokud jsou tyto závady způsobeny chybou ve zdrojovém kódu aplikace nebo ve způsobu (formě) její implementace. Výskyt závady bude objednatel oznamovat dodavateli prostřednictvím HelpDesk.
1.4.2. V případě výskytu závady v provozu aplikace získává objednatel garantovanou dobu jejich odstranění. Služba je poskytována v pracovní dny v době mezi 8:00 a 16:00 v sídle dodavatele.
1.5. Dokumentace a popisy rozhraní
1.5.1. Dokumentace uživatelská – dodavatel je v rámci této služby povinen poskytovat a udržovat 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.

1.5.2. Dokumentace administrátorská – dodavatel je v rámci této služby povinen poskytovat a udržovat administrátorskou dokumentaci pro objednatele, která bude obsahovat detailní popis správy a údržby aplikací a informačních systémů na základě této smlouvy.
1.5.3. Popis rozhraní - Dodavatel je povinen udržovat aktuální a platný popis veškerých rozhraní informačních systémů na systémy a databáze, se kterými je provázán. Taková dokumentace musí být vedena až na úroveň popisu konkrétního způsobu práce rozhraní s daty a uvedení všech jednotlivých datových typů a jednotlivých položek, se kterými pracuje.
1.5.4. Popis jednotlivých rozhraní musí být zpracován tak detailně, aby umožňoval objednateli jeho předání třetí straně, která na základě popisu bude schopna vytvořit bez jakékoliv součinnosti dodavatele odpovídající protikus rozhraní v plném rozsahu a jeho spuštění bude odvislé pouze na povolení komunikace ze strany aplikace/informačního systému dodavatele.
1.5.5. Takový popis rozhraní musí tedy obsahovat minimálně technologii, kterou je rozhraní realizováno, popis jednotlivých datových typů a struktur, se kterými rozhraní pracuje, a způsob, kterým má být prostřednictvím rozhraní komunikováno.
1.5.6. Elektronická forma dokumentace - Veškerá dokumentace bude vedená elektronicky, bude přístupná vždy kontaktním osobám objednatele a bude připravena k tisku.
1.5.7. Veškerá dokumentace bude vždy aktuální k nasazené verzi všech částí aplikací i informačních systémů, které jsou předmětem této smlouvy.
Čl. 2. Práva a povinnosti objednatele
2.1.1. Objednatel se zavazuje poskytnout Dodavateli veškerou součinnost potřebnou k provádění technické podpory podle této smlouvy. Objednatel se zejména zavazuje předávat Dodavateli potřebné nebo důvodně Dodavatelem vyžádané informace a podklady pro provádění těchto služeb a v odůvodněných případech umožnit Dodavateli vzdálený přístup k programové aplikaci. Vzdálený přístup bude zajištěn na základě dohodnutých technických a bezpečnostních podmínek, uvedených v této smlouvě.
2.1.2. Objednatel zajistí nahlášení vady či jiného požadavku, a to v níže uvedeném pořadí prostřednictvím:
- primárně použitím služby HelpDesk dodavatele na adrese =DOPLNÍ účastník zadávacího řízení=
- v případě nedostupnosti služby HelpDesk telefonicky na č.: =DOPLNÍ účastník zadávacího řízení= (kontaktní osoba =DOPLNÍ účastník zadávacího řízení=)
- nebo elektronicky na emailovou adresu: =DOPLNÍ účastník zadávacího řízení=
- popř. písemně na adresu: =DOPLNÍ účastník zadávacího řízení=

2.1.3. Pro požadavek zásahu objednatel zajistí písemné nahlášení závady na HelpDesk, ve kterém bude datum a čas nahlášení závady, závada popsána, stanovena její kategorie dle Podmínek této technické podpory, uvedena osoba objednatele, která o závadě podá podrobnější informaci, a její telefonní číslo, a uvedeno jméno a telefonní číslo ohlašovatele závady. Incident může být nahlášen i emailem, nebude na něj však v takovém případě možné uplatnit odpovídající SLA. Kategorii závady stanovenou objednatelem nesmí Dodavatel změnit bez souhlasu objednatele. V případě nedostupnosti služby HelpDesk na straně dodavatele bude na jakýkoliv další způsob nahlášení závady pohlíženo jako na podaný prostřednictvím služby HelpDesk, a to včetně SLA a jeho důsledků.
2.1.4. Po odstranění závady Dodavatel její odstranění nahlásí službou HelpDesk, případně e-mailem, či i telefonicky objednateli.
2.1.5. Objednatel zkontroluje funkčnost aplikace a potvrdí zpětně Dodavateli, že je závada odstraněna.
2.1.6. Objednatel zajistí Dodavateli pracovní prostor v rozsahu nutném pro provedení služeb technické podpory. Objednatel odpovídá za to, že řádný průběh prací Dodavatele nebude rušen zásahy třetích osob.
2.1.7. Objednatel je povinen informovat Dodavatele o všech opatřeních a zásazích, které na programové aplikaci provedl sám.
Čl. 3. Práva a povinnosti dodavatele

3.1.1. Dodavatel se zavazuje poskytovat technickou podporu v níže uvedených garantovaných termínech plnění.
3.1.2. Každá zjištěná či nahlášená závada bude objednatelem vyhodnocena a zařazena do jedné z následujících kategorií:

- Kritická závada – závada, která má takový vliv na funkčnost systému, že není možné se systémem pracovat, a to ani žádným náhradním způsobem.
- Hlavní závada – závada, která neumožňuje používání systému, následky je možné odstranit přijetím náhradního řešení situace a/nebo je v systému možné provádět hlavní úkony alespoň náhradním postupem bez rizika ztráty nebo poškození dat.
- Drobná závada – závada, která neovlivňuje způsob používání systému, který je předmětem smlouvy z pohledu plynulého provozu, spolehlivosti a souladu s legislativou.

3.1.3. Dodavatel se zavazuje po doručení oznámení objednatele o závadě díla zahájit práci na odstranění závady a odstranit nahlášenou závadu ve lhůtách podle následující tabulky. Do lhůt se započítávají pouze hodiny v pracovních dnech od 8.00 do 16.00 hodin (dále jen pracovní hodiny), tj. 1 pracovní den = 8 hodin. V jednotlivých buňkách jsou vždy uvedené hodiny SLA započítávané v pracovních dnech od 8:00 do 16:00 hodin a jejich projekce do počtu pracovních dnů. Dále jsou v buňkách definovány smluvní pokuty za překročení maximálních lhůt oprav.

	Časová lhůta způsobu řešení – Odstraňování závad aplikace			Aplikace
Kategorie závady	Oznámení o způsobu řešení a odhad termínu odstranění závady	Alespoň částečné zprovoznění (tj. dočasné náhradní řešení) umožňující využívání systému	Úplné odstranění	Smluvní pokuta za každou, byť jen započatou hodinu prodlení s odstraněním závady
Kritická závada	Do 4 hodin od nahlášení	Do 14 hodin	do 24 hodin od nahlášení (3 pracovní dny)	1.000,- Kč
Hlavní závada	Do 8 hodin od nahlášení	Do 24 hodin	do 56 hodin od nahlášení (7 pracovních dní)	500,- Kč
Drobná závada	do 16 hodin od nahlášení	Do 112 hodin od nahlášení (14 pracovních dní)	Do 112 hodin (14 pracovních dnů) nebo v rámci dohodnutého termínu	250,- Kč

3.1.4. Dodavatel je povinen informovat objednatele prokazatelným způsobem o zahájení prací na odstranění závady. Oznámením dodavatele o způsobu řešení se rozumí konkrétní informace kontaktní osobě objednatele.
3.1.5. Dodavatel je povinen respektovat pokyny a připomínky objednatele ke způsobu provádění technické podpory.
3.1.6. Do závazné doby k odstranění závady se nezapočítává čas, který je nutný z hlediska vyvolaných prací na straně Objednatele (například doba na reinstalaci serveru, doba dodání a zprovoznění náhradních serverů a hardwarových komponent, hledání a kopírování záloh, doba nutná na zprovoznění aplikace související, ale dodaná někým jiným než dodavatelem), v případě že tyto činnosti jsou nezbytně nutné k nalezení příčin závady a k jejímu odstranění. Lhůta se rovněž prodlužuje o dobu, která byla nutná na poskytnutí součinnosti pracovníků Objednatele. Lhůty plnění lze dále prodloužit, jestliže půjde o zásah vyšší moci (podle příslušných ustanovení zákona č. 89/2012 Sb., Občanského zákoníku).

3.1.7. Podmínka nutná pro dodržení termínu technické podpory „Odstraňování závad aplikace“ u závady typu Kritická a Hlavní závada je:

- součinnost zodpovědných pracovníků Objednatele v pracovní dny od 8.00 do 16.00 hodin, reakce pracovníků na výzvu k poskytnutí součinnosti je od 30 min. do 60 min.;
- povolení k přímé instalaci do produkčního prostředí bez testování v testovacím prostředí, kterou provádí pracovník Objednatele;
- dočasný plný vzdálený přístup k serverům pro řešení závady, práva budou přidělena pracovníky Objednatele po dohodě kontaktních nebo oprávněných osob.

3.1.8. Nebudou-li splněny nezbytné podmínky pro součinnost ze strany objednatele uvedené v tomto článku, nelze ze strany dodavatele dodržet uvedené termíny k odstranění závady (Service level agreement) a dodavatele nelze penalizovat sjednanými smluvními pokutami.

Čl. 4. Výčet cen technické podpory

4.1.1. Objednatel se dodavateli zavazuje plnit na základě této smlouvy za řádně poskytnuté služby dle článku 1. „Rozsah podpory“ této přílohy č. 1 této smlouvy tyto finanční prostředky.

Název aplikace	Cena za technickou podporu aplikací za **č**tvrtletí v K**č** bez DPH
IDM pro město Klatovy	27 000 Kč

Čl. 5. Rozvoj aplikace

5.1. Rozsah rozvoje a cena rozvoje

5.1.1. Na rozvoj a další níže uvedené služby k aplikacím a informačním systémům i jejich funkcionalitám bude možné čerpat objednatelem služby níže uvedených pozic dodavatele za níže uvedené jednotkové ceny.

5.1.2.

Sazba pozic dodavatele	Programátor	Konzultant Junior	Konzultant Senior	Vedoucí projektu
Hodinová sazba v Kč bez DPH	1 000 Kč	1 000 Kč	1 000 Kč	1 000 Kč
Předpokládaný počet hodin ročně	60	30	20	20
Celkem za jednotlivé pozice (součin sazby a hodin v jednotlivých sloupcích tabulky)	60 000 Kč	120 000 Kč	80 000 Kč	80 000 Kč
Cena celkem v Kč bez DPH za rok (součet součinů hodin a sazeb všech pozic):	130 000 Kč			

5.1.3. Objednatel dodavateli negarantuje žádné minimální odebrání hodin rozvoje. Požadavky objednatele k provedení rozvoje jsou přímo odvislé od potřeb, které vznikají v čase.

5.1.4. Předpokládaný počet hodin jednotlivých pozic není počtem hodin maximálním.

5.1.5. Minimálním časovým rozsahem, který bude dodavatelem na základě této smlouvy fakturován, je polovina hodiny.

5.1.6. Ve výše uvedené tabulce uvedená cena celkem v Kč bez DPH za rok je cenou, kterou na základě této smlouvy objednatel předpokládá čerpat. Objednatel však nevylučuje, že v případě potřeby bude čerpat i rozsah širší, vždy však za dodržení platných legislativních pravidel.

5.2. Předmět rozvoje

5.2.1. Na základě této smlouvy je za rozvojové služby považován zejména tento demonstrativní výčet služeb, kdy každou ze služeb bude moci dle požadavku zadavatele vykonávat kterákoliv z pozic dodavatele (programátor, konzultant junior, konzultant senior či vedoucí projektu),

- Konzultační a analytická podpora související s aplikacemi a informačními systémy,
- rozvoj či úpravy aplikací na základě požadavku zadavatele,
- metodická podpora,
- školení a příprava školících materiálů,
- instalace nových verzí a patchů,
- úprava dat na přání objednatele,
- konfigurace systému včetně specifických přenastavení,
- instalace nových verzí aplikací a informačních systémů (jedná se zejména o implementaci služeb update a upgrade, mimo legislativní podpory),
- úpravy nastavení aplikací dle potřeb objednatele,
- řešitelský a programátorský servis.

5.3. Služba – Profylaxe systému

5.3.1. Za účelem předcházení poruchám a optimalizaci výkonu systému bude dodavatel na základě dílčí objednávky provádět službu inspekce a sledování chodu informačního systému u objednatele a bude provádět potřebné zásahy k optimalizaci chodu a předcházení poruchám.

5.3.2. Předmětem profylaxe budou zejména tyto činnosti:

- Kontrola vazeb (konzistence dat)
- Zaplňování databázového prostoru a návrhy jeho rozšiřování
- Kontrola zálohování a bezpečnosti dat
- Mapování vytížení systému
- Nahrávání opravných dávek

5.3.3. O provedené inspekci bude vyhotoven zápis, který potvrdí kontaktní osoba objednatele. V případě, že výsledky profylaxe ukáží na potřebu provedení dalších úprav aplikace/informačního systému, předloží dodavatel návrh takového řešení včetně předpokládaného rozsahu pracnosti v hodinách objednateli.

5.4. Služba – Školení

5.4.1. Zaškolení administrátora na zprovoznění informačního systému ze zálohy v případě výpadku systému. Jedná se o proškolení 2-3 zaměstnanců objednatele na kompletní informační systém, včetně popisu změn za předchozí období.

5.4.2. Školení uživatelů.

5.4.3. Detailní rozsah dle oboustranně odsouhlasené a akceptované objednávky služby.

5.5. Služba – Kontaktní den

5.5.1. Dodavatel na základě objednávky provede v prostorách objednatele kontaktní den aplikace/informačního systému, za účasti osob schopných řešit rozvoj jakož i vést diskuzi s uživateli aplikace. V rámci tohoto dne proběhne diskuze nad spokojenosti uživatelů s aplikací, možnosti rozvoje, revize závazků, revize platnosti dokumentace a školení na vybrané aplikace.

5.5.2. Detailní rozsah dle oboustranně odsouhlasené a akceptované objednávky služby.

5.6. Typy rozvoje

5.6.1. Rozvoj (evoluce) aplikací, modulů, rozhraní, konektorů a dalšího software, kdy se bude jednat o úpravu nasazeného software na základě dílčích požadavků za účelem přizpůsobení potřebám objednatele nebo aktuálnímu prostředí (např. změna partnerské aplikace nebo IS), předmětem této části rozvoje je především přizpůsobení software potřebám objednatele.

5.6.2. Rozvoj (nové funkcionality) nových funkcionalit, modulů a software, kdy se bude jednat o tvorbu nových samostatných softwarových řešení, za účelem zejména jejich další integrace v prostředí objednatele, když právě aplikace a moduly, ke kterým je

poptáván tento rozvoj, jsou v rámci integrace informačních systémů v prostředí objednatele klíčovými a v mnohých případech i centrálními. Tato samostatná řešení však musí vždy vycházet a navazovat na aplikace a moduly dodavatele řádně nasazené u objednatele. Objednatel tímto rozvojem předpokládá tvorbu rozhraní na další IS, která je potřeba tvořit, měnit a optimalizovat po celý životní cyklus aplikace. Objednatel tímto rozvojem nebude realizovat poptávky ani zadávací řízení na nový software a licence od dodavatele, na který by dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, byl povinen realizovat veřejnou zakázku, a který by bylo možné odebrat i od dodavatele jiného.

5.6.3. Rozvoj-technická podpora funkcionalit, kdy se bude jednat o technickou podporu k novým funkcionalitám na základě realizovaného rozvoje nových funkcionalit. Technická podpora takového rozvoje bude dána výhradně cenou za vytvoření takové nové funkcionality, nikoliv souhrnem cen za další služby související s nasazením takové nové funkcionality, jimž jsou například implementace, školení a dokumentace, které budou vždy uhrazeny pouze jednorázově při pořízení takové nové funkcionality. Výpočet ceny rozvoje-technické podpory nových funkcionalit tak bude dán čistou cenou za realizaci rozvoje nové funkcionality násobenou koeficientem 0,15 ročně. Tento koeficient je stanoven jako 15% ceny pořízení nové funkcionality, který na odpovídajícím trhu informačních systémů a poskytování technické podpory k těmto informačním systémům odpovídá ceně poskytování takových služeb za každý kalendářní rok provozu takového informačního systému (software). Na základě akceptace rozvoje (nové funkcionality) oprávněné osoby na základě této smlouvy zanesou technickou podporu k takovému rozvoji (nové funkcionality) do dokumentu dle vzoru přílohy č. 2 této smlouvy a ten přiloží k originálu smlouvy.

5.7. Objednávka rozvoje

5.7.1. Na popsaný předmět rozvoje odešle objednatel dodavateli předběžnou objednávku s uvedením typu rozvoje.

5.7.2. Do 10 kalendářních dnů zpracuje dodavatel odhadovaný rozsah pracnosti rozvoje v hodinách a ten odešle objednateli k odsouhlasení, případně k jednání o rozsahu úpravy a o hodinovém rozsahu. Součástí odhadovaného rozsahu pracnosti bude vždy rozklad úkonů prováděných jednotlivými pozicemi dodavatele a věcný popis těchto úkonů.

5.7.3. Na základě smluvními stranami dohodnutého předmětu rozvoje a hodinového rozsahu čerpání rozvoje odešle objednatel dodavateli objednávku na provedení požadovaného rozvoje aplikace.

5.8. Realizace rozvoje

5.8.1. Dodavatel je povinen začít práce na objednávce na rozvoj nejpozději do 14 kalendářní dnů ode dne odeslání objednávky objednatelem a o zahájení prací informovat kontaktní osobu dodavatele.

5.8.2. V případě objednávky v rozsahu do 50ti hodin realizuje dodavatel úpravu obvykle do 60 kalendářních dnů ode dne odeslání objednávky objednatelem.

5.8.3. V případě objednávky v rozsahu nad 50 hodin realizuje dodavatel úpravu obvykle do 180 kalendářních dnů ode dne odeslání objednávky objednatelem.

5.9. Společná ustanovení pro rozvoj

5.9.1. Smluvní strany mohou písemně dohodnout i jiné termíny počátku plnění a realizace úprav rozvoje aplikace.

5.9.2. Veškerá komunikace týkající se rozsahu předmětu rozvoje, rozsahu pracnosti v hodinách a změn termínů rozvoje (zahájení, skončení prací) bude realizována písemně (za písemnou formu se považuje i email mezi kontaktními osobami dle této smlouvy). Iniciace objednávky rozvoje musí být zanesena na HelpDesku dodavatele, jedná se o rozhodný okamžik pro běh lhůt.

5.9.3. Ke komunikaci mezi smluvními stranami v rámci rozvoje jsou oprávněny kontaktní osoby obou smluvních stran.

5.9.4. Za jednu hodinu rozvoje je považována člověkohodina odborníka schopného samostatně analyzovat požadavek objednatele a fakticky provést úpravu.

Příloha č. 1 k příloze č. 5 Kupní smlouvy

Evidence technické podpory k provedenému rozvoji – nové funkcionality

Tento evidenční list, vyplněný a podepsaný oběma smluvními stranami, se stává nedílnou součástí smluvního ujednání.

Počátek poskytování služby (měsíc / rok)	Předmět provedeného rozvoje – nové funkcional.	Cena rozvoje – nové funkcional. v Kč bez DPH	Cena technické podpory ročně (cena rozvoje nové funkcional. v Kč bez DPH x 0,15)	Cena technické podpory za čtvrtletí v roce v Kč bez DPH	Podpis oprávněné osoby objednatele	Podpis oprávněné osoby dodavatele
.../20...						
.../20...						
.../20...						
.../20...						
.../20...						
Celková cena za Technickou podporu k rozvoji (nové funkcionality) ke dni podpisu tohoto dokumentu činí:		..... Kč bez DPH za každé čtvrtletí				