Věcná specifikace předmětu díla

Slovníček pojmů

|  |  |
| --- | --- |
| Pojem | Vysvětlení |
| Koncový systém | Informační systém připojený k Identity Manageru. |
| Identita | Fyzická osoba reprezentující uživatele napříč informačními systémy Zákazníka. Jedna identita může mít více uživatelských účtů. |
| Uživatelský účet | Přístup uživatele k informačnímu systému. Zpravidla k účtu náleží přístupové údaje. |
| Identity manager, IdM | Nástroj na správu identit (identity management) |
| Umožnění funkcionality | To, že systém, řešení či jeho část „umožní“, „splní“, „zajistí“ či jinak obstará danou funkcionalitu, znamená, že daná funkcionalita je požadována jako součást dodávky, není-li explicitně uvedeno jinak. |

Nefunkční požadavky

Požadavky na způsob provedení zakázky

Zakázka bude členěna do následujících fází:

* vytvoření a dodání analytické dokumentace řešení a implementace upgradovaného IDM systému (dále jen „**Analýza**“);
* vytvoření a implementaci upgradovaného IDM systému do stávajícího Testovacího prostředí NTK (dále jen „**Implementace do Testu**“);
* implementaci upgradovaného IDM systému do stávajícího Produkčního prostředí NTK (dále jen „**Implementace do Produkce**“);
* zajištění tříměsíčního Zkušebního provozu (dále též jen „**Zkušební provoz**“);
* zajišťování údržby systému IDM po dobu trvání záruky (dále jen „**Údržba**“);
* poskytování odborných služeb po dobu trvání záruky (dále jen „**Odborné služby**“).

Termíny, lhůty a způsob plnění jsou uvedeny v závazném vzoru smlouvy v příloze A zadávací dokumentace.

Požadavky na záruku řešení

Zhotovitel je povinen odpovídat za vady a držet záruku za jakost po dobu 48 měsíců od úspěšné akceptace upgradovaného systému IDM, tedy 48 měsíců od úspěšného ukončení tříměsíčního zkušebního provozu.

Požadavky na SW licence

Veškerý SW a ostatní nehmotné výstupy činnosti Zhotovitele, které budou vytvořeny pro Objednatele, budou podléhat režimu zaměstnaneckého díla ve smyslu Autorského zákona.

V případě, že součástí dodávky bude dílo třetích stran, tj. SW, návrh, plán, dokumentace, konfigurace apod., které nebylo vytvořeno Zhotovitelem pro Objednatele, zavazuje se Zhotovitel zajistit bezplatné udělení licence od oprávněné osoby či podlicence, příp. postoupení odpovídající licence, a to takové, aby Objednatel byl oprávněn získat a držet Zdrojové kódy a Zdrojové formáty tohoto díla, mohl do díla zasahovat, měnit ho a spojovat s jiným dílem, a to v libovolném rozsahu, sám či třetí osobou, a to i bez dodatečného souhlasu Zhotovitele či autora a nebyl při jeho užití místně ani časově omezen, v případě SW a jeho konfigurací pak mohl provozovat jeho instalaci bez množstevních omezení, např. omezení počtu instancí, procesorů, uživatelů, dat apod. Licence tedy bude umožňovat připojení budoucích nových koncových systémů a vložení jejich přístupových rolí a logiky do systému IdM a to bez dalších požadavků na licence.

Součástí licenční dodávky budou i zdrojové kódy aplikace Identity Managementu a jejich možnost je měnit, upravovat a dále distribuovat v souladu s podmínkami výše.

Celé znění požadavků na ochranu autorských práv je uvedeno v závazném vzoru smlouvy přiložené k zadávací dokumentaci.

Systémové požadavky

Řešení IdM musí splňovat následující požadavky. Důvodem specifikace konkrétní (nové či nejnovější) verze produktů a platforem je snížení zátěže správců na údržbu zastaralých verzí produktů a platforem a soulad s vizí "moderního informačního systému" a celkové architektury infrastruktury Zadavatele.

* Provoz zajištěn na OS Linux RHEL 7.
* Řešení má jako jediné úložiště dat (repozitory) relační databázi, řešení pro svůj provoz nevyžaduje LDAP server.
* Řešení pro uložení své repozitory podporuje minimálně jednu z těchto relačních databází: MySQL 5, MS SQL Server 2014, Oracle DB 12, PostgreSQL 9.4, nebo novější verze.
* Řešení podporuje technologii Java 8+ či .NET 4.5+, nebo novější verze.
* Řešení podporuje přístup pomocí zabezpečeného protokolu HTTPS s podporou technologie RSA a ECC. Podpora délky klíčů použitých algoritmů dle [*eIDAS - Cryptographic requirements for the Interoperability*](https://joinup.ec.europa.eu/sites/default/files/eidas_-_crypto_requirements_for_the_eidas_interoperability_framework_v1.0.pdf)

Požadavky na „živost“ nabízeného již existujícího SW

Bude-li součástí řešení již existující SW, musí být tento SW tzv. „živý“, to konkrétně znamená, že musí aktuálně probíhat jeho údržba a vývoj. To dodavatel prokáže tím, že bude demonstrovat jeho aktuálnost, např. odkazem na verze či hot fixy, které nejsou starší než 6 měsíců.

Požadavky na údržbu v záruční době

Zhotovitel musí po dobu záruční doby zajistit údržbu upgradovaného systému IDM.

Pro zajištění komunikace Objednatele se Zhotovitelem související s údržbou systému IDM je Zhotovitel povinen provozovat telekomunikační nástroje, především telefonní linku a aplikaci typu Helpdesk, který bude Objednateli umožňovat:

* hlásit nalezené vady systému IDM;
* vznášet další požadavky na Zhotovitele;
* sledovat stav řešení všech požadavků a jeho soulad se Smlouvou;
* vytvářet souhrnné reporty stav řešení všech požadavků.

Za údržbu se považují především následující činnosti a povinnosti Dodavatele:

* proaktivní ověřování, zda nejsou SW komponenty systému IDM zranitelné a zjištěné či nahlášené zranitelnosti odstraňovat;
* odstraňování veškerých nahlášených vad systému IDM;
* na vyžádání ověřit, že systém IDM je plně funkční a bezpečný v aktualizované verzi operačního systému, na kterém je provozován a v případě nutnosti systém IDM upravit tak, aby byl na aktualizované verzi operačního systému plně funkční a bezpečný;
* poskytování konzultací, převážně telefonických a emailových, souvisejících s údržbou systému IDM;
* vystavení a zasílání měsíčního přehledu všech údržbových aktivit.

Dojde-li při údržbě k nutnosti jakékoliv úpravy systému IDM, je Dodavatel v rámci údržby rovněž povinen:

* patřičně upravit systém IDM a všechny úpravy implementovat v prostředí NTK, přičemž všechny úpravy musí, je-li to možné, před jejich nasazením do Produkčního prostředí NTK nejprve úspěšně otestovat v Testovacím prostředí NTK;
* udržovat systém IDM v Testovacím prostředí NTK ve stejném SW stavu, jako v Produkčním prostředí NTK;
* udržovat veškerou dokumentaci systému IDM aktuální, především Analýzu, Instalační dokumentaci, Zdrojové kódy.

Pro Zhotovitele závazné lhůty pro reakci a vyřešení požadavků Objednatele jsou specifikovány v příloze č. 3 Smlouvy na realizaci upgrade IDM systému.

Požadavky na údržbu po skončení záruční doby

Pokud ani jedna ze smluvních stran nevypoví uzavřenou smlouvu, je Zhotovitel povinen zajišťovat údržbu IDM systému i po ukončení záruční doby.

Požadavky na odborné služby

Zhotovitel k dodanému řešení musí po dobu účinnosti smlouvy rovněž poskytovat odborné služby.

Součástí nabídkové ceny budou odborné služby v rozsahu 100 člověkodní (tedy 800 člověkohodin).

Pro Zhotovitele závazné lhůty na řešení požadavků Objednatele na odborné služby jsou specifikovány v příloze č. 3 Smlouvy na realizaci upgrade IDM systému.

Místem výkonu práce je sídlo zadavatele, pokud není domluveno jinak.

Požadavky na demo řešení

Pro ověření poptávaných funkcionalit Zadavatel požaduje jako součást nabídky přístup k demo produktu, které splní následující parametry:

* demo je přístupné on-line bez nutnosti instalace jakéhokoliv SW či provedení konfigurace na straně zadavatele (např. VPN přístup);
* demo bude dostupné nejpozději ode dne vypršení lhůty pro podání nabídek a to po celou zadávací lhůtu;
* demo produktu pro identity management bude obsahovat minimálně následující funkcionality:
  + Administrátorský přístup:
    - Přehled uživatelů
    - Detail uživatele
    - Koncové systémy s možností přidat nový koncový systém
    - Přehled systémových úloh včetně jejich stavu
    - Minimálně dva reporty z kapitoly Reporting
  + Uživatelský přístup:
    - V rozsahu kapitoly Uživatelské rozhraní.

Rozhraní pro realizaci obou typů přístupů může a nemusí být společné.

* Ukázková data

Součástí nabídky účastníka/zhotovitele bude i datový binární obraz demo řešení vč. instalační dokumentace, na kterém si zadavatel/objednatel může otestovat požadovanou funkcionalitu. Obraz bude poskytnut k dálkovému stažení prostřednictvím internetu. V nabídce bude uvedena jeho URL adresa, datový otisk (hash) ve formátu SHA-512 a přístupové údaje.

**Další upřesnění nefunkčních požadavků je v těle zadávací dokumentace a její příloze A závazném vzoru realizační smlouvy.**

Funkční požadavky

Technické požadavky

Systém musí splňovat požadavky uvedené v následujících kapitolách.

Všeobecné

* Správa různých typů objektů (identit uživatelů, funkčních míst, místností, organizační struktury, rolí, …).
* Podpora některého z uvedených skriptovacích jazyků v konfigurovatelných částech Identity Manageru: Python, EcmaScript, VisualBasic.
* Dávkové akce (příklad: hromadné přejmenování).
* Export/import konfigurace IdM ve formátu XML nebo JSON.
* Logování a reporty chyb.
* Administrátorská a vývojářská dokumentace.
* Schopnost pracovat v režimu vysoké dostupnosti.
* Řešení musí být schopno pracovat v tzv. odlehčeném režimu, kdy funguje pouze jako integrační datový nástroj mezi koncovými systémy.
  + Jedná se o volitelné vypínání náročných administrativních funkcí, jako je workflow.
* Možnost definovat a pravidelně spouštět serverové/systémové úlohy (nejrůznější transformační, kontrolní a notifikační úlohy).
* Možnost vytvářet vlastní konektory ke koncovým systémům jako komponenty nezávislé na verzi IdM.

Autorizační model

Řešení IdM musí být schopné jemné granularity přidělování autorizačních oprávnění:

* Autorizační model je založen na RBAC (Role-Based Access Control) přístupu.
* Oprávnění jsou součástí rolí, role jsou přiděleny uživatelům.
* Musí být možné nastavit, k jaké části uživatelského rozhraní mají uživatelé přístup.

Rozhraní pro integraci

* Řešení IdM musí podporovat možnost vzdáleného programového volání:
  + Možnost volání za pomoci Web service API (SOAP/WSDL) nebo REST API.
  + Možnost volat ekvivalent jakékoli funkcionality, která je dosažitelná z webového rozhraní.
  + Možnost volání jen některých funkcí jádra IdM je pro tyto potřeby nedostatečná.

Integrace s access managementem

IdM musí podporovat integraci s nástrojem pro řízení přístupu (nástroj Access managementu):

* Cílem je zajistit Web SSO do IdM
* IdM musí podporovat SLO - Single Log-Out
  + uživatel se odhlásí v Access managementu a následně je při příštím dotazu odhlášen i v nástroji Identity managementu.
* Do IdM je možné se přihlásit i při výpadku systému Access managementu.

Synchronizace a rekonciliace

Řešení musí splňovat požadavky na synchronizaci a rekonciliaci účtů a oprávnění:

* Synchronizace změn v reálném čase s odolností proti výpadkům informačních systémů - vestavěná podpora opakování propagace změn v případě neúspěchu.
* Obousměrná synchronizace dat jak z IdM do spravovaného systému (např. uživatele a jejich atributy), tak ze spravovaného systému do IdM (např. role v konkrétním systému).
* Paralelní synchronizace několika autoritativních systémů současně – minimálně systém Karty VŠ a aplikace Registrace včetně řešení konfliktů, korelací a eskalačních emailů.
* Mapování atributů mezi informačními systémy na základě pravidel/vzorců.
* Práce s komplexními (tabulky) či binárními atributy uživatele - certifikáty, fotografie, autentizační tokeny.
* Rekonciliace účtů - pravidelná automatická kontrola stavu účtů na koncových systémech s autoritativním vypořádáním nesouladu s možností tuto funkcionalitu pro daný koncový systém vypnout.
* Možnost definice rekonciliačních pravidel pro jednotlivé koncové systémy.
* Rekonciliace oprávnění - pravidelná automatická kontrola stavu oprávnění na koncových systémech oproti stavu chtěnému a náprava (notifikace, zápis do logů, výmaz nadbytečných oprávnění apod.).
* Nastavení párovacích pravidel mezi identitou a účtem (například email identity na login účtu).

Notifikace

Řešení IdM zasílá emailové notifikace:

* Možnost definice šablon emailů, s podporou vícejazyčnosti.
* Možnost konfigurace parametrů odesílání zpráv (SMTP server a podobně).
* Odeslání emailové notifikace správcům IdM v případě chyb plánovaných úloh

Delegovaní administrátoři

Řešení IdM musí umožňovat převést část správy na delegované administrátory. Tito uživatelé musí mít administrátorská práva nad zvolenými komunitami nebo skupinami uživatelů.

Účelem je umožnit lokálnímu administrátorovi správu nad uživateli patřícími do samostatného podřízeného celku (ať už z pohledu interního, tak externího - například dodavatelské účty).

Procesy podporované pomocí IdM

Všechny níže uvedené procesy musí být možné provádět z administrátorského grafického rozhraní IdM.

Všechny níže uvedené propagace do cílových systémů musí být možné časově omezit. Například propagace změny až od data platnosti uvedené změny nebo platnost oprávnění do uvedeného data.

Vznik identity

* Zdrojem dat je více externích systémů a samotná IdM aplikace.
* Propagace identity do úložiště Identity managementu.
* Automatické přidělení oprávnění dle nadefinovaných pravidel.
* Propagace účtů do koncových systémů.
* Odeslání emailové notifikace.

Změna identity

* Zdrojem dat je více externích systémů a samotná IdM aplikace.
* Propagace změn do Identity managementu.
* Propagace změn do koncových systémů.

Změna pozice (reorganizace)

* Zdrojem dat je více externích systémů a samotná IdM aplikace.
* Propagace změn do Identity managementu.
* Odebrání původních oprávnění k definovanému datu.
* Přidělení nových oprávnění dle nadefinovaných pravidel.
* Propagace změn do koncových systémů.
* Odeslání emailové notifikace.
* Proces se týká také změny uživatele z anonymního (pouze karta VŠ) na registrovaného. V tomto případě je nutné zajistit příslušná workflow a notifikace podporující proces.

Žádost o změnu oprávnění

* Zdrojem je Helpdesk systém užívaný zadavatelem, tj. Redmine nebo samotná IdM aplikace.
* Propagace změn do Identity managementu.
* Identity Management zajistí schvalovací workflow a zpětnou informaci Helpdesku o stavu požadavku.
* Propagace změn do koncových systémů.
* Odeslání emailové notifikace.

Zánik identity

* Zdrojem dat je externí systém nebo samotná IdM aplikace.
* Propagace změn do Identity managementu.
* Zrušení (fyzický výmaz, zneplatnění) identity v koncových systémech dle nadefinovaných pravidel.
* Možnost zpožděného výmazu účtů počítaného od data zneplatnění identity a v kombinaci s dalšími vstupy – například zneplatnění expirovaných čtenářů v závislosti na předregistraci.

Správa uživatelů

Součástí dodávky řešení IdM je administrační webové rozhraní pro správu uživatelů, které umožní:

* Vyhledávat uživatele podle atributů (viz níže).
* Editovat profil uživatele.
* Uložit a zobrazit k uživateli fotografii.
* Evidovat u uživatele atributy.
  + Atributy mohou být jednohodnotové, vícehodnotové, binární či definované komplexní struktury (tabulky).
* Uživatele je možné zneplatnit k určitému datu.
* Uživateli je možné přiřadit koncové systémy, role a organizační jednotky.
* Rozlišit jednotlivé typy uživatelů: anonymní uživatelé (přiřazení karty VŠ) a neanonymní uživatele registrované v NTK

Vyhledávání a filtrování uživatelů

Řešení IdM musí umožnit vyhledávání:

* uživatelů podle loginu, jména, příjmení, celého jména, perzistentního identifikátoru a čísla karty,
* rolí podle jména,
* organizací podle jména.

Správa rolí

Řešení IdM musí poskytovat grafické webové rozhraní pro správu rolí (soubor oprávnění). Správa rolí je umožněna minimálně v rozsahu daném následujícími kapitolami pro všechny poptávané koncové systémy, které role obsahují.

Všeobecné

* Roli je možné přiřazovat uživatelům i organizacím.
* Platnost přiřazení role uživateli i organizaci od-do. Možnost nastavit další atributy přiřazení.
* Schvalovatelé role včetně možností dynamického výpočtu.
* Role je možné hierarchicky skládat.
* Řízení autorizačních objektů v koncovém systému
* Možnost svázat definici role s existencí objektu oprávnění v koncovém systému.
  + Například role zodpovídá za vytvoření objektu skupiny v Active Directory.

Mechanismus konfliktních rolí

Řešení IdM musí mít implementovaný mechanismus konfliktních rolí (SoD, Segregation of Duties).

* Musí umožňovat nastavit pravidla pro vzájemně se vylučující role.
* Pokud dojde k pokusu o přiřazení role uživateli, který již má jinou konfliktní roli, musí systém konflikt oznámit a přiřazení neprovést.

Časově omezené role

Řešení IdM musí mít implementovaný mechanismus časově omezených rolí (od-do):

* Musí umožňovat nastavit časové období od-do pro přiřazení role uživateli.
* Pokud časové období uplyne nebo ještě nenastalo, nesmí se přiřazení role uplatnit.

Nastavení práv

Řešení IdM musí umožňovat nastavit práva až na úroveň atributu libovolného typu objektu. Práva musí být přidělitelná uživateli, roli nebo organizaci.

Certifikace rolí

Řešení IdM musí umožňovat mechanismus certifikace rolí. Cílem je ověření, že všechna přidělení rolí jsou aktuální a chtěná.

* V nástroji Identity managementu je možné spustit úlohu z grafického rozhraní, která zajistí schvalování pro všechny role přidělené identitám.
* Tuto úlohu je možné opakovaně spouštět (tzv. recertifikace rolí).

Organizační struktura

Řešení IdM musí poskytovat administrační webové rozhraní pro správu stromové struktury, které umožní:

* Vytváření libovolného počtu stromů.
* Vytváření nezávislých entit (pracovní pozice, funkční místa) ve stromě.
* Definovat atributy entit ve stromě.
* Přiřazovat entitám ve stromě jiné objekty, zejména:
  + role
  + jiné entity stromu
  + účty v koncových systémech.
  + Vizualizace entit pomocí stromové struktury.
  + Entity ve stromě přiřazovat k libovolnému objektu, zejména:
    - roli
    - uživateli
  + Uživatel nebo role může být přiřazen ve více entitách stromu zároveň.
  + Uživatel nebo role může být přiřazen ve více stromech zároveň.
  + Uživatel může mít různé role v různých strukturách (nadřízený v jedné organizační struktuře může být v jiné struktuře podřízený apod.)

Časové omezení při zařazení do stromové struktury

Řešení IdM musí mít implementovaný mechanismus časově omezeného přiřazení do stromové struktury např. do organizací.

* Musí umožňovat nastavit časové období od-do pro přiřazení uživatele do stromové struktury.
* Pokud časové období uplyne nebo ještě nenastalo, nesmí se přiřazení uživatele do stromu uplatnit.

Schvalovací proces

Řešení IdM musí poskytovat grafické rozhraní pro schvalovací procesy. Musí splňovat minimálně následující požadavky:

* Notifikace schvalovatele minimálně emailem.
* Schvalovatelé si mohou zobrazit přehled svých úloh.
* Možnost úlohu schválit či zamítnout včetně uvedení zdůvodnění.
* Schvalovací workflow musí podporovat vícekrokové schvalování.
* Schvalovat může jednotlivec nebo skupina schvalovatelů.
* Je možné určit typ schválení "všichni ze skupiny" nebo "jeden ze skupiny".
* Správce IdM musí být schopen pracovat se všemi úlohami (pro řešení nestandardních situací).

Firemní politiky

Řešení IdM musí podporovat zavádění, vynucování a kontrolu firemních politik.

Politiky hesla

Řešení IdM musí mít implementovaný mechanismus politiky hesla.

Musí umožňovat nastavení pravidel pro minimální a maximální délku hesla, povolené skupiny znaků, počet opakování znaků, minimální a maximální výskyt znaků ze skupiny.

Politiky účtu

Řešení IdM musí mít implementovaný mechanismus politiky účtu.

Musí umožňovat nastavení pravidel pro název účtu - minimální a maximální délka, povolené znaky, zakázaná slova v názvu (například \*admin\*, \*info\*), kontrola na platný formát emailové adresy.

Reporting

Součástí řešení musí být připravení sady reportů v minimálním rozsahu daném následujícími kapitolami.

Reporty je navíc možné exportovat minimálně do všech následujících formátů: PDF, CSV, HTML, XML a formát MS Word a MS Excel.

Auditní report

Kompletní přehled změn provedených nad uživatelem – například synchronizace atributů, přidělení role včetně časového omezení, změna hesla atd.

Kompletní přehled změn provedených nad klíčovými entitami řešení - role, organizace, definice politik a konfigurací.

Záznam o přihlášení uživatele do webového rozhraní IdM.

Report uživatelů

Informuje o tom, jaké mají uživatelé přiřazené role a účty v koncových systémech.

Možnost reportovat uživatele v určité organizaci.

Report rekonciliace

Přehled účtů v koncových systémech, které jsou známy IdM k momentu spuštění reportu.

Možnost identifikace účtů, ke kterým nebyl v IdM nalezen vlastník.

Uživatelské rozhraní

Uživatelské rozhraní musí splňovat tyto parametry:

* Jedno webové rozhraní pro administrátory i pro koncové uživatele.
* V českém a anglickém jazyce.
* Responzivní design - zobrazení stránky bude optimalizováno pro všechny druhy nejrůznějších zařízení (mobilní telefony, notebooky, tablety atd.).
* Použití tlustého klienta není přípustné pro uživatelské, konfigurační ani správcovské činnosti.
* Rozhraní je možné upravovat dle potřeb zadavatele.

Koncoví uživatelé

Rozhraní musí koncovým uživatelům umožňovat zejména:

* Zobrazení základních informací o profilu přihlášeného uživatele:
  + přehled schválených rolí,
  + přehled rolí, které jsou svázány se zastávanou pracovní pozicí,
  + přehled oprávnění na jednotlivých koncových systémech.
* Změnu hesla na všech nebo vybraných koncových systémech.
* Změnu definovaných atributů přihlášeného uživatele.
  + Podle typu uživatele nastavit práva na změnu atributů v profilu uživatele (např. externistům umožnit změnu kontaktní adresy, zaměstnancům naopak pouze změnu osobního emailu)
* Změnu v přiřazení rolí - podléhá schvalovacímu WF:
  + zadat požadavek na zařazení do role, do stromu nebo na přístup do aplikace
* Vedoucím pracovníkům vložit požadavky na změny v přiřazení rolí pro podřízené pracovníky a sledovat stav vyřizování jejich žádostí,

Schvalovatelům umožnit rozhodování o schválení či zamítnutí vznesených požadavků.

Připojené koncové systémy

Součástí dodávky bude analýza současného stavu nasazení IdM v infrastruktuře zadavatele a její následné využití pro nasazení nového řešení. Pro orientaci lze výchozí stav popsat definicí koncových systémů.

Aplikace Registrace

Zdrojová aplikace pro uživatelské účty. Z hlediska IDM jediná tabulka v databázi Oracle.

EKV

Přístupový systém. SOAP webová služba, dostupné WSDL.

Karty VŠ

Flat file, formát CSV. Zdrojová data. Definuje čísla karet anonymních identit. Řešení kolizí s neanonymními identitami bude věcí úvodní analýzy. Součástí dodávky je funkcionalita, která umožňuje definovat hodnotu atributu přístupové zóny na základě toho, zda taková identita a s jakými atributy je již evidována. Rovněž je nutno řešit konflikty, které nutně nastanou na straně přístupového systému, protože nelze předpokládat, která identita (tj. anonymní či neanonymní) vznikne dříve.

Platební systém

SOAP webová služba, dostupné WSDL.

Rezervační systém

SOAP webová služba, dostupné WSDL.

LDAP

OpenLDAP. Z hlediska IdM prosté mapování atributů.

Knihovní systém ALEPH 500

Souhrn webových služeb nepodchycených WSDL a Oracle DB connectoru.

Windows AD

Standardní Windows AD s definovanými skupinami.

Samba AD

Samba 4 v režimu AD. Nutná úprava standardního chování pro AD pro synchronizaci přístupových údajů.

V Praze dne 2. 5. 2017

--------------------------------------------

Ing. Ondřej Koch

vedoucí odboru 5 pro IT, ICT akvizici a infrastrukturu