NÁVRH ŘEŠENÍ

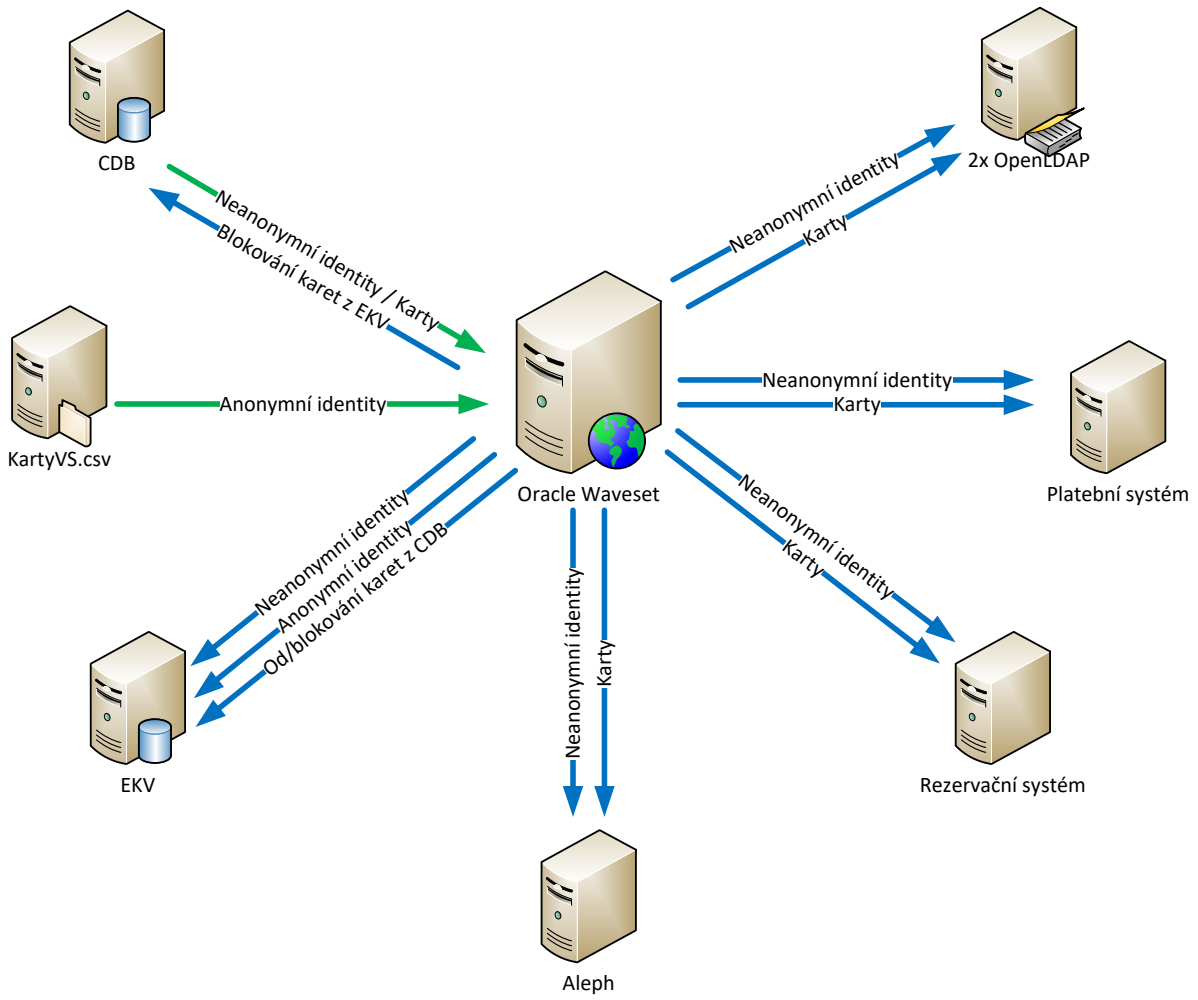
1.1 REIMPLEMENTACE SOUČASNÉHO IDM

1.1.1 Popis současného stavu

V současnosti je v prostředí NTK provozováno IdM řešení Oracle Waveset, které je napojeno na následující systémy:

- Aplikace Registrace / CDB
  - registrace čtenářů
  - zdrojová data o neanonymních identitách (= pojmenované identity)
- KartyVS.csv – karty z vysokých škol - zdrojová data o anonymních identitách (= identity přebírané z vysokých škol, nespárované s registrací čtenářů)
- 2 x OpenLDAP – cílový adresář pro neanonymní identity a karty
- EKV – systém elektronické kontroly vstupu – cílová aplikace pro neanonymní identity a karty
- Aleph – knihovnický systém – cílová aplikace pro neanonymní identity a karty
- RS – rezervační systém – cílová aplikace pro neanonymní identity a karty
- PS – platební systém – cílová aplikace pro neanonymní identity a karty

Grafické znázornění:



Obrázek 1 - Schéma současného stavu

1.1.2 Popis cílového stavu

Cílem je výměna Oracle Waveset za řešení IdM Evolveum midPoint při zachování stávajících funkčností, napojených aplikací a potenciálem ke zvýšení výkonu a bezpečnosti. V novém řešení dojde navíc k připojení 2 nových systémů a to Windows Active Directory a Samba Active Directory.

Jednotlivé funkcionality a napojení na zdrojové či cílové systémy budou v novém řešení nově naprogramovány s případným využitím dostupných zdrojových kódů stávajícího řešení. Zdrojové kódy budou využity zejména ke studiu implementované logiky, v některých případech (zejména u konektorů) je ale možné použít i celé funkční bloky.

Následující podkapitoly shrnují potřebu implementace konektorů pro připojení zdrojových a cílových systémů.

Aplikace Registrace / CDB

Aplikaci CDB bude obsluhovat jeden konektor, který bude číst data o neanonymních identitách a zapisovat zpět zablokování/odblokování přiřazené karty.

OpenLDAP 2x

Dva kontejnery OpenLDAP budou obsluhovány pomocí jednoho konektoru, a to pro neanonymní identity a pro karty.

EKV

Aplikaci EKV bude obsluhovat jeden konektor, který bude zapisovat data o nových neanonymních a anonymních identitách a číst data o blokaci karet.

Aleph

Aplikaci Aleph budou obsluhovat také dva konektory, jeden konektor bude určen pro čtení z tabulek Alephu a druhý konektor bude určen pro zápis nových identit.

RS

Aplikaci RS bude obsluhovat jeden konektor, který bude pomocí volání webservices zapisovat data o neanonymních identitách a o kartách.

PS

Aplikaci PS bude obsluhovat jeden konektor, který bude pomocí volání webservices zapisovat data o neanonymních identitách a o kartách.

1.1.3 Popis IdM Evolveum midPoint

V rámci tohoto výběrového řízení nabízíme IdM produkt Evolveum midPoint. Jedná se o open source řešení identity managementu, s otevřeným kódem, bez nutnosti nakupovat licence. Má otevřenou a rozšiřitelnou architekturu založenou na standardech Java, XML a REST. Snahou je docílit maximální efektivnost při minimálním úsilí.

Veliký důraz je také kladen na vývoj a implementaci nových vlastností přímo do produktu IdM Evolveum midPoint, proto jsou poměrně často vydávány jeho nové verze.

Při vývoji IdM Evolveum midPoint jsou v maximální míře využívány standardy a frameworky založené na jazyku Java - Spring, Spring Security, Prism Objects, Wicket. Dále je možné využít skriptovací jazyky, jako je například Groovy, JavaScript, XPath v2 a další. K připojení zdrojových a cílových aplikací je použito frameworku OpenICF, dále je možné připojit webové služby SOAP/WSDL. Další frameworky a konektory budou postupně doplněny.

Součástí produktu je i webové administrátorské rozhraní, které umožňuje administrátorům konfigurovat IdM midPoint a uživatelům provádět nastavení hesla a zpracování požadavků.

IdM Evolveum midPoint je vyvíjen několika nezávislými vývojovými týmy a společnost Evolveum koordinuje zapracování nových vlastností, vydávání nových verzí a vydávání oprav. Výhodou společnosti Evolveum a produktu midPoint je know-how a cca 11 let zkušeností jejích inženýrů v oblasti IdM implementací a možnost zakoupení plné podpory produktu.

Více informací na http://www.evolveum.com/midPoint/

1.1.4 HW & SW

Technické požadavky pro jedno prostředí IdM Evolveum midPoint:

HW:

- 4 cores CPU
- 8 GB RAM
- 50 GB místa na disku

SW:

- OS Linux RHEL 7
- Apache Tomcat 6
- Java Development Kit 8
- Java Cryptography Extension (JCE)
- MySQL 5 databáze nebo PostgreSQL 9.4 databáze

1.1.5 Vysoká dostupnost

MidPoint je možné provozovat ve třech základních režimech vysoké dostupnosti:

- Virtualizační HA
- Load Balanced se sdílenou HA databází
- Load Balanced s vyhraženou databází

Virtualizační HA

Je nejjednodušší implementací HA funkcionality využívající virtualizovanou infrastrukturu. V případě výpadku single-nodové instance a jejím přesunu na nový host disponuje midPoint automatickou obnovou. Díky tomu je výpadek v řádu pouze několika minut.

Load Balanced se sdílenou HA databází

Několik instancí midPoint serverů využívá k zajištění HA standardního HTTP load balanceru. Všechny midPoint servery přistupují k jediné databázi, která disponuje interním HA řešením. Databázový engine je sdílený s dalšími aplikacemi společnosti.

Load Balanced s vyhraženou databází

To samé, co předchozí varianta jenom s tím rozdílem, že databázový engine využívá pouze midPoint a žádná další aplikace.

1.1.6 Prostředí

Pro implementaci navrhujeme realizovat tři separátní prostředí:

- Provozní prostředí – napojené na ostré verze aplikací, určené pro běžnou činnost.
- Testovací prostředí – pro ověření nových funkcionalit před nasazením do produkce.
- Vývojové prostředí – pro vývoj nových funkcionalit.

Testovací prostředí bude realizováno v síti a na HW NTK. Společnost AMI Praha zde nainstaluje IdM Evolveum midPoint a NTK vytvoří kopie připojovaných aplikací (pokud již není toto prostředí k dispozici). Toto prostředí bude co nejvěrněji simulovat aktuální provozní prostředí IdM v NTK a bude se odlišovat maximálně o nově připravované funkcionality. Prostředí bude sloužit pro ověření a akceptaci nového IdM a nových funkcionalit před nasazením do produkce. Správu a údržbu testovacích aplikací bude provádět NTK kromě IdM Evolveum midPoint, jehož správu může provádět AMI Praha v rámci projektu a následné servisní podpory.

Vývojové prostředí bude realizováno v síti a na HW AMI Praha. Společnost AMI Praha nainstaluje IdM Evolveum midPoint a NTK poskytne součinnost při přípravě simulovaných rozhraní jednotlivých připojovaných aplikací. Správu a údržbu vývojového prostředí bude provádět AMI Praha v rámci projektu a následné servisní podpory. Toto prostředí bude sloužit pro vývoj nových funkcionalit a pro ladění chyb stávajících funkcionalit.

Provozní prostředí bude realizováno v síti a na HW NTK. Předpokládáme, že instalaci IdM Evolveum midPoint včetně konfigurace bude provádět NTK podle dodaného instalačního manuálu. Je možné, aby instalaci a konfiguraci IdM provedla společnost AMI Praha.

1.1.7 Součinnost

Pro zdárné dokončení projektu je vyžadována součinnost za strany NTK v následujících oblastech:

- Zajištění vzdálených přístupů pro členy implementačního tymů do infrastruktury NTK.
- Zajištění HW, instalace OS a databáze včetně nastavení oprávnění na testovacím a produkčním (v případě, že AMI Praha bude provádět instalaci a konfiguraci v produkčním prostředí) prostředí.
- Poskytnutí testovacích eventuálně vývojových rozhraních koncových systémů.

- Poskytnutí zdrojových kódů k existujícímu IdM (existují-li) a konfiguračních XML souborů.
- Součinnost kompetentních osob za jednotlivé koncové systémy pro analytické a validační schůzky.

1.1.8 Migrace dat

Migrace dat spočívá ve vytvoření identit v IdM Evolveum midPoint. Účty v ostatních aplikacích není třeba migrovat a celý proces migrace je neovlivní.

V IdM Evolveum midPoint budou vytvořeny identity podle údajů z autoritativních zdrojů CDB a KartyVS.csv. Identity pak budou podle jednoznačného klíče spárovány s účty v jednotlivých napojených systémech.

1.1.9 Přechod do produkce

Při nasazování nového IdM do produkce bude brán co největší ohled na možný výpadek, který by byl nejprve odsouhlasen NTK.

Z technického pohledu bude zejména nutné zamezit situaci, kdy jeden koncový systém bude řízen dvěma IdM systémy.

Standardně provádíme přechod metodou postupného přepojování po jednotlivých koncových systémech a rovněž i metodu „Big Bang“, kdy přepojíme vše současně.

Úvodní napojení provozních aplikací bude provedeno v následujících krocích:

- Naplnění IdM neanonymními identitami a anonymními identitami ze zdrojových aplikací CDB a KartyVS.csv.
- Vypnutí současného IdM Oracle Waveset.
- Synchronizace uživatelů s cílovými systémy.
- Akceptace úspěšného převodu.
- Zaškolení administrátorů (tato aktivita běží nezávisle na předchozích krocích, je vhodné absolvovat nejpozději do Akceptace převodu).

1.2 POŽADAVKY NA IDM

Navrhované řešení splňuje veškeré požadavky na navrhované řešení uvedené v „Příloha C zadávací dokumentace“. Následující kapitoly obsahují komentáře k jednotlivý požadavkům.

1.2.1 Systémové požadavky

MidPoint vyhovuje všem uvedeným systémovým požadavkům.

1.2.2 Požadavky na životnost

Navrhované řešení je „živou“ aplikací, na které probíhá neustálý vývoj nových funkcionalit a vylepšení a oprav chyb. Přehled jednotlivých verzí včetně plánovaných je na https://wiki.evolveum.com/display/midPoint/midPoint+Releases. Konkrétní činnosti pak lze sledovat na https://github.com/Evolveum/midpoint/commits/master.

1.2.3 Všeobecné požadavky

- V navrhovaném řešení lze spravovat různé typy objektů typu identit uživatelů, rolí a organizačních struktur a je možné implementovat funkční místa, místnosti i další objekty.
- V konfigurovatelných částech je možné používat skriptovací jazyky ECMA Script (JavaScript), Groovy, Python.
- Bulkové operace pro hromadné akce typu přejmenování, disable, enable atd. jsou podporovány.
- Export/Import konfigurace je možný ve formátu XML, JSON a YAML.
- Pro různé komponenty aplikace lze nastavit individuální úroveň logování. Typy úrovně jsou: Trace, Debug, Info, Warning, Error, All. Report chyb je dostupný prostřednictvím aplikačního errorlogu.
- Administrátorská a vývojářská dokumentace je dostupná na adrese https://wiki.evolveum.com. Dokumentace je průběžně aktualizována podle přibývajících funkcionalit a obsahuje řadu příkladů. Další příklady jsou součástí zdrojových kódů aplikace, které lze stáhnout z https://gitlab.com/Evolveum/midPoint.
- Vysoká dostupnost – viz kapitola 2.1.5.
- V navrhovaném řešení je možné volitelně vypínat a opětovně zapínat časově náročné administrativní funkce typu workflow apod.

- Jsou podporovány pravidelné serverově/systémové úlohy typu synchronizací a certifikací včetně notifikací s výsledky.
- Konektory pro připojení koncových/ zdrojových systémů je možné čerpat hned ze tří nezávislých projektů ConnId, OpenICF a Polygon. V současné době midPoint disponuje 44 konektory (viz. https://wiki.evolveum.com/display/midPoint/Identity+Connectors) a neustále vznikají nové. MidPoint komunikuje s jednotlivými konektory prostřednictvím API díky čemuž je nezávislý na konkrétní verzi.

1.2.4 Autorizační model

MidPoint vychází z RBAC (Role-Based Access Control) přístupu. Oproti standardnímu statickému RBAC navíc nabízí parametrizované přidělování rolí, což má za následek nižší počet a jednodušší správu rolí. Více informací na https://wiki.evolveum.com/display/midPoint/Advanced+Hybrid+RBAC. Pomocí autorizace uživatele, lze nastavit možnost přístupu až na jednotlivé části GUI.

1.2.5 Rozhraní pro integraci

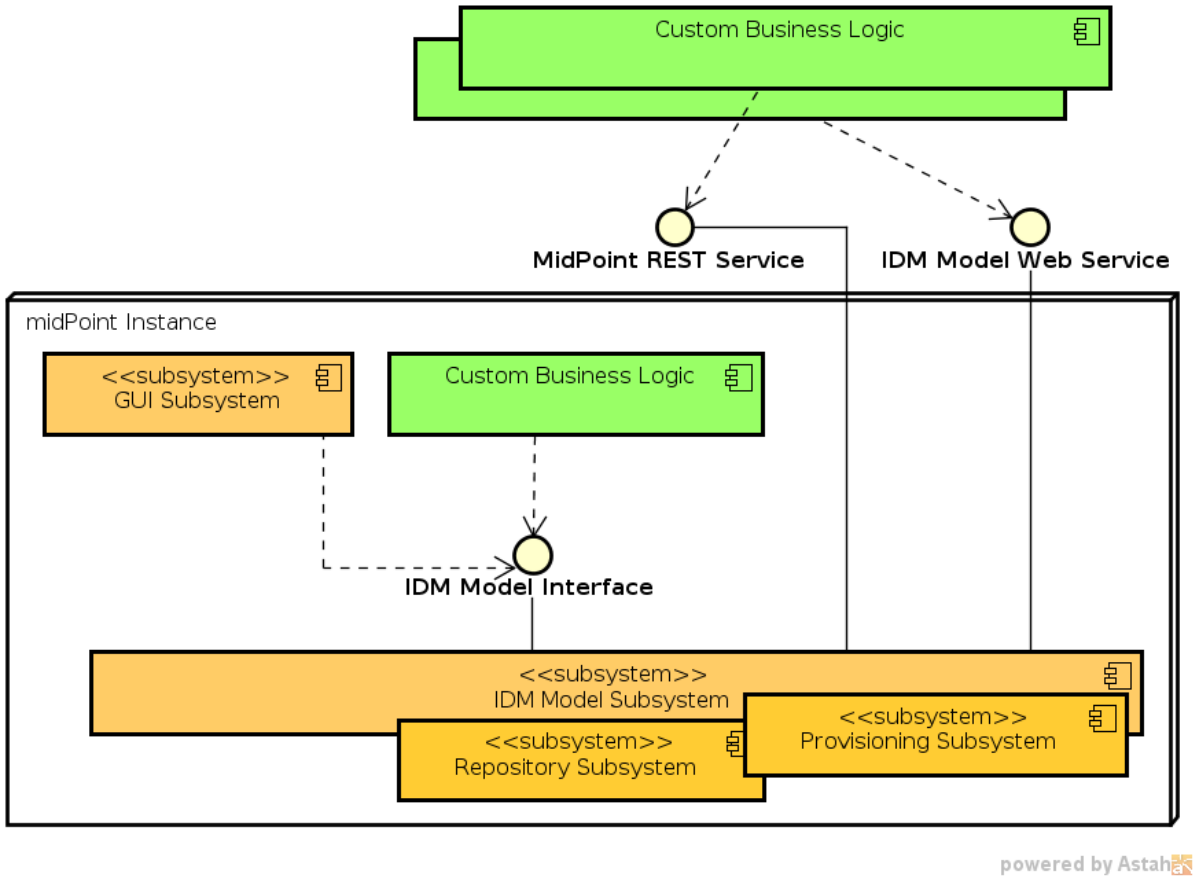
MidPoint nabízí 3 druhy rozhraní k integraci do systémů 3 stran:

- JAVA API (local) (https://wiki.evolveum.com/display/midPoint/IDM+Model+Interface)
- SOAP/WSDL (remote) (https://wiki.evolveum.com/display/midPoint/IDM+Model+Web+Service+Interface)
- REST (remote) (https://wiki.evolveum.com/display/midPoint/REST+API)

Všechna rozhraní umožňují plnou práci se všemi objekty dostupnými přes GUI. Konkrétně se jedná o objekty:

- connectors
- connectorHosts
- genericObjects
- resources
- users
- objectTemplates
- systemConfigurations
- tasks

- shadows
- roles
- valuePolicies
- orgs



Obrázek 2 - IdM model integrace

1.2.6 Rozšiřitelnost

MidPoint pracuje s generickými objekty. Díky tomu umožňuje rozšiřitelnost datových struktur rozšiřováním existujících a dále i vytváření objektů nových. Více na: https://wiki.evolveum.com/display/midPoint/Repository+Subsystem

1.2.7 Integrace s access managementem

MidPoint podporuje integraci s nástroji pro access management. Jako příklad uvádíme odkaz na dokumentaci realizace SSO pomocí nástroje CAS: https://wiki.evolveum.com/display/midPoint/MidPoint+and+SSO+HOWTO.

1.2.8 Synchronizace a rekonciliace

- Synchronizace bude probíhat v reálném čase. Tzn., že jakákoliv vygenerovaná změna ve zdrojovém systému (export csv z aplikace Karty VŠ či změna v db Registrace) vyvolá aktualizaci uživatele v midPoint.
- Změna uživatele v midPoint vyvolá paralelní rekonciliace v ostatních cílových systémech.
- Atributy identit a účtech cílových systému budou mapovány podle definovaných korelačních pravidel.
- Atributy objektů v midPoint mohou být i binární data, např. certifikáty, fotografie, autorizační tokeny, atd.
- V případě neúspěšné rekonciliace účtu na cílovém systému midPoint umožnuje opětovnou propagaci změn.
- O neúspěšné propagaci je možné zaslat notifikaci na administrátora.
- Rekonciliaci konkrétního cílového systému lze dle potřeby vypínat či zapínat.
- Výstupem rekonciliace může být automatické spuštění nápravných opatření (odebrání neautorizovaných rolí, atributů, …) nebo report typu „Evidence vs AsIs“.

1.2.9 Notifikace

MidPoint umožňuje zasílání uživatelských notifikací na vybrané skupiny uživatelů (např. žadatel, pro koho žádám, manažer, vlastník, schvalovatel, …) o proběhlých aktivitách nebo aktivitách, které čekají na moji reakci (např. schválení přidělení/odebrání role). Dalším typem notifikace mohou být notifikace na administrátora IdM při právě vzniklém chybovém stavu.

Notifikace mohou být v prostém textu nebo html formátu a je možné použití šablon prostřednictvím enginu Velocity (http://velocity.apache.org). Šablony lze použít i pro různé jazykové mutace.

Pro různé typy notifikací lze použít různé smtp konfigurace.

1.2.10 Delegovaní administrátoři

Pomocí tzv. autorizace lze definovat s velmi jemnou granularitou přístupy do konkrétních sekcí GUI nebo omezit viditelnost objektů podle umístění v organizační struktuře, atributu,

role apod. Pomocí těchto funkcionalit lze rozdělit celkovou nebo pouze část správy na několik rozlišných typů administrátorů.

1.3 PROCESY PODPOROVANÉ POMOCÍ IDM

1.3.1 LiveCycle identity

MidPoint spravuje identity během jejich celého životního cyklu. Jedná se o procesy:

- Vznik identity.
- Změna identity (Editace).
- Změna pozice (reorganizace).
- Přidělení/odebrání oprávnění.
- Zneplatnění identity.
- Zplatnění identity.
- Zánik identity (smazání / nastavení atributu, např. Enable/Disable).

Všechny procesy je možné zadat s patřičnými oprávněními přes GUI nebo automaticky provádět na základě pravidla. Další možností je doplnění libovolného z procesů o schvalovací workflow a/nebo notifikace (viz. 2.2.6.). U jednotlivých procesů lze zadávat časově omezenou platnost (Od – Do) nebo např. Zánik identity provést až po uplynutí ochranné lhůty.
Veškeré atributy identit jsou editovatelné (není-li definováno jinak) a mohou být jednotypové, vícehodnotové, binární (např. fotografie uživatele, security tokeny, finger printy apod.) nebo i komplexní datové struktury (tabulky).
Identity mohou být různého typu (anonymní / neanonymní uživatel), mohou být u nich evidované různé sady atributů a aplikována rozlišná pravidla (např. pro přiřazení rolí).
Změna typu identity může být podpořena schvalovacím workflow a notifikací.
Identity lze zneplatnit k určitému datu.

1.3.2 Vyhledávání a filtrování identit

Identity lze třídit, vyhledávat a filtrovat podle všech svých evidovaných atributů (loginu, jména, příjmení, celého jména, identifikátoru, čísla karty, …).

Dále je možné vyhledání identity podle přiřazené role, cílového systému, organizační struktury.

1.4 ŘÍZENÍ ROLÍ

Řízení a správu rolí lze provádět v GUI aplikace. Role lze přiřadit nebo odebrat i automaticky na základě stanovených pravidel. Zejména je možné:

- Roli je možné přiřazovat identitám i organizacím.
- Zadat platnost přiřazení Od-Do, podle atributu nebo dalších pravidel.
- Schvalování přiřazení i odebrání role s možností dynamického vypočtu schvalovatele.
- Hierarchické skládání rolí.
- Řízení autorizačních objektů v cílovém systému prostřednictvím rolí.
- Svázání definice role s existencí objektu oprávnění v cílovém systému.
- Načtení seznamu vytvořených rolí v cílovém systému (jestliže to cílový systém umožňuje).
- Řešení mechanismu konfliktních rolí (SoD, Segregation of Duties)
    - Umožnění nastavení pravidla pro vzájemně se vylučující role.
    - Nastavení akcí pro případ výskytu
        - Přiřazení nebude aplikováno.
        - Bude vyvoláno schvalovací workflow.
        - Bude přiřazeno a notifikováno.
        - Další varianty (navrhované řešení umožňuje definování dalších reakcí podle aktuálních potřeb).
- Certifikace přiřazení rolí
    - Certifikaci přiřazení rolí lze spouštět přímo z GUI.
    - Certifikaci lze spouštět opakovaně.
    - Lze spouštět s omezením na konkrétní cílový systém.
    - Lze spouštět s omezením na atribut identity, role, organizační strukturu, …

  - Možnost certifikace na několika úrovních (např. liniový manažer, pak vlastník role, oddělení bezpečnosti, SoD arbiter, …).
  - Výstupem je report s možností akce (např. odebrání necertifikovaných rolí).
- Možnost nastavení práv až na úroveň atributu libovolného objektu (např. uživatel, role nebo organizace).

1.5 ORGANIZAČNÍ STRUKTURA

Organizační strukturu je možné v midPoint spravovat přímo v GUI nebo je možné ji načítat ze zdrojového systému. Organizační strukturu lze využít obecně pro jakoukoliv interpretaci stromové struktury. Navrhované řešení umožňuje správu jedné a více struktur současně. Organizační struktura v midPoint mimo jiné umožňuje:

- Vytváření a editaci nezávislých entit.
- Přiřazovat a odebírat role/účty na koncových systémech podle umístění v organizační struktuře.
- Uživatel nebo role může být ve více entitách organizační struktury zároveň (i v rozdílných rolích – nadřízený, podřízený, vlastník, …).
- Uživatel nebo role může být ve více organizačních strukturách zároveň (i v rozdílných rolích – nadřízený, podřízený, vlastník, …).
- Přiřazení do organizační skupin může být časově omezené, nebo i platné dle atributu nebo jiného pravidla.
- Evidované vztahy v organizační struktuře mohou být využity pro schvalování a certifikace.

1.6 FIREMNÍ POLITIKY

1.6.1 Politiky hesla

MidPoint disponuje implementovaným mechanismem politiky hesla. Umožňuje definovat pravidla na minimální a maximální délku hesla a jeho složitost. Pravidly lze definovat počty opakování znaků, skupiny znaků a minimální a maximální počet znaků ze skupin. Dále je možné definovat i historii hesel, po kterou nelze heslo opětovně použít a metody ukládání hesel v midPoint. Standardně se hesla ukládají v šifrované formě. Je možné použít i ukládání

hashe místo hesla. Politiku hesla lze aplikovat pro identity v midPoint ale i v cílových systémech, které to podporují.

1.6.2 Politiky účtu

MidPoint podporuje definování pravidel pro názvy účtu, jako jsou minimální a maximální délka, povolené a nepovolené znaky, zakázaná slova a syntaktickou validaci (např. emailová adresa).

1.7 REPORTING

Standardní reporting je postaven na technologii Jasper, která poskytuje širokou škálu výstupních formátů (PDF, XLS, CSV, HTML ad.). MidPoint out of the box nabízí tyto druhy reportů:

- Report uživatelů midPoint.
- Report rekonciliace koncového systému – přehled účtů v koncovém systému, jejich přiřazení uživatelům a identifikace neslinkovaných (neevidovaných) účtu.
- Report auditního logu – report obsahuje kompletní přehled změn provedených nad uživatelem, přidělení rolí, změna hesla a pod včetně přihlášení uživatele do systému.
- Reporty certifikačních kampaní – reporty týkající se certifikačních kampaní (přeschválení již přiřazených rolí)

Produkt umožňuje vytvářet nové uživatelské reporty pomocí designeru Jasper Studio (open source) včetně pluginu pro ověření reportu proti skutečným datům v midPoint. Vytvořené reporty je možné jednoduše importovat do midPointu a spouštět je pak z jeho rozhraní.

1.8 UŽIVATELSKÉ ROZHRANÍ

MidPoint nabízí jedno společné prostředí jak pro administrátory, tak i pro běžné uživatele. Rozsah a charakter zobrazovaných informací v GUI je definován autorizačním mechanismem. Grafické rozhraní je možné dále přizpůsobit do souladu s firemním layoutem (upravit barvy headeru, logo apod.). Uživatelské rozhraní nabízeného řešení je v českém jazyce a to včetně nápovědy. Kromě toho řešení obsahuje GUI také v jazycích angličtina, němčina, španělština, estonština, maďarština, polština, ruština, turečtina, slovenština

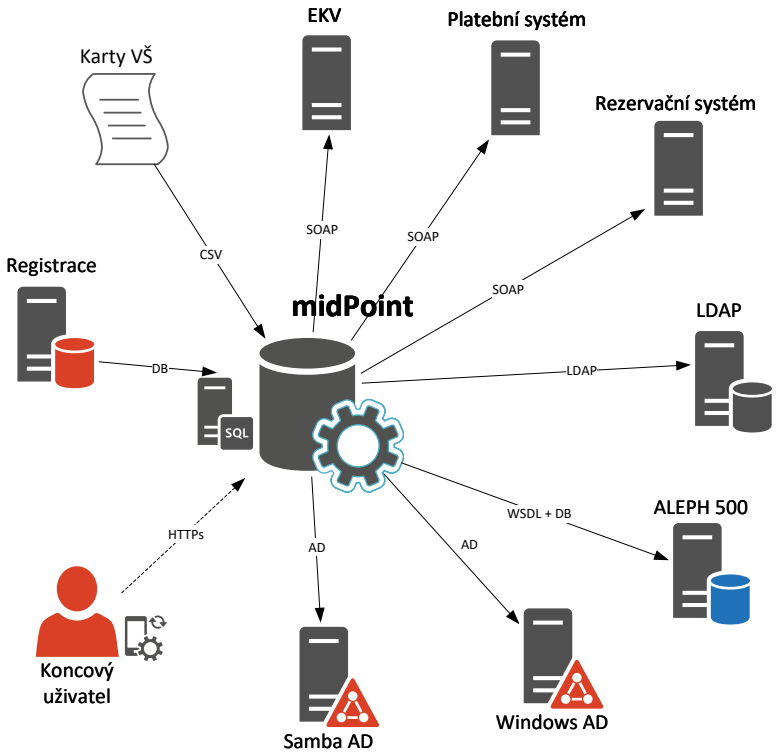
a portugalština. Všechny údaje jsou ukládány v kódování UTF-8, IdM umí správně pracovat se všemi znaky (nejen českými).

Intuitivní uživatelské rozhraní využívá technologie Apache Wicket a je plně responsivní. Je možné k němu přistupovat z PC, tabletů i mobilních telefonů. Více informací na http://wicket.apache.org/.

Podporovány jsou nejnovější verze prohlížeče Internet Explorer, Mozilla Firefox, Opera, Google Chrome.

1.9 PŘIPOJENÉ KONCOVÉ SYSTÉMY

Jednotlivé koncové systémy s komunikací vůči IdM jsou schematicky zobrazeny na následujícím grafu. Směr toku informací je interpretován šipkou, na které je uveden protokol vzájemné komunikace. Chování komunikace bude přeneseno ze stávajícího provedení v případě existujících zdrojových kódů nebo bude vydefinováno na analytických schůzkách.



1.9.1 Koncový uživatel

Nejedná se o koncový systém v pravém slova smyslu. Je zde uveden pro znázornění interakce vůči ostatním systémům. Běžní koncoví uživatelé a administrátoři mají podle své autorizace možnost prostřednictvím GUI provádět činnosti:

- Zobrazit si svůj profil (své atributy, přehled svých schválených nebo automaticky přidělených rolí a oprávnění podle pravidla; např. role na pozici, projektové role, …).
- Změnit heslo do všech nebo vybraných koncových systémech.
- Změna atributů.
- Zažádat o přidělení role pro sebe.
- Zažádat o přidělení role pro podřízené.
- Schválit přidělení role podřízenému.
- Schválit přidělení role schvalovatelem.
- Změnit zařazení v organizační struktuře podle již existujících pravidel.
- Spouštět certifikační kampaně.
- Nahlížet na reporty.
- Spravovat midPoint a napojení na cílové systémy (pouze administrátor nebo jiné autorizované identity).

1.9.2 Aplikace Registrace

Autoritativní zdroj neanonymních identit a rolí. Pro komunikaci bude využit OTB DatabaseTable (JDBC) konektor.

1.9.3 Karty VŠ

Autoritativní zdroj anonymních identit. Jedná se o identity přebírané z vysokých škol a jsou nespárované s registrací čtenářů. Pro komunikaci bude použit OTB CSV konektor.

1.9.4 EKV

Cílový systém, do kterého se budou zapisovat data o nových neanonymních a anonymních identitách. Zároveň se z něj budou číst data o blokaci karet. Pro komunikaci bude použit naprogramovaný SOAP WS konektor.

1.9.5 Platební systém

Cílový systém, do kterého se budou zapisovat data o neanonymních identitách a o kartách. Pro komunikaci bude použit naprogramovaný SOAP WS konektor.

1.9.6 Rezervační systém

Cílový systém, do kterého se budou zapisovat data o neanonymních identitách a o kartách. Pro komunikaci bude použit naprogramovaný SOAP WS konektor.

1.9.7 2 x LDAP

Cílový systém pro neanonymní identity a karty. Pro komunikaci bude použit OTB LDAP konektor.

1.9.8 ALEPH 500

Cílový systém pro neanonymní identity a karty. Pro komunikaci bude použit naprogramovaný SOAP WS + DB konektor.

1.9.9 Windows AD

Pro komunikaci bude použit OTB Active Directory konektor.

1.9.10 Samba AD

Pro komunikaci bude použit OTB Active Directory konektor.

SLOVNÍK POJMŮ A ZKRATEK

Pojem/zkratka	Popis
Aleph	Knihovnický systém používaný v NTK.
Anonymní uživatel	Uživatel přiřazený kartě z VŠ, který je spravován IdM, ale není evidován v CDB.
Aplikace Registrace	Aplikace, kterou NTK nově používá pro správu identit zákazníků, zaměstnanců a návštěvníků (předregistrace, registrace, změna údajů apod.). Pro ukládání dat používá CDB.
Atribut	Údaj popisující určitou vlastnost popisované entity.
CDB	Centrální databáze identit NTK, se kterou pracuje aplikace Registrace a z níž čerpá informace IdM
Cílový systém	Systém, který IdM definovaným způsobem spravuje (tj. IdM do něj i zapisuje).
EKV	Systém elektronické kontroly vstupu používaný v NTK.
ID	Identifikátor
Identity management	Management životního cyklu identit.
Identity Manager	Administrační nástroj pro centralizaci a automatizaci správy uživatelských identit (účtů, skupin atd.) Komunikace s koncovými systémy probíhá pokud možno jejich nativními protokoly (LDAP, JDBC, SSH, ...). Zde v implementaci IdM.
IdM	Sun Java System Identity Manager, Evolveum midPoint
Koncový systém	Cílový nebo zdrojový systém.
LDAP	Lightweight Directory Access Protocol; protokol na dotazování a změnu entit a atributů v adresářových službách.
Neanonymní uživatel	Uživatel evidovaný v CDB. Jeho karta může, ale nemusí být vydaná VŠ.
NTK	Národní technická knihovna
OpenLDAP	Adresářová služba v implementaci Open DAP s rozhraním LDAP.
PIN	Personal identification number – osobní identifikační číslo zabezpečující použití karty, v NTK není uloženo na kartě, ale v CDB a OpenLDAPu
PO	Právnická osoba
PS	Platební systém
RČ	Rodné číslo
RS	Rezervační systém
UID	User ID - identifikátor uživatele
Zdrojový systém	Systém, odkud IdM získává data o uživatelských identitách.
OTB	Out-of-The-Box : součástí produktu