IDM - Identity management

Technická specifikace

1 Obsah

2 Obecná specifikace

2.1 Obecný popis přínosů po zavedení IdM:

- Nepopíratelná odpovědnost - jednoznačná identifikace uživatele oproti identitě.
- Správa přístupů a oprávnění do všech prostředků v SŽDC (IS, aplikace, systémy atd.).
- Správa identit a uživatelů přistupujících k systémům a prostředkům SŽDC.
- Správa přidělování oprávnění uživatelům.
- Evidence všech rolí oprávnění (aplikačních rolí) všech systémů a aplikací a identit, jejich uživatelů včetně přidělených oprávnění.
- Omezení vlivu lidského faktoru a automatizace procesů spojených s nástupy, změnami pozic a výstupy zaměstnanců a externích pracovníků.
- Zavedení schvalovacích procesů do řízení života identit, přidělování oprávnění i samotného zavádění do koncových systémů.
- Naplnění podmínky zákona o kybernetické bezpečnosti.
- Centralizace správy uživatelů napříč IT systémy.
- Úspora práce administrátorů zvýšením automatizace.
- Reporting aktuálního stavu uživatelských účtů a zpětný audit.
- Časově omezené přidělování přístupů a ukončování uživatelů.
- Zavedení business rolí ve vazbě na procesní analýzu.
- Omezení chyb na vstupu informací o uživatelích.
- Eliminace manuálních zásahů a eliminace chyb obsluhy.
- Recertifikace existujících oprávnění uživatelů.
- Automatizované řízení přidělování oprávnění od schválení až po zavedení do koncového systému.
- Logování a monitorování veškerých změn oprávnění, včetně exportu logů mimo dosah administrátorů IdM.

2.2 Zkratky a pojmy

SŽDC	Správa železniční dopravní cesty, státní organizace
IdM	Identity Management
MS AD, AD	Adresářová služba Microsoft Active Directory
PPV	Pracovněprávní vztah
SoD	Segregation of Duties, kontrola konfliktních oprávnění
KS	Koncový systém
WS	Webová služba
Konektor	Komponenta umožňující připojení koncových systémů, nebo autoritativních zdrojů dat.
Autoritativní zdroje dat	Aplikace, které evidují všechny pracovníky a jejich PPV, organizační strukturu atd.
Liferay	Portálové řešení napříč organizací SŽDC
Exchange	Emailové řešení v SŽDC

Certifikace, Recertifikace, někdy také Atestace	Smyslem certifikace je v pravidelných intervalech ověřovat, zda uživatel má přiděleny stále ta oprávnění, která má mít vzhledem ke své pozici, projektu či procesu, který vykonává. Nadbytečná oprávnění jsou po ukončení certifikace odebrána. Proces certifikace je možné chápat jako dodatečnou kontrolu automatických rutin pomocí lidského faktoru, kterým je například nadřízený uživatele nebo auditor.
Koncový systém, koncová aplikace	Aplikace napojená (přímo nebo nepřímo pomocí notifikací) na IdM.
Rekonciliace	Při rekonciliaci se prochází všechny uživatelské účty na koncovém systému a na základě definovaných akcí se aktualizují identity uživatelů v Identity Manageru. Jde o uvedení účtů do souladu s IdM. Tedy účtům v koncových systémech se přidělují vlastníci (identity IdM) na základě logických podmínek např. korelace uživatelského jména, emailu apod. Účty bez vlastníka jsou reportovány, nebo rovnou mazány z koncového systému (podle nastavení IdM). Procesem rekonciliace je vynucen soulad a řád v koncových systémech.
Entitlement	Schopnost nebo nárok přistupovat ke službě či zdroji. Příklad: nový zaměstnanec má nárok (entitlement) na přístup k firemnímu emailu. Ten je mu však přidělen až poté, co je založen v informačních systémech (proběhne provisioning) a jsou mu nastavena patřičná oprávnění.
Business Role	Samostatná entita, která v sobě nese aplikační role do koncových systémů nebo jiné business role.
Aplikační Role	Samostatná entita, která odpovídá objektu v koncovém systému (např. Skupině v Active Directory, Skupině oprávnění v koncové aplikaci).
RBAC, Role-Based Access Control	Model, ve kterém jsou uživateli přiřazeny role, které mu dávají určitý stupeň přístupu ke zdroji. Přiřazení role garantuje uživateli definovanou sadu entitlementů (nároků na oprávnění), které jsou přiřazeny buď automaticky, nebo po splnění určité podmínky, nebo na základě schválení odpovědnými osobami. Výhodou modelu RBAC je opětovná použitelnost přidělených rolí a možnost definování atributů role – např. popis.
Delegace	Je to možnost delegovat vybraný požadavek ke schválení (nebo vybranou skupinu požadavků) na jiného zvoleného schvalovatele.
Zastupování	Je to možnost nastavit zástupce pro všechny požadavky, které budou na určenou dobu směrované na jiného schvalovatele.
Autentizace	Autentizace znamená potvrzení, že uživatel požadující služby je platným uživatelem poskytovaných síťových služeb. Autentizace je dosažena pomocí představení identity a jistého pověření nebo tajemství. Mezi různé typy tajemství patří například hesla, pověření na jedno použití, digitální certifikáty nebo telefonní čísla (ať už volající nebo volaná).
Autorizace	Autorizace znamená udělení specifického typu služby (včetně „žádné služby“) uživateli, na základě jeho autentizace, služeb, které požaduje a aktuálního stavu systému. Autorizace může být založena na omezeních, například omezení na určité hodiny v rámci dne, nebo omezení na fyzickou polohu, nebo omezení vícenásobného přihlášení jednoho uživatele. Autorizace určuje povahu služby, která je poskytnuta uživateli. Typy služeb jsou například: filtrování IP adres, přidělení adresy, přidělení cesty, QoS, řízení šířky pásma/řízení toku, tunelování do konkrétního koncového bodu, nebo šifrování.
Eskalace	Eskalace definuje pravidla, která se mají uplatnit tehdy, pokud v určeném časovém období nedojde k rozhodnutí žádosti, nebo dojde k bezpečnostnímu incidentu. Možnosti jsou například: připomenutí emailem, postoupení na nadřízeného pracovníka, či automatické schválení/zamítnutí žádosti.
SSO	Single Sign On

2.3 Systémové požadavky

- Podpora operačního systému Windows nebo Unix.
- Jediné úložiště dat (repository), a to relační databázi; pro svůj provoz nesmí vyžadovat LDAP server.
- Repozitory podporuje minimálně jednu z těchto relačních databází: MS SQL Server v aktuální verzi nasazené v SŽDC, Oracle DB v aktuální verzi nasazené v SŽDC; alternativně je možné použít jinou relační DB.
- Řešení, které podporuje skriptovací jazyk.
- Řešení podporuje přístup pomocí zabezpečeného protokolu HTTPS s podporou technologie RSA a ECC.
- Řešení podporuje kódování UTF-8 i UTF-16.
- Řešení podporuje Single sign on s možností konfigurace využívaného protokolu. Toto řešení podporuje všechny standardní protokoly, jež jsou definovány v rámci konfigurace systému.

2.4 Licence a další požadavky

- Zadavatel požaduje, aby počet licencí byl bez omezení ve všech těchto aspektech:
  1. Neomezené počty instancí produktu
  2. Neomezené počty uživatelů
  3. Neomezené počty koncových systémů
  4. Neomezené počty konektorů,
  5. Neomezené počty procesorových jader, velikost paměti a jiných hardwarových, softwarových či aplikačních parametrů.
- Součástí dodávky je i předání kompletních zdrojových kódů.
- Zadavatel požaduje možnost připojení budoucích nových koncových systémů a vložení jejich přístupových rolí a logiky do systému IdM bez dodatečných licenčních nákladů.
- Dodavatel se zaručuje, že v dodávce jsou zahrnuty licence třetích stran a používání díla jako celku nevyžaduje žádné další dodatečné náklady.
- Dodavatel se zaručuje, že při uplatnění práv třetí osobou na autorská práva nese následky případných sporů dodavatel.
- Licence opravňuje objednatele k tomu, aby:
  1. Bez omezení využíval dílo v rámci své podnikatelské činnosti
  2. Pořídil si neomezený počet kopií díla pro vlastní potřebu
  3. Sám nebo prostřednictvím třetích osob měnil, rozšiřoval a jinak upravoval dílo v souladu se svými potřebami.

2.5 Demo produktu

- V době podání nabídky musí být přístupné on-line demo produktu bez nutnosti instalace jakéhokoliv SW či provedení konfigurace na straně zadavatele (např. VPN přístup).
- dostupnost dema po dobu minimálně 60 pracovních dní od zpřístupnění.
- ukázková data pro demonstraci požadavků.

Požadovaná funkcionalita pro demo prostředí:

Administrátor

- Přehled identit v IdM

- Detail profilu identity
- Koncové systémy s možností přidat nový koncový systém
- Serverové úlohy
- Minimálně dva reporty z části Reporting (viz níže)

Běžný uživatel

- Přehled účtů v jednotlivých napojených systémech
- Přehled o přidělených oprávněních v systémech
- Žádosti o role

3 Technické požadavky

3.1 Obecné požadavky na uživatelské rozhraní v IdM

Nabízené řešení musí splňovat následující požadavky:

- Kompletní lokalizace do českého jazyka
- Webové rozhraní pro administrátory i pro koncové uživatele
- Responzivní design
- Vyhledávání libovolného obsahu v agendách podle libovolného atributu
- Možnost grafického přizpůsobení korporátní identitě (rozhraní je možné upravovat dle potřeb zadavatele)
- Podpora konfigurace více úrovní oprávnění podle definice v kapitole 3.2

3.2 Autoritativní zdroje dat

Nabízené řešení musí být schopno se napojit na autoritativní zdroje dat, které mohou obsahovat:

- Zdroj pro komunity: interní a externí uživatelé, zákazníci apod.
- Možnosti napojení: CSV import, LDIF import, přímý přístup do DB, preferovány jsou webové služby

3.3 Active Directory

Nabízené řešení musí být schopno spolupracovat s Active Directory. Mezi základní parametry AD patří:

- Multidoménová a multiforestová struktura
- Možnosti napojení: LDAPS, PowerShell, ADSI, .NET, vše v zabezpečených variantách.

3.4 Autorizační model v IdM

- Autorizační model musí být založen na RBAC (Role-Based Access Control) a musí umožňovat nastavit, k jaké části uživatelského rozhraní IdM a k jakým objektům v IdM mají uživatelé přístup až do úrovně atributů.

- Autorizace v IdM se neliší od ostatních KS. Oprávnění k jednotlivým objektům a částem v IdM budou definovány v aplikačních/business rolích.
- Autorizační model v IdM musí být nastaven tak, aby IdM bylo schopno pracovat samo se sebou jako s dalším KS a zároveň vůči IdM jako KS vystupovat.

3.5 Autentizace v IdM

- Je požadováno, aby autentizace do IdM byla prováděna proti AD pomocí SSO. Základem je podpora multiforestového, resp. multidoménového modelu.

3.6 Certifikace oprávnění

Nabízené řešení musí podporovat certifikace a u nich umožnit:

- plánované (automaticky spouštěné) certifikace a certifikace na vyžádání.
- schvalování/zamítnutí přístupů jednotlivě.
- automatické akce při zamítnutí přístupu (např. zamčení účtu v aplikaci).
- definovat rozsah recertifikací (u koho, na jakých rolích, na jaké org. str.).
- logovat a reportovat stav o krocích a o výsledku recertifikace.

3.7 Delegace a zastupování

Nabízené řešení musí podporovat delegace a zastupování:

- Možnost delegovat vybraný požadavek ke schválení (nebo vybranou skupinu požadavků) na jiného zvoleného schvalovatele.
- Na definovanou dobu (od-do) nastavit zástupce pro všechny požadavky, které budou v době od-do směrované na schvalovatele; zastupování musí být aditivní – původní schvalovatel musí být stále schopen požadavek schválit stejně, jako kdyby zástup nebyl nastaven.
- Po definovanou dobu nastavit plnou zastupitelnost na zvoleného uživatele.
- Možnost nastavení delegace i na již rozpracované požadavky.

3.8 Firemní pravidla

Nabízené řešení musí mít vestavěnou možnost zavádění, vynucování a kontroly firemních pravidel a politik.

3.8.1 Politiky hesla

Nabízené řešení musí umožnit konfiguraci politiky hesel tak, aby byla v souladu s politikou hesel na SŽDC. Nastavení politiky hesel musí být plně konfigurovatelné. Politika hesel nebude automaticky načítána z AD do IdM.

Aktuální politika hesel je:

- Heslo má minimální délku dvanáct znaků.
- Password Complexity ve Windows 2012 R2/2016, popř. vyšší:

- Heslo obsahuje alespoň tři z následujících čtyř požadavků:
  - nejméně jedno velké písmeno (A – Z),
  - nejméně jedno malé písmeno (a – z),
  - nejméně jednu číslici (0 – 9) nebo
  - nejméně jeden nealfanumerický znak (t.j. ~!@ #$%^&*_-+=`|\(){}[]:;"'<>,.?/).
- Heslo nesmí obsahovat řetězec vlastního samAccountName (účtu), je-li jeho délka 3 a více znaků, bez ohledu na velká či malá písmena.
- Heslo nesmí obsahovat název účtu (displayName, fullName), a to bez ohledu na velká či malá písmena. Všechny části názvu účtu oddělené mezerou nebo oddělovacími znaménky a delší než dva znaky se posuzují zvlášť.

3.8.2 Pravidla tvorby názvu účtu

Nabízené řešení musí umožnit univerzální konfigurovatelné nastavení pravidel pro název účtu - minimální a maximální délka, povolené znaky, zakázaná slova v názvu (například *admin*, *info*), kontrola na platný formát emailové adresy. Nastavení pravidel tvorby účtu musí být plně konfigurovatelné.

Aktuální pravidla pro tvorbu jména účtu v AD jsou:

- Účet (samAccountName) v Active Directory a poště je u jmenných účtů uživatelů vytvářen z příjmení bez diakritiky.
- Pokud v daném systému (doméně AD, poště) již takový účet existuje, doplní se za příjmení další rozlišovací znak, případně znaky z křestního jména, bez diakritiky.
- Po vyčerpání možností se řetězec doplní zprava nejnižší možnou číslicí od 2 výše tak, aby bylo dosaženo v daném systému jedinečnosti.
- Vyplňuje se plynule bez mezer nebo jiných oddělovacích znamének. Příjmení i jméno použité v aliasu začíná vždy velkým písmenem, např.: Novotny, NovotnyJ, NovotnyJa, NovotnyJan, NovotnyJan2, atd.

Aktuální pravidla pro tvorbu emailové adresy jsou:

- Všichni uživatelé v rámci SŽDC mají primární emailovou adresu obecně tvořenou jako <Prijmeni>@szdc.cz, kde před zavináčem vystupuje řetězec popsaný v tvorbě účtu (viz výše) ve jmenném prostoru @szdc.cz, např.: Novotny@szdc.cz, NovotnyJan2@szdc.cz.
- Speciální jednotka TÚDC má výše uvedené adresy nastaveny jako sekundární; primární adresa je obecně tvořena jako <Jmeno>.<Prijmeni>@tudc.cz, kde <Jmeno> je první křestní jméno bez diakritiky, <Prijmeni> je v případě potřeby doplněno zprava nejnižší možnou číslicí od 2 výše tak, aby bylo dosaženo v daném systému jedinečnosti, např.: Marie.Novotna@tudc.cz, Marie.Novotna2@tudc.cz atd.
- V případě, že uživatel oficiálně uvádí dvě příjmení, použijí se v emailové adrese obě, bez mezery, bez pomlčky, např.: Marie.NovotnaAbelova@tudc.cz
- V případě, že org. celek používá standard emailových adres, který zahrnuje křestní jméno, a uživatel má více křestních jmen, použije se v emailové adrese pouze první z nich, např.: Novotná Marie Anna: Marie.Novotna@szdc.cz

3.9 Rozhraní pro integraci

Nabízené řešení musí poskytovat rozhraní pro integraci a splňovat následující požadavky:

- Za pomoci Web service API (SOAP/WSDL) nebo REST API číst, nebo zapisovat všechna data a volat operace nad objekty v IdM.

- Volat ekvivalent jakékoli funkcionality, která je dosažitelná z webového rozhraní (možnost volání jen některých funkcí jádra IdM je pro tyto potřeby nedostatečná).

Rozhraní musí splňovat následující parametry:

- Umožňovat bezpečný přenos dat mezi IdM a rozhraním koncového systému (např. SSL/TLS, pro AD Kerberos nebo NTLM2).
- IdM se k rozhraní autentizuje dedikovaným technickým uživatelem.
- Aplikační rozhraní (WS SOAP, REST, Java API, Powershell apod.) nebo rozhraní datového úložiště (LDAP, DB procedury, DB tabulka).
- Návratové kódy při zpracování operace.

3.10 Požadavky na integraci

Všechny konektory musí podporovat NTLM2 nebo Kerberos.

3.10.1 Defaultní konektory

Součástí nabízeného IdM systému musí být připojení minimálně k následujícím typům aplikací pomocí konfigurace:

- Active Directory (ADSI, .NET)
- Podpora Powershell
- LDAP
- Databáze

Připojení k těmto typům systémů musí být konfigurovatelné, nesmí se jednat o vývoj nebo využití komponenty třetí strany.

3.10.2 Podpora konektorů do koncových systémů

Nabízené řešení musí podporovat vytváření a vývoj vlastních konektorů.

Jedná se minimálně o:

- Připojení k různorodým webovým službám a využití jejich metod
- Připojení k různým typům a strukturám databází a čtení a zápis dat
- Připojení pomocí LDAP

Cílem zadavatele je vytvořit na straně koncových systémů sadu standardizovaných webových služeb tak, aby různorodost konektorů do těchto koncových systémů byla co nejmenší. Připojování nových koncových systémů tak bude dosaženo pomocí již typově existujících konektorů a jejich využití.

3.11 Synchronizace a rekonciliace

Nabízené řešení musí podporovat:

- 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 koncového systému (např. uživatele a jejich atributy), tak z koncového systému do IdM (např. role v konkrétním koncovém systému).
- Mapování atributů mezi koncovými 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.
- Rekonciliace účtů - zaznamenání stavu účtu vzhledem k ne/existenci vlastníka v IdM.
- Rekonciliace oprávnění - pravidelná automatická kontrola stavu oprávnění na koncových systémech oproti stavu chtěnému a náprava (notifikace, zápis do logů, výmaz nadbytečných oprávnění apod.).
- Nastavení pravidel pro párování mezi identitou a účtem (například email identity na login účtu) skrze všechny koncové systémy.

3.12 Emailové notifikace

Nabízené řešení musí podporovat:

- Možnost definice šablon emailů s podporou vícejazyčnosti a HTML
- Podpora skriptovacího jazyka s možností čerpání dat z databáze
- Možnost konfigurace parametrů odesílání zpráv (SMTP server apod.)
- Možnost zvolit v nastavení více odesílacích SMTP serverů
- Odesílání pomocí SMS gateway zadavatele
- Vkládání hypertextových odkazů na konkrétní odkazované záznamy

3.12.1 Notifikované akce

Nabízené řešení musí minimálně podporovat notifikaci následujících akcí:

- vytvoření, změna, smazání identity,
- přiřazení a odebrání role,
- výzva k akci,
- zakázání a povolení uživatele,
- přejmenování uživatele,
- požadavek na schválení role a na atestaci,
- libovolné akce ve workflow.

3.13 Delegování správy

- Nabízené řešení musí podporovat delegovanou správu.
- Delegovaní správci musí mít administrátorská práva nad zvolenými komunitami, nad skupinami uživatelů nebo obecně nad definovanými objekty IdM - účelem je umožnit lokálnímu administrátorovi správu nad uživateli patřícími do samostatného podřízeného celku (ať už z pohledu interního, tak externího - například dodavatelské účty).

3.14 Workflow

Nabízené řešení musí podporovat tvorbu workflow a u nich umožnit:

- Administrátor IdM musí vytvářet nové definice workflow a modifikovat stávající, pro které se používají nejčastěji základní typy procesů:

    - Procesy monitorování – systém zjišťuje stavy záznamů, atributů a při splnění podmínky nastartuje proces s upozorněním emailem.
    - Řízení toku záznamů (např.: schvalovací workflow pro business role, kde business roli reprezentuje záznam v systému) – systém automaticky přiděluje úkoly zodpovědným lidem, jak je postupně záznam zpracováván.
    - Spouštění workflow uživatelem.

- Všechny workflow mohou spouštět aplikační funkce systému nad zpracovávanými záznamy.
- Workflow dále umožňuje:

    - neomezený počet schvalovacích kroků,
    - neomezený počet schvalovatelů,
    - schválení typu „jeden z X“ a typu „všichni musí schválit“,
    - paralelní schvalování a step-by-step schvalování,
    - definici schvalovatelů na základě jejich členství v roli, funkci nebo v organizační struktuře,
    - automatické schválení na základě hodnoty atributů,
    - automatické schválení na základě pracovního místa, funkce nebo zařazení v organizaci.

- Notifikovat schvalovatele minimálně emailem.
- Zobrazit schvalovatelům přehled svých úloh.
- Úlohu schválit či zamítnout včetně uvedení zdůvodnění.
- Administrátor IdM musí být schopen pracovat se všemi úlohami (pro řešení nestandardních situací).
- Administrátor IdM musí být schopen dynamicky nastavovat workflow (pomocí GUI nebo formou skriptů) bez součinnosti dodavatele.
- Možnost definovat podmíněné kroky (například přiřadit všechny aplikační role až po změně úvodního hesla).

3.15 Rekonciliace

Nabízené řešení musí podporovat rekonciliace a u nich umožnit definovat pro každý připojený systém zvlášť:

- plánované (automaticky spouštěné) rekonciliace a rekonciliace na vyžádání,
- nastavit plán rekonciliací,
- definovat seznam rekonciliovaných objektů,
- definovat typ rekonciliovaných objektů,
- nastavit korelační pravidla,
- podporovat rekonciliaci všech typů objektů (uživatele, role, org. strukturu),
- logovat a reportovat stav výsledku rekonciliace,
- nastavit spuštění akce na základě výsledku rekonciliace (např. spuštění workflow).

3.15.1 Online a offline rekonciliace

Nabízené řešení musí kromě online řízení oprávnění a identit do připojených aplikací podporovat i tzv. offline řízení oprávnění a identit na základě manuálního potvrzení akce odpovědnou osobou nebo na základě informací získaných z exportu aplikace.

3.15.2 Hromadné akce

Nabízené řešení musí nabízet spouštění hromadných akcí, např. hromadné přiřazení rolí uživatelům, kteří vyhovují podmínkám, hromadné schvalování přidělených úkolů atp. Každá změna hromadné akce musí být auditovaná.

3.16 Reporting

Nabízené řešení musí nabízet možnost exportovat minimálně do všech následujících formátů: PDF, CSV, HTML, XML a do formátu kompatibilního s MS Word a MS Excel.

3.16.1 Audit report

Nabízené řešení musí podporovat generování auditního reportu o všech aktivitách v IdM:

- Kompletní přehled změn provedených nad identitou – například synchronizace atributů, přidělení role včetně časového omezení, změn atd.
- Kompletní přehled změn provedených nad libovolnými entitami - role, organizace, definice politik a konfigurací.
- Záznam o přihlášení (úspěšném i neúspěšném) uživatele do webového rozhraní IdM.

3.16.2 Uživatelské reporty

Nabízené řešení musí podporovat generování reportů o stavu objektů v IdM:

- Minimálně informace o tom, jaké mají identity přiřazené role a účty v koncových systémech.
- Možnost nastavit filtr pro výběr identit (např. identity patřící do zvolené organizace).

3.16.3 Report o rekonciliacích

Nabízené řešení musí podporovat generování reportů o rekonciliacích:

- Přehled účtů v koncových systémech, které jsou známy IdM.
- Možnost identifikace účtů, ke kterým nebyl v IdM nalezen vlastník.

3.16.4 Další doporučené reporty

- Seznam uživatelů IdM
- Seznam rolí přidělených identitám v IdM
- Seznam přidělených KS
- Přehled statusů identit v IdM
- Historie změn nad identitou v IdM
- Historie změn nad identitami směrem do vybraného KS
- Historie změn nad rolemi v IdM
- Historie změn nad org. strukturou v IdM
- Přehled úloh v IdM a jejich status
- Přehled spuštěných workflow v IdM
- Přehled zprocesovaných workflow v IdM
- Přehled přihlášení identit do GUI
- Přehled stavů a výsledků rekonciliací

3.17 Agendy a správa objektů

3.17.1 Uživatelé

Nabízené řešení musí podporovat:

- Administrační webové rozhraní pro správu uživatelů bez nutnosti instalovat dodatečný SW.
- Správu skrze integrační vrstvu, tzn. přebírání identit z autoritativních zdrojů.
- Evidence atributů identity.
- Zajištění unikátní identity.
- Zplatnění/zneplatnění identity k určitému datu.
- Přiřazení koncových systémů, rolí či organizace k identitě.
- U koncových systémů evidence uživatelských jmen ve vazbě na identitu (heslo pouze při vytvoření nového účtu).
- Vyhledávání a filtrování podle libovolného (i uživatelsky definovaného) atributu.
- Při vytvoření nového uživatelského účtu bude z bezpečnostních důvodů tento účet bez přiřazení rolí do doby změny úvodního hesla v AD (IdM nepřiřadí aplikační role dřív, než si uživatel změní úvodní heslo).

3.17.1.1 Oddělení komunit

Nabízené řešení musí podporovat oddělené komunity uživatelů. Řešení musí nabízet možnost nastavit tato omezení:

- Konfigurovat přístupová práva určená pro jednu komunitu tak, že nelze přiřadit identitám v jiné komunitě koncové systémy komunity původní.
- Do organizační struktury určené jedné komunitě nelze přiřadit identity z jiné komunity.
- Delegovat správu konkrétní komunity jinému administrátorovi
- Delegovat správu konkrétní organizační struktury jinému administrátorovi

3.17.1.2 Koncoví uživatelé

Nabízené řešení musí podporovat minimálně:

- Přehled přiřazených koncových systémů
- Přehled přiřazených oprávnění (aplikačních rolí) na koncových systémech (pokud je nakonfigurováno)
- Přehled přiřazení do org. struktury
- Schvalování či zamítnutí vznesených požadavků
- Spouštění reportů

3.17.1.3 Definice rolí v IdM

Níže je uveden minimální seznam rolí, které musí být podporovány v rámci IdM nástroje.

- **Administrátor IdM** - Zasahuje do poloautomatických procesů, řeší výjimečné stavy, kontroluje reporting a flow identit, plně správuje IdM. Může delegovat svá oprávnění a přidělovat oprávnění s granularitou až na jednotlivé funkce a objekty.
- **Delegovaný administrátor, Delegovaný správce** - Má administrátorská práva nad zvolenými komunitami, organizační strukturou, koncovými systémy, nad skupinami uživatelů nebo obecně nad definovanými objekty IdM. Účelem je umožnit delegovanému administrátorovi správu nad uživateli patřícími do samostatného podřízeného celku (ať už z pohledu interního, tak externího - například dodavatelské účty).
- **Tvůrce business rolí -** Má všechna nezbytná práva pro tvorbu a úpravu business rolí v IdM. Může do nich zařazovat jiné business role, aplikační role a/nebo koncové systémy.

- **Přidělovatel rolí -** Má všechna nezbytná práva pro přidělování business rolí a aplikačních rolí v IdM. Může identitám v IdM přidělovat business role, aplikační role a/nebo koncové systémy.
- **Správce koncového systému** - Má všechna nezbytná práva pro úpravu definic KS v IdM a jejich aplikačních rolí.
- **Běžný uživatel** - Běžný uživatel, který má práva prohlížet informace o své identitě a přidělených prostředcích v IdM.

3.17.2 Organizační struktura

Nabízené řešení musí podporovat:

- Administrační webové rozhraní pro správu stromové struktury
- Správu skrze integrační vrstvu
- Možnost vytváření libovolného počtu stromů organizačních struktur
- Možnost vytváření nezávislých entit (pracovní pozice, funkční místa) ve stromě
- Možnost definovat atributy entit ve stromě
- Možnost přiřazovat entitám ve stromě jiné objekty, minimálně uživatele, role, organizace z jiných stromů, účty v koncových systémech
- Možnost vizualizace entit pomocí stromové struktury
- Entity ve stromě přiřazovat k libovolnému objektu, minimálně k roli a k identitě
- Identita nebo role může být přiřazena ve více entitách stromu zároveň
- Identita nebo role může být přiřazena ve více stromech zároveň
- Identita může mít různé role v různých strukturách (nadřízený v jedné organizační struktuře může být v jiné struktuře podřízený apod.)
- Možnost nastavit časové období od-do pro přiřazení identity do stromové struktury; pokud časové období uplyne nebo ještě nenastalo, nesmí se přiřazení identity do stromu uplatnit

3.17.3 Business role

Nabízené řešení musí podporovat:

- Administrační webové rozhraní pro správu business rolí.
- Správu skrze integrační vrstvu
- Evidenci business rolí, včetně popisných atributů.
- Business role musí být možné hierarchicky skládat
- Vazbu business rolí na uživatele obsaženého v jakékoliv komunitě či organizační struktuře, označující garanta business role. Tato vazba může být v kardinalitě 1:N ve smyslu hlavní garant, zástupce apod. Tato vazba je rozhodující ve workflow při přiřazování přístupů apod.
- Vazbu na koncové systémy přiřazené do business role v kardinalitě 1:N.
- Vazbu na konkrétní identitu (uživatele) v kardinalitě 1:N a možnost nastavení platnosti přiřazení od-do.
- Možnost nastavení platnosti business role od-do, pokud časové období uplyne nebo ještě nenastalo, nesmí se přiřazení business role uplatnit.
- Při vytváření nových business rolí upozornit na duplicitní definice rolí s jejich výčtem.
- Do business rolí přiřazovat jiné business role, aplikační role, resp. koncové systémy
- Podporovat definici pravidel business rolí včetně možnosti použít regulární výrazy.
- Správu effective rights v rámci tvorby nových business rolí.
- Možnost širšího managementu business rolí.
- Při tvorbě nových business rolí je vyžadována podpora schvalovacích procesů obsahující všechny garanty jednotlivých koncových systémů.
- Delegování správy business rolí.
- Podporu pro vyhledávání duplicitních business rolí ve smyslu duplicity v přiřazení oprávnění do koncových systémů a aplikačních rolí.

3.17.4 Koncové systémy

Nabízené řešení musí podporovat:

- Administrační webové rozhraní pro správu koncových systému.
- Správu přes integrační vrstvu.
- Evidenci koncových systémů, včetně popisných atributů jejich funkce, umístění apod.
- Vazbu koncových systémů na uživatele obsaženého v jakékoliv komunitě, či organizační struktuře, označující garanta koncového systému. Tato vazba může být v kardinalitě 1:N ve smyslu hlavní garant, zástupce apod. Tato vazba je rozhodující ve workflow při vytváření business rolí, přiřazování přístupů apod.
- Vazbu na aplikační role přiřazené ke koncovému systému v kardinalitě 1:N.
- Vazbu na administrátora koncového systému, kterého může představovat uživatel obsažený v jakékoliv komunitě, či organizační struktuře. Tato vazba může být v kardinalitě 1:N ve smyslu hlavní administrátor, zástupce apod.
- Možnost nastavení stavu správy koncového systému na povoleno, či blokováno. Toto nastavení má přímý dopad na řízení přístupů ke koncovému systému.
- Delegování správy koncových systémů

3.17.5 Aplikační role

Nabízené řešení musí podporovat:

- Administrační webové rozhraní pro správu rolí (soubor oprávnění)
- Správu skrze integrační vrstvu.
- Roli je možné přiřazovat koncovým systémům.
- Možnost nastavení platnosti aplikační role s dopadem na řízení přístupů ke koncovému systému.
- Možnost nastavit další atributy přiřazení (např. dle lokality identity)
- Možnost dynamického výpočtu u schvalovací role
- Role musí být možné hierarchicky skládat
- Možnost systému nastavit pravidla pro vzájemně se vylučující role (tzv. SoD), musí umět reportovat a notifikovat konfliktní práva
- Ochranu systému v případě pokusu o přiřazení konfliktní role - pokud dojde k pokusu o přiřazení role identitě, která již má jinou konfliktní roli, musí systém konflikt oznámit a vlastní přiřazení neprovede
- Možnost recertifikace rolí - opakované spouštění schvalování

4 Připojení koncových systémů a propagace unikátní identity

Zadavatel v rámci implementace požaduje připojení koncových systémů a propagaci unikátní identity. Připojení koncových systémů a řízení identit lze rozdělit do několika následujících bodů:

4.1 Plně automatické připojení

Plně automatické připojení ke koncovému systému splňuje tyto požadavky:

- IdM přebírá informace o identitách z autoritativního zdroje a vytváří uživatele v IdM. Na základě rozlišovacích atributů uživatele slučuje do jedné unikátní identity, kterou nadále takto propaguje.
- Na základě rozlišovacích atributů ji přiřazuje do komunit, organizačních struktur.

- Na základě rozlišovacích atributů ji přiřazuje do business rolí. Business role lze přiřazovat i ručně administrátorem, který má potřebná oprávnění.
- Na základě business rolí jsou unikátní identitě přiřazeny koncové systémy a aplikační role v koncových systémech.
- IdM automaticky skrze konektory provádí akce spojené se správou autorizace v koncových systémech.
- IdM automaticky skrze konektory provádí pravidelnou kontrolu stavu účtů na koncových systémech s autoritativním vypořádáním nesouladu a eskalací bezpečnostního incidentu skrze workflow a notifikace.

4.2 Read-only připojení

Read-only připojení ke koncovému systému splňuje tyto požadavky:

- IdM přebírá informace o identitách z autoritativního zdroje a vytváří uživatele v IdM. Na základě rozlišovacích atributů uživatele slučuje do jedné unikátní identity, kterou nadále takto propaguje.
- Na základě rozlišovacích atributů ji přiřazuje do komunit, organizačních struktur.
- Na základě rozlišovacích atributů ji přiřazuje do business rolí. Business role lze přiřazovat i ručně administrátorem, který má potřebná oprávnění.
- Na základě business rolí jsou unikátní identitě přiřazeny koncové systémy a aplikační role v koncových systémech.
- IdM neprovádí automaticky správu autorizace v koncových systémech, ale pomocí notifikace informuje administrátory koncových systémů o přidělení úkolu.
- IdM automaticky skrze konektory provádí pravidelnou kontrola stavu účtů na koncových systémech s autoritativním vypořádáním nesouladu a eskalací bezpečnostního incidentu skrze workflow.

4.3 Offline připojení

Offline připojení ke koncovému systému splňuje tyto požadavky:

- IdM přebírá informace o identitách z autoritativního zdroje a vytváří uživatele v IdM. Na základě rozlišovacích atributů uživatele slučuje do jedné unikátní identity, kterou nadále takto propaguje.
- Na základě rozlišovacích atributů ji přiřazuje do komunit, organizačních struktur.
- Na základě rozlišovacích atributů ji přiřazuje do business rolí. Business role lze přiřazovat i ručně administrátorem, který má potřebná oprávnění.
- Na základě business rolí jsou unikátní identitě přiřazeny koncové systémy a aplikační role v koncových systémech.
- IdM neprovádí automaticky správu autorizace v koncových systémech, ale pomocí notifikace informuje administrátory koncových systémů o přidělení úkolu.
- IdM neprovádí automaticky kontrolu stavu účtů na koncových systémech, ale pomocí webového rozhraní a v rámci workflow procesu umožňuje administrátorovi potvrzení splnění přiděleného úkolu.

4.4 Ruční řízení a připojení

Ruční řízení a připojení ke koncovému systému splňuje tyto požadavky:

- Administrátor s patřičným oprávněním vytváří uživatele v IdM. Na základě rozlišovacích atributů uživatele IdM kontroluje, zda nedochází k duplicitním záznamům a vytváří unikátní identitu, kterou nadále takto propaguje.

- Administrátor s patřičným oprávněním přiřazuje identitu do komunit, organizačních struktur a IdM kontroluje, zda nedochází k porušování pravidel spojených s komunitami a organizačními strukturami.
- Administrátor s patřičným oprávněním přiřazuje identitu do business rolí a IdM provádí kontrolu, zda nedochází ke konfliktním přiřazením oprávnění.
- Administrátor nemůže přiřadit identitě přímo koncový systém a aplikační roli.
- Ke správě autorizace v koncových systémech je možno využít všechny výše popsané metody správy, jedná se tedy o:
    - Plně automatickou správu
    - Read-only správu
    - Offline správu

4.5 Eskalace chyb a neplnění úkolů při správě autorizace v koncových systémech

Zadavatel požaduje konfigurovatelnou správu a eskalaci chyb při správě autorizace v koncových systémech. IdM tak musí umožňovat nastavit tyto parametry:

- Pro plně automatické připojení
    - Počet opakování pokusů spojení s autoritativním zdrojem v určitém časovém intervalu.
    - Po vyčerpání všech určených neúspěšných pokusů vyvolání workflow s notifikací na administrátora IdM
    - Počet opakování pokusů spojení s koncovým systémem skrze konektory v určitém časovém intervalu.
    - Po vyčerpání všech určených neúspěšných pokusů vyvolání workflow s notifikací na garanta koncového systému a administrátora IdM.
    - V rámci notifikace přenos chybové zprávy obdržené při neúspěšném spojení a identifikaci akce, při které došlo k chybě.
- Pro Read-only připojení
    - Počet opakování pokusů spojení s autoritativním zdrojem v určitém časovém intervalu.
    - Po vyčerpání všech určených neúspěšných pokusů vyvolání workflow s notifikací na administrátora IdM
    - Počet opakování pokusů spojení s koncovým systémem skrze konektory v určitém časovém intervalu.
    - Po vyčerpání všech určených neúspěšných pokusů vyvolání workflow s notifikací na garanta koncového systému a administrátora IdM.
    - V rámci notifikace přenos chybové zprávy obdržené při neúspěšném spojení a identifikaci akce, při které došlo k chybě.
- Pro Offline připojení
    - Počet opakování pokusů spojení s autoritativním zdrojem v určitém časovém intervalu.
    - Po vyčerpání všech určených neúspěšných pokusů vyvolání workflow s notifikací na administrátora IdM
    - V rámci notifikace přenos chybové zprávy obdržené při neúspěšném spojení a identifikace akce, při které došlo k chybě.
    - Časový interval pro splnění úkolu, notifikovaného administrátorovi.
    - Počty a intervaly pro upozornění administrátorovi o nesplnění přiděleného úkolu, před vypršením termínu splnění úkolu.
    - Při nepotvrzení splnění úkolu a vypršení termínu splnění úkolu vyvolání workflow s notifikací na garanta koncového systému a administrátora IdM.

- Pro Ruční řízení a připojení dle typu:
    - Plně automatickou správu viz výše.
    - Read-only správu viz výše.
    - Offline správu viz výše.

4.6 Operace spojené s připojením do koncových systémů

Níže je uveden rozsah operací, které musí podporovat IdM ve vztahu k rozhraní koncového systému (KS) tak, aby mohly být řízeny uživatelské účty uložené v tomto koncovém systému. Je uveden maximální rozsah operací, které ale rozhraní koncového systému nemusí podporovat. Jedná se například o zplatnění/zneplatnění účtu, změna hesla apod. Konkrétní implementaci operací rozhraní koncového systému a jejich význam pro data určuje vlastník koncového systému. Jakékoliv operace nesmí být IdM vyžadovány ke své funkčnosti, jedná se o volitelnou možnost. U každého koncového systému bude v rámci analýzy rozhodnuto, zda a v jakém rozsahu budou operace s rolemi mezi IdM a koncovým systémem využity.

4.6.1 Vytvoření účtu

Systém IdM skrze konektor vytváří v koncovém systému nového uživatele a propaguje jeho unikátnost pomocí jedinečného identifikátoru. Dle typu uživatele a přiřazených business rolí vytváří konkrétní přístupy. Vytvoření nového uživatele v koncovém systému tak může být například metodou „Create_user“, která musí splňovat tyto podmínky:

- IdM přenáší do koncového systému unikátní identifikátor.
- IdM vytváří dle firemních pravidel a politik nové heslo, které pokud je to vyžadováno, přenáší do koncového systému.
- IdM vytváří dle firemních pravidel a politik nové uživatelské jméno, které přenáší do koncového systému.
- IdM přenáší do koncového systému všechny požadované atributy, jako jsou například: jméno, příjmení, uživatelské jméno apod.
- IdM vytváří dle firemních pravidel a politik novou emailovou adresu, kterou přenáší do koncového systému.
- IdM notifikuje uživatele o vytvoření uživatelského jména a hesla a tyto informace mu zasílá na email, nebo pomocí sms brány na mobilní telefon. V případě, že uživatel nemá ani email, ani telefon, nebo v jiném vhodném případě tyto informace zasílá přímému nadřízenému, který je identifikován skrze organizační strukturu.
- V případě, že se jedná o uživatele, který má mít účet v AD, IdM nepřiřazuje jakékoliv další business role a tím pádem přístupy do dalších koncových systémů, dokud si uživatel nezmění přidělené heslo. IdM tak kontroluje, zda bylo prvotní heslo změněno, a pokud ano, pokračuje v dalším zpracování business rolí.
- Po přiřazení všech business rolí resp. přístupů do koncových systémů, provádí IdM okamžitou kontrolu přiřazených oprávnění a v případě nesouladu provádí notifikace na administrátora IdM a garanta koncového systému, u kterého došlo k nesouladu.

4.6.2 Aktivace a deaktivace účtu

Systém IdM skrze konektor a pokud to koncový systém umožňuje, provádí aktivaci a deaktivaci konkrétního uživatele. K identifikaci používá přidělený unikátní identifikátor. Jedná se tak například o metody enable_user a disable_user, kde základní parametry jsou:

- Enable_user (unikátní identita, status)
- Disable_user (unikátní identita, status)

Výsledná podoba tak například může být:
- Enable_user (0000-00000000-000000000000000000000000000000001, -1)
- Disable_user (0000-00000000-000000000000000000000000000000001, 0)

4.6.3 Čtení informací o účtu

Systém IdM skrze konektor a pokud to koncový systém umožňuje, čte informace o zavedeném uživateli. Jedná se tak především o atributy, jako jsou například:
- Jméno
- Příjmení
- Uživatelské jméno
- Jiné atributy informačního charakteru, které se u jednotlivých koncových systémů mohou různit.

V žádném případě nelze touto metodou přenášet heslo uložené v koncovém systému, pokud koncový systém heslo ukládá.
Pro identifikaci účtu se výhradně používá jeho unikátní identifikátor.

4.6.4 Update informací účtu

Systém IdM skrze konektor umožňuje aktualizovat zadané informace v koncových systémech. Jedná se o shodné atributy, které jsou přenášeny v rámci metody vytváření účtu, a tato metoda může obsahovat i změnu hesla.
Pro identifikaci účtu se výhradně používá jeho unikátní identifikátor.

4.6.5 Přiřazení aplikačních rolí

Systém IdM skrze konektor umožňuje přiřazení aplikačních rolí unikátní identitě. Jedná se o metodu, skrze kterou se předává ID unikátní identity a unikátní ID aplikační role. Na základě volání této metody koncový systém přiřazuje aplikační roli unikátní identitě a vrací odpověď o úspěšném, či neúspěšném provedení operace.

4.6.6 Odebrání aplikačních rolí

Systém IdM skrze konektor umožňuje odebrání aplikačních rolí unikátní identitě. Jedná se o metodu, skrze kterou se předává ID unikátní identity a unikátní ID aplikační role. Na základě volání této metody koncový systém odebírá aplikační roli unikátní identitě a vrací odpověď o úspěšném, či neúspěšném provedení operace.

4.6.7 Odebrání všech aplikačních rolí

Systém IdM skrze konektor umožňuje odebrání všech aplikačních rolí unikátní identitě. Jedná se o metodu, skrze kterou se předává ID unikátní identity. Na základě volání této metody koncový systém odebírá všechny aplikační role unikátní identitě a vrací odpověď o úspěšném, či neúspěšném provedení operace.

4.6.8 Seznam přiřazených aplikačních rolí

Systém IdM skrze konektor umožňuje čtení informací o všech přiřazených aplikačních rolích unikátní identitě. Jedná se o metodu, skrze kterou se předává ID unikátní identity. Na základě volání této metody koncový systém vrací seznam všech přiřazených aplikačních rolích unikátní identitě a vrací odpověď o úspěšném, či neúspěšném provedení operace.

4.6.9 Seznam aplikačních rolí

Systém IdM skrze konektor umožňuje čtení informací o aplikačních rolích v koncovém systému. Na základě volání této metody koncový systém vrací seznam aplikačních rolí v koncovém systému.

4.6.10 Seznam uživatelů v koncovém systému

Systém IdM skrze konektor umožňuje čtení informací o všech uživatelích (unikátních identitách), které jsou v koncovém systému zavedeny. Na základě volání této metody koncový systém vrací seznam všech unikátních identit, které jsou v systému zavedeny, spolu se všemi dostupnými atributy. Seznam těchto atributů se může lišit v závislosti na konkrétním koncovém systému.

4.7 Požadavky na dokumentaci

Všechna dokumentace musí být verzována, opatřena seznamem autorů, přehledem změn jednotlivých verzí a musí být obsahově úplná pro tu část systému, kterou popisuje. Dokumentace musí být napsána v českém jazyce a před finálním odevzdáním zpracovaná jazykovým korektorem. Požadujeme jako součást dodávky následující dokumentaci:

4.7.1 Dokumentace jádra systému

Dokumentace jádra systému, jeho funkcí, služeb a rozhraní. Dokumentace bude obsahovat kompletní popis architektury jádra systému, výčet a podrobný popis všech jeho funkcí, přehled a popis služeb, které jádro poskytuje dalším komponentám systému, modulům a knihovnám.

4.7.2 Dokumentace pro vývoj nových konektorů

Dokumentace pro vývoj nových konektorů bude obsahovat kompletní popis tvorby nových konektorů, včetně vazeb na systém IdM tak, aby nově vzniklý konektor bylo možné zapojit do všech již existujících procesů v IdM.

4.7.3 Příručka administrátora IdM

Příručka bude distribuována úzké skupině uživatelů, správců systému. Musí obsahovat kompletní popis všech funkcí pro práci s administrací IdM. Příručka bude využívána jako materiál pro školení nových administrátorů. Příručka musí obsahovat solidně zpracovaný popis kroků pro jednotlivé implementované funkce s vhodným doprovodným obrazovým materiálem ve formě výřezů obrazovek.

4.7.4 Uživatelská příručka

Příručka bude distribuována uživatelům. Musí obsahovat kompletní popis všech uživatelských funkcí pro práci s IdM. Příručka bude využívána jako základní materiál pro školení nových uživatelů. Příručka musí obsahovat solidně zpracovaný popis kroků pro jednotlivé implementované funkce s vhodným doprovodným obrazovým materiálem ve formě výřezů obrazovek.

5 Další požadavky

5.1 GDPR

Výsledné dílo musí splňovat požadavky na GDPR, obecné nařízení o ochraně osobních údajů (angl. General Data Protection Regulation), novou legislativu EU, která výrazně zvyšuje ochranu osobních dat.

Ing. Radoslav Remiš

Digitálně podepsal Ing. Radoslav Remiš
DN: c=CZ, o=Správa železniční dopravní cesty, státní organizace, ou=Generální ředitelství, cn=Ing. Radoslav Remiš, email=Remis@szdc.cz, serialNumber=MPSV-1641488904
Datum: 2017.11.04 11:38:59 +01'00'