Integrace aplikace do IDM

Příloha standardů a podmínek dodávek informačního systému VZP ČR

UPOZORNĚNÍ:

Tento dokument je zpracován Všeobecnou zdravotní pojišťovnou České republiky (dále též jen „VZP ČR“ nebo „VZP“). Všeobecná zdravotní pojišťovna České republiky jej uveřejňuje v rámci zadávací dokumentace jí zadávaných veřejných zakázek. Tento dokument umožňuje utvořit si představu o standardech informační architektury ICT VZP ČR. Účelem jeho uveřejnění je poskytnout informace nezbytné pro integraci dodávané komponenty se stávajícím informačním systémem v souladu se Standardy ICT- VZP- NIS.

Uveřejněním tohoto dokumentu není dotčena právní odpovědnost spojená s jeho zneužitím.

V tomto dokumentu bylo použito názvů subjektů a názvů produktů, které mohou být chráněny příslušnými právními předpisy.

Otevřením tohoto dokumentu berete výše uvedené skutečnosti na vědomí.

Obsah

Seznam obrázků

Historie dokumentu

Verze	Datum	Autor	Popis
1.06	17.10.2017	ÚICT VZP ČR	Vytvoření dokumentu

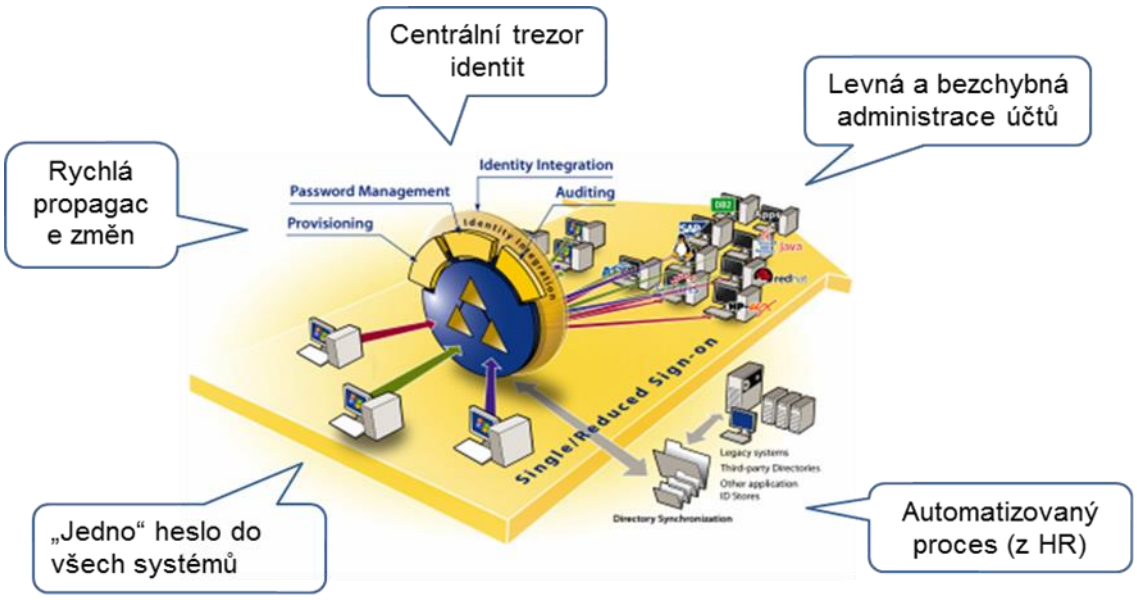
1. Úvod

Dokument obsahuje sadu standardů pro vybudování integračních vazeb nově dodávaných komponent informačního systému se stávajícími komponentami prostřednictvím integrační platformy v souladu se Standardy ICT VZP ČR. Vytvořené standardy jsou základem pro další rozšiřování systému zaváděním nových komponent a to jak „standardních“, tak i vytvářených dle specifických požadavků VZP ČR. Tento dokument je součástí výše uvedených Standardů ICT.

V případě specifikace rozšíření informačního systému zaváděním nových komponent ve smlouvě s dodavatelem, má specifikace uváděná v této smlouvě přednost před Standardy.

2. Integrace aplikace

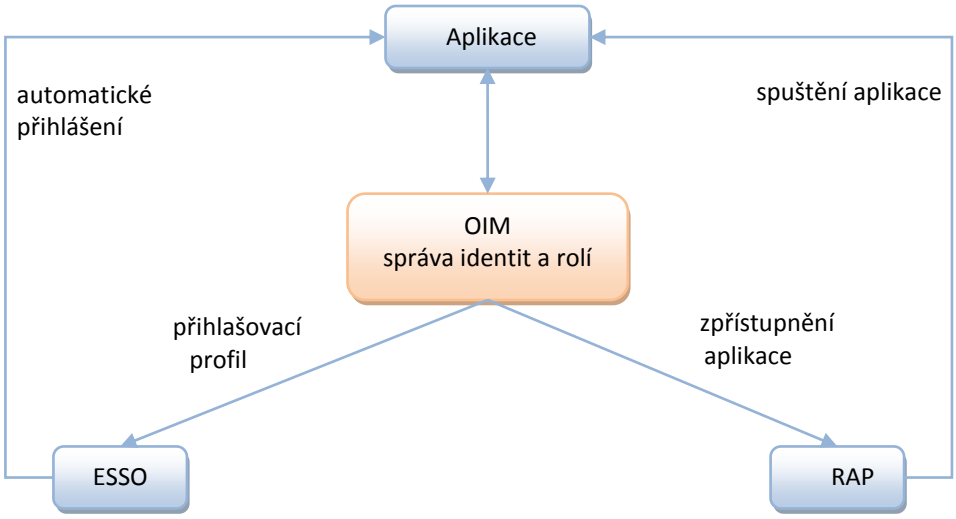
Dokument si klade za cíl seznámení s principy integrace aplikace do řešení IDM (Identity Management). Detailní informace o IDM řešení lze získat z dokumentace, která je uvedena v kapitole Refernce.



Co nabízí integrace aplikace s řešením IDM?

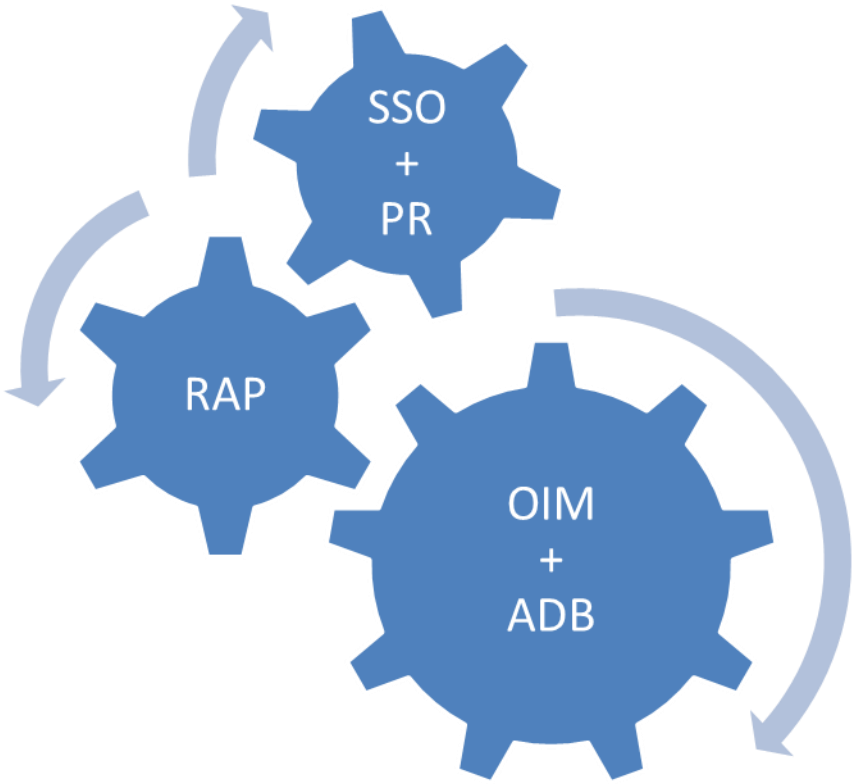
- Centrální správa uživatelských účtů a rolí pomocí Oracle Identity Manager (viz kapitola 2.1)
    - Správa identit uživatelů (jméno / heslo)
    - Správa oprávnění uživatelů pro přístup do aplikace (role, práva)
- Metodicky řešená podpora řízení oprávnění na základě rolí resp. hierarchie rolí
- Externí, konsolidované repozitory autentizačních a autorizačních dat s podporou specifik VZP – komponenta ADB (Autorizační Databáze)
- Řízené zpřístupnění aplikace (odkazu) cílovým uživatelům pomocí Rozcestníku aplikací (viz kapitola 2.6)

- Podporu Single Sign On (SSO) - automatické přihlášení cílových uživatelů do aplikace pomocí produktu Oracle Enterprise Single Sign-On Logon Manager (viz kapitola 2.5). Přihlašovací údaje do integrovaných aplikací pak spravuje OIM a vlastní přihlašování provádí Oracle eSSO LM.



Další kapitoly jsou členěny dle nabízených funkčností IDM řešení:

- Volba formy integrace s IDM (OIM)
- OIM – správa identit
- Řízení oprávnění na základě rolí
- ADB - externí, konsolidované úložiště uživatelských oprávnění
- eSSO – automatické přihlášení uživatele
- RAP – rozcestník aplikací



Obrázek 1 - Přehled IDM komponent

2.1 Varianty integrace s IDM/OIM

Aby bylo možné připojit aplikaci OIM a vyžívat tak všech možností z toho plynoucích, je nejdříve nutné zvolit způsob integrace.

Způsob se volí dle druhu úložiště dat o uživatelích a jejich rolích:

1. **Externí úložiště dat** – jedná se o preferovaný způsob integrace. Aplikace využívá externí úložiště uživatelů aplikace a jejich rolí. Úložištěm dat je Autorizační databáze ADB, která je již s OIM integrována a zajišťuje tedy plnou spolupráci s OIM. Z pohledu OIM se jedná o nepřímou integraci.
2. **Vlastní úložiště dat** – pokud aplikace buď neumožňuje použít externí úložiště dat, nebo je tento způsob z nějakého důvodu nevhodný, lze nadále využívat vlastní úložiště dat provést takzvanou přímou integraci s OIM.

2.1.1 Externí úložiště uživatelských dat (integrace s ADB nebo AD)

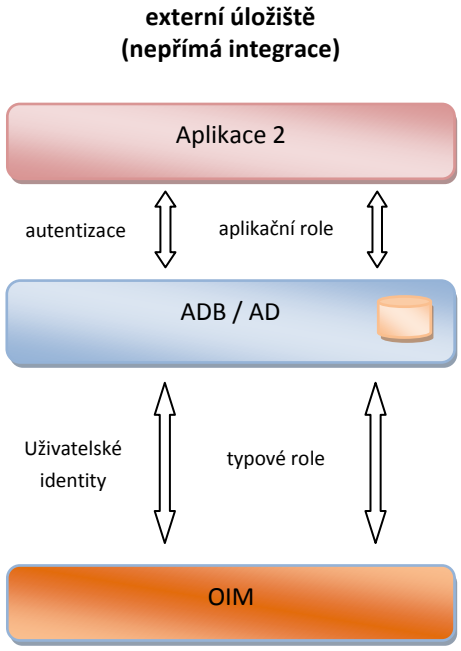
V rámci nepřímé integrace je třeba připravit aplikaci pro oddělení svého úložiště autentizačních a autorizačních dat a jeho nahrazení autorizační databází ADB pomocí ADBLib knihovny (podrobné informace viz dokumentace ADB API uvedená v kapitole Reference. Podle typu aplikace se zvolí formát dodané knihovny ADB.

- Knihovna „jar“ – aplikace využívající technologii java
- Knihovna „pll“ – aplikace vytvořené v technologii Oracle Forms

Dále je třeba připravit seznam aplikačních rolí a jmenování zástupce, který se bude účastnit jednání o mapování typových a business rolích.

Pro vývojáře je k dispozici:

- Dokumentace ADB knihovny
- Knihovna ADB pro vývoj (verze XML) a integrační testy v TVS (verze WS)
- Podpora knihovny ADB ze strany dodavatele ADB



Obrázek 2 – Integrace aplikace - externí úložiště

2.1.2 Vlastní úložiště uživatelských dat

V případě, že aplikace preferuje použití vlastního úložiště dat, je nutné implementovat přímou integraci se systémem OIM – Oracle Identity Manager. Integrační rozhraní dovoluje obousměrnou komunikaci, v terminologií OIM / IDM se jedná o tzv.:

- Provisioning – poskytování údajů z IDM do integrované aplikace, tj. směr komunikace je z OIM do integrované aplikace
- Reconciliation – sjednocení údajů v IDM dle stavu dat v integrované aplikaci, tj. směr komunikace je z integrované aplikace do OIM

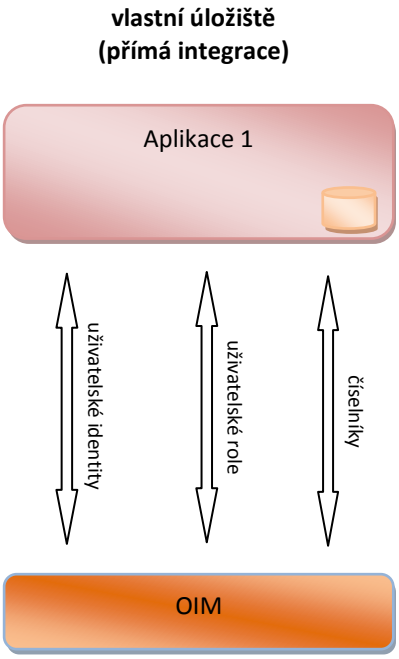
Pro implementaci integrace je nutné provést následující:

- Implementovat PL/SQL rozhraní na straně integrované aplikace (viz příloha), které slouží pro účely „provisioningu“

- Připravit tabulky/view na straně integrované aplikace pro účely „reconciliation“. Tabulky obsahují následující typy dat:
    - tabulka uživatelů (identit)
    - tabulka rolí přiřazených k uživatelům
    - tabulky číselníky, mezi které například patří číselník rolí

Pro možnost inkrementální „rekonciliace“, tj. přenosu pouze části dat, u kterých nastala změna od poslední „rekonciliace“, je nutné, aby tabulky (view) obsahovaly sloupec s datem poslední aktualizace.

Pro integrační testy je nutné předat IDM týmu přihlašovací údaje k databázi, tj. IP adresa a port, verze DB, SID DB, username, heslo atd.



Obrázek 3 – Integrace aplikace - vlastní úložiště

2.1.2.1 Přenosu dat z aplikace do OIM

Pro umožnění přenosu z aplikace do OIM stačí v databázi definovat tabulku nebo view. Každá taková tabulka nebo view by měly obsahovat sloupec určující datum a čas poslední změny daného řádku. OIM se pak snadno do takového databázového objektu podívá a získá údaje o posledních provedených změnách.

Přenášená data:

- Uživatelské identity (například přihlašovací jméno, heslo, jméno, příjmení, telefon, …)
- Uživatelské typové role (například administrátor aplikace, evidence uživatelů, …)
- Číselníky (například seznam pracovišť, seznam skupin, …)

2.1.2.2 Přenos dat z OIM do aplikace

Pro zajištění funkcionality OIM vzhledem k uživatelům a jejich rolím v aplikaci, je definováno komunikační rozhraní PL/SQL API, které umožňuje základní operace s uživatelskými účty a jejich rolemi:

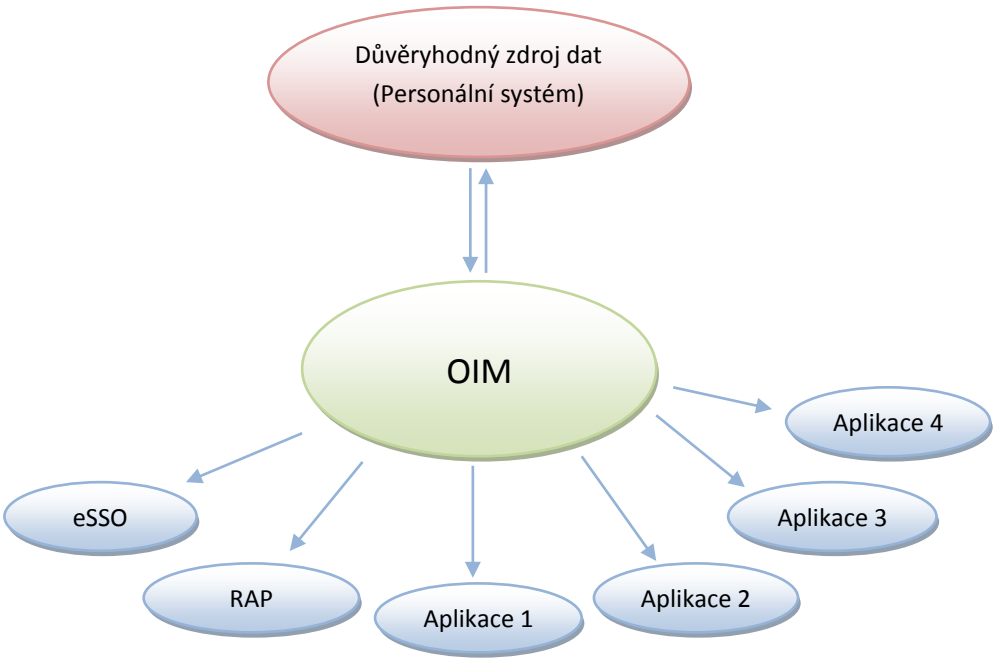
- **CreateUser** – Vložit uživatelský účet
- **UpdateUser** – Aktualizovat údaje o uživatelském účtu
- **LockUser** – Pozastavení uživatelského účtu
- **UnlockUser** – Obnovení uživatelského účtu
- **DeleteUser** – Smazání uživatelského účtu
- **ChangePassword** – Změna hesla uživatelského účtu
- **AddRole** – Přidání role
- **RemoveRole** – Odebrání role

Podrobnější informace o komunikačním rozhraní viz příloha PL/SQL API.

2.2 OIM

Oracle Identity Manager (OIM) zajišťuje centralizaci správy identit integrovaných aplikací a práv identit (rolí). Informace o uživateli jsou uložené na jednom místě a odtud automaticky propagovány do integrovaných aplikací (viz Obrázek 4 - Schéma správy identity pomocí OIM). Například pokud se uživatelka vdá a změní příjmení, je tato změna propagována do všech integrovaných aplikací. Zároveň OIM může z integrovaných aplikací získávat aktuální data (například změny v číselnících) a případně je propagovat dále.

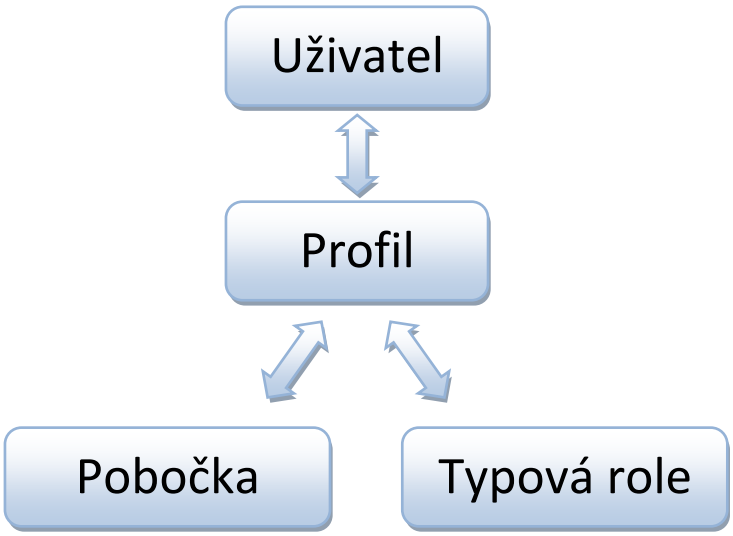
V rámci celé společnosti je tedy uživatel vždy zastoupen jednou identitou v OIM. Tato identita obsahuje všechny potřebné údaje o uživateli (v případě VZP jsou získávané z personálního systému VEMA). OIM řídí, do kterých aplikací má daná identita přístup a jaké má oprávnění (role) v aplikaci.



Obrázek 4 - Schéma správy identity pomocí OIM

2.3 ADB

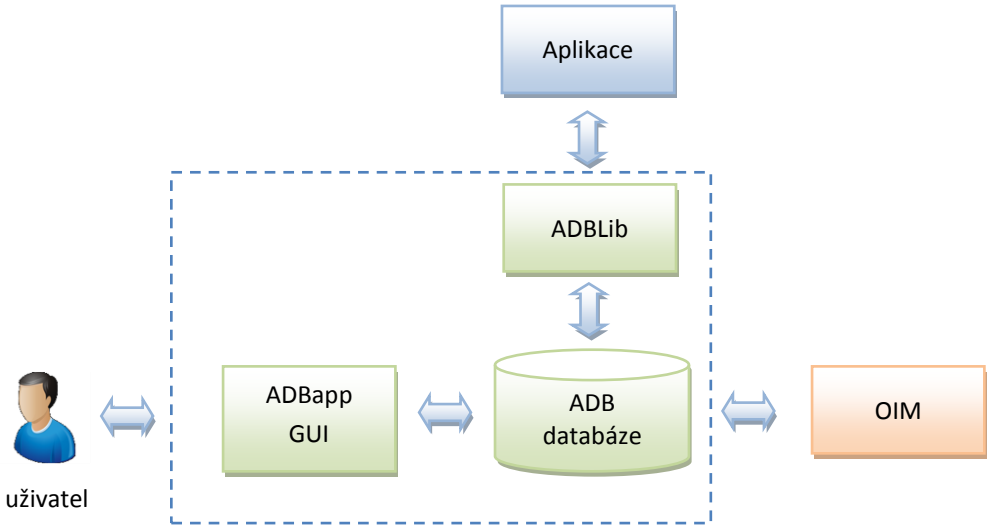
Autorizační databáze (ADB) je centrálním a konsolidovaným úložištěm dat určeným pro správu uživatelů a jejich rolí vzhledem k aplikacím. K vytvoření ADB vedly specifické požadavky v prostředí VZP. Každý uživatel ve VZP má přiřazeny své typové role (každá typová role může obsahovat jednu a více aplikačních rolí), které jsou ale zároveň vázány na konkrétní pracoviště. Vzhledem k velkému množství uživatelů, pracovišť a rolí tak vznikla ADB, která ukládá tyto údaje v jednoduchém relačním modelu (viz Obrázek 5 - Relační model ADB).



Obrázek 5 - Relační model ADB

Následující schéma zobrazuje komponentový pohled na ADB řešení. ADB data jsou přístupná 3 způsoby:

1. Uživatelským rozhraním (GUI), které dovoluje plnou kontrolu na ADB daty.
2. Aplikace využívající ADB jako externího úložiště – pomocí API (ADBLib) dovolují číst data z ADB.
3. Řídící IDM systém (OIM) má plnou kontrolu nad ADB daty. Přístup je realizován skrze dedikované API pro OIM.

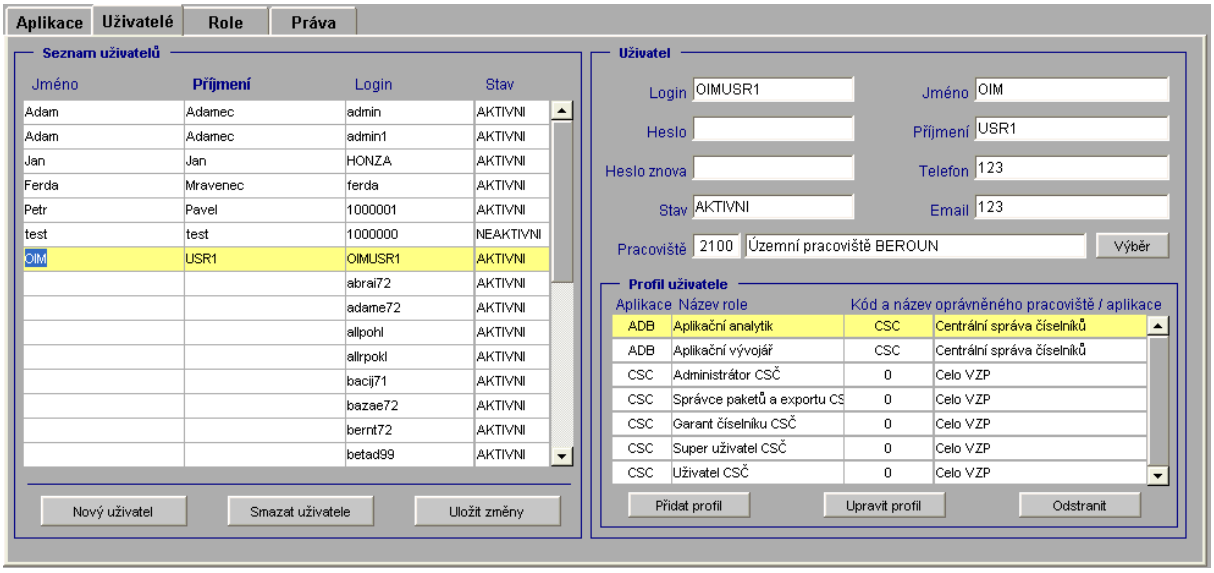


Obrázek 6 - Řešení ADB

2.3.1 Výhody použití ADB

Externí úložiště uživatelských dat v podobě ADB má následující výhody:

- Již vytvořená aplikace pro kompletní správu údajů, vytvořená v technologii Oracle Forms. Odpadá tedy nutnost vytváření vlastní správy uživatelů a jejich oprávnění v aplikaci.
- K dispozici jsou různé verze knihoven s jednotným rozhraním pro komunikaci s ADB. Stačí tedy odladit aplikaci, například s použitím XML verze knihovny, bez potřeby mít přístup k celé ADB, a po dokončení úprav jen vyměnit knihovnu a připojení s ADB bude fungovat.
    - Knihovna určená primárně pro vývoj, která umožňuje používat XML zdroj dat.
    - Knihovna určená pro komunikace s ADB prostřednictvím webových služeb.
    - V dohledné době bude k dispozici verze knihovny pro komunikaci s ADB prostřednictvím LDAP protokolu.
- Možnost zjednodušení práce s aplikačními rolemi pomocí typových rolí, které sdružují více aplikačních rolí dohromady, podle typu práce s aplikací. Typové role se pak snadněji u uživatelů spravují a mapují na business role.
- Aplikace nepotřebuje provádět žádnou správu svých uživatelů. To obstará ADB. Aplikace se pouze ptá (nepotřebuje provádět žádný zápis do oprávnění):
    - Existuje přihlašovaný uživatel?
    - Je heslo přihlašovaného uživatele správné?
    - Jaká oprávnění (aplikační role) má daný uživatel v aplikaci?
- Jednotný / konsolidovaný systém evidence uživatelů a oprávnění.
- Připravené GUI pro práci s ADB daty.



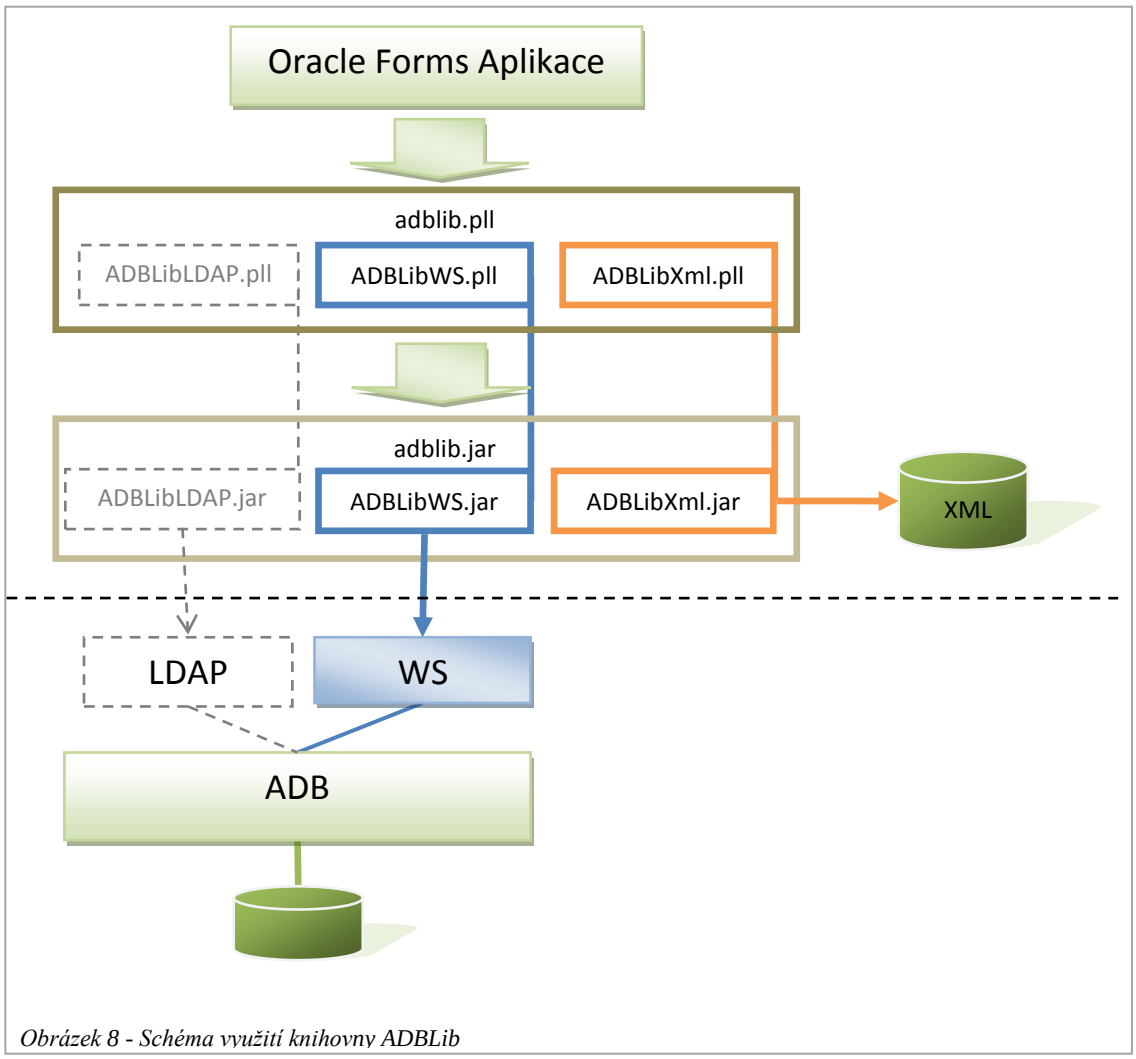
Obrázek 7 - Ukázka GUI ADB aplikace - seznam uživatelů

2.3.2 Knihovna

Knihovna ADBLib slouží ke komunikaci s autorizační databází ADB. V současné době jsou k dispozici 2 verze této knihovny (třetí verze, určená pro komunikaci prostřednictvím LDAP protokolu, bude dostupná později):

- Verze XML určená hlavně pro usnadnění vývoje, protože pro úpravu stávající či vývoj nové Oracle Forms aplikace není potřeba mít k dispozici celý systém autorizační databáze, ale stačí vytvořit si pouze data pomocí XML souborů.
- Verze WS, která v současné představuje dočasné řešení komunikace s vlastní Autorizační databází, než bude k dispozici rozhraní LDAP

Jednotné rozhraní knihovny ADBLib umožňuje vývoj Oracle Forms aplikace například na XML verzi, její odladění a poté prostou výměnou dvou souborů na aplikačním serveru Oracle Forms lze docílit výměnu verze ADBLib knihovny.



Obrázek 8 - Schéma využití knihovny ADBLib

2.3.3 Role

ADB nabízí možnost vytvoření typových rolí, které obsahují více aplikačních rolí. Více informací o rolích je k dispozici v následující kapitole.

2.3.4 Lokality

Typové role jsou vázané na pracoviště – lokality. Daná typová role uživatele může být na různých lokalitách a zároveň může mít uživatel v jedné lokalitě mít více typových rolí.

2.4 Role

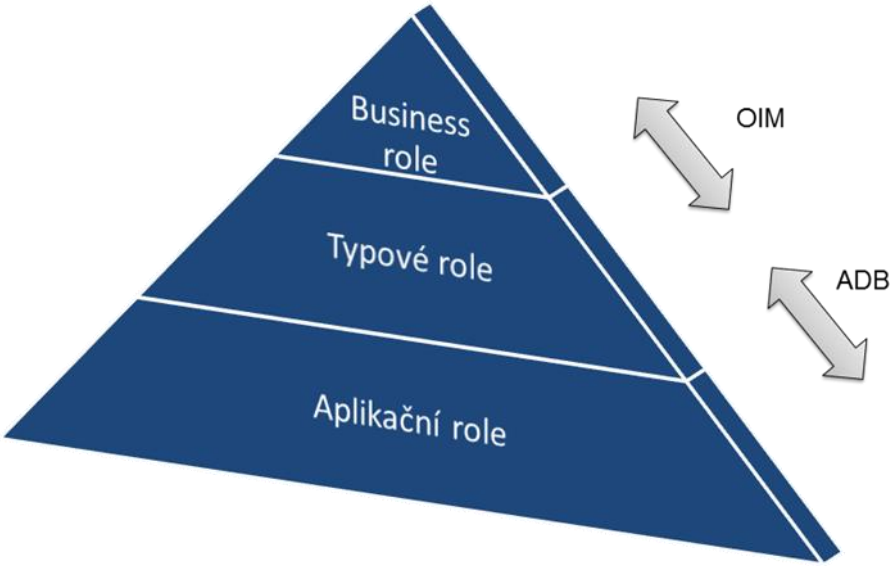
Role představují realizaci řízení oprávnění v aplikacích. Přiřazení role uživateli může být založeno na základě různých atributů uživatele: pracovního zařazení, pracoviště, dočasné potřeby, atd… Cílem je umožnit uživateli přístup pouze k informacím, ke kterým přístup má mít a umožnit mu s informacemi pracovat je tak, jak mu přísluší. K realizaci řízení bezpečnosti slouží 3 úrovně rolí.

Význam jednotlivých úrovní řízení bezpečnosti:

- AR - Aplikační role představuje zabezpečení na úrovni aplikace. Povoluje či zabraňuje tak vykonání konkrétní funkce aplikace. V případě vlastního úložiště dat se o správu aplikačních rolí stará sama

aplikaci. V případě použití externího úložiště ADB se o aplikační role stará ADB a na požádání aplikační role předává aplikaci.

- TR - Typové role představují seskupení oprávnění do logických (nedělitelných) celků. Umožňují usnadnění správy oprávnění v rámci jedné aplikace. K mapování aplikačních rolí na typové role dochází buď v ADB, tedy v případě využití externího úložiště dat anebo přímo v aplikaci, pokud to aplikace podporuje. V případě, že aplikace je aplikace integrována přímo, typové role nepodporuje a aplikačních rolí je málo, je možné prohlásit aplikační role za typové a provést tedy přímé mapování business rolí na role typové.
- BR - Business role seskupují typové role (tedy jednu a více aplikačních rolí) napříč více aplikacemi a odpovídají tak přiděleným zodpovědnostem (rolím) v rámci podnikových procesů. Například BR1=TR1+TR4+TR6… K mapování BR na TR dochází v OIM.

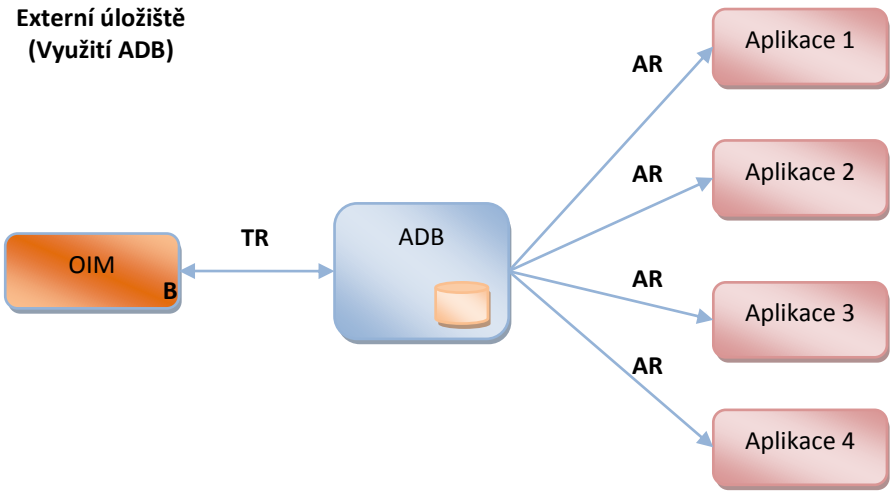


Obrázek 9 - Pyramida rolí

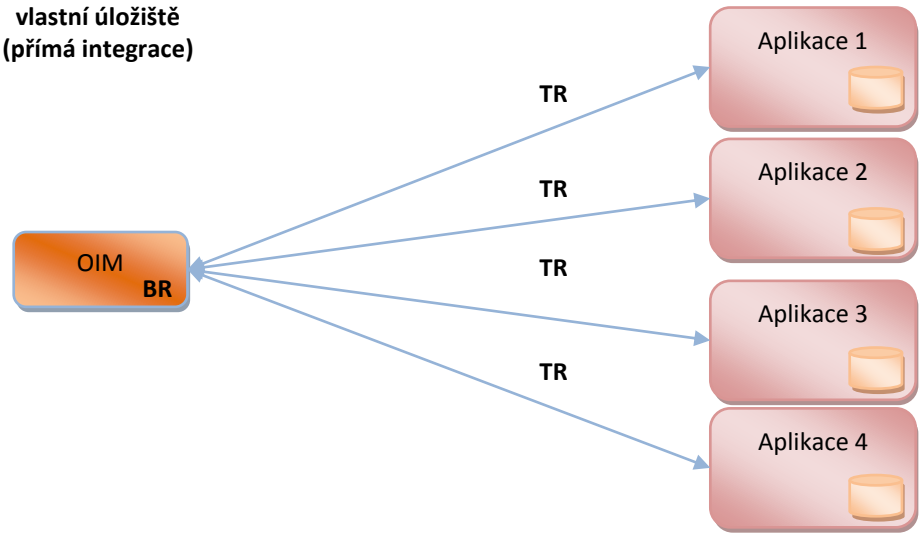
Důvodem použití více úrovní rolí je zajištění jak snadné správy přiřazení rolí uživateli, tj. práce s malým množstvím rolí, tak i v možnosti definovat velké množství oprávnění (aplikačních rolí) na úrovni aplikace.

Jednotlivé úrovně jsou umístěny v různých systémech a to na základě typu použité integrace:

- Mapování Business rolí na Typové role jsou vždy umístěny přímo v OIM
- Mapování Typových rolí na role aplikační se liší dle použité integrace
    - **Nepřímá integrace** – typové role jsou na aplikační mapovány v externím úložišti dat, v ADB (viz Obrázek 10 – Role v nepřímé integraci)
    - **Přímá integrace** – typové role jsou na aplikační mapovány ve vlastním úložišti aplikace (viz Obrázek 11 - Role v přímé integraci)



Obrázek 10 – Role v nepřímé integraci



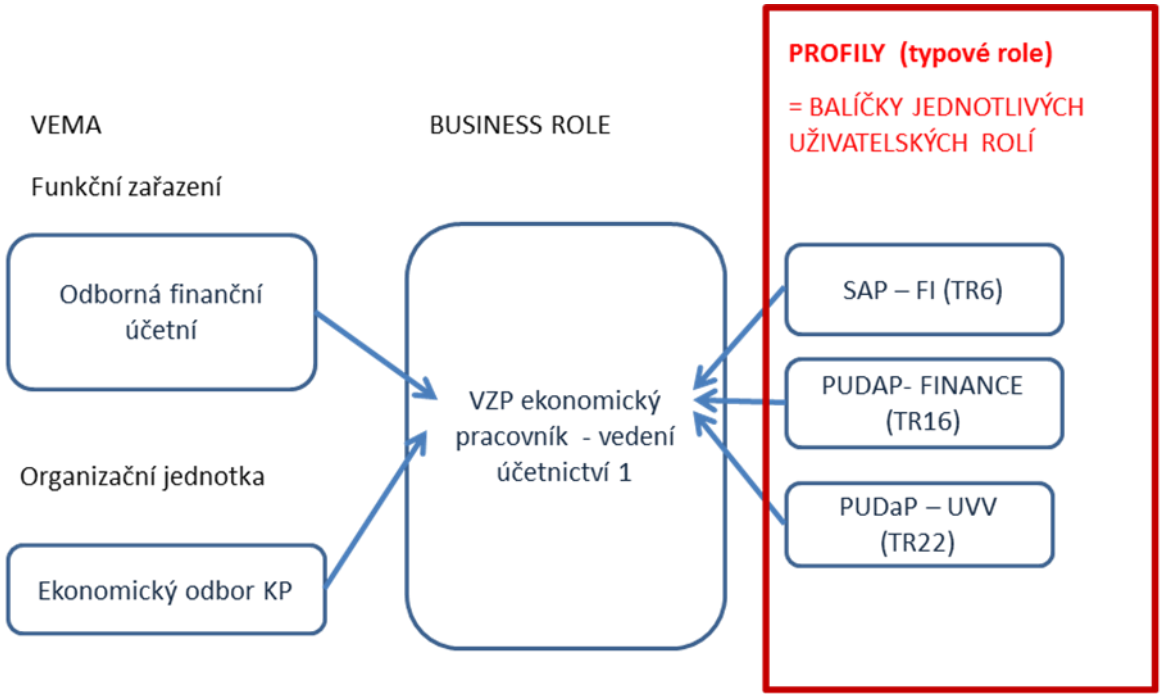
Obrázek 11 - Role v přímé integraci

2.4.1 Metodika definování rolí

Jednotlivé úrovně rolí mají rozdílný význam v interpretaci dané role.

- Aplikační role – představují identifikace rolí, které jsou jednoznačně interpretovatelné aplikační logikou aplikace, tj. řídí možnosti oprávnění v aplikaci

- Typové role – představují procesní kroky v agendě, která je aplikací podporovaná. Příkladem může být – zanesení objednávky, schválení faktury, rozhodnutí o žádosti, agenda EU dokladů atd. TR se skládá z AR, tj. TR náleží jedné aplikaci.
- Business role – představuje roli v podnikových procesech, tj. jedná se o tzv. kategorii zaměstnance – například účetní, krajský účetní kontrolor, ekonomický ředitel, přepážková pracovnice atd.

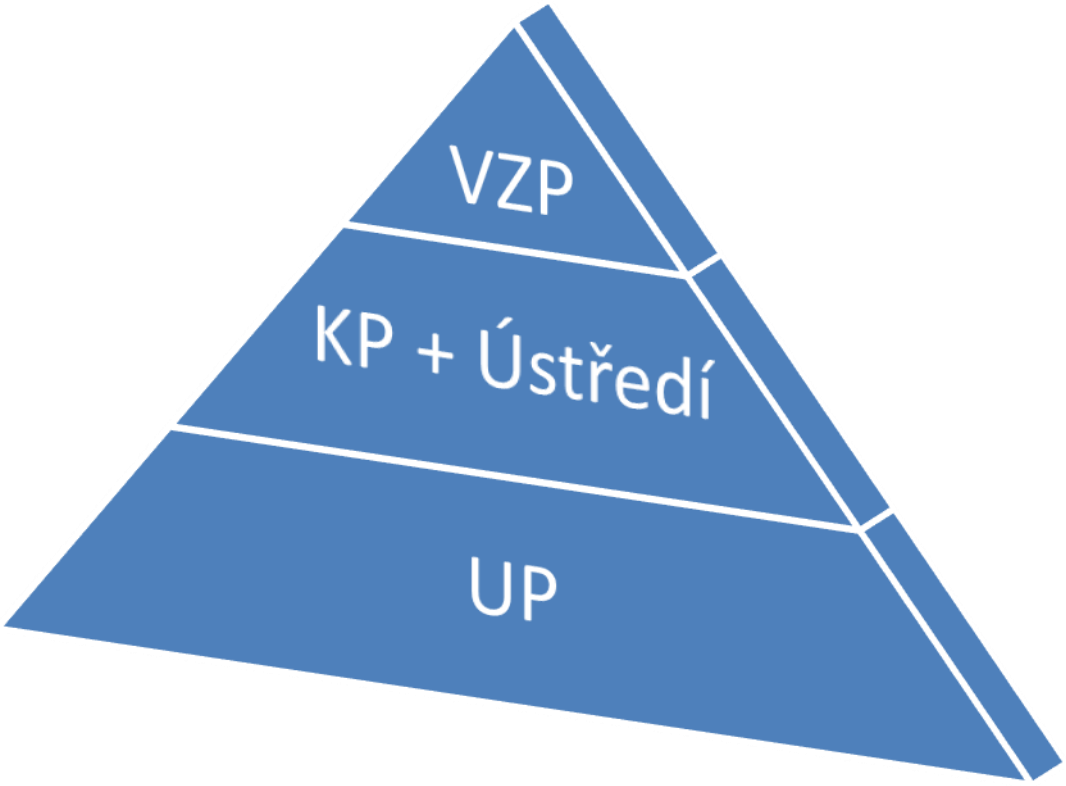


Obrázek 12Příklad Business role a vazby na typové role

2.4.2 Kombinace „Role“ a „Pracovní úsek“

V předchozím textu byl výraz „role“ použit pro funkční vymezení v rámci možností VZP. Toto vymezení ale není úplné, konkrétní role, která se přiděluje uživateli, musí ještě obsahovat vymezení se k pracovnímu úseku VZP, tj. vymezuje se datově. Kombinaci „role“ a „pracovního úseku“ budeme označovat jako instanci role. Tato konvence platí pro všechny úrovně rolí – pro business role, typové role i aplikační role.

Následující schéma zobrazuje hierarchické uspořádání pracovních úseků VZP:



Hierarchie se má úrovně:

- VZP – veškerá data VZP
- KP (včetně ústředí) – krajské celky VZP a ústředí, tj. 14 krajů a ústředí
- UP – územní pracoviště, cca 80 okrasních měst ČR, každé územní pracoviště přísluší právě jednomu kraji

Kód pro VZP je 0, kraje mají kódy 1 až 14, ústředí má kód 9800, územní pracoviště mají 4 ciferný kód, kde 3 a 4 pozice je 0, např. 2100.

Příklady instancí rolí jsou:

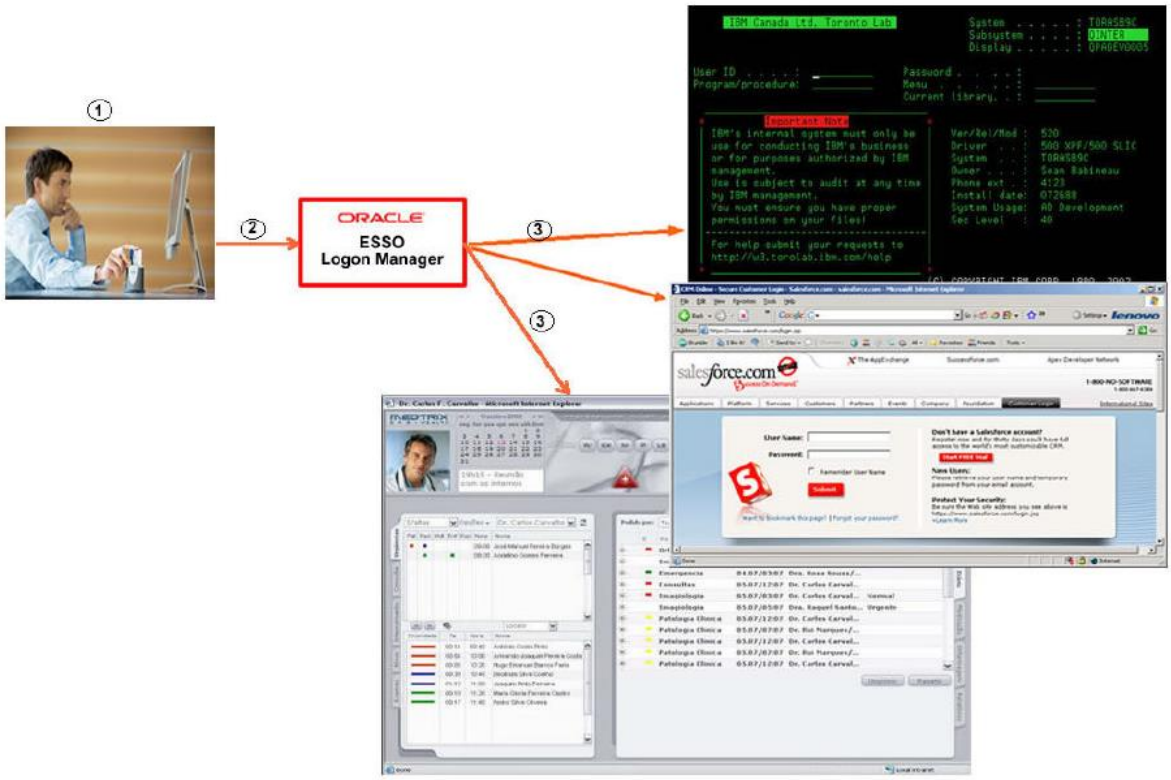
- FIN_TR34_7200
- BR15_0
- RSZP_PK_U66_15

2.5 ESSO LM

Oracle Single Sign-On Logon Manager (eSSO LM) zajišťuje zabezpečené uložení přihlašovacích informací a umožňuje automatické přihlášení do různých druhů aplikací, například:

- Windows aplikace
- Internetové aplikace

- Java aplikace
- Oracle Forms aplikace



Obrázek 13Princip Oracle eSSO LM

Ke spárování uživatele a profilu v eSSO LM slouží uživatelův doménový účet.

Aby bylo možné přihlášení k aplikaci pomocí jejího přihlašovacího dialogu, je potřeba zajistit identifikovatelnou tohoto dialogu, například jednoznačně identifikovatelným textem v názvu přihlašovacího dialogu.

Pro úspěšnou integraci aplikace do IDM řešení je nutné vytvořit přihlašovací profil aplikace v systému eSSO LM. Přihlašovací profil zajišťuje rozeznatelnost přihlašovací dialog aplikace pro automatické zadání jména a hesla systémem Logon Manager, který je nainstalován na pracovní stanici uživatele. V průběhu procesu integrace může být identifikována potřeba provést úpravu přihlašovacího dialogu tak, aby ho mohl Logon Manager jednoznačně identifikovat přihlašovací dialog.

Systém Oracle eSSO není jediným způsobem zajištění SSO ve VZP. Mezi další způsoby patří například metody / technologie:

- Kerberos,
- NTLM,

které se ve VZP využívají, především v prostředí technologií společnosti Microsoft.

2.5.1 Spolupráce systémů OIM a eSSO

Systém OIM je řídícím prvkem mezi IDM systémy, řídí tedy i životní cyklus účtů v integrovaných aplikacích, tj. včetně událostí typu založení účtu, změna hesla k účtu atd. Systémem OIM při těchto operacích

paralelně komunikuje se systémem eSSO a předává mu přihlašovací údaje, které jsou právě modifikovány v integrované aplikaci. Uživatel nezná přihlašovací údaje a systém eSSO vyplňuje přihlašovací údaje za uživatele v okamžiku zobrazení přihlašovacího dialogu integrované aplikace.

2.6 RAP

Rozcestník aplikací (RAP) je z pohledu uživatele aplikace, která zobrazuje seznam dostupných aplikací a umožňuje jejich spuštění. Za aplikací je skryt celý systém pro evidenci dostupných aplikací k jednotlivým uživatelům.

Obrázek 14 - Schéma zobrazení aplikace RAP

Každý uživatel systému RAP musí mít vytvořený uživatelský účet a mít nastaveny pracovní plochy a aplikace. Spuštěním klientské aplikace RAP dojde k přihlášení uživatele (resp. klienta – tj. klientské aplikace) do systému RAP. Uživatel je ověřován na základě uživatelského jména, pod kterým je přihlášen do domény. Při úspěšném přihlášení je uživateli vygenerováno komunikační číslo, které nadále slouží pro vlastní komunikaci se systémem. Dále je uživateli nastavena klientská aplikace RAP. Jsou zjištěny pracovní plochy uživatele, záložky (karty) a aplikace na nich. Klient také získá hodnotu intervalu pro pravidelné oznamování stavu systému RAP.

V tuto chvíli je klient přihlášen a může spouštět přidělené aplikace. Spouštěné aplikace je opět realizováno webovou službou. Dle typu spuštěné aplikace klient rozhodne o způsobu využití vráceného příkazu z odpovědi služby.

- V případě aplikace typu **EXE** dojde k přímému spuštění aplikace na počítači uživatele.
- Pokud se jedná o aplikaci typu **URL**, dojde ke spuštění Internet Exploreru s přednastaveným url.
- U aplikace typu **HOST**, která je vzdálenou aplikací (tzv. server-side) se nejprve na základě tzv. load-balancingu vybere aplikační server a dojde ke spuštění internetového prohlížeče s otevřením aplikace z

vybraného aplikačního serveru. Tento případ může nastat zejména pro aplikace běžící na technologii Oracle Forms.

2.6.1 Integrace aplikace s RAP

Pro integraci aplikace se systémem RAP je třeba:

- Určit typ aplikace
- Připravit název a popis aplikace tak, jak bude vystupovat na kartě pracovní plochy uživatele
- Připravit způsob spouštění aplikace (příkazový řádek, URL, parametry, server …)
- Případně i připravit ikonu představující aplikaci

2.7 GMUSERS – Katalog uživatelů

Dalším tématem spolupráce IDM a podnikových aplikací je distribuce katalogu uživatelů. Katalog uživatelů je spravován personálním systémem VEMA, obsahuje veškeré personální informace.

Katalog je realizován ve formě tabulky GMUSERS a primárním úložištěm je sdílený číselník.

Tabulka GMUSERS obsahuje veškeré zaměstnance VZP a je možné jí mít k dispozici pomocí SDI (silné datové integrace).

Sloupec	Typ	Nepovinný (Nullable)
AD_USERNAME	VARCHAR2(30)	No
JMENO	VARCHAR2(30)	No
PRIJMENI	VARCHAR2(30)	No
TITUL	VARCHAR2(20)	Yes
TEL	VARCHAR2(1000)	Yes
FAX	VARCHAR2(100)	Yes
EMAIL	VARCHAR2(100)	Yes
PRAC_USEK	VARCHAR2(4)	No
FUNKCE	VARCHAR2(300)	No
PLATNOST	CHAR(1)	No

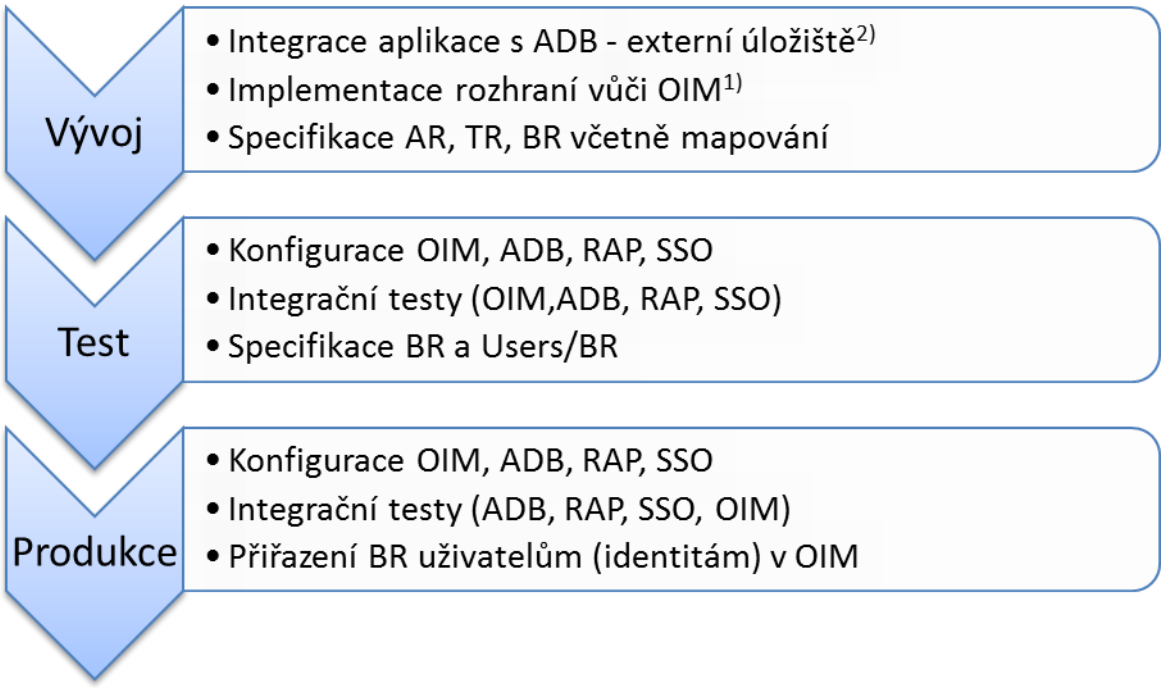
3. Fáze integrace aplikace

Integrace aplikace do IDM není otázkou jednoho kroku, ale představuje komplexní proces, který trvá typicky několik týdnů a obsahuje řadu nutných součinností.

Z pohledu dodavatele aplikací proces integrace do IDM dělíme do 3 fází:

- **Vývoj** – vlastní úprava aplikace pro integraci do IDM
- **Test** – mapování business a typových rolí, provádění integračních testů

- **Produkce** – konfigurace a nasazení do produkčního prostředí včetně přidělení business rolí koncovým uživatelům



Poznámky:

1) *Jedná se o variantu integrace „vlastní“ úložiště / přímá integrace s OIM*
2) *Jedná se o variantu integrace „externí“ úložiště / integrace skrze ADB*

Samotná proces integrace aplikace se dá dělit do dvou oblastí:

- Technologická oblast – integrační vrstva, tj. jedná se o samotné zajištění komunikace IDM komponent a integrované aplikace.
- Aplikační oblast - business úroveň, tj. jedná se o problematiku řízení identit a rolí v integrovaných aplikacích – definování business rolí, schvalovacích procesů, typových rolí atd.

Ve fázi vývoje se typicky řeší úlohy z technologické (integrační) vrstvy. Ve fázích testů a produkčního provozu se naopak řeší především oblast aplikační.

3.1 Kroky a zodpovědnosti během integrace aplikace do IDM řešení

Fáze	Procesní krok	VZP - IDM	VZP - garant aplikace	Dodavatel aplikace	HP/GEM	Komentář
	Předání materiálů pro integraci s IDM					Dokumentace, knihovny, přístupová oprávnění
VÝVOJ	Implementace API (rozhrání) pro OIM komunikaci[1)]			X		
	Vhodnost LOGIN dialogu aplikace pro SSO			X		
	Integrace s ADB (ADB knihovna)[2)]			X		Případná změna modelu řízení oprávnění
	Podpora dodavatele při integraci s IDM				X	
	Seznam TR, AR (včetně mapování) pro nastavení ADB[2)]			X		
	Seznam TR pro nastavení OIM[1)]			X		
	Specifikace BR a schvalovacích procesů		X		X	
	Rozšíření konfigurace OIM (BR, konektor k aplikaci)				X	
TEST	Konfigurace ADB dle podkladů TR/AR[2)]	X				
	Konfigurace OIM včetně BR [1)]	X				
	Podklady pro RAP, eSSO			X	X	URL, test uživatel/heslo
	Konfigurace RAP, eSSO	X				
	Specifikace BR a schvalovacích procesů		X		X	
	Specifikace mapování „uživatelů VZP a BR“		X			
	Integrační testy (RAP, eSSO, OIM, ADB)	X		X	X	
PRODUKCE	Konfigurace ADB dle podkladů TR/AR[2)]	X				
	Konfigurace OIM včetně BR [1)]	X				
	Přiřazení BR v OIM dle mapování „uživatelů a BR“	X				
	Integrační testy (RAP, eSSO, OIM, ADB)					
	Podklady pro RAP, eSSO		X	X		
	Konfigurace RAP, eSSO	X	X			Zpřístupnění aplikace pro koncové uživatele

Poznámky:

1) *Jedná se o variantu integrace „vlastní“ úložiště / přímá integrace s OIM*
2) *Jedná se o variantu integrace „externí“ úložiště / integrace skrze ADB*

4. PL/SQL API – komunikační rozhraní

4.1 Procedura Create User

Tato procedura je určena k vytvoření uživatelského účtu.

```
PROCEDURE CreateUser
(
UserID in varchar2,
FirstName in varchar2,
LastName in varchar2,
Organization in varchar2,
EmployeeType in varchar2,
ManagerID in varchar2,
Email in varchar2,
Telephone in varchar2,
UserLocked in varchar2,
StartDate in DATE,
EndDate in DATE,
UserPassword in varchar2,
Result out varchar2
)
```

Parametry:

- *UserID – jedinečný identifikátor uživatele*
- *FirstName – jméno uživatele*
- *LastName – příjmení uživatele*
- *Organization - organizace*
- *EmployeeType – typ uživatele*
- *ManagerID – jedinečný identifikátor nadřízeného daného uživatele*
- *Email – email uživatele*
- *Telephone – telefon uživatele*
- *UserLocked – určuje, zda je uživatelský účet aktivní (uživatel může přistupovat do Forms aplikace)*
- *StartDate – začátek platnosti účtu*
- *EndDate – konec platnosti účtu*
- *UserPassword – heslo pro uživatelský účet*
- *Result – výsledek procedury*

4.2 Procedura UpdateUser

Tato procedura je určena k změně parametrů uživatelského účtu.

```
PROCEDURE UpdateUser
(
UserID in varchar2,
FirstName in varchar2,
LastName in varchar2,
Organization in varchar2,
EmployeeType in varchar2,
ManagerID in varchar2,
Email in varchar2,
Telephone in varchar2,
StartDate in DATE,
EndDate in DATE,
Result out varchar2
)
```

Parametry:

- *UserID – jedinečný identifikátor uživatele*
- *FirstName – jméno uživatele*
- *LastName – příjmení uživatele*
- *Organization – organizace*
- *EmployeeType – typ uživatele*
- *ManagerID – jedinečný identifikátor nadřízeného daného uživatele*
- *Email – email uživatele*
- *Telephone – telefon uživatele*
- *StartDate – začátek platnosti účtu*
- *EndDate – konec platnosti účtu*
- *Result – výsledek procedury*

4.3 Procedura ChangePassword

Tato procedura je určena k změně hesla k uživatelskému účtu.

```
PROCEDURE ChangePassword
(
UserID in varchar2,
UserPassword in varchar,
```

```
Result out varchar2
)
```

Parametry:

UserID – jedinečný identifikátor uživatele

UserPassword – nové heslo pro uživatelský účet

Result – výsledek procedury

4.4 Procedura LockUser

Tato procedura je určena k uzamčení uživatelského účtu. Uživatelský účet se stává neaktivním.

```
PROCEDURE LockUser
(
UserID in varchar2,
Result out varchar2
)
```

Parametry:

- *UserID – jedinečný identifikátor uživatele*
- *Result – výsledek procedury*

4.5 Procedura UnlockUser

Tato procedura je určena k odemčení uživatelského účtu. Uživatelský účet se stává aktivním.

```
PROCEDURE UnlockUser
(
UserID in varchar2,
Result out varchar2
)
```

Parametry:

- *UserID – jedinečný identifikátor uživatele*
- *Result – výsledek procedury*

4.6 Procedura DeleteUser

Tato procedura je určena k vymazání uživatelského účtu ze správy uživatelů.

```
PROCEDURE DeleteUser
(
UserID in varchar2,
Result out varchar2
)
```

Parametry:

- *UserID – jedinečný identifikátor uživatele*

- *Result – výsledek procedury*

4.7 Procedura AddRole

Tato procedura je určena k přidání role pro daného uživatele.

```
PROCEDURE AddRole
(
UserID in varchar2,
Workplace in varchar2,
Role in varchar2,
Result out varchar2
)
```

Parametry:

- *UserID – jedinečný identifikátor uživatele*
- *Workplace – pracoviště uživatele*
- *Role – role uživatele*
- *Result – výsledek procedury*

4.8 Procedura RemoveRole

Tato procedura je určena k odebrání role pro daného uživatele

```
PROCEDURE RemoveRole
(
UserID in varchar2,
Workplace in varchar2,
Role in varchar2,
Result out varchar2
)
```

Parametry:

- *UserID – jedinečný identifikátor uživatele*
- *Workplace – pracoviště uživatele*
- *Role – role uživatele*
- *Result – výsledek procedury*

4.9 Návratové kódy

USER_NOT_EXIST - Uživatelský účet neexistuje (UpdateUser, ChangePassword, LockUser, UnlockUser, DeleteUser)

USER_EXIST - Uživatelský účet již existuje (procedura CreateUser)

USER_IS_LOCKED - Uživatelský účet je již zamčen (procedura LockUser)

USER_IS_UNLOCKED - Uživatelský účet je již odemčen (procedura UnlockUser)

USER_PHONE_NULL - Není vyplněn telefonní kontakt (procedury CreateUser)

USER_PASSW_BAD - Neplatné uživatelské heslo, nelze nastavit nové heslo (procedury CreateUser, ChangePassword)

USER_LAST_NAME_NULL - Chybí příjmení uživatele (procedury CreateUser)

USER_FIRST_NAME_NULL - Chybí jméno uživatele (procedury CreateUser)

/ návratové kódy související s přiřazením rolí */*

ROLE_NOT_EXIST - Dané přiřazení role neexistuje (procedura RemoveRole)

ROLE_EXIST - Dané přiřazení role již existuje (procedura AddRole)

ROLE_USER_NOT_EXIST - Uživatelský účet pro přiřazení role neexistuje (procedura AddRole)

ROLE_WORKPLACE_NOT_EXIST - Pracoviště pro přiřazení role neexistuje (procedura AddRole)

ROLE_RIGHTS_NOT_EXIST - Skupina práv (role) pro přiřezení neexistuje (procedura AddRole)

/ návratový kód pro ostatní případy */*

OIM_UNKNOWN_ERROR - Ostatní chyby (všechny procedury při neznámé chybě)

5. Reference

Následující tabulka obsahuje seznam dokumentů, které má VZP k dispozici, včetně krátkého popisu obsahu dokumentu.

Název dokumentu	Popis
ADB_API.doc	Popis knihovny ADB
ADB_uzivatelska_prirucka.doc	Uživatelská příručka aplikace ADB
GMRAP_UzivatelskaPriruckaAdmin.doc	Uživatelská příručka administrátora RAP
GMRAP_UzivatelskaPrirucka.doc	Uživatelská příručka uživatele RAP
OIM_PL_SQL_API.docx	Popis rozhraní aplikace pro komunikaci s OIM 1)

Poznámky:

1) *Popis rozhraní aplikace pro komunikaci s OIM je uveden v kapitole 4. tohoto dokumentu*