



Identity Management



ORACLE





Minorits István

IT Lead



Kriszt Norbert

Operations Manager



1.

Bevezetés

Identity Management rendszerek

Identity Management rendszerek

- Szervezetek, felhasználók, jogosultságok kezelése
- Szervezeti vezetők és beosztottak kapcsolata
- Főbb feladatai egy ilyen rendszernek:
 - User lifecycle: A felhasználók „élelciklusának” kezelése
 - Authentication: Egységes belépési módszer biztosítása a szervezet alkalmazásaihoz
 - Authorization: Jogosultságok nyilvántartása



Miért előnyös az IDM egy nagyvállalatban?

- Automatizálja a manuális lépéseket a felhasználókezelésben
- A felhasználói élmény emelése
- Egyedi házirendek betartására
- Auditálás és Riportolás támogatása
- Centralizált felhasználó- és jogosultságkezelés

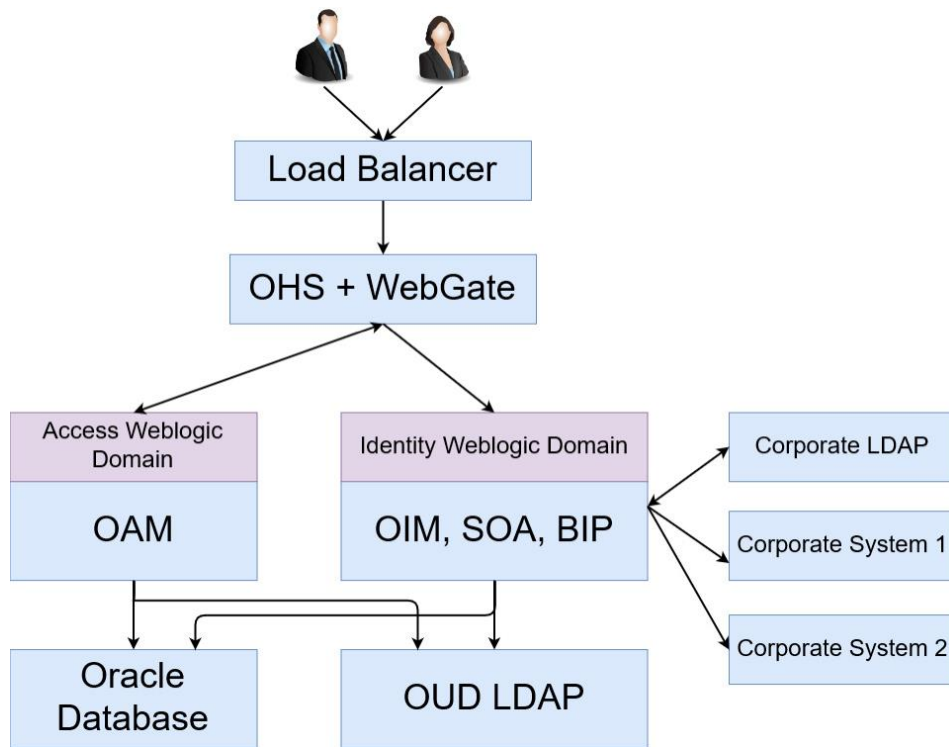
Oracle IDM előnyei

- Oracle Identity and Access Management termékcsalád
- Közepes- és nagyvállalatok számára ideális, ahol:
 - számítanak a növekedésre,
 - komplex folyamatokkal rendelkeznek
- Könnyen és támogatottan integrálható komponensek
- Új rendszerek bevonása
- Nagymértékben szabható a vállalati igényekhez
- Nagy mennyiségű dokumentáció

Erste Bank elvárások és igények

- Általános elvárások
 - szerepkör alapú jogosultságkezelés, automatizált folyamatok
 - reconciliation folyamatok, rendszeres felülvizsgálatok
 - online, offline és hibrid rendszerek, adatbázisok jogosultságkezelése
- Egyedi igények
 - technikai userok, privilegizált accountok nyilvántartása és jogosultságkezelése
 - többszintű jóváhagyások kezelése, leányvállalatok kezelése
 - paramétereizhetőség, bővíthetőség

Felépítés



IDM Identity

The screenshot displays the Oracle Identity Self Service user interface. At the top, the Oracle logo is followed by the text "Identity Self Service". To the right, there are three navigation tabs: "Self Service" (highlighted in blue), "Compliance", and "Manage". Below the navigation is a "Home" breadcrumb. The main content area consists of eight tiles arranged in a 2x4 grid. Each tile has a colored header with an icon, a title, and a brief description.

Tile Title	Icon Description	Description
My Information	Person with pencil	Manage your profile, passwords and challenge questions
My Access	Person with key	See what you have access to
Request Access	Key on document	Request access for yourself or for others
Track Requests	Magnifying glass	Track the status of your pending requests
Provisioning Tasks	Calendar	Take action on fulfillment tasks assigned to you
Certifications	Document with ribbon	Take action on certifications assigned to you
Pending Approvals	Clock with '1' notification	Take action on requests assigned to you for approvals
Pending Violations	Warning triangle	Take action on audit violations assigned to you

BI Publisher

The screenshot displays the Oracle BI Publisher Enterprise interface for editing a data set. The main window shows the 'OPAM General Data Model' with a 'Data Model' tree on the left and a 'Diagram' tab active. A 'Global Level Functions' panel is visible, containing a list of functions such as IAU_COMPONENTTYPE, IAU_INITIATOR, IAU_EVENTTYPE, IAU_EVENTCATEGORY, IAU_EVENTSTATUS, IAU_TSTZORIGINATING, IAU_MESSAGETEXT, IAU_RESOURCE, and IAU_TARGET. A dialog box titled 'Edit Data Set - General Report' is open, showing the following details:

- Name: General Report
- Data Source: OIM JDBC
- Type of SQL: Standard SQL
- SQL Query:

```
select "IAU_COMMON"."IAU_COMPONENTTYPE" as "IAU_COMPONENTTYPE",
"IAU_COMMON"."IAU_INITIATOR" as "IAU_INITIATOR",
"IAU_COMMON"."IAU_EVENTTYPE" as "IAU_EVENTTYPE",
"IAU_COMMON"."IAU_EVENTCATEGORY" as "IAU_EVENTCATEGORY",
"IAU_COMMON"."IAU_EVENTSTATUS" as "IAU_EVENTSTATUS",
"IAU_COMMON"."IAU_TSTZORIGINATING" as "IAU_TSTZORIGINATING",
"IAU_COMMON"."IAU_MESSAGETEXT" as "IAU_MESSAGETEXT",
"IAU_COMMON"."IAU_TARGET" as "IAU_TARGET",
"IAU_COMMON"."IAU_RESOURCE" as "IAU_RESOURCE"
from "IAU_COMMON"
where "IAU_COMMON"."IAU_COMPONENTTYPE" != 'JPS'
and "IAU_COMMON"."IAU_INITIATOR" LIKE NVL(user_name, '%')
and "IAU_COMMON"."IAU_EVENTTYPE" IN ('event_name')
and REGEXP_LIKE
('IAU_COMMON"."IAU_TARGET"' || INVI ('target name.' || INVI ('account name.' ||
```

The dialog also features a 'Query Builder' button and 'Generate Explain Plan', 'OK', and 'Cancel' buttons at the bottom.



WEBVÁLTÓ

BI Publisher

The screenshot displays the Oracle BI Publisher Enterprise web interface. The top navigation bar includes the Oracle logo, the text "BI Publisher Enterprise", a search field with "All" entered, and links for "Administration", "Help", and "Sign Out". Below this, the page title is "General Report : General Report". The interface is divided into several sections:

- Data Source:** A tree view on the left showing a hierarchy of data sources under "DATA_DS", including "p_date_from", "p_date_to", and two groups "G_1" and "G_2".
- Components:** A central toolbar with icons for "Layout Grid", "Data Table", "Chart", "Pivot Table", "List", "Repeating Section", "Text Item", "Gauge", and "Image".
- Page Elements:** A secondary toolbar with icons for "Page Break", "Page Number", and "Total Pages".
- Report Design:** A large central area showing a preview of the report. It features the Oracle logo, the title "General Report", and the subtitle "Oracle Privileged Account Manager". Below the title is a table with the following data:

Event	Status	User ID	Target	Resource ID	Message	Time
CheckoutAccount	1	jdoe			Checkout Account: 73e9183a96e548fe80ffc2dc17e946d3	3/15/12 3:39 AM
CheckoutAccount	1	jdoe			ShowPassword Account: 73e9183a96e548fe80ffc2dc17e946d3	3/15/12 3:40 AM
CheckinAccount	1	jdoe			Checkout Account: 73e9183a96e548fe80ffc2dc17e946d3	3/15/12 3:50 AM
CheckoutAccount	1	jdoe			Checkout Account: 73e9183a96e548fe80ffc2dc17e946d3	3/15/12 4:11 AM
CheckinAccount	1	jdoe			Checkout Account: 73e9183a96e548fe80ffc2dc17e946d3	3/15/12 4:14 AM
	5					

Below the table, there is a text prompt: "[Double click here to edit]".



WEBVÁLTÓ

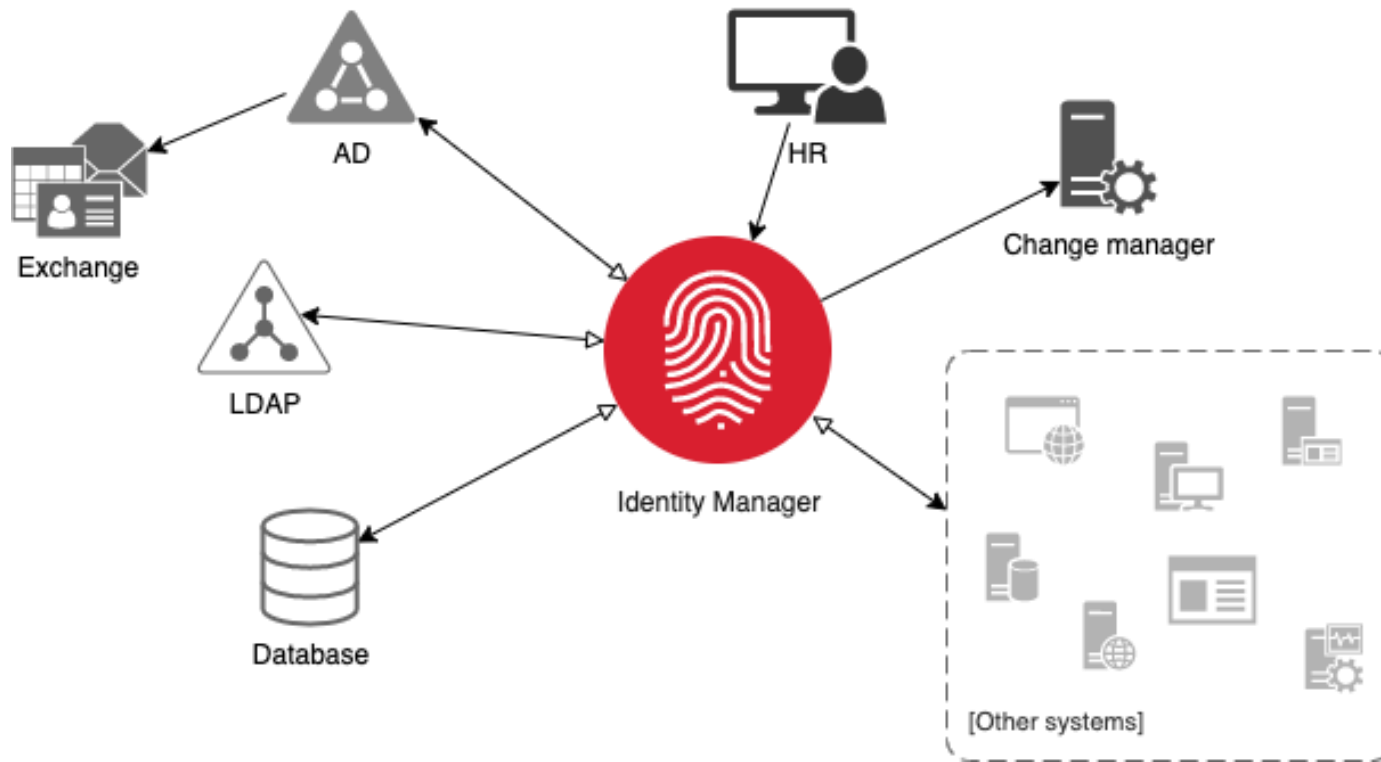
2.

Egyedi fejlesztések

Egyedi megoldások a bank igényeire



WEBVÁLTÓ



Séma mapping

ORACLE Identity Self Service Self Service Manage

Home Applications x

Basic Information **Schema** Settings Cancel Apply

Schema

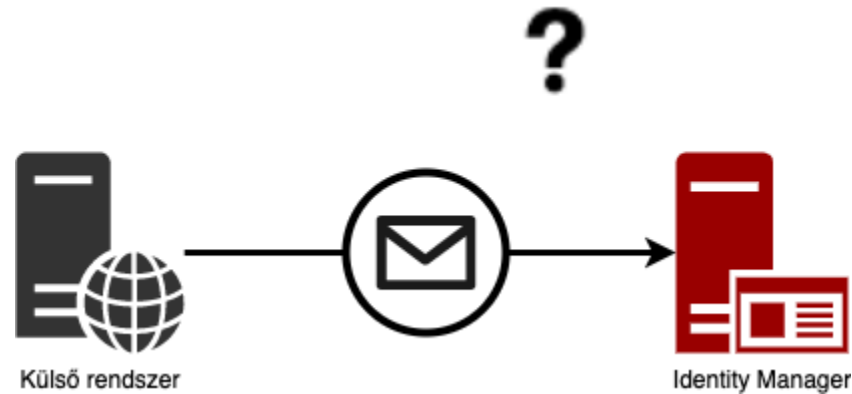
- User
- AD User
- + Add Attribute

Application Attribute				Provisioning Property		Reconciliation Properties					
Identity Attribute	Display Name	Target Attribute	Data Type	Mandatory	Provision Field	Recon Field	Key Field	Case Insensitive			
User Login	User Id	sAMAccountName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
First Name	First Name	givenName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Middle Name	Middle Name	middleName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Last Name	Last Name	sn	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Full Name	Full Name	displayName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Common Name	Common Name	cn	String	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Telephone Number	Telephone Num	telephoneNumber	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Email	E Mail	mail	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	



Egyedi integrációk

Külső rendszerek egyedi integrációja az Identity Manager rendszerbe



Konnektor, mint megoldás...?

- Néhány esetre nem ad megoldást, mivel:
 - Túl speciális eset
 - Számptalan egyedi use-case és validáció
 - Az IDM csak rendelkezésre áll, nem kezdeményez

Egy másik megközelítés

- Valami olyat kell készíteni, ami figyelembe veszi:
 - A kapcsolódó rendszer korlátait (egyedi működés)
 - A Bank egyedi folyamatait, szabályait
 - IDM rendszer működését
- Kritikus a specifikációs szakasz

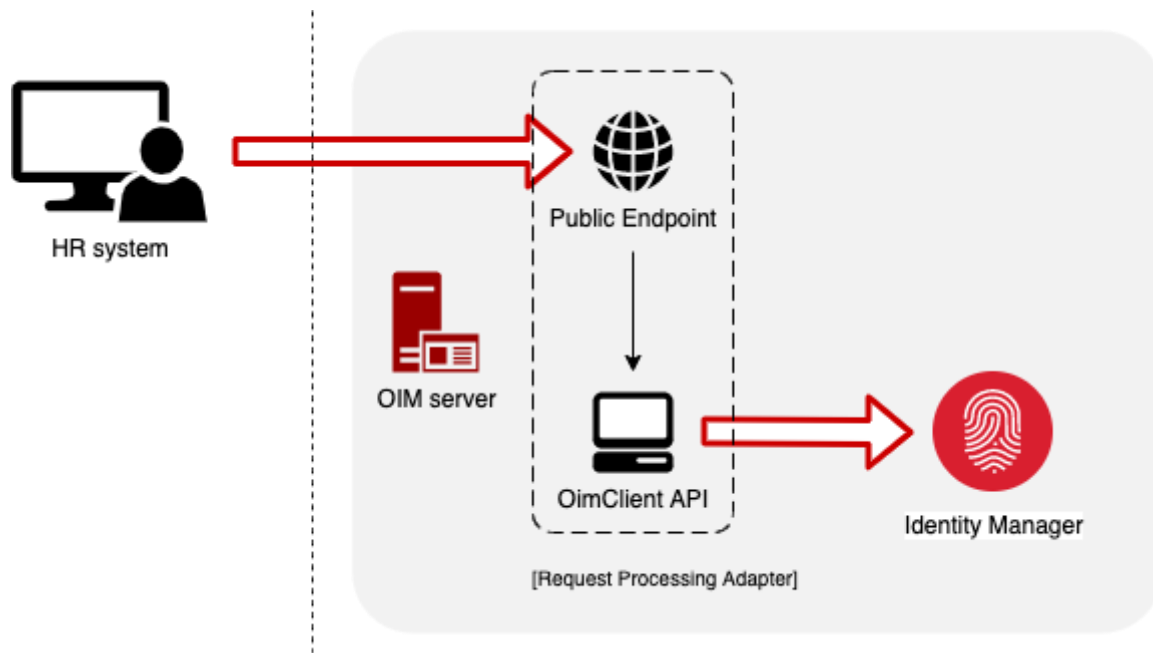
Webservice alapú integráció

- Kívülről hívható endpoint
- Megkötés nélkül lehet üzeneteket definiálni
- Egyedi validáció, feldolgozás
- OIM szerverre telepítve
- Hogyan kommunikáljunk az IDM rendszerrel?

OimClient

- IDM rendszer biztosítja
- Távoli csatlakozást tesz lehetővé
- Remote API hívás
- Bejelentkezés és jogosultságok szükségesek
- Csak előre definiált hívások/műveletek érhetőek el

Custom request processing



Default műveletek

- Előre definiált műveletek, események
- Pl: create, modify, disable, enable, list all
- Ezek nem mindig elégségesek
- Saját eventek küldése?!

Saját események

- Default eseménykezelésre építkezve
- Események indítása:
 - Standard Orchestration használata
 - Külső környezetből tudjunk indítani
 - OrchestrationEngine API-t használtuk fel
- Események kezelése:
 - Eseménykezelők regisztrálása a saját eseményünkhöz
 - Standard módon, de saját műveletre hivatkozva
- Korlátlan lehetőség

Best practice

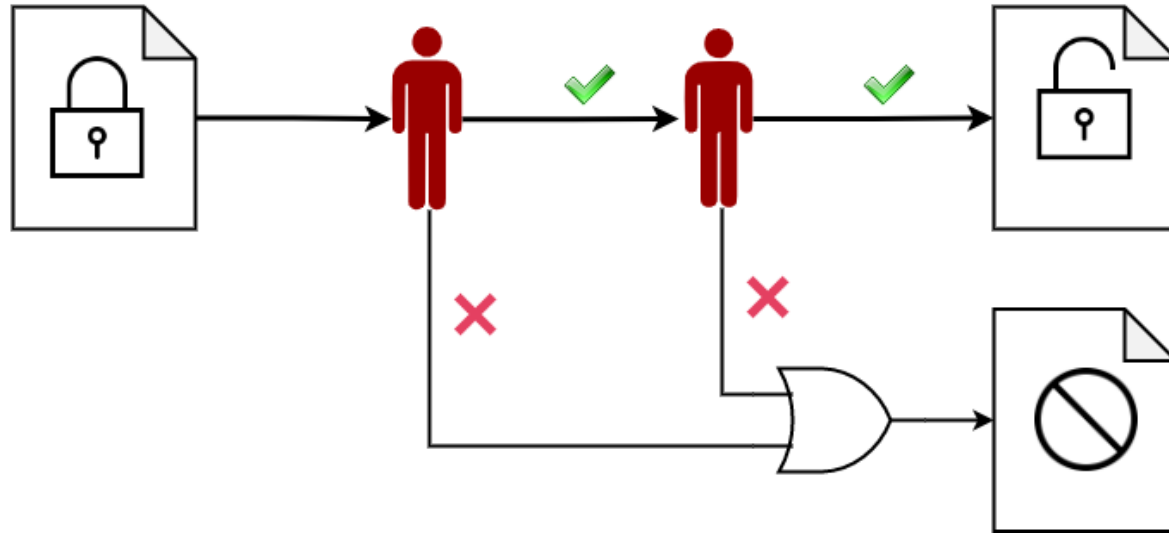
- Raw requestek naplózása, mentése
- Probléma esetén hasznos
- Hibakeresés és audit
- Illeszkedik az Oracle IDM specifikációjához

Jóváhagyási folyamatok

Jogosultság igények elfogadási folyamata másodlagos jóváhagyó bevezetésével



WEBVÁLTÓ



Jogosultság jóváhagyási folyamat

Implementáció folyamata

1. Másodlagos jóváhagyók betöltése, eltárolása

Betöltés, eltárolás

- Adatbázis tábla létrehozása
- Ütemezett feladat fejlesztése
- Xlsx feldolgozása
 - Validáció:
 - Létező alkalmazáshoz
 - Szinkronizált jogosultságok
 - Létező, aktív felhasználók
 - Feldolgozási riport

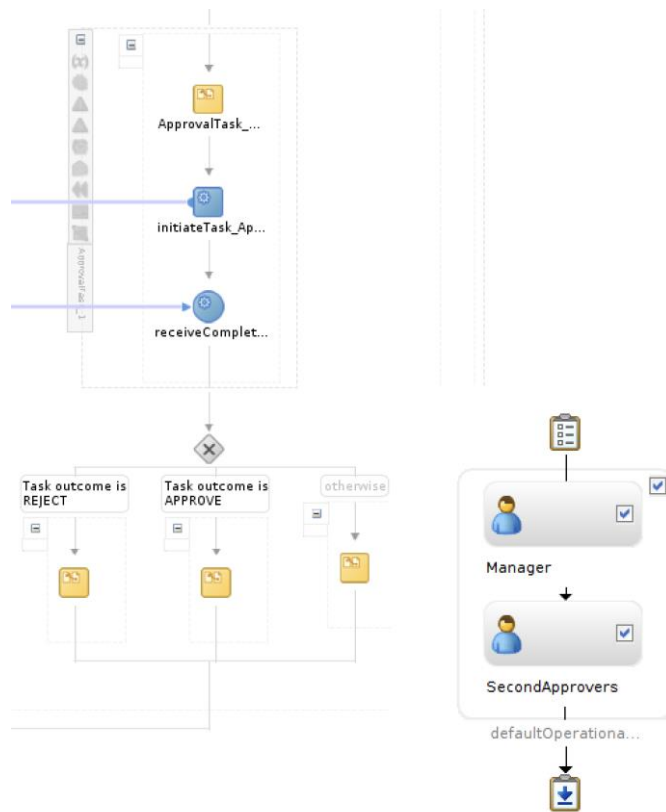
	Megnevezés: *	Leírás: *	Jóváhagyók: *	Jogosultság
Alkalmazás:	Teszt Rendszer	Bemutatóhoz teszt rendszer		
Szerepkör_1:	Rendszergazda	Teszt rendszerben rendszergazda	USR001, USR003	TESZ_RENDSZER_ADMIN
Szerepkör_2:	Könyvelő	Teszt rendszerben könyvelő	USR002, USR003, USR004, USR006	TESZ_RENDSZER_ACCOUNTANT
Szerepkör_3:	Vezető	Teszt rendszerben vezető	USR002, USR004	TESZ_RENDSZER_LEADER
Szerepkör_4:	Üzemeltető	Teszt rendszerben üzemeltető	USR0001	TESZ_RENDSZER_OPERATOR
Szerepkör_5:	Asszisztens	Teszt rendszerben asszisztens	USR001, USR003, USR008	TESZ_RENDSZER_ASSISTENT
Szerepkör_6:	Régióvezető	Teszt rendszerben régióvezető		TESZ_RENDSZER_REGION_LEADER
Szerepkör_7:	Tanácsadó	Teszt rendszerben tanácsadó	USR009	TESZ_RENDSZER_CONSULTANT

Implementáció folyamata

1. Másodlagos jóváhagyók betöltése, eltárolása
2. SOA Composite fejlesztése

SOA Composite

- Egyedi composite fejlesztése
- SOA/BPEL ismerete
- IDM és SOA közötti kommunikáció előre definiált üzenetekkel
 - Pl: felhasználó adatainak lekérdezésére
- Hogyan tudunk saját lekérdezéseket küldeni az IDM rendszer felé?!

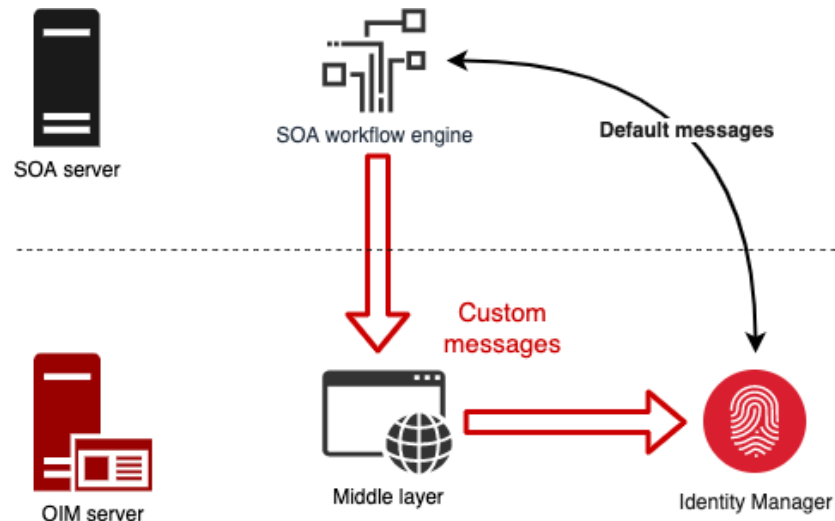


Implementáció folyamata

1. Másodlagos jóváhagyók betöltése, eltárolása
2. SOA Composite fejlesztése
3. Köztes kiszolgáló réteg bevezetése

Köztes kiszolgáló réteg

- Fő feladatai:
 - SOA oldalról hívható
 - IDM rendszer elérése
 - Egyedi hívások kiszolgálása
 - Korlátlan bővíthetőség
- Globális elem: minden IDM-SOA kommunikációra
- JAX-WS Webservice
- IDM elérés OIMClient segítségével



3.

Fejlesztés támogatás

Az alap működést kiegészítő funkciók

Telepítési nehézségek

- Fejlesztéseket mozgatni kell a környezetek között
- Rengeteg manuális folyamat
- Különböző elemeket külön helyeken kell kezelni
 - Számos felület
 - Parancssorból, ant script
 - Mindenhez külön jogosultság
- Adminisztráció, követhetőség hiánya
- Az elemek között sorrend függőség van

Automatikus telepítés

- Telepítést automatizáló eszköz fejlesztése
- Fő szempontok:
 - Az összes elem típust telepítését támogassa
 - Környezetfüggetlen, kívülről konfigurálható
 - Teljesen automata
 - Nyomonkövethetőség
 - Környezeti igények minimalizálása
- Implementáció: parancssorból indítható java alkalmazás
- Pipeline bevezetése



Developer tool

- Igény volt egy olyan eszközre, ami:
 - Kezeli a telepített fejlesztéseket
 - Elérést biztosít a napló állományokhoz
 - Fejlesztések telepítése/törlése/letöltése
 - Szerver managelése
- Vízió:
 - Teljes telepítés vezérlése
 - IDM rendszergazdai funkciók megvalósítása

Developer Tool

- Home
- Manage plugins
- Manage jars
- Manage servers
- Track developments
- Logs
- Settings
- About

Plugin manager

Register
Control Panel
Unregister

Name	Type	Version
TestTask	TaskSupport	1.0
OrganizationCreateTestPlugin	EventHandler	1.0
Qualified name		Type
idm.plugins.test.OrganizationCreateTestPlugin		oracle.iam.platform.kernel.spi.EventHandler
FinalCommitTestPlugin	EventHandler	1.0
UserCreateTestPlugin	EventHandler	1.0
UserModifyTestPlugin	EventHandler	1.0
TestPlugin	EventHandler	
EntitlementProvisioningTestPlugin	EventHandler	

Download: UserModifyTestPlugin.zip

Unregister: idm.plugins.test.UserModifyTestPlugin

EventHandler kezelő felület

Összegzés

- Számos OIM konfiguráció, fejlesztés és integráció
- Saját kiszolgáló rétegek
 - HR rendszer felé
 - SOA felé
- Telepítő eszköz + CI/CD
- Developer tool
- KRITIKUS specifikációs szakasz
 - Tervezni kell vele
 - Időt és költségeket kell allokálni rá

Köszönjük a figyelmet!

Q&A