ERSTE Bank

Identity Management

ORACLE

WEBVÁLTÓ

Minorits István

IT Lead

ERSTE Bank

Kriszt Norbert

Operations Manager

WEBVÁLTÓ

1.

Bevezetés

Identity Management rendszerek

WEBVÁLTÓ

Identity Management rendszerek

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

WEBVÁLTÓ

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

WEBVÁLTÓ

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

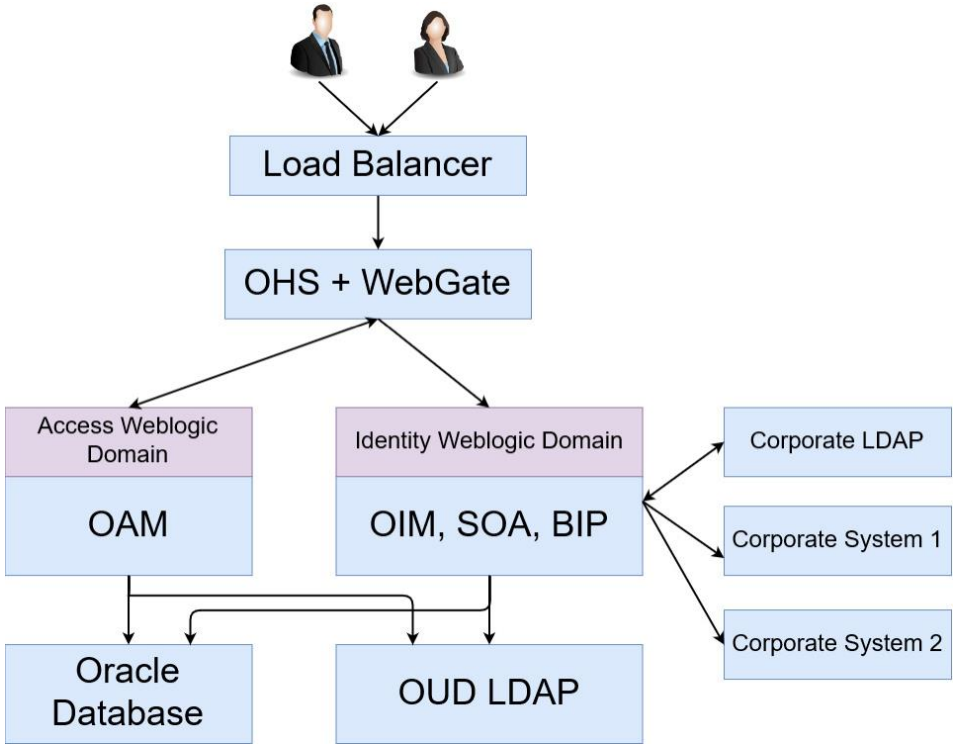
WEBVÁLTÓ

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 userek, privilegizált accountok nyilvántartása és jogosultságkezelése
  - többszintű jóváhagyások kezelése, leányvállalatok kezelése
  - paraméterezhetőség, bővíthetőség

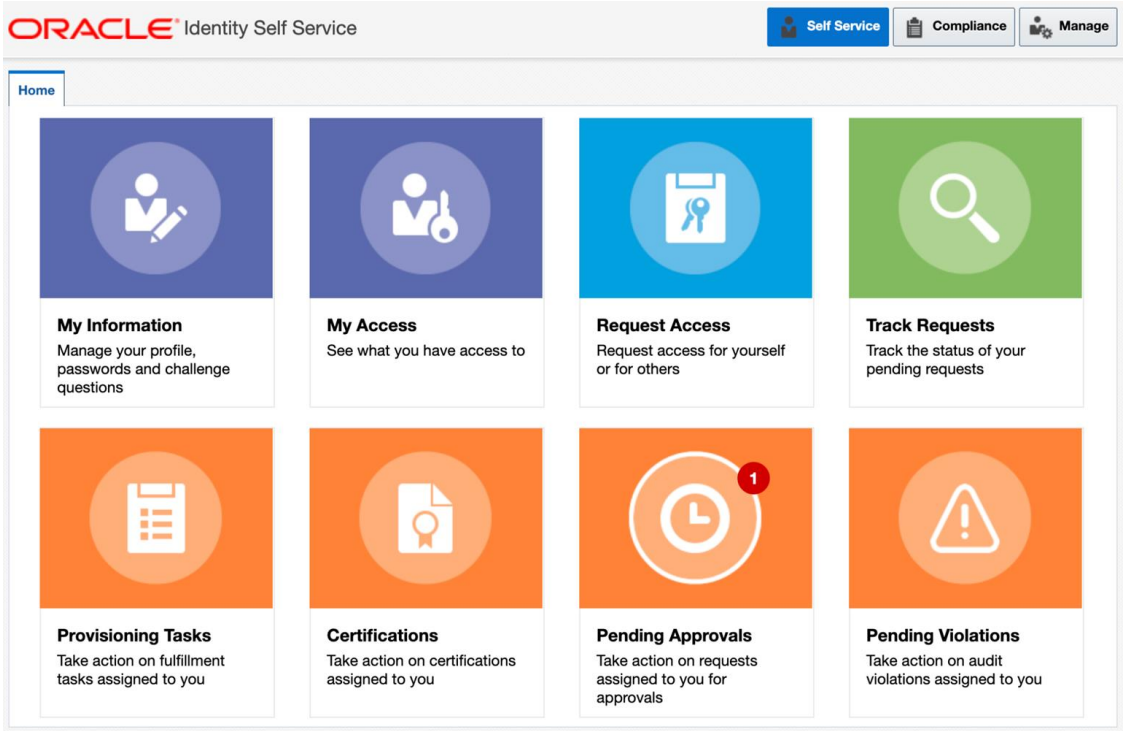
WEBVÁLTÓ

Felépítés



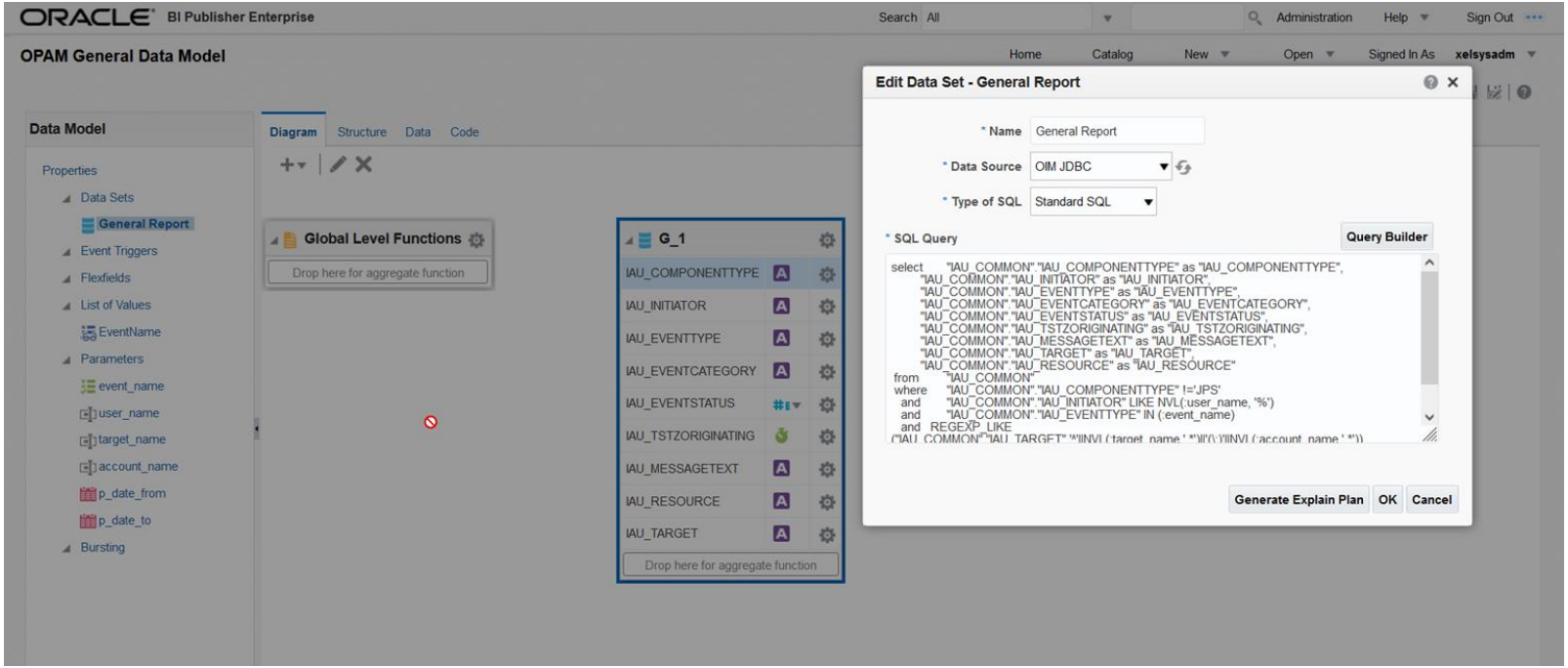
WEBVÁLTÓ

IDM Identity



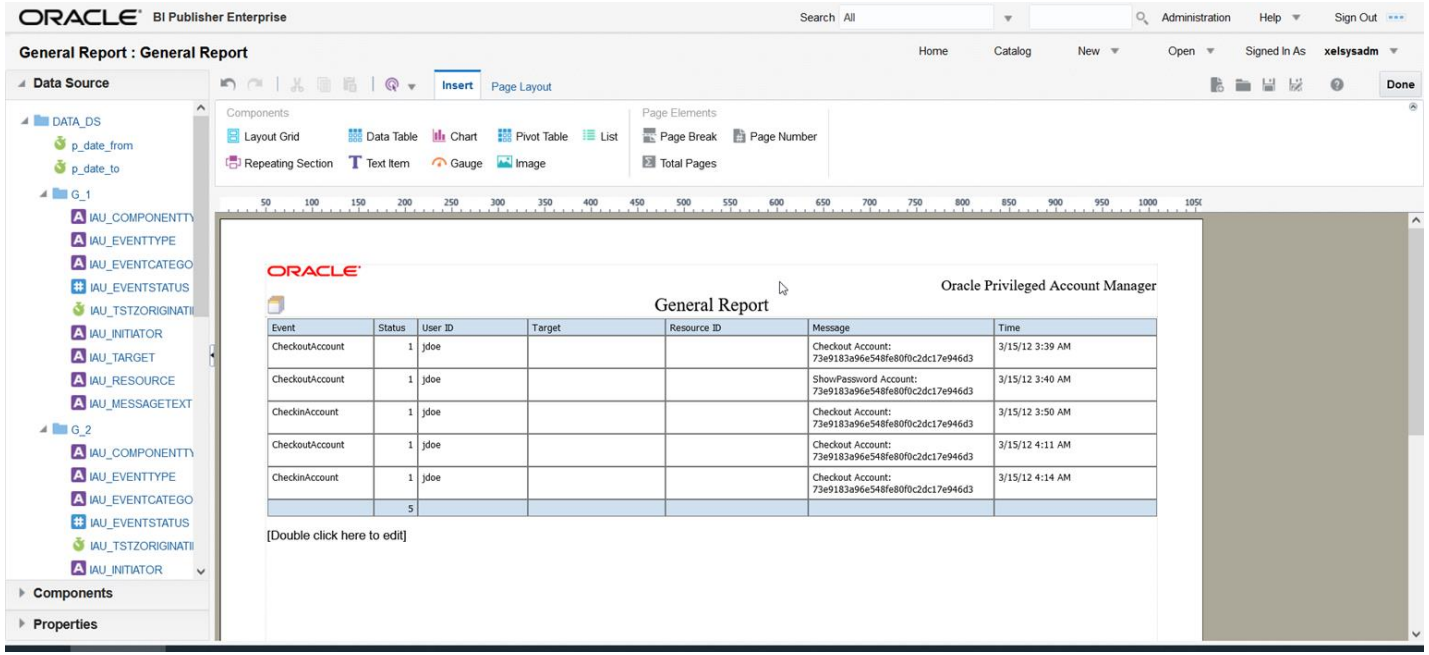
WEBVÁLTÓ

BI Publisher



WEBVÁLTÓ

BI Publisher



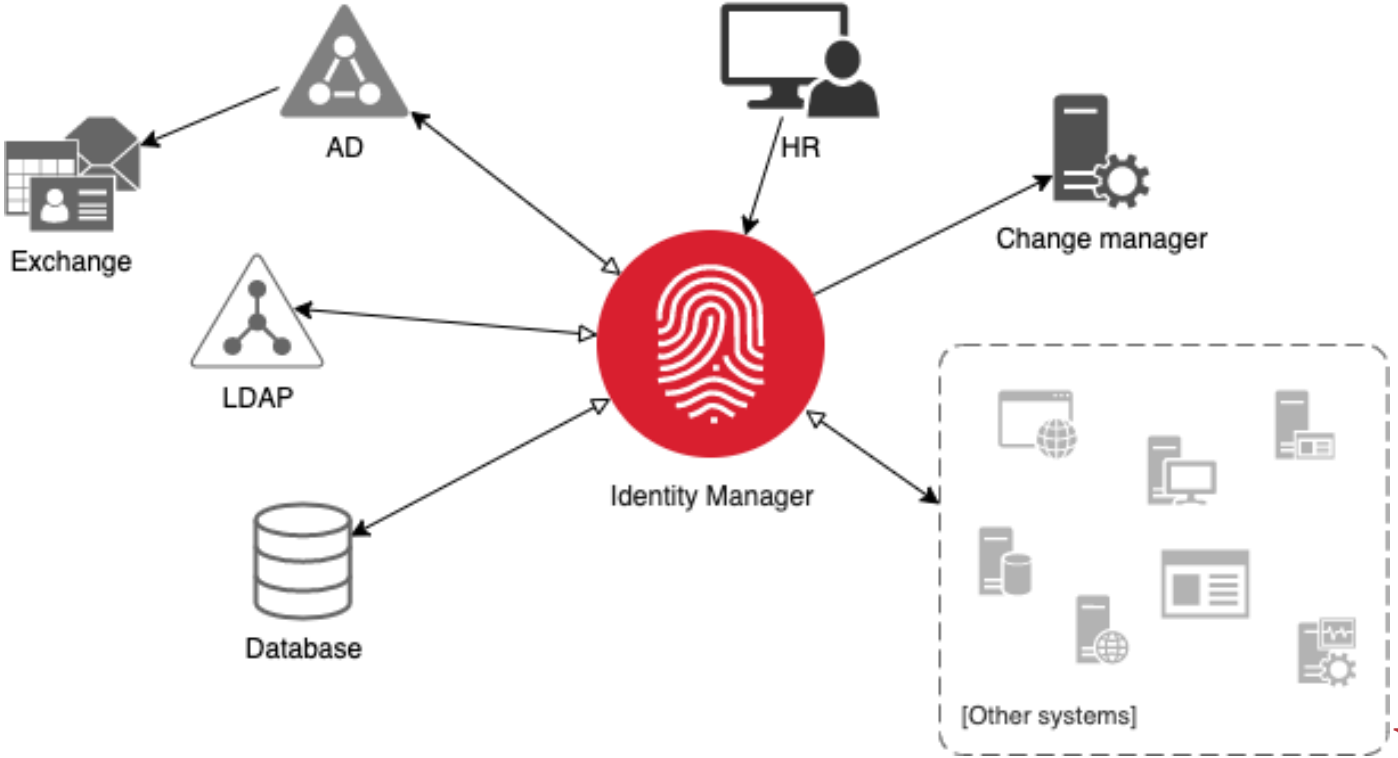
WEBVÁLTÓ

2.

Egyedi fejlesztések

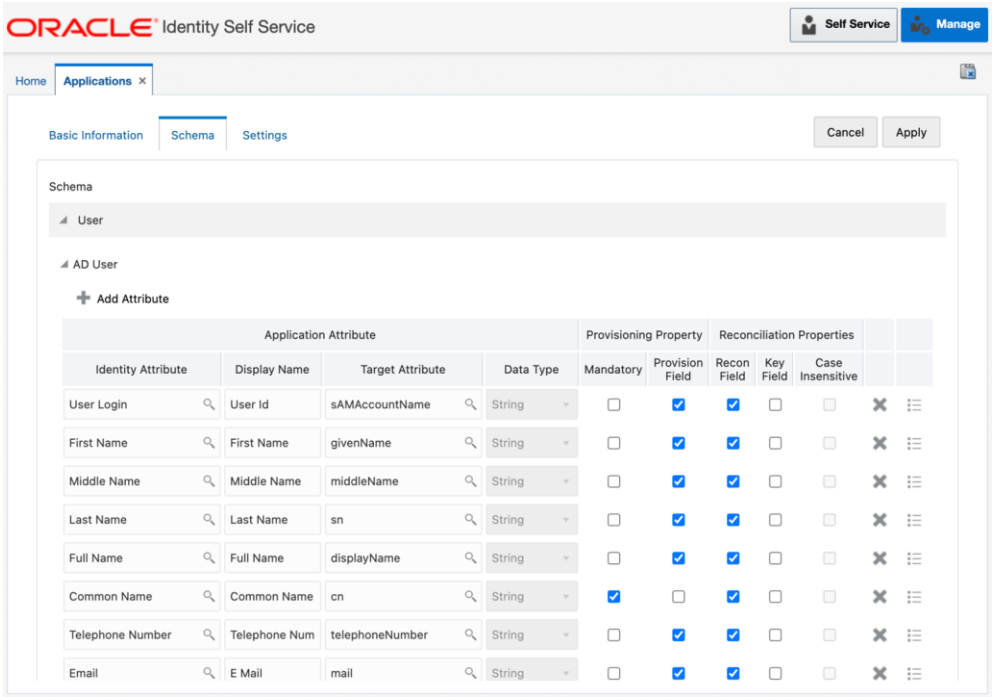
Egyedi megoldások a bank igényeire

WEBVÁLTÓ


AD
HR
Exchange
Change manager
LDAP
Identity Manager
Database
[Other systems]

WEBVÁLTÓ

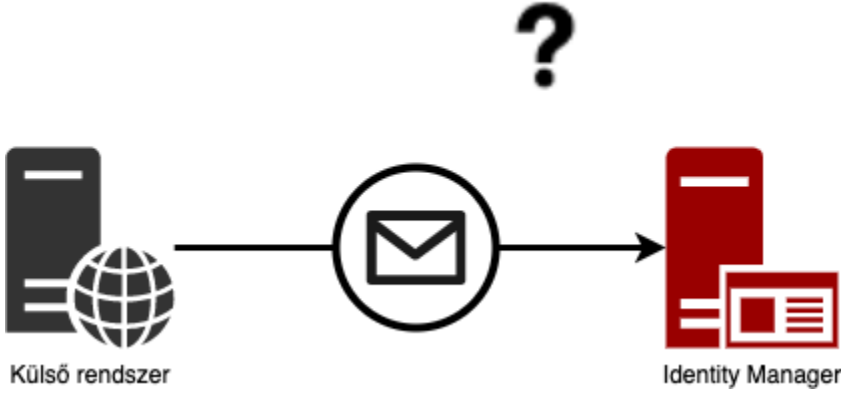
Séma mapping



WEBVÁLTÓ

Egyedi integrációk

Külső rendszerek egyedi integrációja az Identity Manager rendszerbe



WEBVÁLTÓ

Konnektor, mint megoldás...?

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

WEBVÁLTÓ

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

WEBVÁLTÓ

Webservice alapú integráció

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

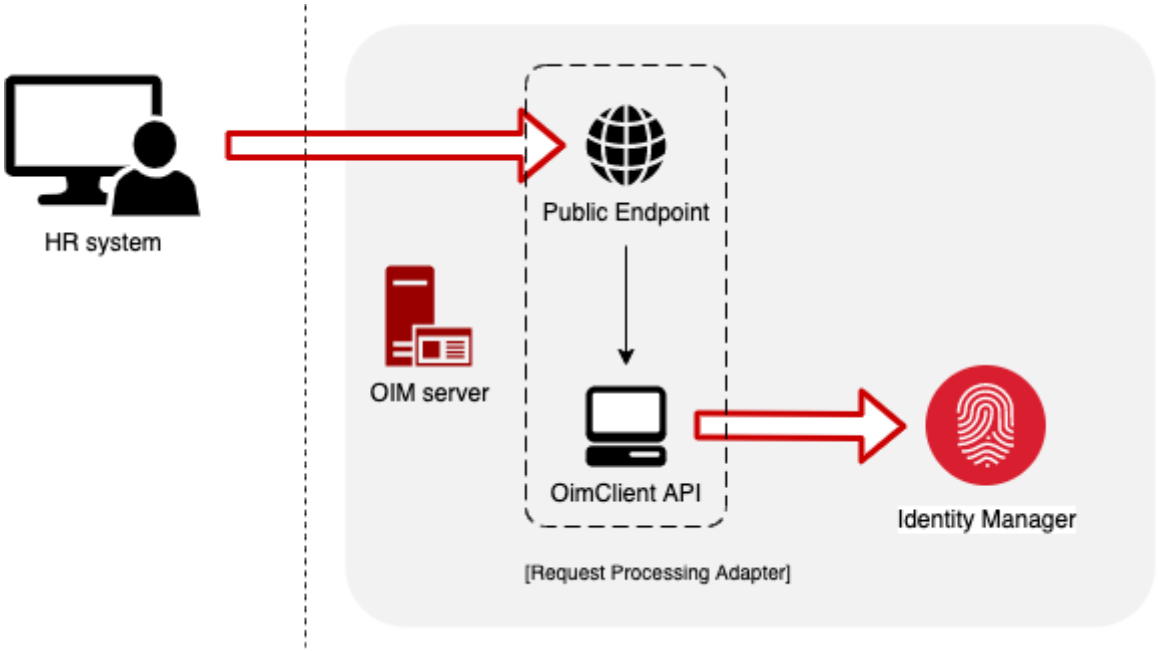
WEBVÁLTÓ

OimClient

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

WEBVÁLTÓ

Custom request processing



WEBVÁLTÓ

Default műveletek

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

WEBVÁLTÓ

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

WEBVÁLTÓ

Best practice

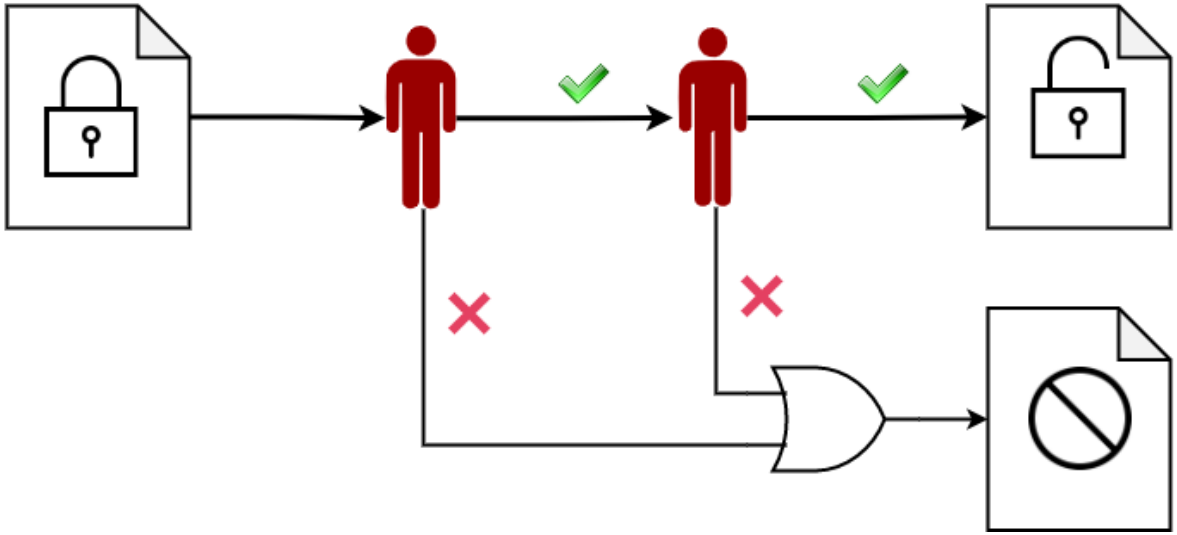
- Raw requestek naplózása, mentése
- Probléma esetén hasznos
- Hibakeresés és audit
- Illeszkedik az Oracle IDM specifikációjához

WEBVÁLTÓ

Jóváhagyási folyamatok

Jogosultság igények elfogadási folyamata másodlagos jóváhagyó bevezetésével

WEBVÁLTÓ



Jogosultság jóváhagyási folyamat

WEBVÁLTÓ

Implementáció folyamata

1. Másodlagos jóváhagyók betöltése, eltárolása

WEBVÁLTÓ

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	Bemutatáshoz 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

WEBVÁLTÓ

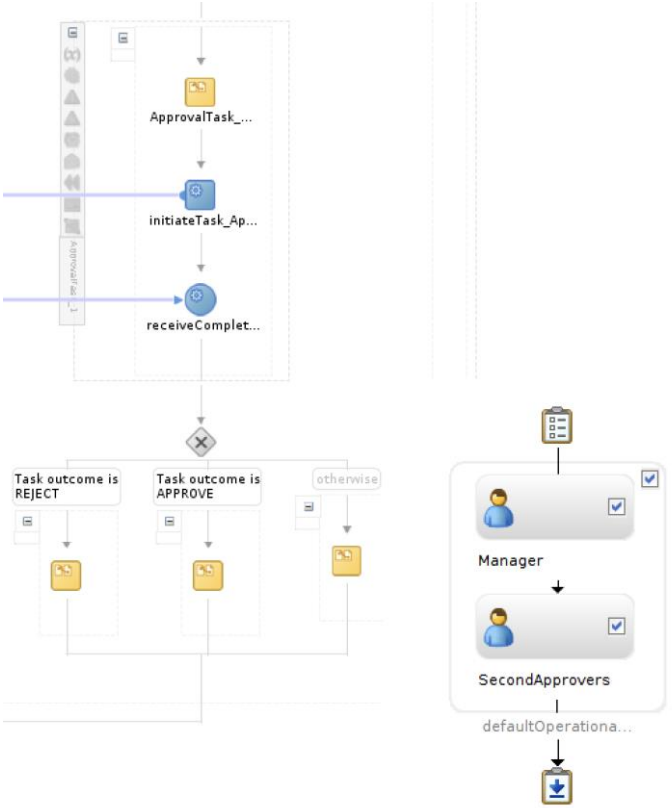
Implementáció folyamata

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

WEBVÁLTÓ

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?!



WEBVÁLTÓ

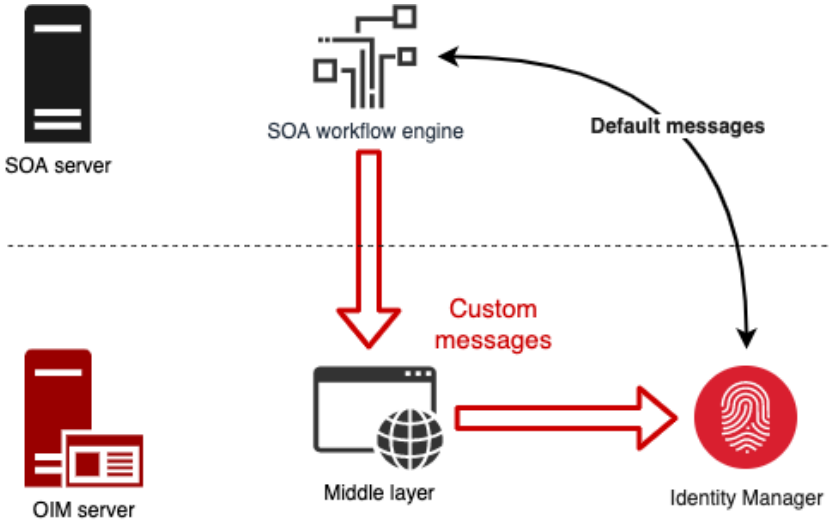
Implementáció folyamata

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

WEBVÁLTÓ

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



WEBVÁLTÓ

3.

Fejlesztés támogatás

Az alap működést kiegészítő funkciók

WEBVÁLTÓ

Telepítési nehézségek

- Fejlesztéseket mozgatni kell 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

WEBVÁLTÓ

Automatikus telepítés

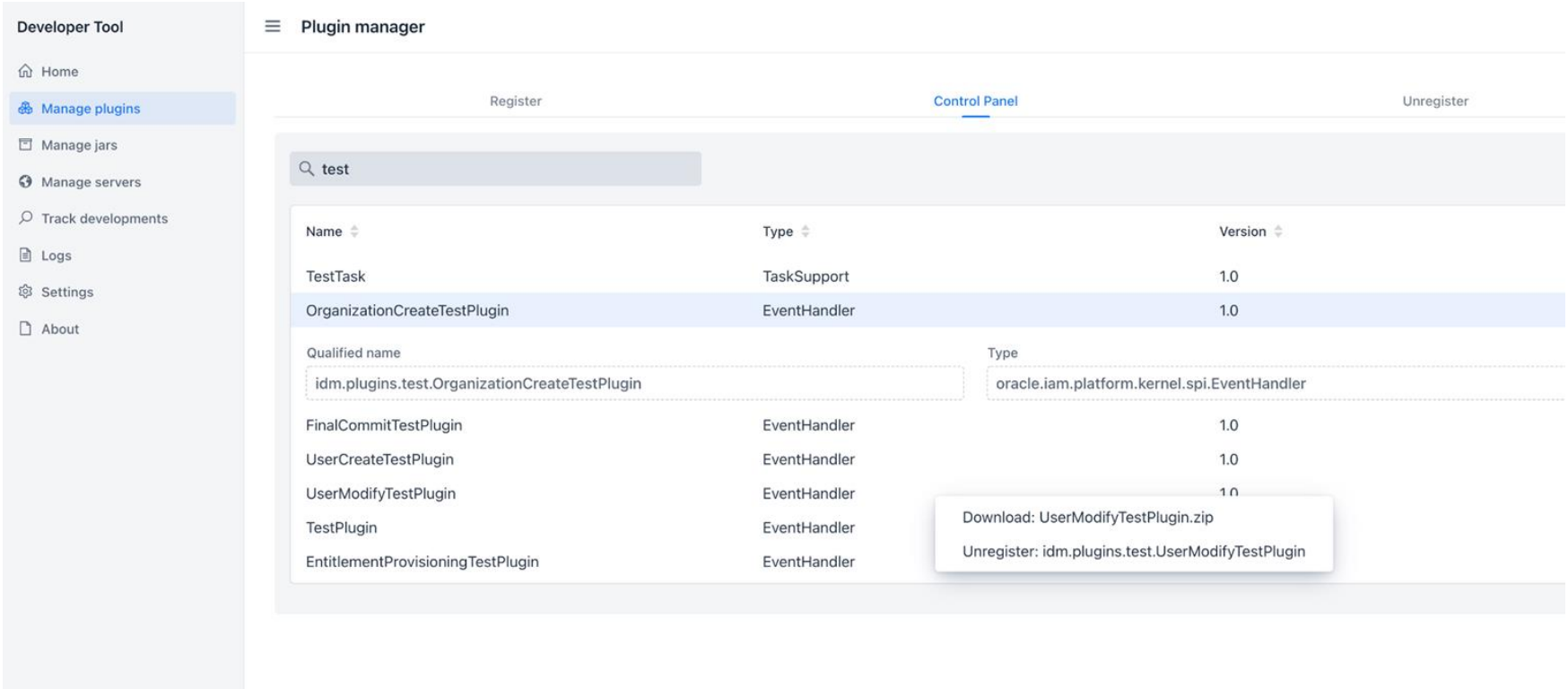
- Telepítést automatizáló eszköz fejlesztése
- Fő szempontok:
  - Az összes elem típust telepítését támogassa
  - Környezetfüggetlen, kívülről konfigurálható
  - Teljesen automata
  - Nyomonkövethetőség
  - Környezeti igények minimalizálása
- Implementáció: parancssorból indítható java alkalmazás
- Pipeline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

WEBVÁLTÓ

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

WEBVÁLTÓ



Eventhandler kezelő felület

WEBVÁLTÓ

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

WEBVÁLTÓ

Köszönjük a figyelmet!
Q&A

WEBVÁLTÓ