EBS R12: MOAC - KORAK NAPRIJED

Tomislav Kušanić
IN2 d.o.o.
Zagreb, Josipa Marohnića 1/1
01/6386-800
tomislav.kusanic@in2.hr
www.in2.hr

SAŽETAK

U EBS-u R11i je konceptom MultiOrg-a omogućeno praćenje poslovanja po organizacijskim jedinicama. U EBS-u R12 taj koncept je evoluirao u Multi-Org Access Control (MOAC) koncept. U ovom predavanju će biti prezentirane nove vrijednosti koje MOAC donosi korisnicima EBS-a u odnosu na MultiOrg kroz nove funkcionalnosti te tehnološki koncepti kojima je to ostvareno.

ABSTRACT

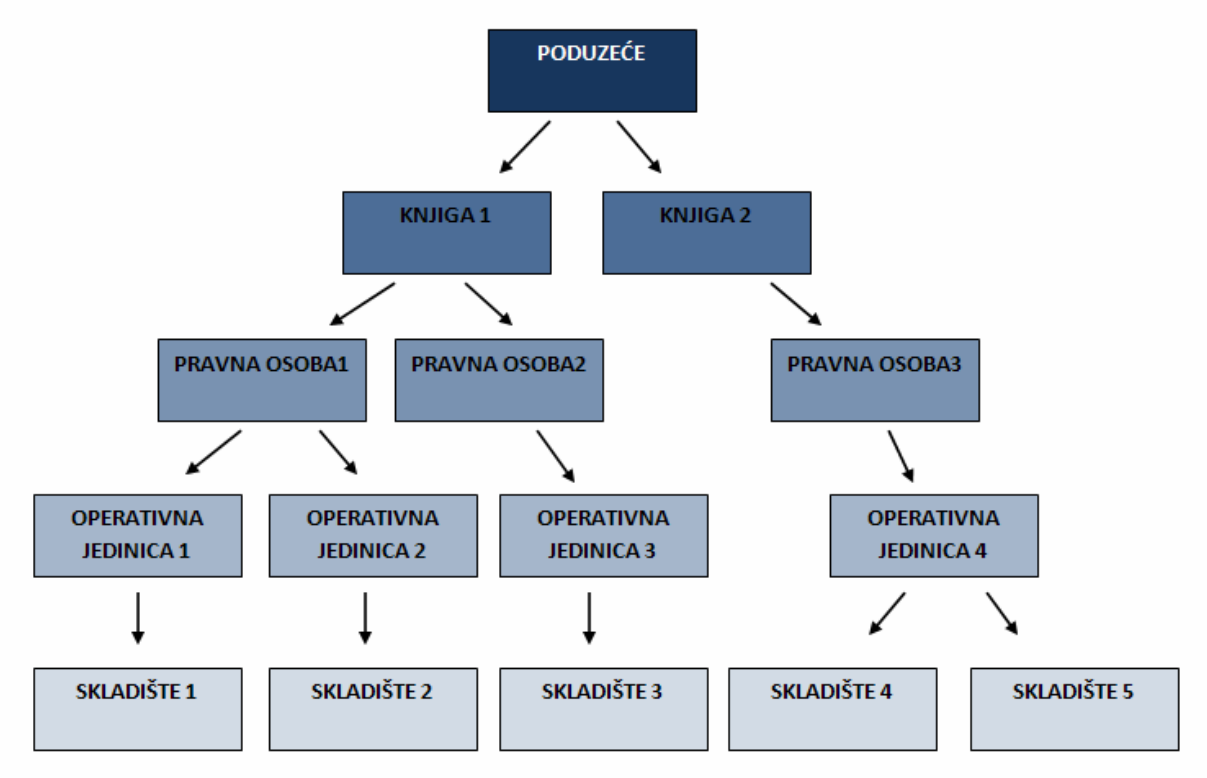
In EBS R11i with using MultiOrg concept it is possible to track bussiness flow by organization units. In EBS R12 this concept evolved into Multi-Org Access Control (MOAC) concept. In this lecture I will talk about new values that MOAC gives to the EBS users comparing to MultiOrg through new functionalities and about technological concepts that were used to implement this new functionalitites.

UVOD

U svakoj tvrtki koja posluje na globalnom tržištu postoji više lokacija na kojima tvrtka posluje. U takvim tvrtkama ima segmenata poslovanja koji su jednaki za sve lokacije na razini tvrtke, ali neki segmenti poslovanja su ovisni o lokaciji i postoje razlike ovisno o lokaciji. Kako bi se omogućilo vođenje podataka za segmente poslovanja koji ovise o lokaciji na kojoj tvrtka posluje u EBS-u je uvedena funkcionalnost organizacijske jedinice koja nam omogućuje da u istom sustavu pratimo podatke sa svih poslovnih lokacija, a opet da se pregled i ažuriranje osigura na razini organizacijskih jedinica. Sama sigurnost podataka je omogućena korištenjem pogleda koji su ovisni o trenutno postavljenom organizacijskom kontekstu kao i ovlaštenja koja su ovisna o organizacijskom kontekstu.

Praksa je pokazala da to rješenje, iako dobro i fleksibilno, u slučaju kompleksnih organizacija može otežati posao održavanja prava pristupa i korištenja samog sustava zbog potrebe da se neka prava i dozvole definiraju na razini svake organizacijske jedinice te da se definiraju ista ovlaštenja za svaku pojedinu organizacijsku jedinicu što u slučaju tvrtke sa mnogo organizacijskih jedinica u velikoj mjeri otežava administraciju korisnika. Zbog toga je u verziji 12 uveden koncept više organizacijske kontrole pristupa – Multi Org Access Control (MOAC). U ovom predavanju ću govoriti o novim funkcionalnostima koje koncept MOAC-a donosi u odnosu na MultiOrg prisup iz verzije 11 i kako se to odražava na radih tehničkih konzultanata za EBS..

1. EBS R11 – MULTIORG PRISTUP



Slika 1 - Struktura organizacije

MultiOrg pristup ćemo objasniti na primjeru šifri poreza u sustavu.

Uzmimo za primjer tvrtku koja posluje na području naše regije, pa tako među ostalim ima podružnice u Hrvatskoj i Sloveniji.

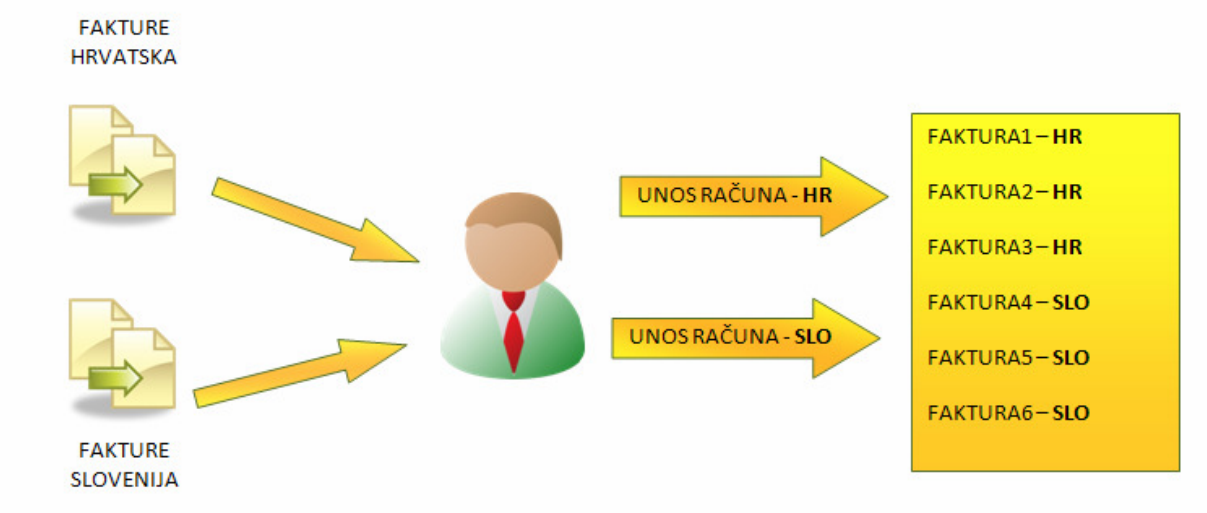
Hrvatska ima različite porezne propise od Slovenije i stoga su definirane različite šifre poreza za Hrvatsku i za Sloveniju. Sam sustav za čitavu regiju nalazi se na jednom serveru za obje podružnice i u sustavu su definirane šifre poreza i za Hrvatsku i za Sloveniju. Korisnik koji unosi ulazne račune u podružnici u Sloveniji ne želi kod unosa vidjeti šifre poreza i za Hrvatsku. I obratno, korisnik u hrvatskoj podružnici ne želi vidjeti šifre poreza koje vrijede u Sloveniji.

U EBS-u to se ostvaruje kroz nekoliko funkcionalnosti koje čine temelj MultiOrg svojstva EBS-a.

Kao prvo u EBS-u se definiraju dvije organizacijske jedinice. „RP Hrvatska“ za Hrvatsku i „RP Slovenija“ za Sloveniju. Sama organizacija može biti definirana kao organizacija za ljudske potencijale, skladišna organizacija, poslovna grupa, operativna jedinica ili neki od mnogobrojnih drugih tipova.

U sljedećem koraku definiramo ovlaštenja „Unos računa – Hrvatska“ za korisnika koji unosi ulazne račune u hrvatskoj podružnici te „Unos računa – Slovenija“ za korisnika koji unosi ulazne račune u slovenskoj podružnici.

U trećem koraku se ovlaštenju „Unos računa – Hrvatska“ dodjeljuje operativna jedinica „RP Hrvatska“,a ovlaštenju „Unos računa – Slovenija“ operativna jedinica „RP Slovenija“.



Slika 2 - unos računa u MultiOrg okruženju

Nakon toga se kod unosa podataka specifičnih za pojedinu operativnu jedinicu popunjava polje identifikatora operativne jedinice kojoj pripada unešeni podatak. Sama kolona identifikatora se automatski popunjava na temelju operativne jedinice koja je dodijeljena ovlaštenju pod kojim korisnik unosi podatke.

Slično tako i kod dohvata će se dohvaćati podaci samo za onu operativnu jedinicu koja je dodijeljena ovlaštenju sa kojim korisnik trenutno radi.

Na taj način je učinkovito osiguran pristup podacima na razini pojedine operativne jedinice. I da bi se korisniku omogućio pristup podacima za određenu organizacijsku jedinicu potrebno je samo dodijeliti mu ovlaštenje kojemu je dodijeljena odgovarajuća operativna jedinica.

2. EBS R12 – MOAC PRISTUP

MultiOrg pristup koliko god je dobar pristup u omogućavanju sigurnosti na razini poslovne jedinice toliko je na današnjem globaliziranom tržištu postao ograničavajući faktor u pogledu kompleksnosti korištenja i ažuriranja.

Naime danas se racionalizacijom poslovanja često neki poslovi centraliziraju i to nas dovodi do situacije da pojedini korisnici moraju moći pristupati podacima više operativnih jedinica.

Na našem primjeru tvrtke koja radi na području zemalja naše regije moglo se pristupiti centralizaciji unosa ulaznih faktura od dobavljača tako da se definira da je recimo ured u Zagrebu zadužen za unos faktura od dobavljača iz svih zemalja regije. U EBS-u R11 gdje je implementiran MultiOrg koncept zaštite podataka to bi značilo da sada korisnik koji radi na unosu ulaznih faktura u zagrebačkom uredu mora imati po jedno ovlaštenje za unos faktura za svaku operativnu zemlju regije, tj. za svaku definiranu operativnu jedinicu.

Ta činjenica komplicira i usporava proces obrade ulaznih faktura dobavljača jer ili ulazne fakture kod zaprimanja moraju biti sortirane prema organizacijskim jedinicama ili osoba koja radi na unosu ulaznih faktura mora svako malo mijenjati ovlaštenje sa kojim unosi ulazne fakture.

Sličan problem se javlja i sa izvještajima koji također prikazuju podatke prema operativnoj jedinici koja je dodijeljena ovlaštenju iz kojega je pokrenut izvještaj. Što zahtijeva izradu nekih dodatnih izvještaja ako se na jednom mjestu žele gledati izvještaji iz regije ili dijela regije.

Također je i samo održavanje ovlaštenja kompliciranо zato jer kod dodavanja neke nove funkcije ovlaštenju za unos ulaznih računa dobavljača potrebno je tu promjenu napraviti na svim ovlaštenjima za unos ulaznih računa dobavljača za svaku pojedinu organizcijsku jedinicu. Što sve usložnjava proces održavanja i implementacije sigurnosti podataka u sustavu.

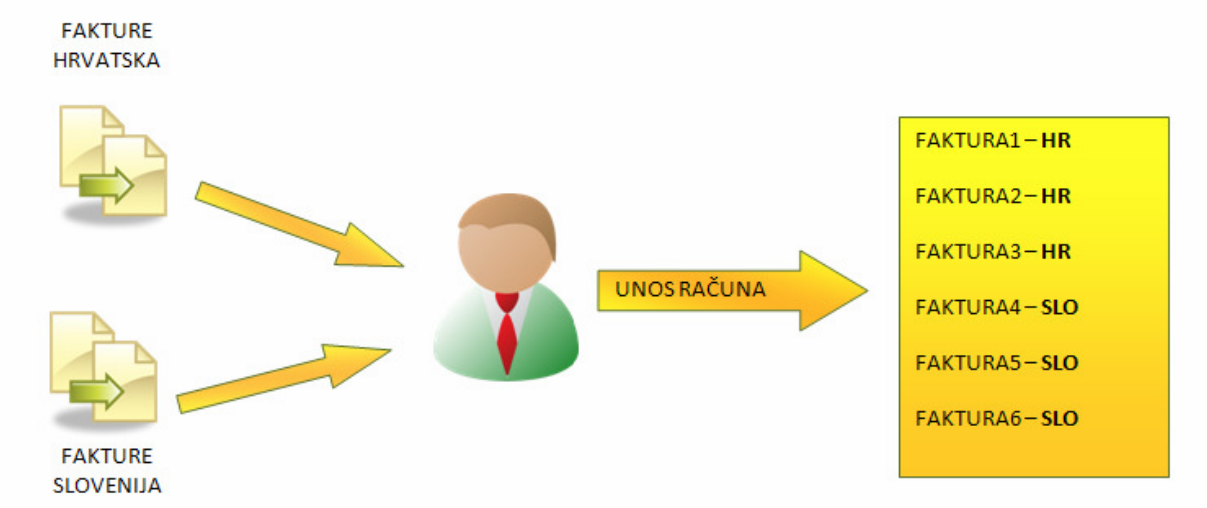
Sa ciljem povećanja fleksibilnosti rada i pojednostavljenja održavanja sigurnosti u takvim tvrtkama, a opet zadržavajući mogućnost zaštite podataka na razini organizacijske jedinice pristupilo se dizajniranju MultiOrg Access Control (MOAC) koncepta zaštite podataka po organizacijskim jedinicama.

Temelj novog koncepta je organizacijska hijerarhija i sigurnosni profili poznati iz modula upravljanja ljudskim resursima EBS-a (Human Resource Management System – HRMS). Naime u organizacijskoj hijerarhiji HRMS-a moguće je definiriati stablo hijerahije organizacija i odjela u tvrtki. Nakon toga se definira sigurnosni profil kojemu se može dodijeliti dio ili cijela organizacijska hijerarhija. I onda se sam sigurnosni profil dodjeljuje ovlaštenju koje onda ima pristup svim organizacijskim jedinicama koje se nalaze u onom dijelu hijerarhijske organizacije koji je dodijeljen sigurnosnom profilu ovlaštenja.

Time smo dobili mogućnost određenom ovlaštenju dodijeliti pristup prema više organizacijskih jedinica istovremeno.

Na našem primjeru to znači da više nećemo morati imati po jedno ovlaštenje za unos ulaznih računa dobavljača za svaku zemlju regije nego jedno ovlaštenje za unos ulaznih računa koje će imati pristup podacima svih organizacijskih jedinica regije i samim time korisnik neće morati mijenjati ovlaštenje svaki puta kad mu dođe ulazni račun iz neke druge zemlje.

Također će i održavanje ovlaštenja biti jednostavnije zato jer će se sada nova funkcionalnost dodavati samo jednom ovlaštenju, a ne na više gotovo identičnih ovlaštenja.



Slika 3 - Unos računa u MOAC okruženju

Po drugoj strani ako imamo potrebu u nekim dijelovima poslovanja zadržati razdvojenost poslovnih procesa na razini organizacijske jedinice jednostavno definiramo novi sigurnosni profil kojemu je dodijeljena samo jedna organizacijska jedinica i onda ovlaštenju koje smije pristupiti podacima samo jedne organizacijske jedinice dodijelito odgovarajući sigurnosni profil.

3. EBS R11 – MULTIORG PRISTUP – TEHNIČKI POGLED

Temelj MultiOrg koncepta su tablice za podatke koji su ovisni o organizacijskoj jedinici, a koje imaju kolonu org_id za identifikator pojedine organizacijske jedinice kojom se definira pripadnost pojedinog zapisa u tablici određenoj organizacijskoj jedinici. Ta kolona se automatski popunjava kod unosa podataka u tu tablicu na temelju organizacijske jedinice koja je dodijeljena ovlaštenju sa kojim se unose ti podaci. Takve tablice možemo u modelu podataka prepoznati po nastavku _ALL u nazivu.

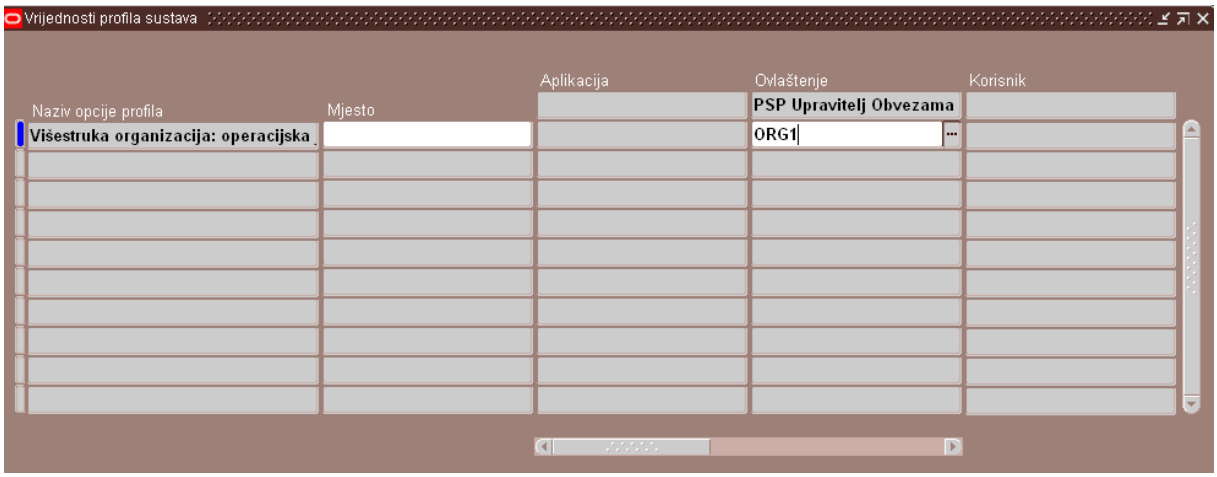
Nad tim tablicama se kreiraju view-ovi koji imaju isti naziv kao tablica nad kojom su definirani samo bez _ALL sufiksa. U takvom view-u se dohvaćaju svi podaci iz pripadne MultiOrg tablice pri čemu se u upitu dodaje uvjet koji provjerava koja organizacijska jedinica je definirana za trenutno ovlaštenje:

WHERE NVL (ORG_ID,NVL (TO_NUMBER(DECODE (SUBSTRB (USERENV ('CLIENT_INFO'), 1, 1),' ', NULL,SUBSTRB (USERENV ('CLIENT_INFO'), 1, 10))),-99)) = NVL (TO_NUMBER(DECODE (SUBSTRB (USERENV ('CLIENT_INFO'), 1, 1), ' ', NULL,SUBSTRB (USERENV ('CLIENT_INFO'), 1, 10))),-99)

Kod pristupanja podacima iz baze kroz aplikaciju sama aplikacija postavlja potrebni organizacijski kontekst kod promjene ovlaštenja na onaj koji je dodijeljen odabranom ovlaštenju. Međutim spajanjem direktno na bazu podataka sam korisnik mora postaviti organizacijski kontekst pozivom procedure FND_CLIENT_INFO.set_org_context(p_org_id); gdje je p_org_id identifikator organizacijske jedinice koju želimo postaviti kontekst i za koju želimo dohvaćati podatke putem MultiOrg view-ova.

Ako slučajno ne postavimo kontekst dohvat podataka korištenjem MultiOrg view-ova neće vratiti nikakve podatke zato jer MultiOrg uvjet u view-u neće biti zadovoljen.

Da bi mogli koristiti MultiOrg funkcionalnosti u samoj aplikaciji potrebno je dodijeliti organizacijsku jedinicu pojedinom ovlaštenju postavljajući vrijednost profil opcije „Višestruka organizacija: operacijska jedinica“(MO: Operating Unit) na razini određenog ovlaštenja na odgovarajuću organizacijsku jedinicu koristeći formu za postavljanje Vrijednosti profila sustava dostupnu kroz ovlaštenje System Administrator.



Slika 4 - dodjela organizacijske jedinice ovlaštenju

4. EBS R12 – MOAC PRISTUP – TEHNIČKI POGLED

4.1. VPD

Virtual Private Database (VPD) je sigurnosni koncept koji omogućuje omogućuje korisniku definiranje ograničavanja pristupa zapisima u tablici na temelju sigurnosnog pravila implementiranog u obliku PL/SQL funkcije koja vraća niz znakova.

U prvom koraku se definira PL/SQL funkcija koja vraća niz znakova koji sadrži uvjet kojim se ograničava dohvat podataka prema kriteriju propisanom sigurnosnim pravilom.

Npr. kreiramo funkciju test koja će osiguravati da se upitom vraćaju samo podaci koje je kreirao neki od korisnika koji se nalazi u XX_TRUSTED_USERS tablici:

```
create or replace function test (p_schema in varchar2
                        , p_object in varchar2)
return varchar2
as
begin
   return 'created_by in (SELECT USER_ID FROM XX_TRUSTED_USERS)';
end;
```

U drugom koraku se ta funkcija registrira u kontekstu tablica, pogleda ili sinonima koje se želi zaštiti korištenjem DBMS_RLS PL/SQL paketa.

Prije definiranom funkcijom želimo zaštiti podatke u tablici XXIN2.test_tbl:

```
dbms_rls.add_policy ( object_schema     => 'XXIN2'
                , object_name       => 'test_tbl'
                , policy_name       => 'test_sig'
                , policy_function   => 'test');
```

Sama primjena sigurnosnog pravila je ostvarena tako da u trenutku pokretanja upita nad zaštićenim objektom RDBMS poziva jednu ili više VPD funkcija registriranih za zaštićeni objekt koje vraćaju uvjete koji se onda prije samo izvođenja upita dodaju samom upitu i time dodatno ograničavaju dohvat podataka u našem upitu.

U našem primjeru ako pokušamo dohvatiti podatke iz tablice XXIN2.test_tbl sa upitom:

```
select  *
   from    XXIN2.test_tbl
   where   trunc(creation_date) > sysdate - 30
```

VPD će proširiti upit uvjetom koji vraća funkcija test pa će se u konačnici izvesti upit:

```
 select  *
   from    XXIN2.test_tbl
   where   trunc(creation_date) > sysdate - 30
   and     created_by in (SELECT USER_ID FROM XX_TRUSTED_USERS)
```

Prednost ovakvog pristupa u odnosu na zaštitu putem pogleda proširenih funkcijama je u tome da je ova zaštita u potpunosti transparentna i ne može se zaobići neovisno o načinu pristupanja bazi

podataka (u slučaju MultiOrg pogleda uvijek je moguće raditi upit direktno nad tablicom i zaobići ograničenje ugrađeno u pogled).

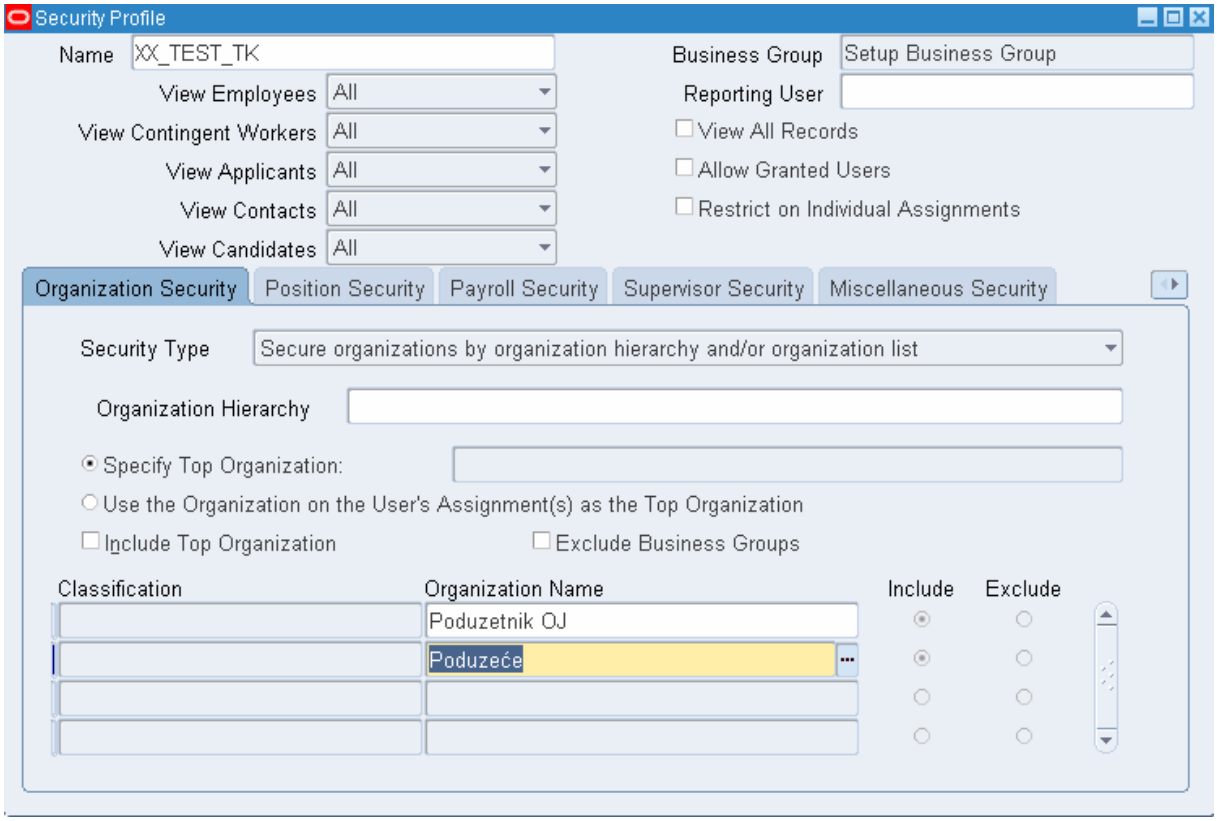
Nadalje održavanje je puno jednostavnije jer je sigurnosno pravilo ugrađeno na jednom mjestu pa se centralno i održava i dorađuje.

4.2. Sigurnosni profili

Da bi bilo moguće iskoristiti mogućnost MOAC koncepta da jedno ovlaštenje ima prisut više organizacijskih jedinica potrebno je kreirati sigurnosni profil na kojemu će biti definirana lista organizacijskih jedinica kojima određeni sigurnosni profil ima pravo pristupati.

Riječ je o sigurnosnom konceptu prisutnom u HRMS modulu EBS-a prisutnom od prije koji se koristio za osiguranje podataka o korisnicima.

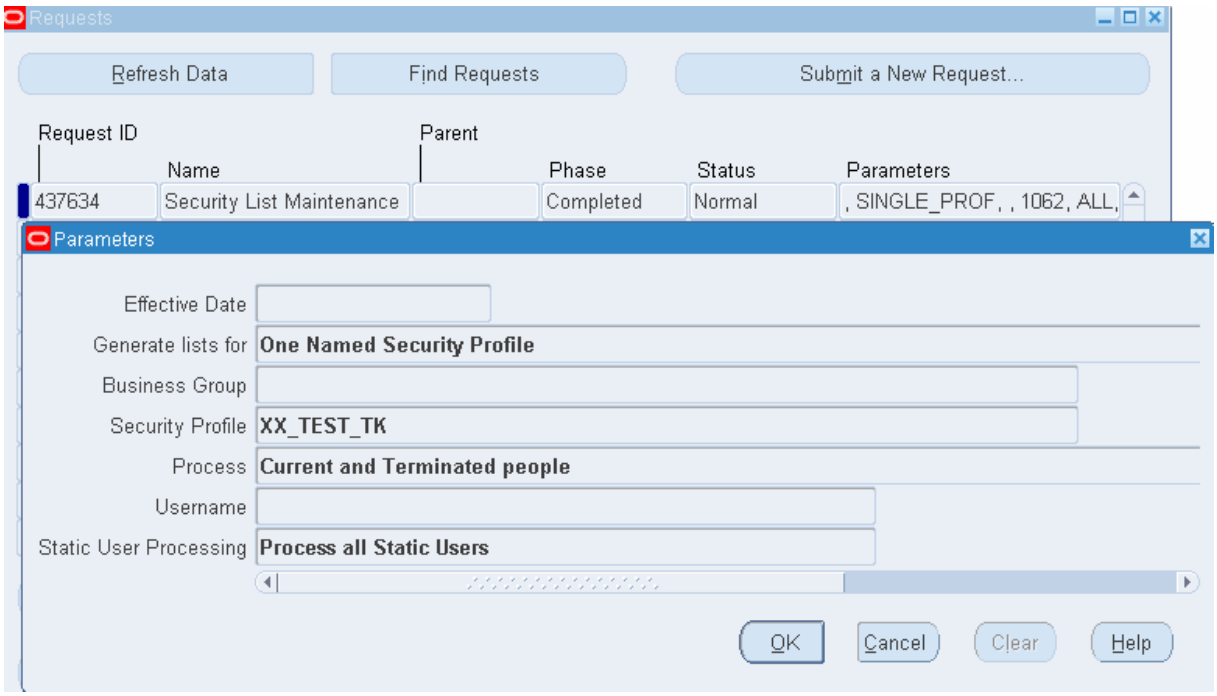
Sigurnosni profil se kreira kroz neko od HRMS ovlaštenja koje ima pravo pristupa formi za definiranje sigurnosnih profila:



Slika 5 - definiranje sigurnosnog profila

Novo definiranom sigurnosnom profilu dodijelimo organizacijske jedinice kojima će se putem tog sigurnosnom profila moći pristupati.

Nakon toga prije korištenja samog sigurnosnog profila potrebno je pokrenuti istodobni program za održavanje liste sigurnosnih profila: „Održavanje sigurnosnog popisa“.



Slika 6 - Održavanje sigurnosnog popisa

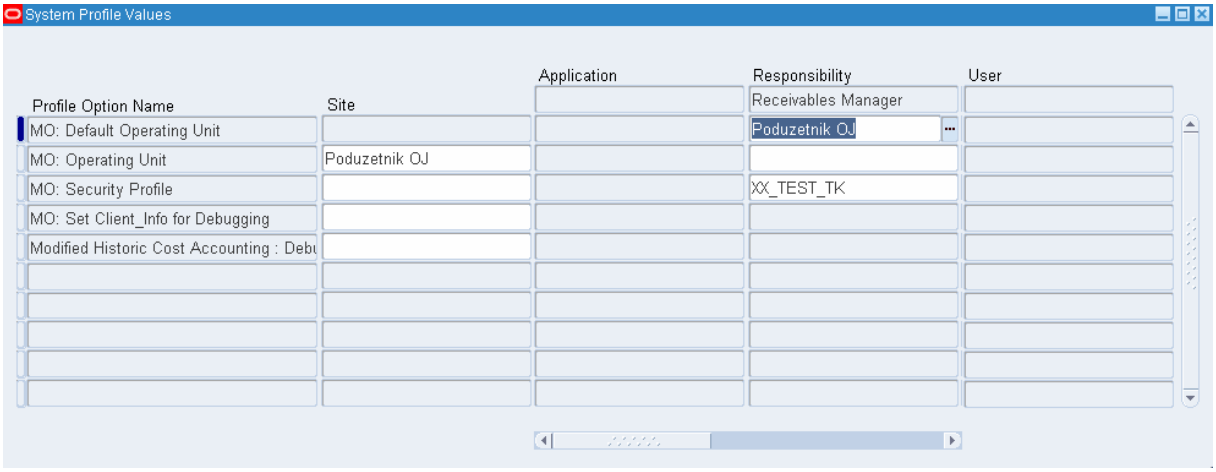
4.3. Profile opcije

Za potrebe postavljanja MOAC sigurnosnog modela postoje tri profile opcije u sustavu:

„MO:Operating Unit“ – riječ je o profile opciji prisutnoj već u starom MultiOrg konceptu koji nam u MOAC okruženju omogućava da MOAC koncept koristimo nalik na MultiOrg koncept kod kojega jednom ovlaštenju ili korisniku omogućavamo pristup samo jednoj organizacijskoj jedinici.

„MO:Security Profile“ – riječ je o profile opciji koja je uvedena sa MOAC konceptom u EBS. Ona nam omogućava da pojedinom ovlaštenju dodijelimo određeni sigurnosni profil i time potencijalno omogućimo pojedinom ovlaštenju pristup podacima iz više organizacijskih jedinica ako je u dodijeljenom sigurnosnom profilu definirano više organizacijskih jedinica kojima sigurnosni profil ima pristup.

„MO:Default Operating Unit“ – riječ je također o profile opciji koja je uvedena sa MOAC konceptom u EBS. Koristi se u slučaju da je nekom ovlaštenju dodijeljen sigurnosni profil koji ima pristup podacima iz više organizacijskih jedinica i ako će se dotičnim ovlaštenjem pretežno pristupati podacima iz jedne organizacijske jedinice. Tada se dodatno postavi ova profile opcija na razini istog tog ovlaštenja na tu organizacijsku jedinicu kako bi se korisniku na svim formama gdje se treba unositi organizacijska jedinica to polje automatski popunjavalo sa tom najčešće korištenom operativnom jedinicom i time se ubrzao i pojednostavio rad korisnika.



Slika 7 - dodjela sigurnosnog profila i default organizacijske jedinice ovlaštenju

4.4. VPD u ostvarenju MOAC-a

Za ostvarenje MOAC koncepta putem VPD funkcionalnosti koristi se sigurnosna funkcija mo_global.org_security koja vraća uvjet koji ograničava pristup samo jednoj ili nekolicini organizacijskih jedinica ovisno o tome kako je postavljen sustav:

```
IF g_access_mode = 'M' THEN
    RETURN 'EXISTS (SELECT 1
                    FROM mo_glob_org_access_tmp oa
                   WHERE oa.organization_id = org_id)';
  ELSIF g_access_mode in ('A','B') THEN
    RETURN 'org_id <> -3113';          ELSIF g_access_mode = 'S' THEN
    RETURN 'org_id = sys_context(''multi_org2'',''current_org_id'')';
  ELSIF g_access_mode = 'X' THEN
    RETURN '1 = 2';
  END IF;
```

Kao i u slučaju MultiOrg koncepta temelj su tablice za podatke koji su ovisni o organizacijskoj jedinici, a koje imaju kolonu org_id za identifikator pojedine organizacijske jedinice kojom se definira pripadnost pojedinog zapisa u tablici određenoj organizacijskoj jedinici, a možemo ih u modelu podataka prepoznati po nastavku _ALL u nazivu.

Nad tim tablicama se kreiraju synonym-i koji imaju isti naziv kao tablica nad kojom su definirani samo bez _ALL sufiksa. Nad tim synonym-ima se registira korištenje sigurnosne funkcije mo_global.org_secuirity i onda se na temelju MOAC postavki u sustavu kod izvođenja upita nad synonym-om na upit dodaje dodatni uvjek za organizacijski kontekst ovisno o tome kako je postavljen MOAC kontekst za trenutno ovlaštenje i aplikaciju.

Da bismo mogli dohvatiti podatke iz tablica zaštićenih MOAC funkcionalnostima direktno iz baze moramo postaviti odgovarajući kontekst koristeći funkciju za postavljanje MOAC konteksta pozivom procedure mo_global.set_policy_context (p_access_mode VARCHAR2, p_org_id NUMBER).

U slučaju da želimo podatke filtrirane za samo jednu organizacijsku jedinicu pozvat ćemo proceduru sa parametrom p_access_mode = 'S' (označava da ćemo se ograničiti na samo jednu organizacijsku jedinicu) i predat ćemo broj organizacijske jedinice.

Ako pak želimo dohvatiti podatke iz nekoliko organizacijskih jedinica potrebno je prvo inicijalizirati aplikacijski kontekst pozivom procedure:

```
fnd_global.apps_initialize(user_id in number,
                           resp_id in number,
                           resp_appl_id in number,
                           security_group_id in number default 0,
                           server_id in number default -1);
```

Za resp_id predajem identifikator ovlaštenja nad kojim smo definirali sigurnosni profil sa pravom pristupa podacima iz više organizacijskih jedinica, a za resp_appl_id identifikator pripadne aplikacije.

Nakon toga je potrebno pokrenuti inicijalizaciju MOAC okruženja sa pozivom procedure: mo_global.init(p_appl_short_name VARCHAR2) gdje kao p_appl_short_name predajemo šifru aplikacije za koju smo u prethodnom koraku postavili aplikacijski kontekst.

I u trećem koraku potrebno je pozvati proceduru mo_global.set_policy_context sa parametrima p_access_mode = 'M' (označava da ćemo dohvaćati podatke iz svih organizacijskih jedinica definiranih u sigurnosnom profilu za zadano ovlaštenje i aplikaciju) i p_org_id = null.

Izvršenjem te tri naredbe se popunjava global temporary tablica mo_glob_org_access_tmp u kojoj je popis organizacijskih jedinica kojima zadano ovlaštenje ima pristup i na temelju koje će se ograničiti dohvat iz MultiOrg tablica.

5. ZAKLJUČAK

Dakle uvođenem MOAC koncepta zaštite podataka na nivou organizacijske jedinice zadržan je nivo sigurnosti prisutan u MultiOrg konceptu iz R11, ali je dobio novu dimenziju fleksibilnosti sigurnosnog modela potrebama korisnika.

Također se i sam standardni izvještajni sustav koji dolazi sa EBS-om lakše prilagođava organizacijskoj strukturi tvrtke u koju se implementira EBS.