Toepassing van 'juiste' autorisatie van essentieel belang voor BI-trajecten

Dynamische front-end autorisatie

Vincent Wylenzek

Het begrip autorisatie is erg breed en kan op vele manieren ingevuld worden. Bij het ontwerpen van de autorisatie acceptatiecriteria speelt primair de vraag 'Wie mag welke informatie (binnen welke kaders en via welke interface(s)) zien', daarnaast worden tevens eisen gesteld aan de beheer- en beheersbaarheid, de flexibiliteit en transparantie.

Veelal blijkt uit de eerste informatieanalyse dat de autorisatiewensen erg complex zijn en een bepaalde mate van dynamiek bevatten. De autorisatie heeft daarnaast meestal betrekking op meerdere interfaces, denk aan OLAP-cubes, (ad hoc) rapporten, het DBMS en eventueel nog een portal. Bij Ordina is het bovenstaande uitgewerkt in de vorm van een tweetal best practices, die ontstaan zijn gedurende een Microsoft SQL Server 2008 BI-traject. Het proces is generiek, de technische uitwerking is echter wel Microsoft specifiek.
Veelal bieden front-end tools de mogelijkheid om autorisatie 'hard' in te regelen. In projecten waar er sprake is van een zeer beperkte omvang van de autorisatie acceptatiecriteria is dit gewenst. In projecten met complexe, frequent wijzigende criteria en wijzigingen in de onderliggende data, heeft een dergelijke mogelijkheid een gigantische impact op de activiteiten voor beheer. In dit artikel wordt beschreven hoe door middel van een stringente procedure en bijbehorende producten een basismodel opgezet kan worden, waarbij de dynamiek vervolgens mogelijk wordt gemaakt door 'slim' gebruik van ETL en configuratietabellen.

Autorisatie acceptatiecriteria

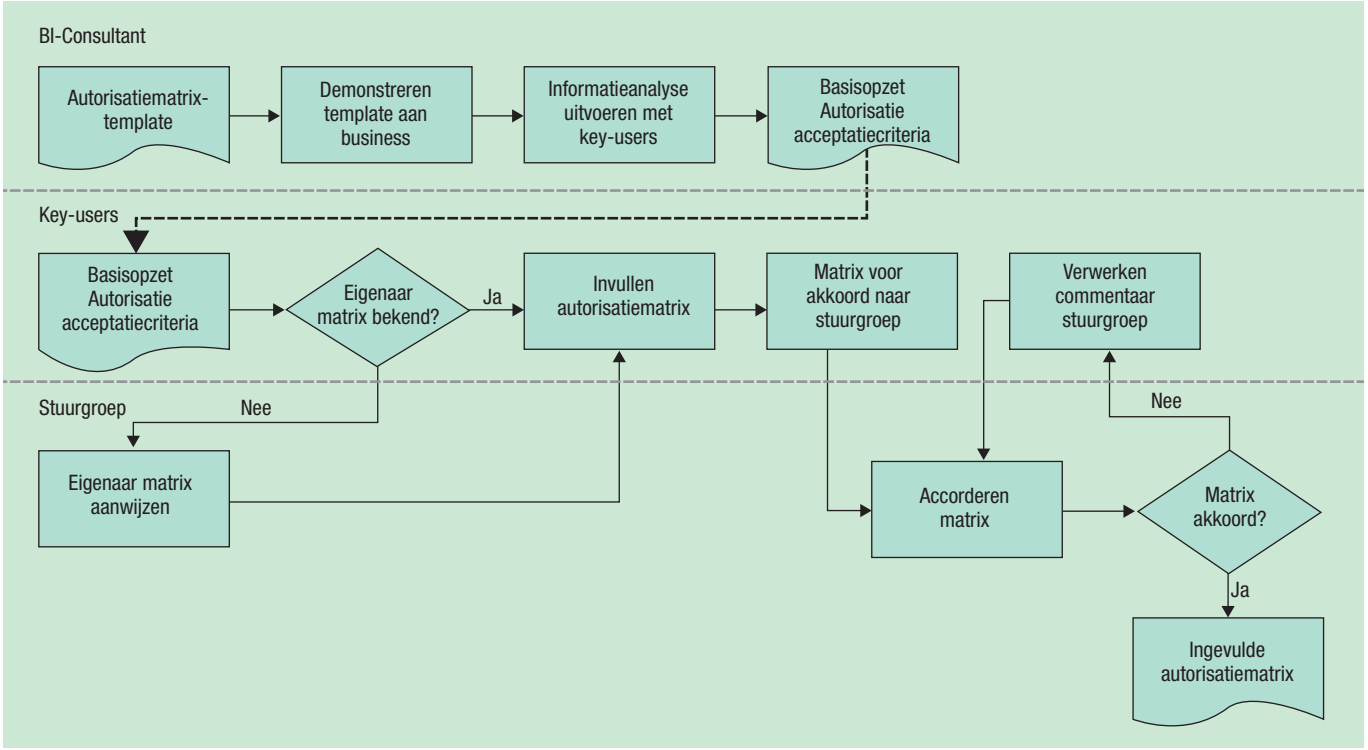
Voorafgaand aan de inrichting van de autorisatie van een BI-traject is het van belang dat de acceptatiecriteria helder zijn. Zonder duidelijke, door de klant goedgekeurde criteria, kan een project niet of nauwelijks succesvol worden afgesloten. Onduidelijk gedefinieerde criteria zorgen bij de gebruikersacceptatietest (GAT) voor een groot aantal issues en hebben daarmee een grote invloed op het project. Daarnaast is het belangrijk dat de autorisatieproducten een eigenaar hebben met (senior) businesskennis. Dit voorkomt lastige situaties in het geval van wijzigingen op één of meer van deze producten. Kortom, een duidelijke procedure om de autorisatiecriteria te bepalen en te beheren is onmisbaar. Een nadere toelichting over deze producten volgt hieronder.

Producten en proces

De volgende producten zijn van belang voor de autorisatie:
- Autorisatiematrix/Autorisatiematrices;
- Overzicht van de te autoriseren interfaces.

Autorisatiematrix.
Om tot een autorisatiematrix te komen kan er gebruik gemaakt worden van een template en een uitgangsdocument voor de autorisatie acceptatiecriteria. Deze documenten zorgen ervoor dat de kaders waarin de autorisatiecriteria worden opgesteld afgebakend zijn en kunnen uitstekend als handvat dienen om tot een volledige en voor alle key users eenduidige matrix te komen. Om een succesvolle matrix te kunnen opstellen is uiteraard commitment nodig vanuit alle aangestelde key users. Het proces om tot een autorisatiematrix te komen is in afbeelding 1 te zien.

Interfaces.
In het overzicht van de te autoriseren interfaces wordt aangegeven welke objecten in welke interfaces geautoriseerd moeten worden en wat bij initiatie de verwachte hiërarchiediepte in de betreffende autorisatie is. Dit overzicht kan er uitzien als in afbeelding 2. Uitgaande van de situatie in afbeelding 2, komt de configuratietabel er uit te zien zoals in afbeelding 3.
Vanuit deze configuratietabel kunnen de tabeldefinities worden bepaald voor de autorisatie-brontabellen. De DDL voor de tabel kan uiteraard met behulp van een SQL Script (Procedures) worden gegenereerd.
De autorisatie-brontabellen zijn benodigd om een doorvertaling te maken van de autorisatiematrix naar het laagste (business key) niveau. Een rol kan namelijk geautoriseerd worden op het



Afbeelding 1: Proces naar autorisatiematrix.

hoogste niveau (bijvoorbeeld holding in een organisatiedimensie); in de database moet echter wel bekend zijn welke business keys hier bijhoren. Er van uitgaande dat de tabel in afbeelding 3 correspondeert met de autorisatiematrix, zien de tabellen (één tabel per interface) er uit als in afbeelding 4, 5 en 6.

De tabellen in afbeelding 4 en 5 worden door middel van ETL gevuld vanuit de autorisatiematrix. De gebruiker-rollentabel in afbeelding 6 moet met een bepaald interval worden gesynchroniseerd, met bijvoorbeeld de Active directory of lokale Windows gebruikers; er kunnen immers mutaties plaatsvinden in de gebruikeraccounts. Voor de rapporteninterface geldt voor Microsoft dat de naam van de rapporten bijgehouden wordt in de Reporting Services catalog. Voor tools waarin de naam van de rapporten niet uit de catalog te extraheren is, moeten de hiërarchie en naam van de rapporten op een andere manier worden ingevoerd.

Voor de OLAP-cube autorisatie wordt de autorisatiematrix gekoppeld met de dimensietabel om de onderliggende business keys op te halen. Wanneer een dimensierecord gewijzigd wordt op het niveau waarop geautoriseerd wordt – bijvoorbeeld 'afdeling x' verandert in 'afdeling y' – dan moet dit tevens worden doorgevoerd in de autorisatiematrix. Voor de onderliggende niveaus wordt de autorisatie automatisch meegenomen. Een alternatief is om te autoriseren op codes of ID's, voorwaarde is dan wel dat deze aanwezig zijn.

De templates in afbeelding 7, 8 en 9 kunnen uitstekend gebruikt worden voor de autorisatiematrix. In het voorbeeld zijn deze ingericht op OLAP- en datamartniveau en rapportniveau.

Richtlijnen zijn:

- Probeer de differentiatie en daarmee het aantal verschillende rollen te beperken;
- Regel de autorisatie op een zo hoog mogelijk niveau in;
- Werk met rollen/groepen in plaats van specifieke gebruikers;
- Geef de rollen een duidelijk te herkennen naam en spreek een naamgevingsconventie af met Systeembeheer, zodat duidelijk herkenbaar is welke groepen voor het BI-systeem van toepassing zijn.

Best practices

In het eerste gedeelte van dit artikel zijn het proces en de technische verwerking van de autorisatiematrix beschreven. In het nu volgende deel worden twee best practices voor implementatie

Interface	Component	Aantal Hiërarchische Niveaus[1]
Rapportenportal	Rapporten	2
OLAP-Cube	Dimensie <naam>	4
	Dimensie <naam2>	3
	Dimensie <naam(n)>	n
DBMS	Database	1

1. Het maximum aantal niveaus dient als input voor de configuratietabel in de database. In de praktijk komt het voor dat een niveau wordt verwijderd of toegevoegd, vandaar dat het aan te bevelen is om rekening te houden met additionele niveaus (maximum aantal niveaus + 2).

Afbeelding 2: Tabel.

Interface	Niveaus
Rapportenportal	4
OLAP-Cube	6

Afbeelding 3: Configuratietabel.

CONGRES

HOLIDAY INN LEIDEN 5 NOVEMBER 2009

Rick van der Lans | Daniel Linstedt | Richard Hackathorn | Hans Lamboo

CONGRES DATAWAREHOUSING & BUSINESS INTELLIGENCE 2009

Vierde editie van dit succesvolle congres
5 november 2009

Met internationale topsprekers
Rick van der Lans, Daniel Linstedt en Richard Hackathorn

Uw dagvoorzitter is Hans Lamboo

WHAT'S ON THE EVENT HORIZON FOR BI/EDW?

BI AS A SERVICE – HYPE OF REALITEIT?

DATA WAREHOUSE APPLIANCES: ACHIEVING THE BUSINESS VALUE

HET DATA DELIVERY PLATFORM - EEN UPDATE

Datawarehousing & Business Intelligence is bestemd voor u!
Bent u direct of indirect betrokken bij het ontwerpen en ontwikkelen van datawarehouse-databases en het opzetten van business intelligence omgevingen? Dan mag u dit congres niet missen!

Abonneekorting en vroegboekkorting
Database Magazine-abonnees profiteren van korting. Indien u zich uiterlijk 5 weken voor het congres aanmeldt, profiteert u van 10% vroegboekkorting. Als u zich met meerdere personen van een bedrijf tegelijk aanmeldt profiteert u van korting die kan oplopen tot 30%. Zie de website voor de voorwaarden.

Kijk snel op www.dwbicongres.nl voor het complete programma!

Array SEMINARS

COMPUTABLE

Onder auspiciën van DB/M DATABASE MAGAZINE

Rol	Begindatum	Einddatum	Actief	Niv.1	Niv.2	Niv.3	Niv.4	Rapportnaam

Afbeelding 4: Tabel cfg.tbl_Rapportenportal.

Rol	Dimensie	Begindatum	Einddatum	Actief	Niv.1	Niv.2	Niv.3	Niv.4	Niv.5	Niv.6	Business key

Afbeelding 5: Tabel cfg.tbl_RolOLAP.

Rol	Gebruiker

Afbeelding 6: Tabel cfg.tbl_GebruikerOLAP.

van deze matrix in respectievelijk Analysis Services en Reporting Services uitgewerkt. De implementatie van autorisatie binnen de reporting services portal valt verder buiten de scope van dit artikel.

Best Practice: Implementatie autorisatie in Microsoft SQL Server Analysis services.

In SQL Server Analysis services maken we gebruik van de hiervoor beschreven autorisatietabellen. In de tabel cfg.tbl_RolOLAP zien we welke records terugkomen voor de rol 'Noord-Financiën', zie afbeelding 10.

Uit deze tabel kan worden afgelezen dat de autorisatie voor alle gebruikers met de rol 'Noord-financiën' nog geldig is. Alle business keys waarvoor zij geautoriseerd zijn, zijn tevens uit deze tabel af te lezen. De autorisatie is hier aangebracht op niveau drie, namelijk 'Financiën' en het onderliggende ETL-proces heeft door middel van een lookup de business keys uit de grootboekdimensie er bij gehaald. Het is op deze manier mogelijk om op een zestal niveaus autorisatie toe te kennen. De ETL realiseert de doorvertaling naar business key niveau.

In SQL Server Analysis services maken we handig gebruik van deze tabel. Het datamodel in afbeelding 11 van een fictieve financiële datamart wordt in deze best practice gebruikt als basis voor het toepassen van de autorisatie.

Uit de autorisatietabel is af te lezen dat de autorisatie toegepast moet worden op de grootboekdimensie. Om dit te realiseren in SSAS, moeten we een koppeltabel toevoegen. Deze koppeltabel bevat de gebruikers en business keys uit de te autoriseren dimensie. De gebruikersnamen komen uit de cfg.tbl_GebruikerOLAP tabel en de Grootboek_id's uit de cfg.tbl_RolOLAP tabel, want de autorisatie is bepaald op rolniveau en wordt doorvertaald naar gebruikersniveau. Indien autorisatie

Dimensie-1												
Niveau-1	**Niveau-2**	**Niveau-3**	**Niveau(N)**	Raad van Bestuur	Directeur Noord	Directeur Midden	Directeur West	Directeur Zuid	Noord - P&O	Noord - Financiën	Manager ICT	Noord - Financiële admin. Jun.
Holding	Bedrijf – Noord	Financiën	Vaste activa Kosten Resultaten									
		P&O	Opleidingen …									
		Productie										
	Bedrijf – Midden	Financiën	Vaste activa Kosten Resultaten									
	Bedrijf – Zuid	Financiën	…									
		P&O	…									
		Productie	…									

Afbeelding 7: OLAP-autorisatie Matrix 1.

Dimensie(N)												
Niveau-1	**Niveau-2**	**Niveau-3**	**Niveau(N)**	Raad van Bestuur	Directeur Noord	Directeur Midden	Directeur West	Directeur Zuid	Noord - P&O	Noord - Financiën	Manager ICT	Noord - Financiële admin. Jun.
…	…	…	…									

Afbeelding 8: OLAP-autorisatie Matrix 2.

Niveau-1	Niveau-2	Niveau(N)	Raad van Bestuur	Directeur	Noord - P&O	Noord - Financiën	Manager ICT	Noord - Financiële admin. Jun.
Financiële rapporten	Kosten vs. Opbrengsten	…						
	Kosten vs. Begroting	…						
	Kosten vs. Begroting vorige maand	…						
	…	…						
Personele rapporten	Begrote vs. Werkelijke fte	…						
	Medewerkers vs. Target	…						
	…	…						
Dashboard	…	…						

Afbeelding 9: Rapportautorisatie Matrix 3.

voor meerdere tabellen is geconfigureerd moet bij de toevoeging van de gebruikers- en rolnamen een filter toegepast worden op het dimensieattribuut. In ons voorbeeld resulteert dit in het volgende filter: [WHERE DIMENSIE="Grootboek"]. Het datamodel ziet er nu uit als in afbeelding 12.

Nu de gebruikers- en de, te autoriseren business keys bekend zijn in het model, kan er via een MDX-script autorisatie worden toegevoegd. In de praktijk werkt dit als volgt:

1. Gebruikers die gebruik gaan maken van de SSAS OLAP-cube, moeten worden toegevoegd aan de juiste Active Directory- of Lokale Windows gebruikersgroep;
2. Maak een nieuwe autorisatie-role aan (Roles -> New);
3. Vul bij de 'Allowed member set' in de 'dimension data – advanced' het volgende MDX-statement in:
   Exists([Grootboek].[Grootboek_id].Members, StrToMember("[GrootboekAutorisatieGebruiker]. [Gebruiker].[Login].&[" + UserName + "]"), "GrootboekAutorisatieGebruiker");
4. Enable Visual Totals. (Als dit niet aan staat wordt de autorisatie niet toegepast, want de GrootboekAutorisatieGebruiker tabel wordt alleen maar indirect benaderd en enable visual totals zorgt ervoor dat de autorisatie altijd over de gehele datasource view wordt toegepast).

De autorisatie binnen SSAS is nu gerealiseerd. Het MDX statement controleert op basis van de Windows credentials (Active directory of Windows local), welke data de gebruiker mag inzien. De overige data worden er uitgefilterd. De autorisatie wordt doorgegeven aan alle tools die op basis van de Windows credentials gebruik maken van de SSAS OLAP-cube (bijvoorbeeld de SSMS MDX query tool of de SSRS Rapportage tool). Het openen van een SSRS-rapport dat gebaseerd is op de OLAP-cube wordt bij aanvraag geautoriseerd conform de gedefinieerde rol-autorisatie.

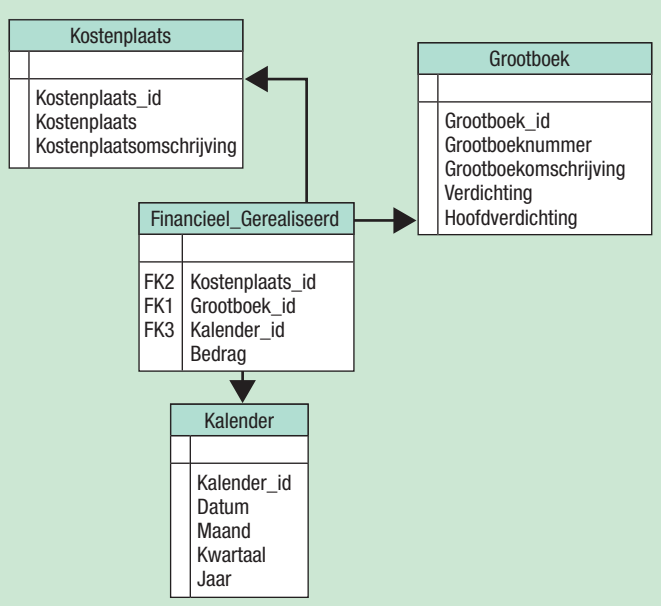
De autorisatie is nu ingeregeld voor de dimensie 'Grootboek'. Wanneer er over meerdere dimensies geautoriseerd moet worden kan men de voorgaande stappen herhalen en een tabel toevoegen in de datasource view voor de andere dimensie. Opmerking: Het is helaas (nog) niet mogelijk om SSAS direct op rolniveau te laten autoriseren, vandaar dat de autorisatie op rolniveau is bepaald, maar op gebruikersniveau is ingeregeld.

Best Practice: Implementatie autorisatie in Microsoft SQL Server Report Models.

De voorgaande best practice was gerealiseerd in SSAS. Nu hoeft niet elk DWH per definitie een OLAP-cube te bevatten. Het komt regelmatig voor dat alleen een datamart beschikbaar is en dat een klant met Reporting Services (SSRS) de datamart wil benaderen. Ook daar gelden dan weer dezelfde autorisatiespecificaties voor als we in de vorige best practice hebben uitgewerkt. Deze specificaties zijn te realiseren door middel van Report Models. De Report Models kunnen vervolgens gebruikt worden als datasource in Reporting Services. Daarnaast is het ook mogelijk om ad hoc rapporten te bouwen op basis van Report Models, met behulp van de Report Builder. Microsoft heeft voor SQL Server 2008 onlangs Report Builder 2.0 uitgebracht, die een groot aantal nieuwe features bevat en in tegenstelling tot SQL 2005, uitstekend voor ad hoc doeleinden te gebruiken is.
Report models kunnen worden gebaseerd op een datamart of SSAS-OLAP-cube. In onze best practice maken we gebruik van de datamart.

Rol	Dimensie	Begindatum	Einddatum	Actief	Niv.1	Niv.2	Niv.3	Niv.4	Niv.5	Niv.6	Business key
Noord - Financiën	Grootboek	01-07-2009	NULL	1	NULL	NULL	Financiën	NULL	NULL	NULL	411029
Noord - Financiën	Grootboek	01-07-2009	NULL	1	NULL	NULL	Financiën	NULL	NULL	NULL	411030
Noord - Financiën	Grootboek	01-07-2009	NULL	1	NULL	NULL	Financiën	NULL	NULL	NULL	411031
Noord - Financiën	Grootboek	01-07-2009	NULL	1	NULL	NULL	Financiën	NULL	NULL	NULL	[etc….]

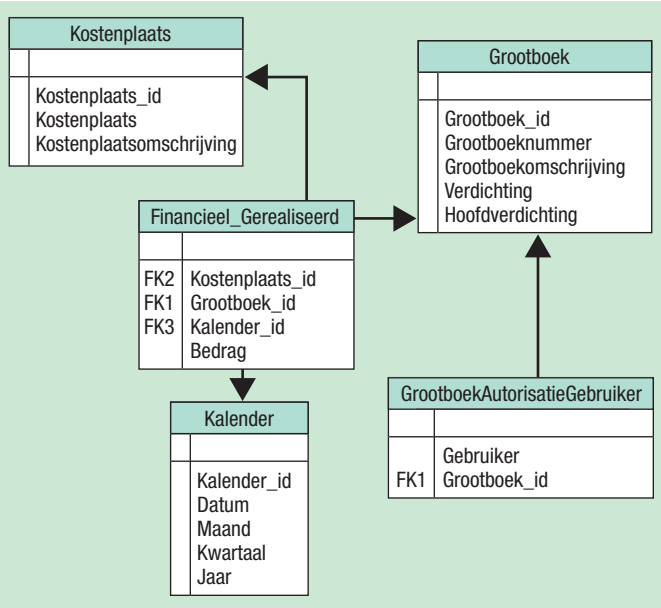
Afbeelding 10: Rol 'Noord-Financiën'.



Afbeelding 11: Datamodel.

Implementeren autorisatie in Report Models

Met behulp van de Report Model designer in Visual Studio kunnen autorisatiefilters worden gedefinieerd. De designer werkt met datasource views, net als SSAS. De datasource view voor de fictieve financiële datamart met autorisatie op de Grootboekdimensie is daarom ook gelijk aan die van de vorige best practice en wordt hier niet meer beschreven. De methode van autoriseren werkt echter wel anders. In de Report Models wordt er gebruik gemaakt van een autorisatiefilter en een 'inheritence' property.
Als eerste stap na het bouwen van de datasource view moet een gebruikersnaam-autorisatiefilter (security filter in de designer) worden toegevoegd. Voeg een nieuwe 'entity' toe die de naam van de autorisatiefilter heeft. Geef vervolgens de 'binding' tussen deze filter en de brontabel aan. Dit is de gelijknamige tabel met de gebruikersnamen en te autoriseren business keys (GrootboekAutorisatieGebruiker).
De volgende stap is het toevoegen van de 'source fields' Gebruiker en Grootboek_id. Daarna kunnen de filters worden toegevoegd binnen deze entiteit door in plaats van 'new Source Field', 'Filter' te selecteren. Er zijn minimaal twee filters, namelijk één om de gebruiker te filteren en één om de bijbehorende dimensie (Grootboek) keys te filteren.
Nu moet er nog door middel van overerving 'inheritence' aangegeven worden dat de gebruikersnaam-autorisatiefilter op de feitentabel (Financieel gerealiseerd) en de grootboekfilter op de dimensie (Grootboek) van toepassing is. Dit is te realiseren via de inheritence property's.
Geef nu de gebruikersnaam filter als default security filter property voor de feitentabel aan. Voor de Grootboek dimensie is de grootboek_id-filter de default security filter.
In de filter expression (property van het filterattribuut) kan er voor de gebruikersnaam het volgende ingevuld worden:
LOWER(Gebruiker) = LOWER(GETUSERID()).
Voor de autorisatiefilter op de grootboekdimensie werkt dit op dezelfde wijze, namelijk Grootboek_id = Grootboek_id.
De designer houdt in het onderliggende XML-script bij uit welke tabel dit attribuut afkomstig is.
Beperking: Als een gebruiker in twee rollen zit levert dit een verdubbeling van rijen op. Om dit te voorkomen kan er een beleid gehanteerd worden van maximaal één Rol per gebruiker (uiteraard wel meerdere gebruikers in één rol). Mocht dit niet mogelijk zijn dan kan er in een additionele stap een samenvoeging van deze groepen geprogrammeerd worden. Dit is niet de meest elegante oplossing maar zorgt er wel voor dat er geen verdubbelingen ontstaan.



Afbeelding 12: Aangepast datamodel.

Conclusie

Autorisatie is en blijft complexe materie. Indien er gebruik gemaakt wordt van stringente procedures en een stukje techniek is de kans op succes enorm vergroot. Het is belangrijk dat de complexiteit van de autorisatie naar een minimum wordt teruggebracht en dat er consensus wordt bereikt over deze eisen. Het dynamische karakter van de autorisatiecriteria en onderliggende data brengt bij het gebruik van de standaardtools een enorme hoeveelheid werk, en daarmee meer kans op fouten, voor beheer met zich mee. Met behulp van de besproken procedures en technieken kan hiermee ook een flinke besparing worden bereikt.
Voor projecten en/of organisaties waar een zeer beperkte hoeveelheid autorisatiecriteria is opgesteld en de onderliggende data grotendeels van een statisch karakter zijn, heeft de in dit artikel beschreven methode geen toegevoegde waarde. Voor projecten en/of organisaties waar één van de hiervoor genoemde eigenschappen wel speelt, heeft het wel degelijk een toegevoegde waarde.

Ing. **Vincent Wylenzek** is Business Intelligence Consultant bij Ordina.