VIII. AUTORISATIEMANAGER

VIII.1. INLEIDING

In organisaties zullen dikwijls diverse afdelingen met elk één of meer medewerkers gebruik willen maken van één of meer databases. Het kan echter wenselijk zijn dat niet elke medewerker alle denkbare operaties op alle gegevens mag uitvoeren. De filiaalhouder van een winkel zal vermoedelijk meer operaties mogen verrichten op de database-inhoud dan een verkoopster van deze winkel.

Evenzo zal in een bedrijf de salarisadministratie-afdeling geen inzage mogen hebben in de medische gegevens van personeelsleden. Voor een bedrijfsgeneeskundige dienst en zeker voor de medisch deskundigen van deze dienst moeten medische gegevens wel toegankelijk zijn. Voor alle medewerkers van een bedrijfsgeneeskundige dienst zal gewenst zijn dat ze geen toegang hebben tot salarisgegevens van medewerkers.

Kortom het is uit een oogpunt van gegevensbescherming en van privacy wenselijk dat een DBMS de mogelijkheid biedt om aan verschillende gebruikers of **groepen** verschillende rechten te verlenen.

Rechten van toegang kunnen betrekking hebben op groepen, individuele gebruikers, databases, samengestelde typen en attributen. Rechten op operaties kunnen betreffen: opvragen, toevoegen, wijzigen en verwijderen van bepaalde gegevens.

Tevens moet gezorgd worden dat een gebruiker zijn rechten nooit kan overschrijden. Verder is het wenselijk dat een gebruiker alleen via z’n persoonlijke "log-in" - gegevens toegang krijgt tot het DBMS.

De geschetste wensen hebben geleid tot een onderverdeling van het autorisatiegedeelte in drie hoofdmodules: de herkenner, de arbiter en de manager.

De herkenner

Deze module heeft tot taak gebruikers te identificeren bij binnentreden van het DBMS. Zodra een gebruiker als gerechtigde DBMS-gebruiker is herkend dient zijn profiel (de verzameling van rechten) bepaald te worden.

Het DBMS leidt uit de inloggegevens af tot welke groep de gebruiker behoort en welke rechten deze gebruiker heeft. Inloggen gebeurt door achtereenvolgens een gebruikersnaam en een password in te toetsen.

De arbiter

Deze module dient te zorgen dat een gebruiker nooit een operatie kan uitvoeren die niet toegestaan is gezien het vastgelegde profiel van rechten van deze gebruiker.

De manager

Met deze module wordt het mogelijk gemaakt dat het profiel van rechten van gebruikers (groep en/of personen) op een gebruiksvriendelijke wijze wordt vastgelegd. Naast rechten op toegang en/of manipulatie bestaat er ook een mogelijkheid om rechten door te geven, bijvoorbeeld een groep kan rechten doorgeven naar een subgroep. Verder is het mogelijk rechten te wijzigen.

Voor de gebruiker is alleen de manager een zichtbaar deel van het DBMS. Werking en gebruik van de autorisatie manager zullen worden toegelicht vanaf paragraaf VIII.2.

VIII.2. CONCEPTEN IN DE AUTORISATIEMANAGER

In de inleiding was sprake van afdelingen (groepen) en gebruikers. Een groep of afdeling wordt opgevat als een verzameling van gelijksoortige en gelijkberechtigde gebruikers. Dikwijls zal een groep (afdeling) één of meer subgroepen (onderafdelingen) hebben.

Binnen het XPLAIN DBMS is gekozen voor twee uitgangspunten ten aanzien van groepen:

1. **Elke groep heeft een profiel van rechten.**
   De gebruikers krijgen het profiel van de groep waartoe ze behoren. De gebruiker moet in principe deel uitmaken van een bepaalde groep.

2. **De groepen zijn hiërarchisch geordend.**
   De rechten van een groep kunnen nooit minder zijn dan die van de bijbehorende subgroepen. Anders gezegd: een groep kan aan een subgroep **hoogstens** dezelfde rechten doorgeven als ze zelf heeft.

Het profiel van rechten van een groep (en dus ook de leden van een groep) heeft betrekking op de volgende aspecten:

1. **Databases.**
   Een groep heeft wel of niet toegang tot een bepaalde database. Indien een bepaalde database niet toegankelijk is voor een bepaalde groep dan is er natuurlijk geen enkele mogelijkheid meer nodig om de toegang tot deelaspecten (typen, attributen, operaties, panels en queries) van de uitgesloten database te regelen.
   Indien een groep geen toegang heeft tot een bepaalde database, dan wordt deze database ook niet getoond in het database-selectie scherm.

2. Samengestelde typen en attributen.
Voor groepen die tot een bepaalde database toegelaten zijn kan worden vastgelegd welke operaties toegestaan zijn op typen en attributen.

We maken een onderscheid naar drie soorten groepen:

1. De DBA-groep.
Dit is de groep met dezelfde rechten als de database administrateur (DBA). De DBA-groep mag alles doen wat mogelijk is binnen het DBMS. Dit betreft alle databases, data-definitie, alle typen, alle attributen en alle operaties. De DBA-groep heeft ook het recht om rechten door te geven.

2. Groepen met doorgeefrecht.
Deze groepen mogen hoogstens hun eigen rechten doorgeven aan hun subgroepen.

3. Groepen zonder doorgeefrecht.
Deze groepen mogen hun profiel van rechten niet overdragen en mogen ook geen subgroepen hebben.

Gebruikers kunnen vervolgens onderscheiden worden via de groep waartoe ze behoren en de functie die ze binnen deze groep vervullen:

1. Een DBA-gebruiker.
Dit is een gebruiker die tot de DBA-groep behoort en dus alles mag doen wat mogelijk is binnen het DBMS, **inclusief datadefinitie**.

Alle leden van de DBA-groep mogen ook rechten doorgeven aan een subgroep.

2. Een niet-DBA-gebruiker.
Deze gebruiker mag geen datadefinitie doen. De toegestane datamanipulatie hangt af van het profiel van rechten van deze gebruiker.

De rechten van de niet-DBA-gebruiker worden bepaald door:
- de groep waartoe de gebruiker behoort en
- de rol van deze gebruiker binnen de groep (wel of niet groepshoofd).

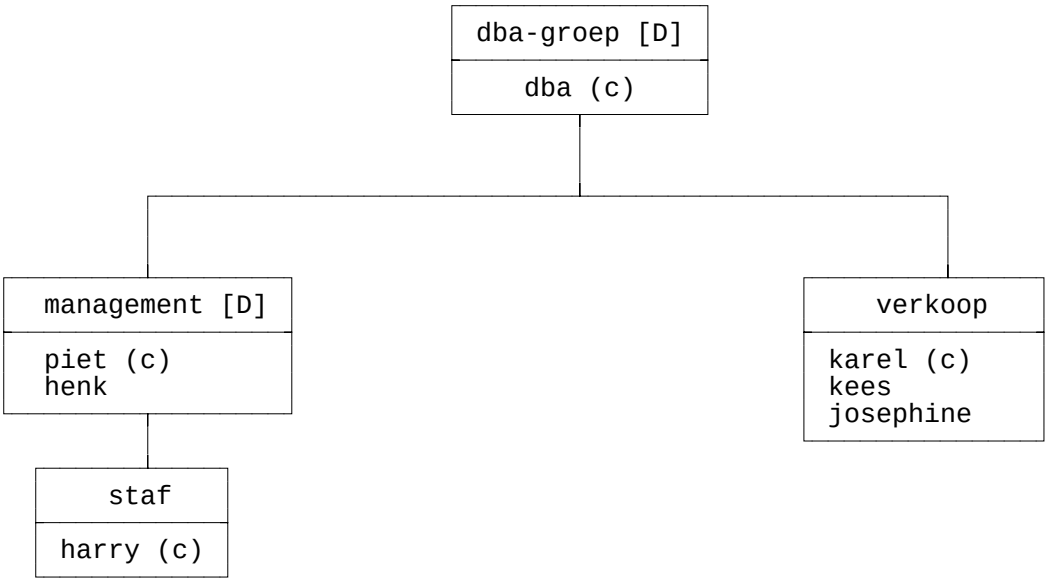
We kunnen binnen de niet-DBA-gebruikers de volgende gebruikers onderscheiden:
a. Een groepshoofd van een groep **met** doorgeefrechten.
Dit groepshoofd mag binnen de autorisatie manager elke operatie doen. D.w.z. dat dit groepshoofd ook rechten mag doorgeven aan een subgroep.
b. Een groepshoofd van een groep **zonder** doorgeefrechten.
Dit groepshoofd mag binnen de autorisatie manager alleen operaties doen die betrekking hebben op de gebruikers van de **eigen** groep. Dit groepshoofd mag geen rechten doorgeven aan een subgroep.

c. Een niet-groepshoofd.
Deze gebruiker mag alleen z’n eigen password wijzigen; dus mag geen rechten doorgeven aan een subgroep.

De genoemde classificatie van verschillende gebruikersrechten wordt toegelicht met de hierna volgende fictieve organisatie.

Van elke groep wordt genoemd:
- de groepsnaam (bovenaan)
- de leden van de groep
- een groepshoofd, met (c) aangeduid
- doorgeefrecht, met [D] aangeduid

In de volgende figuur is sprake van de groepen: "dba-groep", "management" en "verkoop". De "staf" is een subgroep van "management".



De gebruikers van deze fictieve organisatie zijn als volgt te classificeren:

DBA-gebruiker: dba

Niet-DBA-gebruikers:
Chef van groep met doorgeefrecht: piet
Chef van groep zonder doorgeefrecht: karel, harry
Geen chef: henk, kees, josephine

Tijdens het manipuleren van rechten en het manipuleren van groepen en gebruikers kunnen groepen in drie hoedanigheden optreden:

1. Als groep die nergens bij betrokken is.

Deze groep is niet betrokken bij manipulaties, niet als brongroep en niet als doelgroep. Leden van zo'n groep mogen het DBMS niet gebruiken.

2. Als brongroep.

Dit is de groep van waaruit gebruikers en subgroepen gemanipuleerd kunnen worden. Vanuit deze groep worden rechten verleend of doorgegeven. Met manipulatie wordt nu bedoeld de definitie van groepsleden, eventuele subgroepen en eventuele rechten.

3. Als doelgroep.

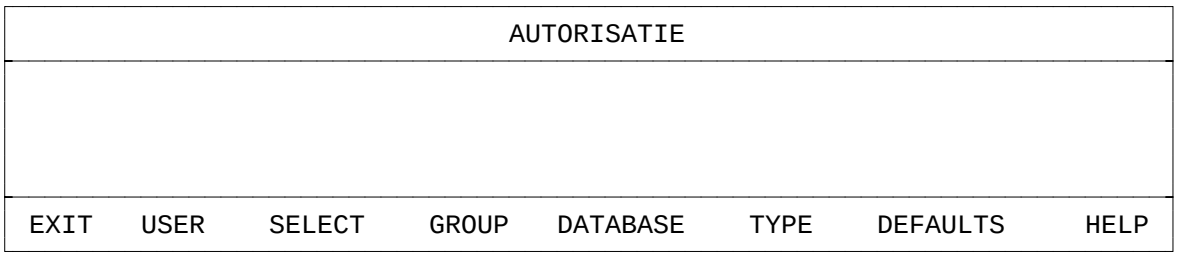
Deze groep speelt alleen een rol bij de manipulatie van rechten. Het is de groep waarvan de rechten worden gemanipuleerd vanuit de brongroep. De rechten kunnen aan de doelgroep verleend worden of kunnen worden ingetrokken.

Na deze introductie van een aantal nieuwe begrippen kan worden overgegaan tot de volgende paragraaf VIII.3. Hierin wordt het gebruik van de autorisatie manager beschreven.

VIII.3. GEBRUIK VAN DE AUTORISATIEMANAGER

Om de autorisatie manager te kunnen gebruiken dient vanuit het **hoofdmenu** de optie **ACCESS** gekozen te worden. Na deze keuze ziet men dan het autorisatiemenu op het scherm staan met in het info-gedeelte de nu mogelijke opties. **Indien nog geen groepen gedefinieerd zijn staan naast EXIT en HELP alleen de opties USER en GROUP ter beschikking (van de dba-groep).** Nadat een nieuwe groep gedefinieerd is, staan ook de opties SELECT, DATABASE en TYPE ter beschikking.

Het autorisatiemenu ziet er ongeveer als volgt uit nadat minstens één groep onder de dba-groep vastgelegd is:



VIII.3.1. USER: manipulaties op gebruikersrechten

Via de optie USER is het mogelijk om manipulaties te doen op gebruikers die behoren tot de brongroep. Overigens kunnen groepen gemanipuleerd worden via de optie SELECT.

De mogelijke manipulaties op gebruikers zijn:

INSERT
Hiermee kan men een gebruiker toevoegen aan de brongroep. Achtereenvolgens worden dan gevraagd: gebruikersnaam, password (minstens twee keer), of de gebruiker groepshoofd is (ja/nee) en of de gebruiker inderdaad toegevoegd moet worden. Binnen een bepaalde groep moet een gebruikersnaam uniek zijn. Het password wordt net zo lang gevraagd totdat twee keer direct opeenvolgend een zelfde password is ingetoetst. Er is een maximum aan het aantal gebruikers per groep.

DELETE
Hiermee kan men een gebruiker uit de brongroep verwijderen. Men dient de te verwijderen gebruiker aan te wijzen met de pijltjestoetsen.
Hierna dient men de gewenste verwijdering nogmaals te bevestigen. Een gebruiker wordt niet toegestaan zich zelf te verwijderen. Indien een gebruiker dit toch probeert wordt dit door het DBMS geweigerd met een passende melding. Overigens is de optie DELETE (gebruiker) alleen van toepassing indien er minstens één gebruiker in de brongroep gedefinieerd is.

CHANGE
Via deze optie kan men binnen de brongroep de gegevens van een gebruiker wijzigen. Allereerst dient men de te wijzigen gebruiker te selecteren. We kunnen hierbij twee gevallen onderscheiden:

1. Het betreft de gebruiker zelf. Dan is alleen het wijzigen van het password mogelijk. Eerst wordt het oude password gevraagd, daarna wordt steeds het nieuwe password gevraagd totdat twee keer opeenvolgend het zelfde nieuwe password is ingetoetst.
2. Het betreft een andere gebruiker. Nu kunnen alle gegevens van deze andere gebruiker worden gewijzigd. Voor het password geldt dat bij direct intoetsen van <Return> het oude password gehandhaafd blijft. Een nieuw password dient op de eerder aangegeven wijze twee keer achtereen ingetoetst te worden.

De optie CHANGE is alleen van toepassing indien er minstens één gebruiker bij de brongroep is gedefinieerd.

LIST
Met deze optie kan men een overzicht krijgen van alle gebruikers van de brongroep.

PRINT
Met deze optie kan men de lijst van gebruikers van de brongroep afdrukken.

PAGING
Indien niet alle gebruikers op één scherm passen, dan kan men via deze optie vooruit of achteruit "bladeren" in de lijst van gebruikers van de brongroep.

VIII.3.2. SELECT: wijzigen van de brongroep

Via de optie SELECT is het mogelijk de brongroep te wijzigen. De brongroep is de groep van waaruit geopereerd wordt. Dit betekent voor de overige opties:

USER:	de groep waarbij de gebruikers gemanipuleerd worden.
GROUP:	de groep waarbij de subgroepen gemanipuleerd worden.
DATABASE:	de groep van waaruit autorisatie op databases verleend wordt.
TYPE:	de groep van waaruit autorisaties op typen en attributen verleend worden.

Het aanwijzen van de brongroep gebeurt door het omhoog en omlaag bewegen in een hiërarchisch opgebouwde boom van groepen.

Na SELECT gekozen te hebben zal men na eerdere definitie van twee groepen vanuit de dba-groep ongeveer het volgende scherm zien:

```
                        Selecteren brongroep
─────────────────────────────────────────────────────────────────────────────

Brongroep is dba

Toegankelijke groepen zijn:

salarisadmin    boekhouding

─────────────────────────────────────────────────────────────────────────────
EXIT          DOWN                                                    HELP
```

Niet alle opties staan op het scherm: zo ontbreekt bijvoorbeeld UP omdat deze optie niet zinvol is in de aangegeven situatie. Immers de DBA-groep staat bovenaan in de hiërarchie. Hierna volgt een toelichting op de mogelijke opties betreffende het selecteren van de brongroep.

DOWN
Via deze optie kan men omlaag bewegen in de groepenboom.

Men krijgt de gelegenheid om met de pijltjestoetsen de gewenste groep te selecteren. Deze wordt dan invers op het scherm getoond. De keuze wordt bevestigd door op <Return> te drukken.

Deze optie DOWN is alleen beschikbaar als er onder de brongroep (de groep van de gebruiker) nog minstens één subgroep bestaat.

UP
Via deze optie kan men omhoog bewegen in de groepenboom.

Keuze en bevestiging verlopen zoals bij DOWN is aangegeven. Het is niet mogelijk hoger

in de groepenboom te komen dan de groep waartoe de gebruiker behoort, d.w.z. de brongroep.

FORWARD / BACKWARD
Indien niet alle subgroepen die onder een groep vallen op één scherm passen, dan kan men met de opties FORWARD of BACKWARD "bladeren" in de lijst van subgroepen.

Overigens zal men automatisch het menu voor het selecteren van de brongroep binnentreden als men vanuit het autorisatiemenu gekozen heeft voor één van de opties DATABASE of TYPE.

Overigens wordt dan een scherm getoond met "Selecteren doelgroep" in de kop. Er wordt dus niet meer van brongroep gesproken.

VIII.3.3. GROUP: manipulaties op subgroepen

Via de optie GROUP kan men manipulaties verrichten op subgroepen van de brongroep. (Zie ook de optie SELECT).

De mogelijke groepsmanipulaties zijn INSERT, DELETE, CHANGE, LIST, PRINT en eventueel PAGING. De mogelijkheden van de manipulatie op subgroepen staan ook op het scherm en worden hierna toegelicht:

INSERT
Met de optie INSERT kan men een subgroep toevoegen aan de brongroep. Het systeem leidt uit de inloggegevens van een gebruiker af welke de brongroep is.

Achtereenvolgens worden gevraagd : naam van de subgroep, of de groep doorgeefrecht heeft en of de subgroep inderdaad toegevoegd moet worden. De naam van een (sub)groep dient uniek te zijn. Er is een maximum aan het aantal subgroepen per groep.

DELETE
Met de optie DELETE kan een subgroep van de brongroep verwijderd worden. Men dient de te verwijderen subgroep te selecteren met de pijltjestoetsen. Vervolgens dient men de verwijdering al dan niet te bevestigen. Deze optie DELETE is alleen van toepassing als er minstens één subgroep bij de brongroep bestaat. Indien de betreffende subgroep echter zelf een subgroep onder zich heeft dan wordt de aangewezen subgroep niet verwijderd.

CHANGE
Met de optie CHANGE kan men vanuit de brongroep de gegevens van een subgroep wijzigen. Eerst dient men met de pijltjestoetsen de betreffende subgroep te selecteren. Deze optie CHANGE is alleen van toepassing als er minstens één subgroep bij de brongroep bestaat.

LIST
Met de optie LIST krijgt men een overzicht van subgroepen van de brongroep. Per subgroep

wordt o.a. vermeld wel of geen doorgeefrecht.

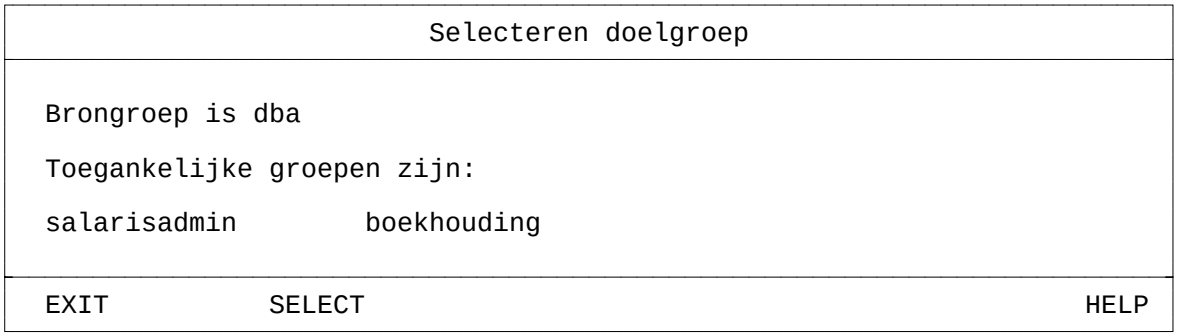
PRINT
Met de optie PRINT krijgt men een afdruk van het overzicht van subgroepen van de brongroep.

PAGING
Indien er meer subgroepen zijn dan op het scherm geplaatst kunnen worden, kan men de optie PAGING gebruiken om door de subgroepen te bladeren. FORWARD (vooruit bladeren) en BACKWARD (terug bladeren) zijn nu de beschikbare opties.

VIII.3.4. DATABASE: manipulatie op databases

Met behulp van de optie DATABASE kunnen manipulaties gedaan worden op databases. Aangezien deze manipulaties gedaan moeten worden vanuit een bepaalde groep dient men eerst de doelgroep te selecteren.

Men krijgt eerst het scherm te zien met de brongroep en de eventuele hiervan afhankelijke subgroepen. Dit scherm ziet er bijvoorbeeld zo uit voor de DBA-groep:



Men dient in deze fase eerst de doelgroep te kiezen. Dit geldt ook indien uw eigen brongroep een andere is dan de dba-groep. In deze fase zijn de volgende opties mogelijk, hoewel ze niet altijd nodig zijn en dan ook niet zichtbaar zijn:

SELECT
Via deze optie kan een doelgroep gekozen worden. Dit gebeurt weer door aanwijzen van de gewenste doelgroep met de pijltjestoetsen gevolgd door <Return>. Bevindt men zich in de verkeerde brongroep dan dient men via EXIT terug te gaan naar het autorisatiemenu en dan daar via SELECT een andere brongroep te kiezen.

FORWARD
Hiermee kan een bladzijde vooruit gebladerd worden. Deze optie is alleen van toepassing als niet alle subgroepen op één scherm passen en men zich niet op de laatste bladzijde bevindt.

BACKWARD
Hiermee kan een bladzijde achteruit gebladerd worden. Deze optie is alleen van toepassing als niet alle subgroepen op één scherm passen en men zich niet op de eerste bladzijde bevindt.

Nadat in de aangegeven voorbeeldsituatie vanuit de brongroep de groep "salarisadmin" is aangewezen als doelgroep kan men een volgende scherm te zien krijgen (zie volgnde pagina).

Aangezien voor de doelgroep "salarisadmin" geen databases zichtbaar of toegankelijk zijn, zijn niet alle mogelijke opties in deze fase beschikbaar. Zoals eerder al toegelicht kan men vanuit de brongroep niet meer rechten doorgeven dan men zelf heeft, zodat hier voor de gekozen doelgroep hoogstens de getoonde vier databases toegankelijk gemaakt kunnen worden. In principe zijn de volgende mogelijkheden beschikbaar:

```
                    Autorisatie op databases
─────────────────────────────────────────────────────────────────────

Zichtbare databases voor brongroep dba zijn:

proef           burgerlijke stand       speciaal
fabrieksituatie

Bij doelgroep salarisadmin zijn geen databases zichtbaar.

─────────────────────────────────────────────────────────────────────
EXIT  GRANT                    GRALL          PRINT          HELP
```

GRANT
De optie GRANT maakt het mogelijk toegang te verlenen tot een nog aan te wijzen database. Hierbij geldt dan natuurlijk de beperking tot de eerder gekozen doelgroep. Wenst men voor de betreffende doelgroep meerdere databases toegankelijk te maken dan dient men herhaalde keren deze optie GRANT te kiezen.

In deze fase (na GRANT) dient men weer m.b.v. de pijltjestoetsen en <Return> de toegankelijk te maken database te selecteren.

De optie GRANT is niet zichtbaar als de gekozen doelgroep reeds toegangsrecht heeft tot alle databases die voor de brongroep toegankelijk zijn.

REVOKE
Met de optie REVOKE is het mogelijk voor een gekozen doelgroep het toegangsrecht tot een database in te trekken. Men dient met pijltjestoetsen en <Return> de betreffende database te selecteren.

De optie REVOKE is vanzelfsprekend niet zichtbaar als de gekozen doelgroep geen enkele database mag gebruiken. Overigens wordt de opdracht REVOKE databasetoegang niet uitgevoerd als het toegangsrecht voor de geselecteerde database reeds was doorgegeven aan

een subgroep van de gekozen doelgroep. Dit houdt verband met de hiërarchische structuur van het profiel van rechten.

GRALL
De optie GRALL (GRANT ALL) maakt het mogelijk om met één enkele opdracht **alle** database toegangsrechten van de brongroep door te geven aan de eerder geselecteerde doelgroep.

De optie GRALL is niet zichtbaar als alle database-toegangsrechten reeds doorgegeven zijn aan de betreffende doelgroep.

REVALL
De betekenis van REVALL is "REVOKE ALL", oftewel **alle** database-toegangsrechten van de doelgroep worden met één opdracht ingetrokken.

De opdracht REVALL wordt niet uitgevoerd als de doelgroep reeds een database-toegangsrecht aan een subgroep verleend heeft. In principe is de optie REVALL beschikbaar zolang de doelgroep nog minstens één database mag gebruiken.

PRINT
Met de optie PRINT kan men een overzicht afdrukken van de databases die toegankelijk zijn voor de doelgroep.

VIII.3.5. TYPE: manipulaties op typen/attributen

Vanuit het autorisatiemenu kan men tenslotte ook nog de optie TYPE selecteren. Hiermee is het mogelijk rechten betreffende manipulatie op types en attributen vast te leggen voor een bepaalde groep. Na voor TYPE gekozen te hebben krijgen we weer het al eerder beschreven scherm (zie de optie DATABASE) te zien dat aangeeft de brongroep (afgeleid uit de inlog-gegevens van de gebruiker) en de bijbehorende subgroepen. Men dient dan eerst op de bekende wijze (pijltjestoetsen gevolgd door <Return>) de doelgroep te selecteren uit de subgroepen.

Overigens kan het voorkomen dat men naar een andere brongroep wil gaan; men dient dan terug te keren naar het autorisatiemenu (via EXIT of <PF1>) en vervolgens moet men de optie SELECT kiezen, etc.

De beschikbare commando’s bij het selecteren van de doelgroep (SELECT, BACKWARD, FORWARD) zijn reeds bij de behandeling van de optie DATABASE in de vorige paragraaf toegelicht.

We hanteren nog steeds hetzelfde voorbeeld als gebruikt in deze vorige paragraaf.
Nadat "salarisadmin" geselecteerd is als doelgroep krijgen we ongeveer het volgende scherm te zien:

```
Toegankelijke databases voor brongroep dba zijn:

proef              burgerlijke stand          speciaal
fabrieksituatie

Bij doelgroep salarisadmin zijn geen databases zichtbaar.

De doelgroep kent GEEN zichtbare databases                  RETURN
```

In de gegeven situatie wordt nu een wijziging aangebracht door via <PF1> terug te keren naar het autorisatiemenu. Daar wordt DATABASE gekozen en vervolgens wordt de opdracht GRALL gegeven voor de doelgroep "salarisadmin". Vervolgens keren we via de opties TYPE en SELECT terug. Het scherm ziet er dan als volgt uit:

```
                        Selecteer database

Zichtbare databases voor brongroep dba zijn:

proef                  burgerlijkestand                speciaal
fabrieksituatie

Bij doelgroep salarisadmin zijn geen databases zichtbaar.

EXIT         SELECT                                          HELP
```

Nu dient de optie SELECT gekozen te worden. Vervolgens selecteert men met de pijltjestoetsen en <Return> de gewenste database. Gekozen is voor de database "proef". We krijgen dan ongeveer te zien:

```
              Autorisatie voor database proef (typen)

Brongroep is dba:                    Doelgroep salarisadmin heeft
                                     geen toegankelijke typen.

persoon           gid
inkomen           gid
miljonair         gid

EXIT         GRANT         GRALL          LIST        PRINT      HELP
```

In deze situatie zijn alleen de zinvolle opties zichtbaar. Alle mogelijke opties (GRANT, REVOKE, GRALL, REVALL, LIST, PRINT, PAGING) worden hierna in aparte paragrafen toegelicht. "gid" betekent: get-, insert-, delete- bevoegdheid.

VIII.3.5.1. GRANT (rechten verlenen op typen)

Via de optie GRANT kan men rechten doorgeven aan de doelgroep die betrekking hebben op de typen van de gekozen database (hier "proef"). We onderscheiden de permissies GET, INSERT en DELETE. Na GRANT gekozen te hebben zien we het volgende scherm, waaruit men het gewenste type moet selecteren:

```
            Autorisatie voor database proef (typen) GRANT
 Brongroep dba:                          Doelgroep salarisadmin heeft
                                         geen toegankelijke typen.
 persoon             gid       {persoon: invers getoond}
 inkomen             gid
 miljonair           gid
 EXIT        GRANT          GRALL          LIST        PRINT      HELP
```

Na selectie van het type "persoon" zien we ongeveer het volgende scherm met een **deel** van de mogelijke opties:

```
           Autorisatie voor database proef (typen ) GRANT
 Brongroep dba:                        Doelgroep salarisadmin:
 persoon                               persoon
 Permissie(s): GET, INSERT, DELETE     Permissie(s):---
 EXIT         GET          INSERT        DELETE                  HELP
```

- Met **GET** wordt de get-permissie doorgegeven aan de doelgroep v.w.b. het eerder geselecteerde type.

- Met **INSERT** wordt de insert-permissie doorgegeven.
  Overigens wordt automatisch ook de get-permissie doorgegeven indien deze nog niet was verleend.

- Met **DELETE** wordt de delete-permissie doorgegeven.
  Verder wordt ook de get-permissie verleend, althans indien de get-permissie nog niet was verleend.

Overigens zijn er nog twee opties mogelijk die niet altijd zinvol zijn:

UNDO
Met de optie UNDO is het mogelijk de **laatste** verlening van een permissie ongedaan te

maken. Overigens kan met UNDO een voorafgaande UNDO weer ongedaan gemaakt worden.

Het effect van een opdracht wordt zichtbaar op het scherm: de permissies voor de doelgroep worden voor het betreffende type op het scherm getoond. Niet zinvolle opties worden na uitvoering van een opdracht niet meer getoond.

ATTR
Met de optie ATTR kan men permissies van de doelgroep manipuleren betreffende de attributen behorende tot het geselecteerde type. Mogelijke opdrachten betreffende attributen zijn GRANT, REVOKE, GRALL, REVALL en PAGING.

Voorbeeldsituatie:
Er is eerst permissie verleend aan de doelgroep "salarisadmin" voor get-, insert- en delete-manipulaties op het type "persoon".

Vervolgens is uit de dan nog beschikbare opties ATTR gekozen. We zien dan ongeveer het volgende scherm:

```
              Autorisatie voor database proef (attributen)

   Type persoon.

   Brongroep dba:                Doelgroep salarisadmin:

   naam                   gu     naam                              g
   straat                 gu     straat                            g
   plaats                 gu     plaats                            g


   EXIT          GRANT            GRALL                             HELP
```

Ook nu is maar een zinvol gedeelte van de opties zichtbaar.
"gu" betekent: get- en update-permissie.
"g" betekent: get-permissie.
De opties worden hierna toegelicht.

GRANT (attribuutrecht)
Via de optie GRANT kunnen aan de doelgroep permissies verleend worden op een nog te selecteren attribuut van het al eerder gekozen type. De gebruiker (uit de brongroep) selecteert het gewenste attribuut op de bekende wijze met de pijltjestoetsen, gevolgd door <Return>. Hierna zijn als optie beschikbaar GET, UPDATE en UNDO:
UPDATE: met deze opdracht verleent men de update-permissie op het geselecteerde attribuut aan de doelgroep. Bovendien wordt hiermee ook de get-permissie toegekend indien deze nog niet verleend was.

GET : met deze opdracht wordt de get-permissie op het geselecteerde attribuut aan de doelgroep verleend.

UNDO : hiermee kan men de laatst verleende permissie ongedaan maken. Een UNDO kan hiermee ook ongedaan gemaakt worden.

REVOKE (attribuutrecht)
Met de optie REVOKE kan men een permissie aan de doelgroep betreffende een attribuut van het eerder gekozen type intrekken. Men dient op de bekende wijze met pijltjestoetsen , gevolgd door <Return> het gewenste attribuut te selecteren.
REVOKE is niet meer van toepassing indien het betreffende recht reeds is doorgegeven aan een subgroep van de doelgroep. REVOKE is ook niet van toepassing indien er geen enkel recht betreffende een attribuut verleend is aan de doelgroep.

GRALL (GRANT ALL) (attribuutrecht)
Hiermee verleent men aan de doelgroep alle permissies op een nog te selecteren attribuut. Met de pijltjestoetsen en <Return> wordt het betreffende attribuut geselecteerd.
GRALL is alleen van toepassing als nog niet alle attribuut-permissies verleend zijn.

REVALL (REVOKE ALL) (attribuutrecht)
Hiermee worden alle rechten betreffende het nog aan te wijzen attribuut ingetrokken. Aanwijzen gebeurt weer met pijltjestoetsen en <Return>. REVALL is niet van toepassing indien aan een subgroep van de doelgroep attribuutpermissies doorgegeven zijn. REVALL is ook niet van toepassing indien geen enkel attribuutrecht verleend is.

PAGING (attribuutlijst)
Met deze optie kan men bladeren door de attributen van het geselecteerde type. Deze optie is alleen van toepassing indien de lijst van attributen bij de brongroep niet op één scherm past.

VIII.3.5.2. REVOKE (rechten intrekken op typen)

Indien men uit het autorisatiemenu na TYPE de optie REVOKE gekozen heeft dan kan men rechten betreffende typen of attributen intrekken. Overigens dient men eerst de doelgroep te selecteren. Dit kan m.b.v. het scherm dat zichtbaar wordt na de REVOKE opdracht. Met pijltjestoetsen en <Return> wordt de doelgroep geselecteerd. In het te gebruiken voorbeeld is "salarisadmin" als de doelgroep gekozen. Overigens: REVOKE is niet van toepassing als permissies doorgegeven zijn aan een subgroep van de doelgroep. Hierna krijgt men dan een scherm te zien waaruit m.b.v. de pijltjestoetsen en <Return> de gewenste database geselecteerd moet worden. In ons voorbeeld is de database "proef" gekozen. Nu zien we ongeveer het volgende scherm:

```
                Autorisatie voor database proef (typen)

   Brongroep dba:                Doelgroep salarisadmin:

   persoon              gid      persoon                        gid
   inkomen              gid
   miljonair            gid

   EXIT     GRANT     REVOKE     GRALL     REVALL     LIST     PRINT
```

In deze fase wordt REVOKE geselecteerd. Het effect van deze opdracht is een scherm waarbij de optie REVOKE extra oplicht:

```
           Autorisatie voor database proef (typen) REVOKE

   Brongroep dba:                Doelgroep salarisadmin:

   persoon              gid      persoon                        gid
   inkomen              gid
   miljonair            gid

   EXIT     GRANT     REVOKE     GRALL     REVALL     LIST     PRINT
```

In voorafgaand scherm dient men nu bij de doelgroep een type te selecteren (pijltjestoetsen en <Return>). In dit geval wordt ’persoon’ gekozen, een andere keuze is overigens nu niet mogelijk. We zien hierna ongeveer het volgende scherm:

```
            Autorisatie voor database proef (typen) REVOKE

   Brongroep dba:                      Doelgroep salarisadmin:

   persoon                             persoon
   Permissie(s): GET, INSERT, DELETE   Permissie(s): GET, INSERT, DELETE

   EXIT      GET      INSERT      DELETE      ATTR              HELP
```

De nu niet zinvolle optie UNDO is niet zichtbaar. De opties worden hierna toegelicht.

Met **GET** wordt de get-permissie ingetrokken van de doelgroep voor het gekozen attribuut. Indien insert- en delete-permissie gegeven was worden deze twee permissies ook ingetrokken.

Met **INSERT** wordt de insert-permissie van de doelgroep op het gekozen type ingetrokken.

Met **DELETE** wordt de delete-permissie van de doelgroep op het gekozen type ingetrokken.

Met **UNDO** wordt het laatst gegeven commando ongedaan gemaakt. Dit geldt ook voor het UNDO-commando.

Met **ATTR** kan men de permissies van de doelgroep die betrekking hebben op attributen van het gekozen type weer intrekken. Overigens kan men nu ook rechten verlenen!

De na ATTR beschikbare opties zijn: GRANT, REVOKE, GRALL, REVALL en eventueel PAGING. Deze opties zijn al beschreven in de vorige paragraaf over GRANT (rechten betreffende samengesteld type).

VIII.3.5.3. GRALL (GRant ALL op samengesteld type)

Als vanuit het autorisatiemenu na TYPE voor GRALL gekozen is dient men op de reeds meerdere keren beschreven wijze eerst de doelgroep te selecteren, gevolgd door het selecteren van de database. Het GRALL-commando is niet van toepassing als de permissies al verleend zijn. Nadat respectievelijk gekozen is voor de doelgroep ’salarisadmin’ en de database ’proef’ wordt het GRALL-commando gegeven.

Het effect van dit commando is dat alle rechten betreffende typen **en** attributen van de gekozen database worden doorgegeven aan de doelgroep. Na de GRALL-opdracht ziet in ons voorbeeld het scherm er ongeveer als volgt uit:

```
                Autorisatie voor database proef (typen)

  Brongroep dba:                      Doelgroep salarisadmin:

  persoon             gid             persoon                   gid
  inkomen             gid             inkomen                   gid
  miljonair           gid             miljonair                 gid

  EXIT          REVOKE          REVALL          LIST          PRINT
```

Hierna zijn natuurlijk geen manipulaties van rechten meer nodig op attributen.

VIII.3.5.4. REVALL (REVoke ALL op samengesteld type)

Ook bij deze optie geldt weer dat men eerst de doelgroep en vervolgens de database moet selecteren. Hierna kan men REVALL selecteren. Deze opdracht heeft als effect dat alle bestaande manipulatierechten van de doelgroep betreffende typen **en** attributen van de selecteerde database worden ingetrokken. Overigens kan dit alleen als de betreffende rechten niet zijn doorgegeven aan een subgroep van de doelgroep. In ons voorbeeld ziet na het uitvoeren van de REVALL-opdracht het scherm er ongeveer als volgt uit:

```
                Autorisatie voor database proef (typen)

   Brongroep dba:              Doelgroep salarisadmin heeft
                               geen toegankelijke typen.

   persoon              gid
   inkomen              gid
   miljonair            gid


   EXIT          GRANT           GRALL           LIST          PRINT
```

VIII.3.5.5. LIST (permissies op typen/attributen)

Na selectie van doelgroep en database zou men in de situatie van de voorafgaande paragraaf het GRALL-commando kunnen geven, zodat de groep ’salarisadmin’ toch weer toegang krijgt op typen en attributen van de database ’proef’. Vervolgens is het effect van de LIST-opdracht dat men dan een overzicht krijgt van permissies betreffende de typen en attributen van database ’proef’ die gegeven zijn aan ’salarisadmin’:

```
              Autorisatie voor database proef (typen)  LIST

   Het model van database proef voor groep salarisadmin:

   persoon    (g, i, d)   = naam (g,u), straat (g,u), plaats (g,u)
   inkomen    (g, i, d)   = persoon (g,u), bedrag (g,u)
   miljonair  (g, i, d)   = [persoon] (g,u), janee (g,u)


                                                          RETURN
```

VIII.3.5.6. PRINT (permissies op typen/attributen)

Met deze optie krijgt men hetzelfde resultaat als met LIST, echter worden de permissies op typen en attributen nu op papier gezet.

VIII.3.5.7. PAGING

Met de optie PAGING kan men "bladeren" door de typen van de gekozen database. De optie is alleen beschikbaar als niet alle typen met attributen op één scherm passen.

VIII.3.6. DEFAULTS

Met deze optie kunnen de defaultwaarden en preferenties van de gebruiker zichtbaar worden gemaakt. Deze waarden kunnen door het gebruik van Xplain DBMS worden gewijzigd.