SQL Server käyttäjätunnukset ja käyttäjäryhmät

Harkinnan varaiset oikeudet:
Alla on esitelty SQL komentoja, joiden avulla voi määritellä oikeudet harkinnan varaisesti (discretionary access control, ks. Ramakrishan, Gihrke. Database Management Systems. 2003. McGraw-Hill s. 695):

Tarvittaessa haluttu schema voidaan luoda tietokantaan seuraavalla tavalla (ks. http://msdn2.microsoft.com/en-us/library/ms189462.aspx):

```
USE AdventureWorks;
CREATE SCHEMA Sprockets AUTHORIZATION Annik
    CREATE TABLE NineProngs (source int, cost int, partnumber int)
    GRANT SELECT TO Mandar
    DENY SELECT TO Prasanna;
GO
```

Ja tarvittavat kirjautumisessa käytettävät käyttäjätunnukset (login:t) ja tietokantaoikeudet (user) tietokannalle ja schemalle voidaan luoda seuraavalla tavalla:

```
CREATE LOGIN matti
WITH PASSWORD = 'salasana1',
DEFAULT_DATABASE = AdventureWorks

CREATE USER matti FOR LOGIN matti
WITH DEFAULT_SCHEMA = HumanResources
```

`CREATE LOGIN` ks. http://msdn2.microsoft.com/en-us/library/ms189751.aspx
`CREATE USER` ks. http://msdn2.microsoft.com/en-us/library/ms173463.aspx

```
(GRANT CONNECT TO guest)
```

Tietokannan käyttäjän omistaman tietokanta roolin luonti (ks. http://msdn2.microsoft.com/en-us/library/ms187936.aspx):

```
USE AdventureWorks;
CREATE ROLE buyers AUTHORIZATION BenMiller;
GO
```

Tietokanta roolin luonti, jonka omistaa kiinteä tietokanta rooli:

```
USE AdventureWorks;
CREATE ROLE auditors AUTHORIZATION db_securityadmin;
GO
```

Rooleja ovat SQLServer:ssä:

a) Palvelinroolit:
   bulkadmin
   dbcreator
   diskadmin
   processadmin
   securityadmin
   serveradmin
   setupadmin
   sysadmin
   Lisäksi jokaisella login id:llä on:
   public –rooli

b) Tietokantaroolit:
   db_accessadmin
   db_backupoperator
   db_datareader (asiakas käyttäjälle)
   db_datawriter (asiakas käyttäjälle)
   db_ddladmin
   db_denydatareader
   db_denydatawriter
   db_owner
   db_securityadmin

Oikeuksien määrittely:

GRANT –komennosta on kolme eri tyyppiä:

I) SELECT tietokantaoikeuden myöntäminen user matille scheman taululle, jonka hän voi antaa muillekin GRANT komennolla:

```
GRANT SELECT ON SCHEMA.TAULU1 TO matti WITH GRANT OPTION
```

II) INSERT ja DELETE tietokantaoikeuksien myöntäminen roolille scheman tauluun:

```
GRANT INSERT, DELETE ON SCHEMA.TAULU1 TO testirooli
```

III) Roolin myöntäminen tunnukselle (user) tehdään proseduurin avulla:

```
sp_addrolemember 'testirooli', 'matti'
```