# Management of Groups and Group Roles in VOMRS

***Second Draft***

*T. Levshina*

## *Introduction*

Virtual Organization Management Registration Service (VOMRS) supports the notion of group and group roles. A group is an organizational entity defined by the VO which refers to a subdivision of the VO's overall project, and to which some subset of the VO's members are assigned, according to their responsibilities in the project. Group roles are roles that correspond to particular computing privileges at a grid site and to which VO members may be assigned. Group roles are defined VO-wide, not by group. The combination of group and group roles defines the privileges a user has on the grid.

## *Current Implementation*

In VOMRS groups are organized hierarchically. All members are assigned to a root group and can not be removed from it. A member assigned to a given group (somewhere down in the hierarchy) is automatically granted membership in the group's top parent group, although not in any intermediate parent groups (The feature is forced by group and group role handling in VOMS).  Each group may have assigned a Group Owner and Group Manager. The ownership attribute of a parent group is automatically inherited by a child group.

Group Owner has the following privileges and responsibilities within his group:

- Access to members public information
- Creation/deletion of subgroups
- Creation/deletion of group roles
- Assigning/removing members to/from group and group role
- Assigning administrative roles of Group Owner and Group Manager to members

Group Manager has following privileges and responsibilities within his group:

- Access to members public information
- Assigning/removing members to/from group and group role
- Assigning administrative role of  Group Manager to members

VO Admin has all the rights of Group Owner and Group Manager.

An applicant or a member in good standing can select to be assigned group and group role at any time. Member’s group and group assignment is propagated to VOMS if VOMRS is synchronized with an appropriate VOMS instances.

VO Admin, Group Owner, Group Manager can assign or de-assign member to/from the group or group role at any time. As soon as a member is de-assigned from the group (group role) he is blocked from selecting this group (group role) again. Only administrator can re-assign this person to blocked group (group role).

## *New Requirements*

The following changes have been requested:

- Each group and group role should have definition that will be available to the users during selection
- An administrator  should have means to change the group and group role definition via VOMRS interface
- An administrator should be able to connect/disconnect a group role to a particular group
- An administrator should be able to approve/disapprove group and group role selection before a user becomes the valid member of the group
- A member should be able to request re-assigning to a group and a group role via VOMRS interface
- A member assigned to a subgroup is automatically assigned to all parent groups
- A member with “Denied” access to a parent group is automatically removed from all subgroups and the group roles she/he is assigned within subgroups of abovementioned group

## *Proposed Implementation*

In order to satisfy the abovementioned requirements and try to minimized the effort required from administrators to maintain groups and group roles configuration we proposed the following solution:

### Groups

1. Groups are organized hierarchically
2. A group can be created at any time by authorized administrators
3. A group can be deleted only when there are no members assigned to the group or its subgroups
4. Deletion of the parent group will cause the deletion of all subgroups of the group
5. A group may have group roles associated with it
6. Each group has the following  attributes:

    a. Name: FQN that listed all the parent group names separated by “/”
    b. Description: defines the purpose of the group
    c. Access – where “Open” means that a user can select this group without administrator approval, a “Restricted” access means that a user can submit a request to be a member of this group and will need administrators approval
    d. List of group roles relevant to this group

7. A subgroup of the restricted group has “Restricted” access, it can be modified only after access to the parent group becomes “Open”

## Group Roles

1. A group role can be created at any time by authorized administrators
2. A group role can be deleted by authorized administrators only when there are no members assigned to this group
3. A group role can be associated with any group
4. Each group role can be associated with multiple groups
5. A group role can be assigned to a group by authorized administrators
6. A group role can be de-assigned from a group by authorized administrators only if there are no members assigned to this group role within this group
7. A group role has the following attribute:
    a. Name
    b. Description: defines the purpose of the group role
8. A tuple (group,group role) within this group has an additional attribute: access. An “Open” access means that a user can select this group,group role without administrator approval, this access can be assigned to a tuple only if the group has “Open” access, a “Restricted” access means that a user can submit a request to be a member of this group,group role and will need administrators approval.

## Users and Group/Group Roles selection

1. A user is always assigned to a root group
2. A user can not be de-assign from the root group
3. During Phase II of registration an applicant can indicate the group and group roles she/he would like to be assigned
4. A member can indicate the group and group roles she/he would like to be assigned at any time
5. An applicant or a member when selecting group roles within the group can choose only group roles relevant to this group
6. An applicant or a member assigned to a subgroup is automatically assigned to all parent groups of this subgroup
7. An applicant or a member de-assigned from the parent group is automatically de-assigned from all the subgroups of this group as well as all the group roles within the subgroups

8. An applicant or a member rights to belong to any group and group roles within the group are defined by her/his status within the group and group role
9. There are following statuses:
    a. New:  is assigned when a user is requested to join "Restricted" group and any group role within the group, or when a user tries to reapply to the membership in the group/group role that has been previously denied
    b. Approved: is assigned when a user is requested to join "Open" group and any group role within the group or when user's selection of  "Restricted" group is approved by an authorized administrator
    c. Denied: is assigned when user's selection is denied. Once the selection is denied user have to get an approval to rejoin the group even if the group access is "Open"
10. Only a member in good standing will be added to relevant VOMS instance under the root group
11. Only a member in good standing with "Approved" group and group role status will be assigned the corresponding group and role in VOMS

## Group Administrators

There are three types of authorized administrators that manage groups, groups roles and groups membership.

*Group Manger*

A Group Manager is a member in good standing who is assigned a Group Manager role for a particular group within a VO. A Group Manager role can be assigned/de-assigned by a VO Admin or by this group's Group Owner (see below).   A Group Manager of the parent group is automatically a manager of all the subgroups. A Group Manager has the following privileges and responsibilities:

- Has access to members' public data
- Can assign any member to a group and group role within the group. The status of the membership within a group, group role is set to "Approved" automatically.
- Can approve user's request to join the group (and group role within the group).
- Can de-assign a user from a particular group. This user will be removed from all subgroups as well as group roles of the selected group  The status of the membership for the selected group becomes "Denied"
- Can de-assign a user from a particular group role within a selected group. The status of the membership for the selected group & group role becomes "Denied"

A Group Manager of a particular group is automatically a member to this group and all its subgroups. A Group Manager can not be de-assigned from the groups she/he manages. In order to do so she/he needs to be de-assigned from Group Manager role first.

*Group Owner*

A Group Owner is a member in good standing who is assigned a Group Owner role for a particular group within a VO. A Group Owner role can be assigned/de-assigned by a VO Admin.   A Group Owner of the parent group is automatically an owner of all the subgroups. A Group Owner of a group has all rights of group's Group Manager as well as the following additional privileges and responsibilities:

- Can change access to the group
- Can change group description
- Can add/remove group roles association with this group
- Can create a new subgroups
- Can assign/de-assign Group Manager to the group or its subgroups

A Group Owner of a particular group is automatically a member to this group and all its subgroups. A Group Owner can not be de-assigned from the groups she/he owns. In order to do so she/he needs to be de-assigned from a Group Owner role first.

*VO Admin*

A VO Admin is a "top" administrator of the VO that has all rights of Group Owner of the root group. Below are listed additional right relevant to groups and group roles management:

- Can create a group role
- Can change group role description
- Can delete a group role if there is no member assigned to this role
- Can assign/de-assign  Group Owner role

## *Use Cases*

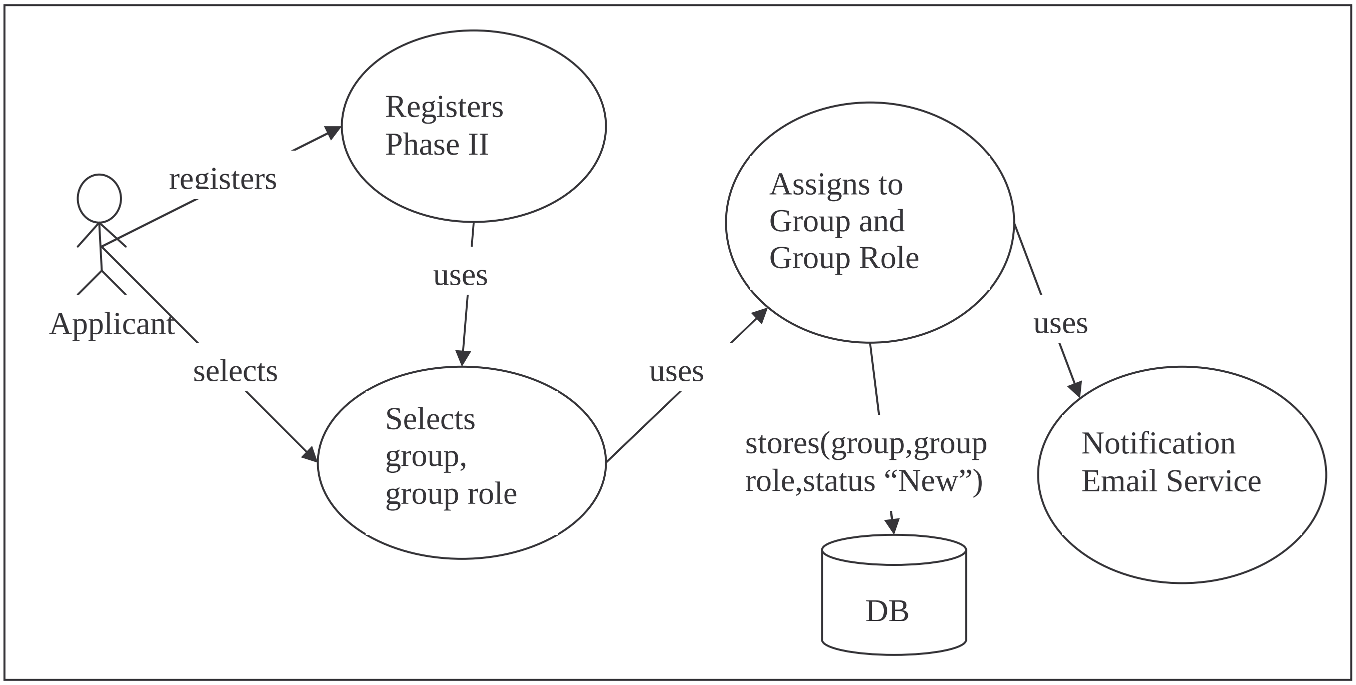
Registers Phase II
registers
Applicant
uses
Assigns to Group and Group Role
uses
selects
uses
Selects group, group role
stores(group,group role,status "New")
Notification Email Service
DB

**Figure 1 Group and group role selection by an Applicant**

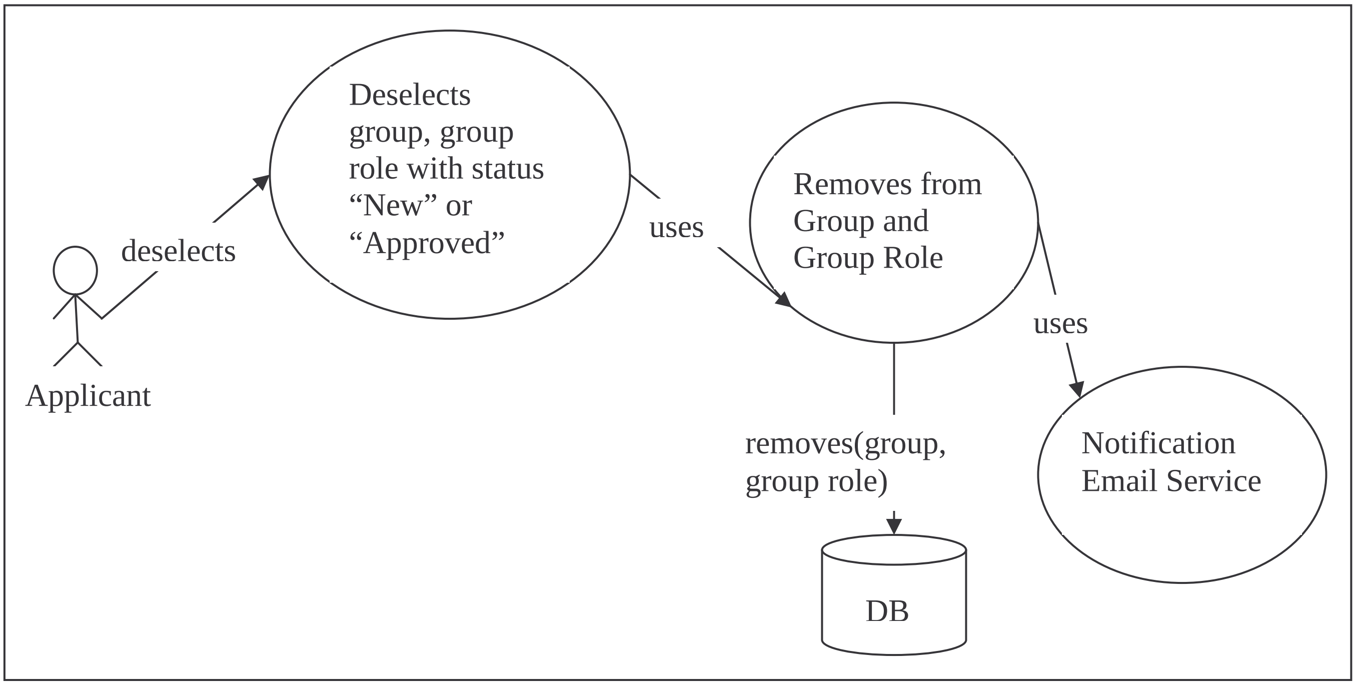
Deselects group, group role with status "New" or "Approved"
uses
Removes from Group and Group Role
deselects
Applicant
uses
removes(group, group role)
Notification Email Service
DB

**Figure 2 Group and group role de-assignment by an Applicant**

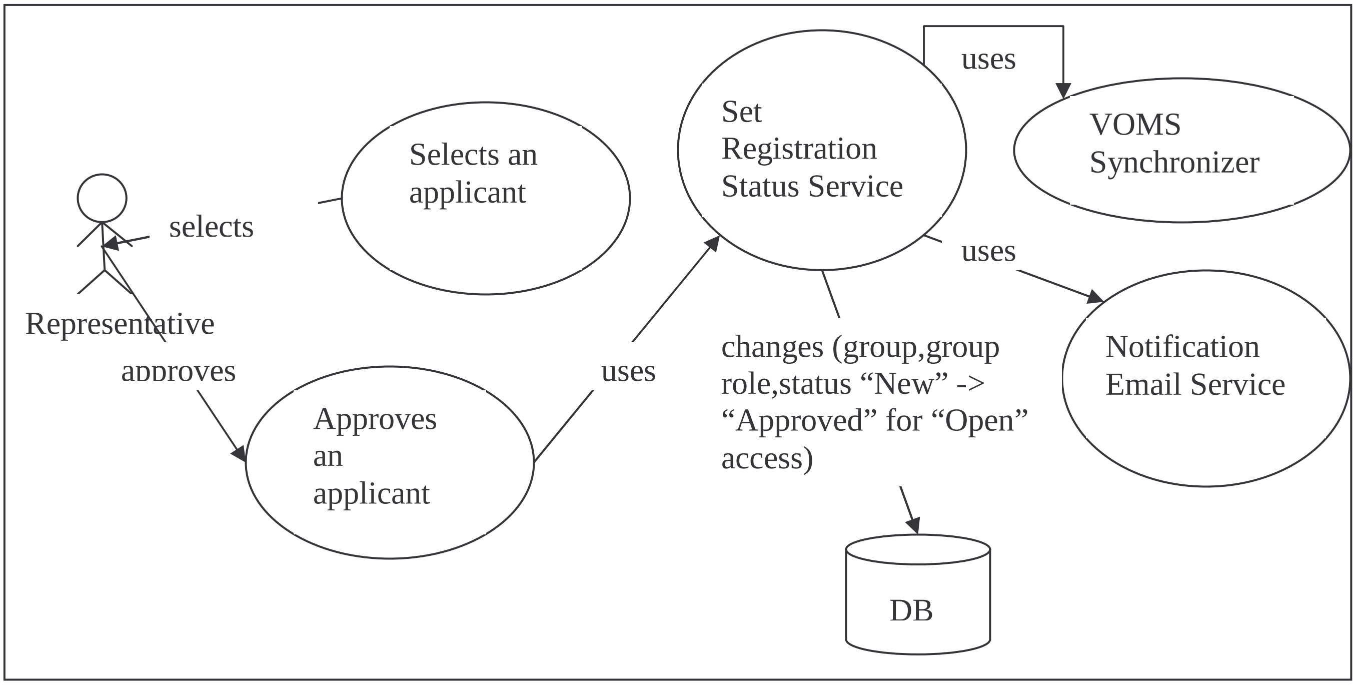

**Figure 3 A Representative approves an applicant**

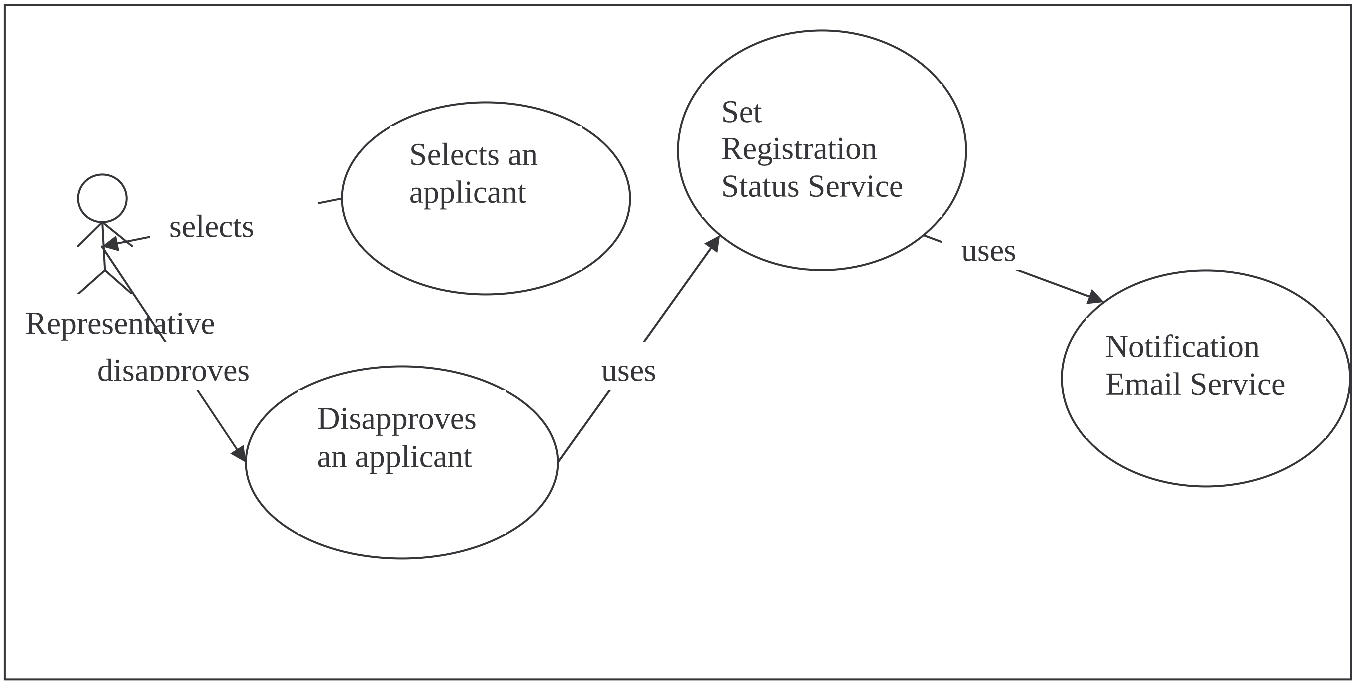

**Figure 4 A Representative disapproves an applicant**

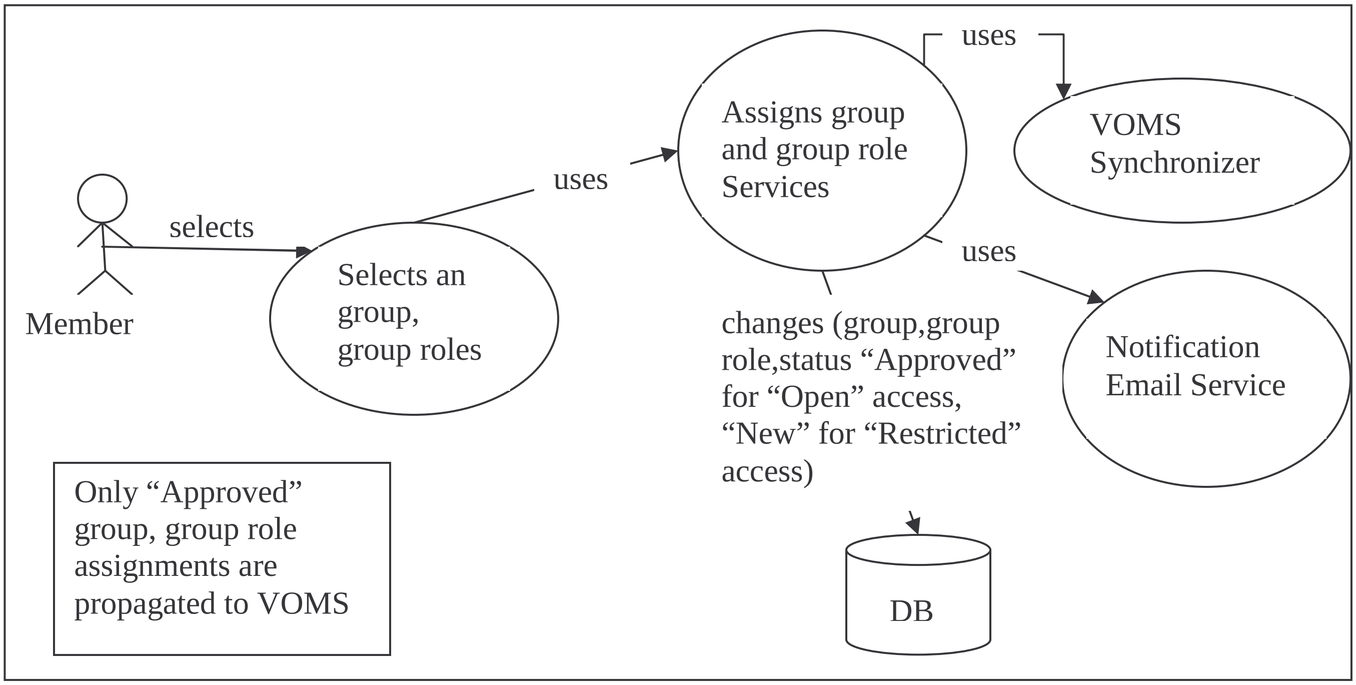
uses
Assigns group and group role Services
VOMS Synchronizer
Member
selects
uses
Selects an group, group roles
uses
changes (group,group role,status “Approved” for “Open” access, “New” for “Restricted” access)
Notification Email Service
Only “Approved” group, group role assignments are propagated to VOMS
DB

**Figure 5 A Member selects group and group roles**

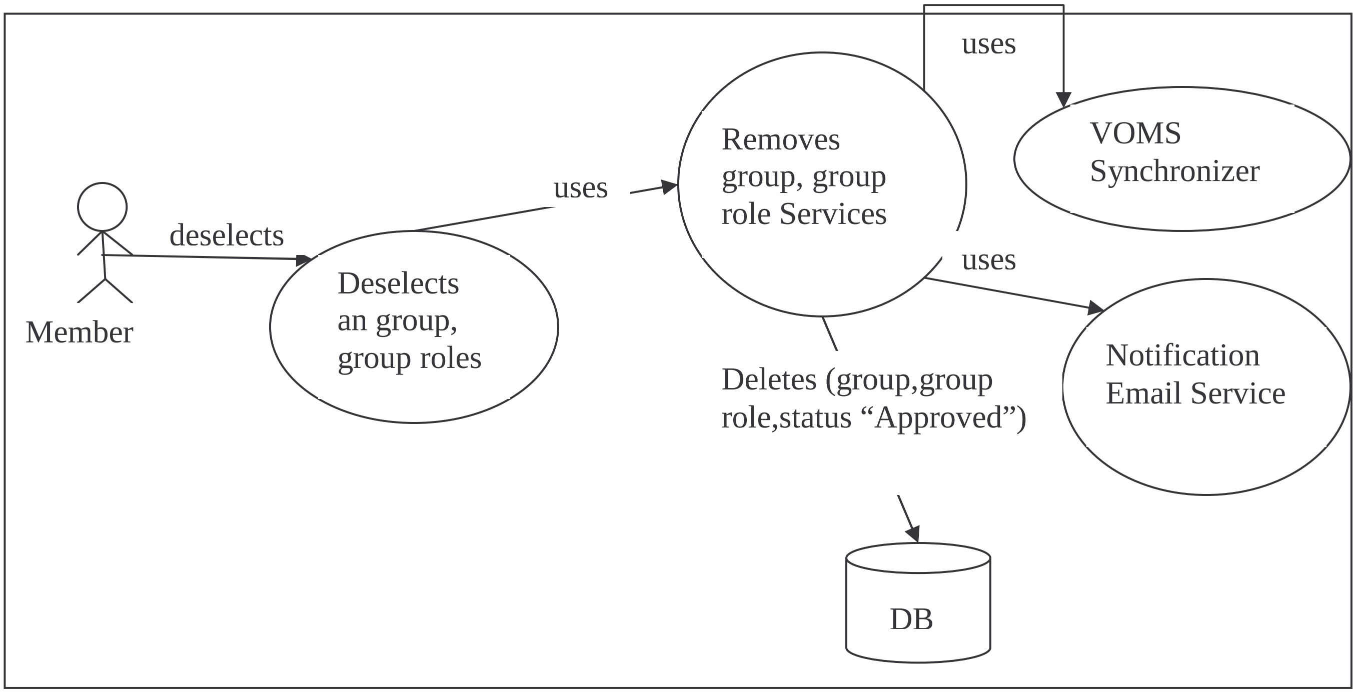
uses
Removes group, group role Services
VOMS Synchronizer
Member
deselects
uses
Deselects an group, group roles
uses
Deletes (group,group role,status “Approved”)
Notification Email Service
DB

**Figure 6 A Member deselects group and group role**

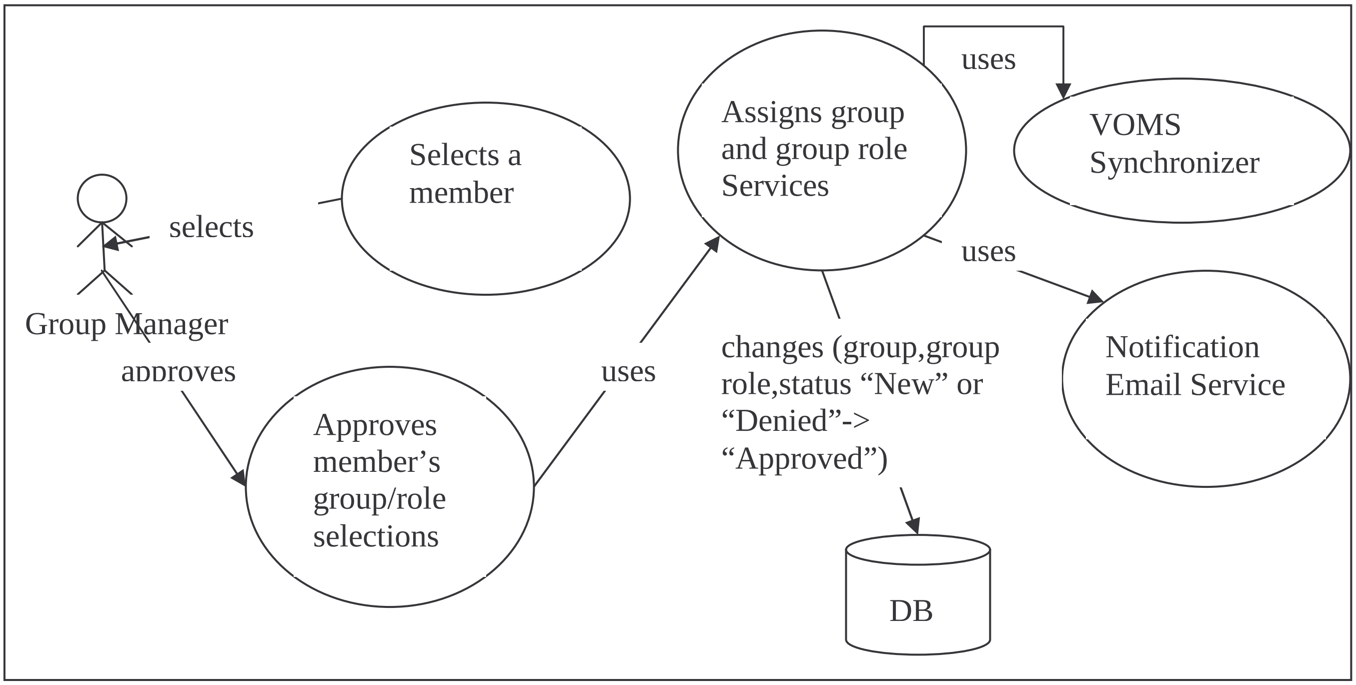
Group Manager
selects
Selects a member
approves
Approves member's group/role selections
uses
Assigns group and group role Services
uses
VOMS Synchronizer
uses
Notification Email Service
changes (group,group role,status "New" or "Denied"-> "Approved")
DB

**Figure 7 A Group Manager assigns group/group role to a member**

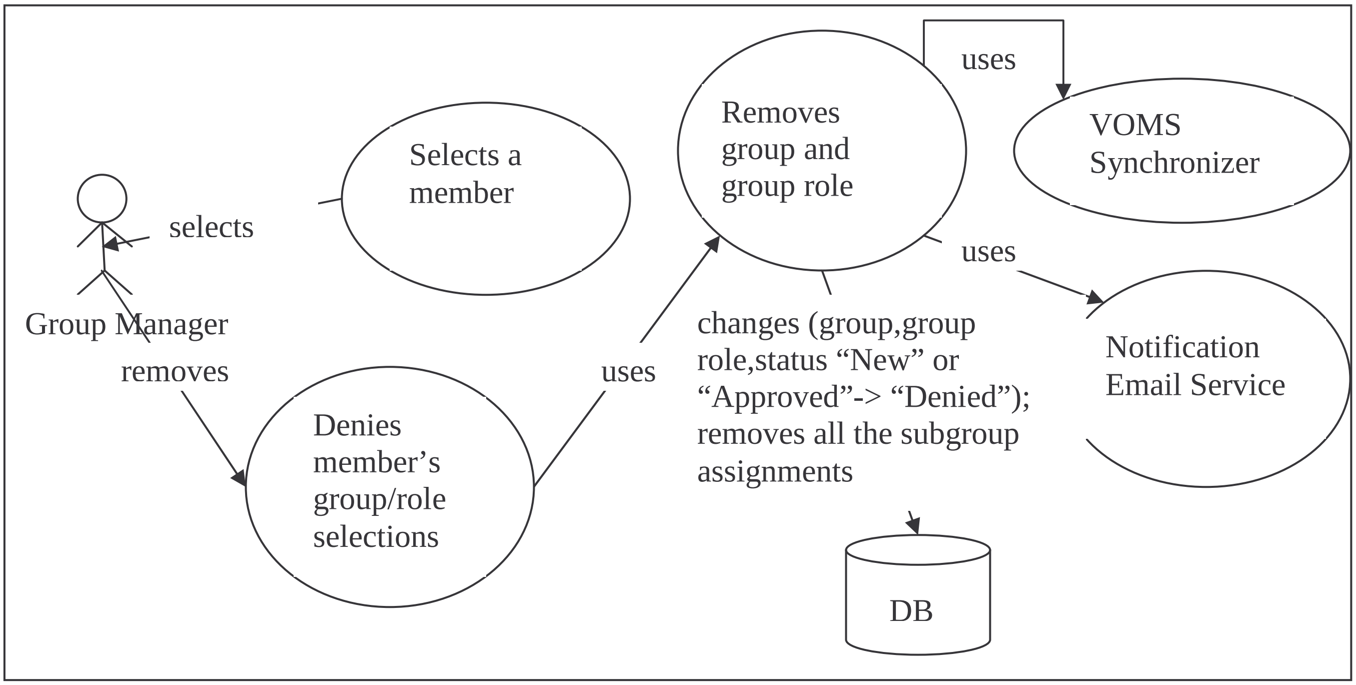
Group Manager
selects
Selects a member
removes
Denies member's group/role selections
uses
Removes group and group role
uses
VOMS Synchronizer
uses
Notification Email Service
changes (group,group role,status "New" or "Approved"-> "Denied"); removes all the subgroup assignments
DB

**Figure 8 A Group Manager deassigns a member from group/group role**