



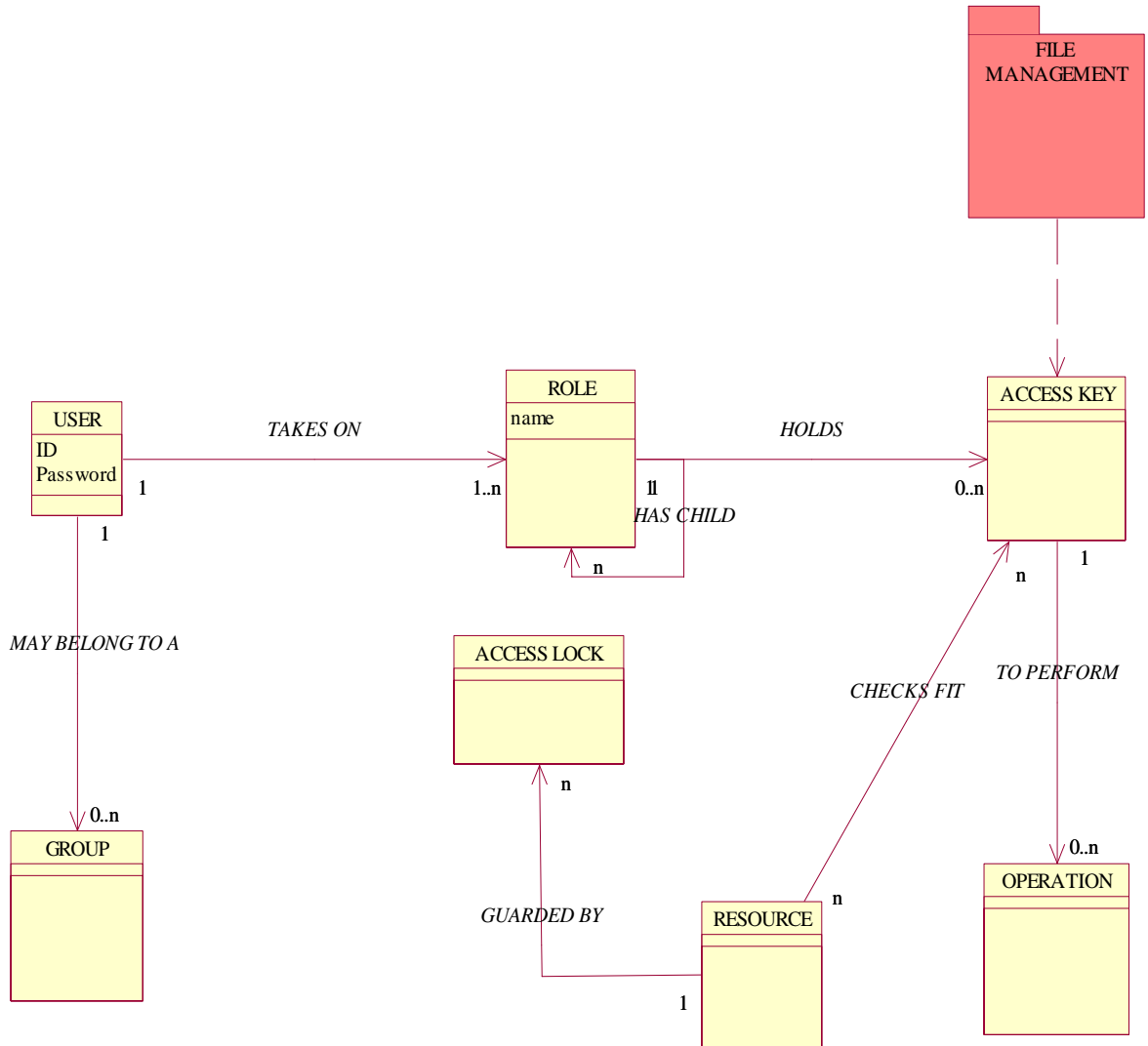
**Comp 6471
Assignment 2
Team 7- Component 2**

**User Management System
For
CU WME**

**Asif Ali Dogar
ID: 5696569
a_doga@encs.concordia.ca**

Winter 2006

1. Domain Model



2. Description of three main classes.

1. USER.

A user in computing context is one who uses a computer system, in our case it is the Concordia University Work Management Environment. The “User” class will hold the information about the user. This information will include the name of the user, the user id and password of that user. Other information may include, the roles that the user assumes, or the memberships of different groups that the user holds etc. Since “User” is a very broad term, this class should be extensible to allow new classes of users to be defined and managed,

2. ROLE

A Role may be defined as a job function within an organization, with associated authority and responsibilities. Under RBAC framework, users are granted different roles based on their job description. User management system will define new roles and will manage those roles. User management will then keep a mapping of user to role(s). Roles are very crucial because the operations that a user is allowed to perform are based on the user’s role. User memberships into roles can be revoked and new memberships into roles may be granted. Roles might be hierarchical; that is one role may include the operations that are associated with another role. A Role may have many children.

3. ACCESS KEY.

Access key can be thought of as a permission to perform some operations on some objects (files, documents, workstation, and printer). The access keys (access rights) are not set by the user management system but, this information will come from file management system. The file management system will define the access rights for a role to access some resource (documents). Access rights are grouped by role type and the right to access particular resources is restricted to someone who assumes a role. User management system doesn’t enforce anything. The User management system just keeps a mapping of users to roles to keys to resources. For example if a user is trying to access some object (file), the file management system first checks with the User management system if that user (role) has the permission to access that object.

3. Description of three main associations.

1. USER "*Takes on a*" ROLE

Concordia University Work Management Environment will have different classes of users and every user will have his requirements from the system. Under Role Based Access control, users assume roles, and the system allows a role to do something with the system. So the relationship "User takes on a role" carries great importance. The system will not be designed to allow or restrict access to individual users; rather the system will consider roles. So a user has to know the role it takes. A User may have one or more roles and can enjoy privileges associated with different roles it assumes. The arrow pointing towards the Role means that a user who enters the system with a certain id and password has to know his role, or in short "User knows about the role", the role doesn't have to know the user.

2. ROLE "*has child*"

Roles may have overlapping responsibilities, which means that users belonging to different roles may perform similar operations. Role hierarchies can be used to provide for the natural structure of an organization. A role hierarchy defines some roles that may contain other roles. So a role can have children. For example the role the project manager will implicitly include the role of team member. This means that the Role "Project manager" has certain privileges but it also holds the privileges of a "team member". The arrow means that a role needs to know about its children.

3. ROLE "*holds*" ACCESS KEY

Every resource is guarded by a ACCESS KEY for the sake of protection. A role thus needs to have the appropriate key to access a resource and perform some operation on some resource. The ACCESS KEY is an access right that the role possesses. A role may have zero or many keys to a resource. The relationship emphasizes that the role needs to know about his key, in other words, the role needs to know its rights. The user management system keeps a mapping of role to keys and when a role is accessed, the sub system responsible for that resource may ask the UMS whether that role possesses the key or not.

4. Brief descriptions of other classes

1. GROUP

A USER may belong to a group. In Collaborative publication environment, it is very likely that a USER doesn't work alone. A USER may be a member of one or many project teams.

2. RESOURCE

A Resource may be a document, a workstation, or a printer .RESOURCE is a very wide term. The User management system is responsible for managing access not only to the documents but to other things as well.

3. ACCESS LOCK

Every Resource is guarded by an Access lock. This lock is necessary to ensure that the resource doesn't go in the wrong hands. This Access lock is basically restriction on some resource which is imposed by the owner of the resource.

4. OPERATION

Operation includes reading or writing documents, adding comments, logging on a workstation, printing from a printer etc. Only the user with the right key can perform operation on a resource.

Brief description of other associations

1. USER "*may belong to*" GROUP

As mentioned above a USER may belong to one or many groups. A user can be working on many projects and thus be a member of many groups. This association emphasizes that the user should know his group.

2. RESOURCE "*Guarded by*" ACCESS LOCK

A resource will be protected by a access lock. For example a workstation or a document is guarded by a password; a printer is guarded by a access card.

3. RESOURCE "*checks fit*" ACCESS KEY

Once a resource is accessed, it checks the access key to see if that is the right access key or not, so the Resource knows about the ACCESS KEYS.

4. ACCESS KEY “*to perform*” OPERATION

In order to perform some operation a resource, a role needs to have the key to perform any operation. The arrow pointing towards operation means that a key has some operations associated with it. For example a certain key, if possessed by a role, gives the role to do any operation on the resource. In other words, an ACCESS KEY knows its operations.

5. Component Consistency

The User management system will provide information to all other components in the system, because it will have all the information relating to users, their roles and their rights.

The User management system will work closely with the File management system. Whenever a user will try to access a file through the File management system, the file management system will check with the User management system if that user has the key (access right) to access that document. File Management System has a class called Resource, and the File management system also has a class with the same name but the granularity is different; A Resource in the user management system can be anything from a document, to a printer, to workstation, whereas A Resource in file management system is a file. It might be a text file or an image file.

If some user is trying to start a new project for example, it will first check with the User management system to check if that user is entitled to start a new project.

NOTE: Other components request some services from UMS by sending messages (request) and user management system sends the appropriate reply. In the domain model, we are not show the messages being exchanged between components, that is why the exchange of messages is not shown in the domain model, but that does not mean that the User management system does not talk to any other component in the system.