

Data model - CustomerID

 Last reviewed: 2017-10-13

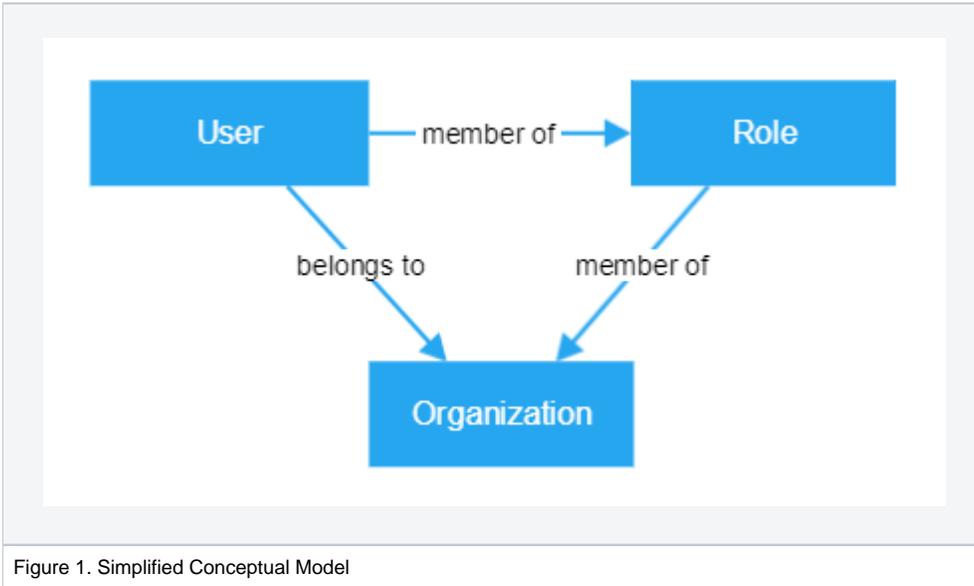


Figure 1. Simplified Conceptual Model

Users

Statuses

User accounts in CustomerID can be in different statuses. Here is a list of all the statuses:

Status name	Status code	Technical name	Description
Pending	0	pending	User has registered, but is waiting for approval to become an enabled user.
Enabled	1	enabled	Normal user status. User can access systems according to defined permissions.
Disabled	2	disabled	User has been disabled. This means that user can not login into services until user is enabled again.
Locked	3	locked	User authentication method has locked the user account. This usually occurs because too many failed login attempts have been performed. This is usually a temporary status for the user. A locked user may for example become enabled again after a certain time interval or an administrator user can in some cases unlock the user account.
Not initialized	4		This is purely a technical user status and it should not occur in production.
Waiting for registration	5	waiting_for_registration	User has been invited to the system, but hasn't registered yet.

Roles and Organizations

Roles and organizations are configurable. For example, the role requests through the self-service interface can be configured as follows:

- You can define that roles can only be requested from within the home organization, that is, the organization where the user object resides in.
- You can create role lists. There are two types of role lists:
 - **Black list.**
End-users cannot request roles in the black list. They can only request roles not in the black list.
 - **White list.**
End-users can only request roles in the white list. They cannot request any other roles.

Roles

In Ubisecure CustomerID, all roles are described as **EntityNames**. Supported characters are basic letters ("a-zA-Z"), Scandinavian characters ("äöåÄÖÅ"), numbers ("0-9"), space (" ") and some special characters ("._-"). All other characters are replaced with a space. The following is an example of an **EntityName** of a role:

```
Societies/Lapland/OrganizationMainUser
```

In this example:

- The role is located in the Ubisecure CustomerID Users branch (eIDM Users) of the Ubisecure Directory or Active Directory
- The organization is Societies
- The suborganization is Lapland
- The role is OrganizationMainUser

In Ubisecure Directory, the Distinguished Name (DN) for the example role above would be as follows:

```
cn=OrganizationMainUser,ou=Lapland,ou=Societies,ou=eIDM Users,<ROOT DN>
```

The user object has a membership for the role:

```
# Ubisecure Directory
ubiloginMemberOf= cn=OrganizationMainUser,ou=Lapland,ou=Societies,ou=eIDM Users,<ROOT DN>
# Microsoft Active Directory
memberOf= cn=OrganizationMainUser,ou=Lapland,ou=Societies,ou=eIDM Users, <ROOT DN>
```

Organizations

Organizations have a technical name and a display name. The technical name is the actual path (relative name) of the organization in the main repository, and the display name is the name that is shown in user interfaces.

There are two types of organizations, physical and virtual. Physical organizations are used to mimic the hierarchical structure of an organization where each user belongs to only one organization. Virtual organizations mirror a project structure where users can belong to many projects. In virtual organizations, the users are not physically located in any of the projects but they are part of them through roles.

Organizations have an organization type, which can be used to classify organizations into groups. In configuration, it is possible to define roles that will be created into these organization types by default. The needed information is the name of the organization type and the roles.

Roles can be added to and removed from an organization in the Ubisecure CustomerID Administrative user interface, although roles that are not removable from organizations can also be created via configuration. Similarly it is possible to protect role names via configuration, so that roles with specific names cannot be created in the Administrative user interface.

The configurations for roles and configurations described above are done in the `permissions.properties` file. For more information, see [Internal access control \(permissions\) - CustomerID](#).

Organizations have the following attributes:

Attribute name	Format	Description
Organization ID	UUID (RFC4122), Max length 36 characters	Internal Organization ID that is generated when organization is initially created to CustomerID.
Technical name	Case insensitive, max 1024 characters. Additional limitations may apply depending on organizationalUnit object class limit in the used directory server.	Technical name is the rightmost component in the Entity name path that must be unique in relation to its sibling organizations.
Friendly name	UTF-8 text, not empty, max 1024 characters.	A friendly name for the organization to display in the UI. All UTF-8 characters are safe.
Entity name	Case Insensitive Unique path within CustomerID naming context.	Path-like identifier uniquely identifying organization within its path-based scope. Technical name validity is configurable and is often constrained to a certain pattern within a scheme such as Finnish company ids or international VAT number. Entity name is a translation of the Organizational Unit (OU) path within the directory in exclusive relation to the Organizational Unit "eIDM Users".
Status	Numeric 0..6	Organizations use the same status enumeration as the User object.
Level	Numerical 0...2147483647	This number shows the amount of parent organizations in the path hierarchy.

Type	UTF-8 text, max 1024 characters.	Organization type (formerly known as Organization class) identifies which type configuration organization conforms to, as configured in eidm2.properties.
Created	Timestamp	This timestamp shows when this organization object was initially created.
Last modified	Timestamp	This timestamp shows when any information relational to this organization was last modified