E-vote 2011

Use case specification: 0.1 Definition of roles

Project: E-vote 2011

NORWEGIAN MINISTRY OF LOCAL GOVERNMENT
AND REGIONAL DEVELOPMENT

CONTENT

1. Executive Summary

In order to meet security objective OS 7 (Ref [2]), the system shall have a role based security model. The system must have functionality that supports:

1. The creation, amendment and inactivation of roles
2. The creation, amendment and inactivation of users
3. The mapping of users to roles
4. The creation, amendment and inactivation of permissions
5. The mapping of roles to permissions
6. The listing of securable objects
7. The mapping of permissions to securable objects
8. Filtering and searching for users, groups, permissions and securable objects returning the relations between these. The administrator must be able to see what securable objects the various roles/users have access to and what their access level is in relation to that object.

2. Purpose

The purpose of this use case is to facilitate the management of users, roles, securable objects and permissions and to provide administrators with functionality for showing the relations between these.

3. Actors

Actor	Description
Central/Local administrator	The user of the role creation module
ES	Election System

4. Pre-Conditions

ID	Description	Comments
0.1.1	User must be authenticated with sufficient rights for the management of users, roles, securable objects, permissions.	See use case 9.1 ‘Authentication’

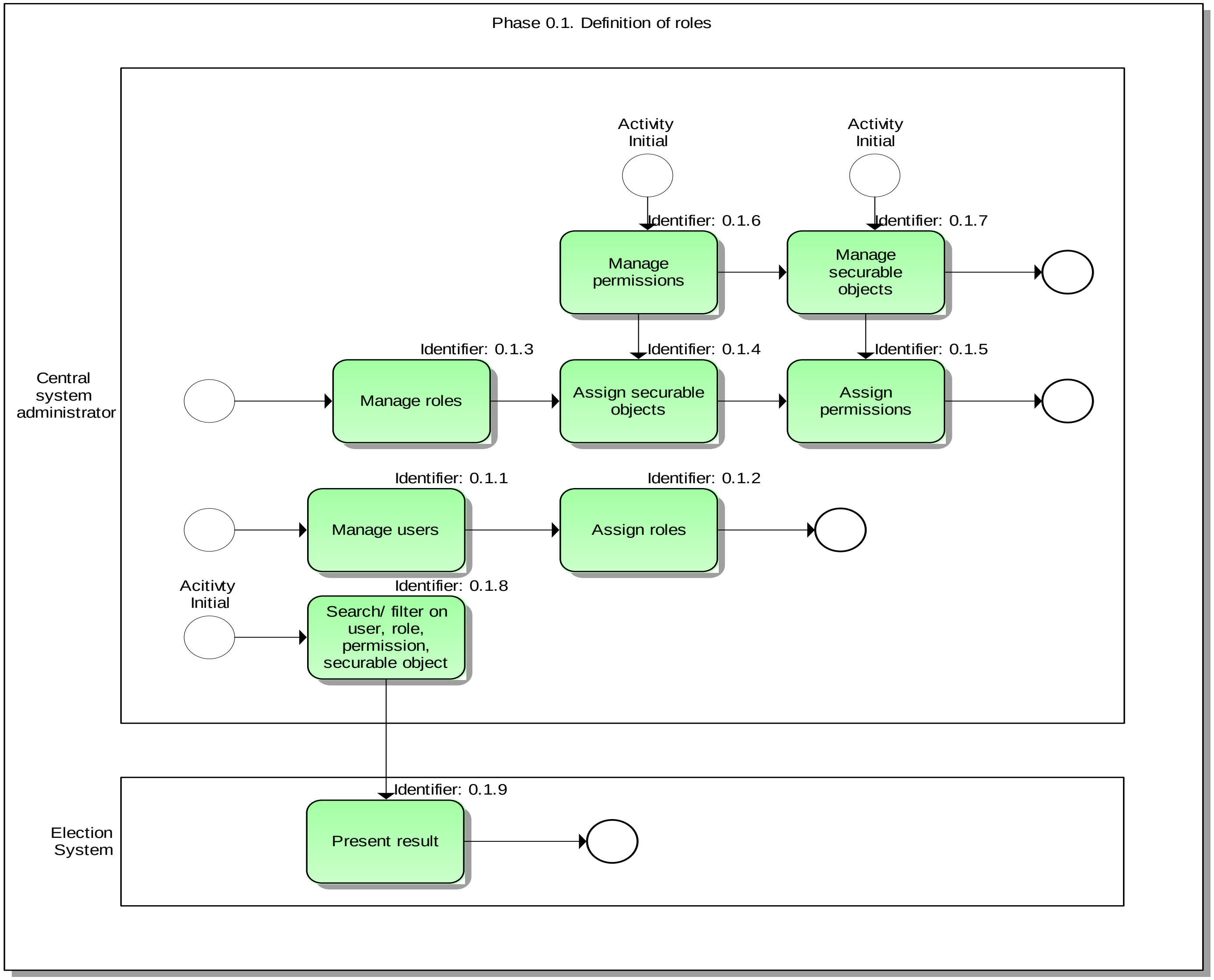
5. Post-Conditions

ID	Description	Comments
0.1.2	New users, roles, permissions, securable objects are stored in the system	
0.1.3	Changes to users, roles, permissions, securable objects are stored in the system	

6. Trigger

The need for creating new or amend existing users, roles, securable objects or permissions in the system. The need for checking the relations between user/groups, securable objects and permissions.

7. Main Flows - Functional Requirements



7.1. Main flow 1 - Manage users

ID	Actor	Function (Requirement)	Requirement description	Ref
F 0.1.1	Central/Local administrator	Manage users	The system must have functionality for the management of users. The system must have functionality for: 1. The creation of new users. Each user must have a unique identifier. 2. The maintenance of existing users 3. The deactivation of users 4. The assignment of authentication method to a user System administrators must be able to provide users with a link to a web page where users can communicate their needs regarding access to functionality in the system so that the administrator can assign roles based on their needs.	
F 0.1.2	Central/Local administrator	Assign roles	The system must have functionality for the assignment of users to one or more roles	

7.2. Main flow 2 - Manage roles

ID	Actor	Function (Requirement)	Requirement description	Ref
F 0.1.3	Central/Local administrator	Manage roles	The system must have functionality for the management of roles. The system must have functionality for: 1. The creation of new roles. It must be possible to create a new role from scratch or based on an existing one. Each role must have a unique identifier. 2. The maintenance of existing roles 3. The deactivation of roles 4. The assignment of securable objects to a role 5. The assignment of allowed actions a particular role may perform on a securable object 6. The assignment of authentication method to a role 7. The assignment of owner(s) to a role	

			Users may have several roles in the system, but some roles will be mutually exclusive. The system must have functionality for defining (flagging) what roles are mutually exclusive.	
F 0.1.4	Central/Local administrator	Assign securable objects	The system must have functionality for the mapping of securable objects to a role.	
F 0.1.5	Central/Local administrator	Assign permissions	The system must have functionality for the mapping of permissions (Create, Read, Update etc.) to a role (In relation to securable objects).	

7.3. Main flow 3 - Manage permissions

ID	**Actor**	**Function (Requirement)**	**Requirement description**	**Ref**
F 0.1.6	Central/Local administrator	Manage permissions	The system must have functionality for the management of permissions. Permission levels may include read, create, modify, delete, approve etc. The system must have functionality for: 1. The creation of permissions and permission levels. It must be possible to create a new permission level based on an existing one 2. The maintenance of existing permissions and permission levels 3. The deletion or in-activation of permissions and permission levels	

7.4. Main flow 4 - Manage securable objects

ID	Actor	Function (Requirement)	Requirement description	Ref
F 0.1.7	Central/Local administrator	Manage securable objects	The system must have functionality for the management of securable objects. Securable objects may include data sets, databases input fields, output fields, sets of functionality/module etc. The system must have functionality for: 1. The listing of all securable objects within the application. 2. Inheriting permissions and assigned roles from another securable object 3. Breaking inheritance between securable objects	

7.5. Main flow 5 - Search/filter on user, role, securable object or permission

ID	Actor	Function (Requirement)	Requirement description	Ref
F 0.1.8	Central/Local administrator	Search/Filter on user, role, securable object or permission	1. The system must have functionality for searching/filtering on user, role, securable object and permission. 2. The system must have functionality for viewing the inheritance hierarchy of secureable objects/roles/permissions	
F 0.1.9	ES	Present results	The system shall present the relations between user, role, securable object and permission .	

8. Non-Functional Requirements

8.1. Accessibility and usability

ID	Requirement description	Ref
0.1.4	See ‘Accessibility and usability’ requirements	8.1

8.2. Security

ID	Requirement description	Scope
OS0.19	Before executing any action required by the election officers, the election system shall identify and authenticate the election officers and verify the officers right to perform the action.	
OS7.3	The access control system shall be sufficiently flexible and granular to support the change of existing, or introduction of new roles.	
OS7.17	Administrator, operator and auditor access to the election system shall require strong authentication (i.e two factor authentication).	

8.3. Rules & regulations

ID	Requirement description	Scope
0.1.5	This use case refers to regulations described in the Representation of the People Act (the Election Act). http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/Representation_of_the_People_Act170609.pdf	
0.1.6	This use case refers to regulations relating to parliamentary and local government elections (Representation of the People Regulations) http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/Regulations_2003_EN_170609.pdf	
0.1.7	This use case also refer to the Council of Europe e-vote Recommendation Rec(2004) 11. http://www.coe.int/t/dgap/democracy/activities/GGIS/E-voting/Key_Documents/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf	

8.4. Performance (frequency)

ID	Requirement description	Scope
P 0.1.1	Checking of permissions for access to securable objects shall not cause any significant increase in the election system response times.	