

Design Document for caArray

Use Cases

Issue <1.5>

Revision History

Date	Issue	Description	Author
01/02/2004	1.1	Initial version	Carleen Dickerson
01/14/2004	1.2		Carleen Dickerson
01/14/2004	1.3		Carleen Dickerson
02/05/2004	1.4	Modified to be sure to pick up all sub- use cases.	Carleen Dickerson
3/26/2004	1.5	Printed for final review	Harris Johnson

Table of Contents

1.	Actors.....	7
1.1	UserManager	7
1.2	Data Owner.....	7
1.3	User.....	7
1.4	Repository Curator	7
1.5	ExperimentManager	7
1.6	ConfigurationManager.....	7
1.7	Application	7
1.8	Curator.....	7
2.	Use Cases	8
2.1	ManageUsersDetails.....	9
2.1.1	Create User	9
2.1.2	Remove User	10
2.1.3	Create Role	10
2.1.4	Remove Role	10
2.1.5	Assign Roles To User.....	10
2.1.6	Select Consortiums to Limit Roles For User.....	10
2.1.7	Create Consortium.....	10
2.1.8	Remove Consortium	10
2.1.9	Remove Person	10
2.1.10	Modify User.....	10
2.1.11	Modify Role.....	10
2.1.12	Modify Consortium	10
2.1.13	Modify Person	11
2.1.14	Modify Organization	11
2.1.15	Remove Organization	11
2.1.16	Create Organization.....	11
2.1.17	Promote Person to User	11
2.1.18	Demote User to Person	11
2.1.19	Create Person.....	11

2.1.20	Register as New Person	11
2.1.21	Change Own Password	11
2.2	ManageDataAccessDetails	12
2.2.1	Update Protected Data.....	13
2.2.2	Read Protected Data	13
2.2.3	Login.....	13
2.2.4	Logout.....	13
2.2.5	Add Protected Data to System.....	13
2.2.6	Submit Request to Share Data.....	13
2.2.7	Specify Visibility of Protected Data.....	13
2.2.8	Delete Protected Data from System.....	13
2.2.9	Specify Owner of Protected Data.....	13
2.3	ManageExperimentDetails	14
2.3.1	Submit MAGE-ML Experiment.....	15
2.3.2	Submit Affy Experiment	15
2.3.3	Submit Genepix Experiment	15
2.3.4	Submit Experiment	15
2.3.5	ModifyExperiment.....	15
2.3.5.1	Add Affymetrix .cel File	16
2.3.5.2	Add Affymetrix .chp File	16
2.3.5.3	Add Genepix .gpr File.....	16
2.3.5.4	Retrieve Publication Data	17
2.3.5.5	Lock Experiment.....	17
2.3.5.6	Unlock Experiment	17
2.3.5.7	Change Experiment Basic Data	17
2.3.5.8	Add Hybridization.....	17
2.3.5.9	Remove Hybridization	17
2.3.5.10	Add Publication.....	17
2.3.5.11	Remove Publication	17
2.3.5.12	Annotate Experiment	17
2.3.5.13	Add Other Files to Experiment	17
2.3.5.14	Remove Other Files from Experiment	17
2.3.6	Specify Visibility of Protected Data.....	17
2.3.7	Remove Experiment	18
2.3.8	Lock Experiment	18
2.3.9	Unlock Experiment.....	18
2.3.10	Search Experiments	18

2.3.11	Download Experiment Files	18
2.3.12	Download Experiment MAGE-ML	18
2.3.13	Download Original MAGE-ML	18
2.3.14	*Download Experiment Protocol Report	18
2.4	ManageBioMaterialsDetails	19
2.4.1	Split.....	19
2.4.2	Pool.....	19
2.4.3	Label	19
2.4.4	Treatment.....	19
2.4.5	Specify BioMaterialCharacteristics.....	19
2.4.6	Modify BioMaterial.....	20
2.4.7	Search BioMaterials	20
2.4.8	Add BioSource	20
2.4.9	Duplicate BioMaterial	20
2.4.10	Remove BioMaterial.....	20
2.4.11	Deactivate/Activate BioMaterial	20
2.4.12	Apply Treatments	20
2.4.13	Transfer Ownership	20
2.5	ManageArrayDesignsDetails	21
2.5.1	Submit MAGE-ML Array Design	21
2.5.2	Submit Affy Array Design.....	21
2.5.3	Submit Genepix Array Design	22
2.5.4	Remove Array Design	22
2.5.5	Specify Visibility of Protected Data.....	22
2.5.6	Search Array Designs	22
2.5.7	Submit Array Design	22
2.5.8	Modify Array Design.....	22
2.5.8.1	Apply Manufacture Protocol.....	22
2.5.8.2	Add Array Design Provider.....	23
2.5.8.3	Remove Array Design Provider	23
2.5.8.4	Modify Array Design General Information	23
2.5.9	*Make Array Design Obsolete	23
2.6	ManageProtocolsDetails	24
2.6.1	Specify Visibility of Protected Data.....	25
2.6.2	Remove Protocol	25
2.6.3	Search Protocols	25

2.6.4	Create New Protocol.....	25
2.6.5	Add Parameter to Protocol	25
2.6.6	Remove Parameter from Protocol	25
2.6.7	Add Hardware to Protocol.....	25
2.6.8	Remove Hardware from Protocol.....	25
2.6.9	Add Software to Protocol	25
2.6.10	Remove Software from Protocol	25
2.6.11	*Upload File Containing Protocol Details	25
2.6.12	*Download File Containing Protocol Details	26
2.6.13	Modify Protocol Details	26
2.7	ManageSoftwareAndHardwareDetails.....	26
2.7.1	Add Software.....	26
2.7.2	Remove Software	26
2.7.3	Modify Software.....	27
2.7.4	Add Hardware Parameter	27
2.7.5	Remove Hardware Parameter	27
2.7.6	Modify Hardware Parameter Value.....	27
2.7.7	Modify Software Parameter Value	27
2.7.8	Add Software Parameter.....	27
2.7.9	Remove Software Parameter	27
2.7.10	Modify Hardware	27
2.7.11	Remove Hardware	27
2.7.12	Add Hardware.....	27

caArray Use Cases

1. Actors

1.1 UserManager

A UserManager is a user that is expected to use the system only for the purposes of making it accessible to other users. A user manager is responsible for creating data sharing consortiums, users, organizations and people. The user manager is responsible for assigning role and consortium access to users and thus is responsible for determining which users can perform which actions on which data.

1.2 Data Owner

A data owner is any user that is currently listed as the owner of any protected data element in the system. Protected data elements include experiments, protocols and array designs.

1.3 User

A User is any individual who will use the system to submit data or search through and utilize existing data.

1.4 Repository Curator

A repository curator is a user who is responsible for the integrity of the data stored in the repository.

1.5 ExperimentManager

An ExperimentManager is a user who is responsible for maintaining the data associated with experiments for their groups.

1.6 ConfigurationManager

A ConfigurationManager is a user that is expected to manage the protocols, hardware, software and array designs that are utilized by a particular group.

1.7 Application

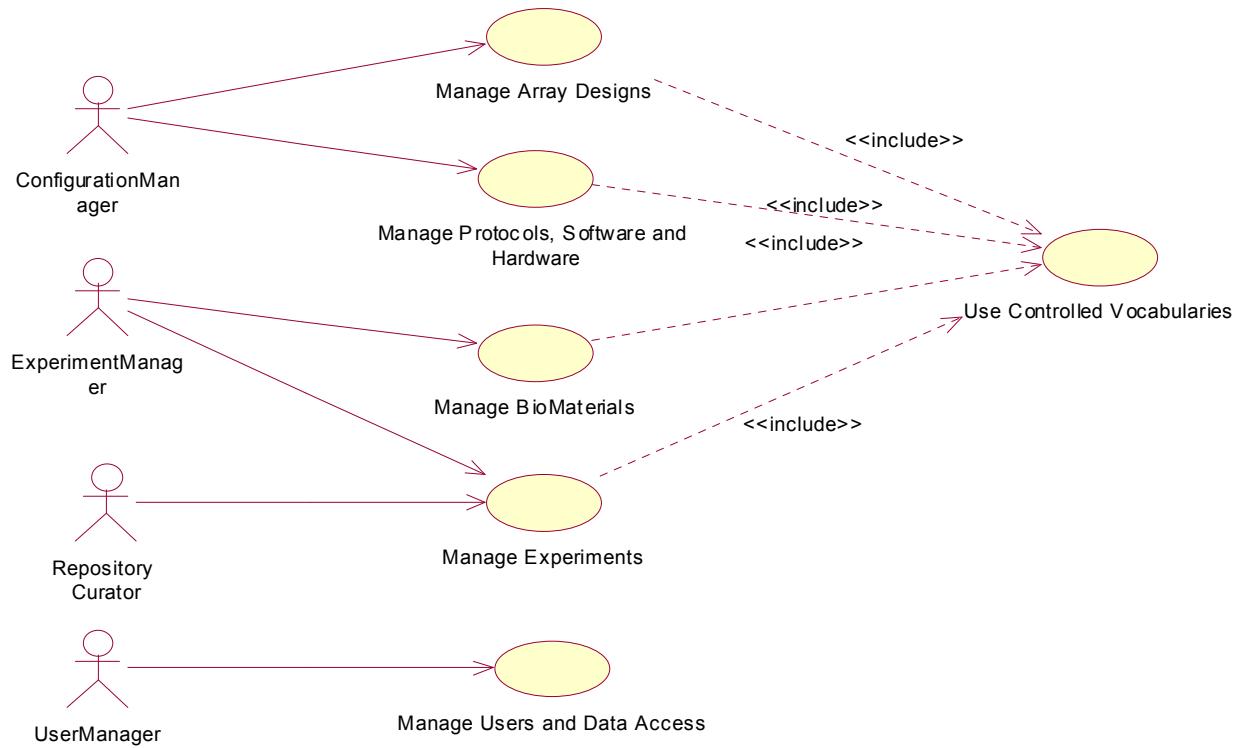
An application is a user of the SecurityManager. The application will login to the SecurityManager service and perform security checks/operations on behalf of the user.

1.8 Curator

A curator is a user who is responsible for the integrity of the data for a particular set of groups.

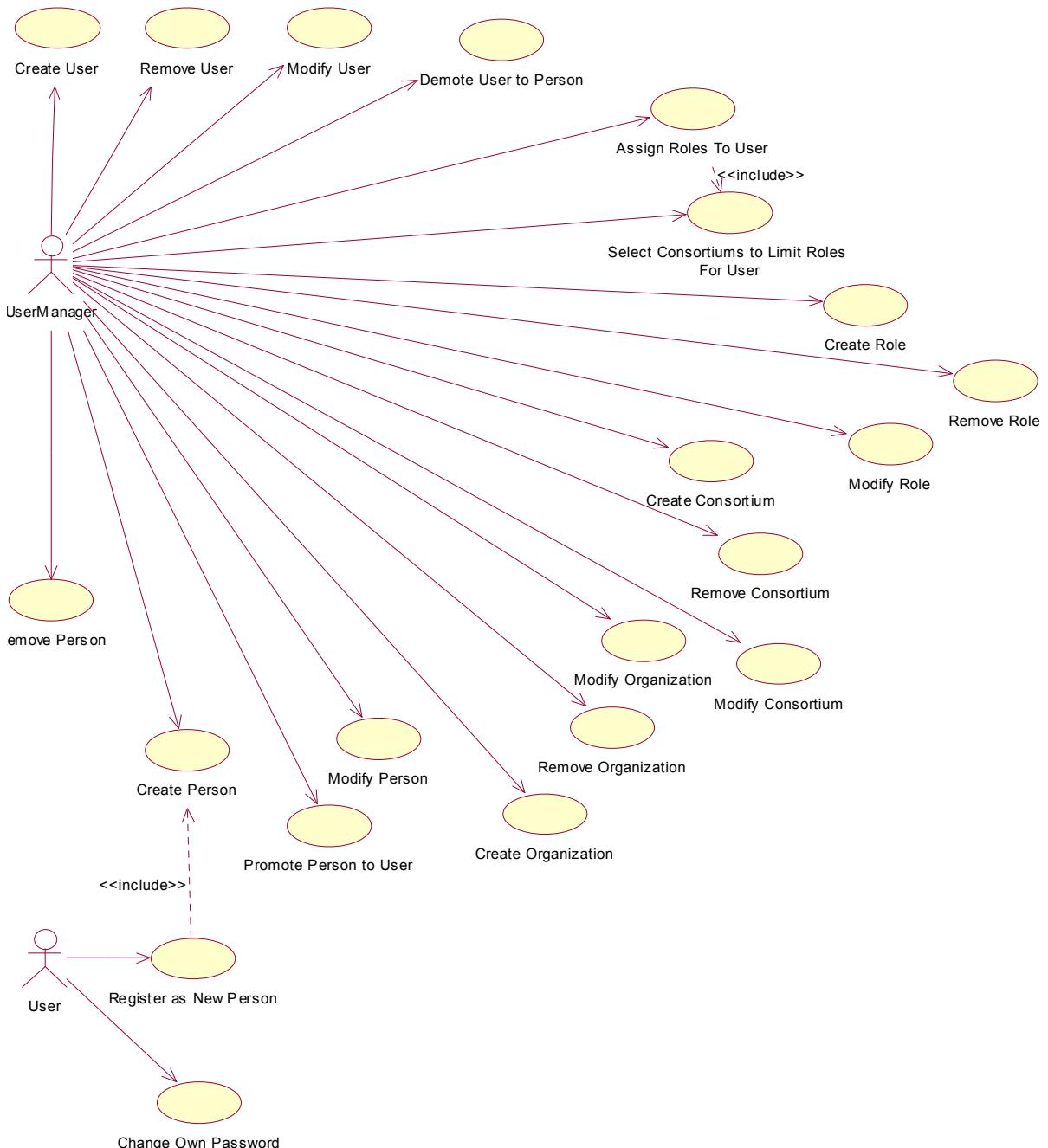
2. Use Cases

caArrayTop



This diagram shows the uses of the caArray system from the top level. Users of the system will be able to manage array designs, protocols, software, hardware, biomaterials, users and experiments. This diagram also shows the high level breakout of responsibilities to different classes of users.

2.1 ManageUsersDetails



This diagram shows the actions that a user may perform related to managing users of the system.

2.1.1 Create User

A user with sufficient privileges (generally an administrator) may create a new user of the system. The new user will initially have no rights.

2.1.2 Remove User

A user with sufficient privileges (generally an administrator) may remove a user from the system. If the user is logged in when removed, they will be able to use the system until they log out. They will not be able to log in again.

2.1.3 Create Role

A user with sufficient privileges (generally an administrator) may create a new role for use in the system. A role specifies a collection of privileges that should be granted to all users that it is assigned to.

2.1.4 Remove Role

A user with sufficient privileges (generally an administrator) may remove an existing role from the system.

2.1.5 Assign Roles To User

A user with sufficient privileges (generally an administrator) may assign an existing role to an existing user. Doing so will grant the user all privileges assigned to that role. The new privileges will take effect the next time that user logs in.

2.1.6 Select Consortiums to Limit Roles For User

A user with sufficient privileges (generally an administrator) may specify which protected data elements the role assignment pertains to. Thus a user may be granted a role that contains the "modify experiment data" privilege, and that assignment may be limited by specifying that this user can only modify experiments for consortium A.

2.1.7 Create Consortium

A user with sufficient privileges (generally an administrator) may create a new consortium for sharing protected data. The new consortium will initially not be associated with any experiments or roles.

2.1.8 Remove Consortium

A user with sufficient privileges (generally an administrator) may remove an existing consortium. The consortium that is being removed will be disassociated from any data that it was protecting, and from any roles.

2.1.9 Remove Person

An administrative user may remove an existing person from the system. The person may not be removed if there are experiments where he/she is selected as a contact. In this case, the user will be shown the list of experiments that are preventing the removal.

2.1.10 Modify User

A user with sufficient privileges may modify the attributes of a user. This includes all of the contact information as well as the user's password.

2.1.11 Modify Role

A user with sufficient privileges may modify an existing role.

2.1.12 Modify Consortium

A user with sufficient privileges may modify the attributes of a consortium.

2.1.13 Modify Person

A user with sufficient privileges may modify a person.

2.1.14 Modify Organization

A user with sufficient privileges may modify an organization.

2.1.15 Remove Organization

A user with sufficient privileges may remove an organization. If this organization is referenced by other entities in the system such as hardware or software, it will not be removed. In this case the user will receive an error message telling them what entities are referencing the organization.

2.1.16 Create Organization

A user with sufficient privileges may create a new organization.

2.1.17 Promote Person to User

A user with sufficient privileges may promote a person to a user. The user performing the promotion will need to specify a login id and password for the person to use.

2.1.18 Demote User to Person

A user with sufficient privileges may demote a user to a person. When this is done the user will no longer be able to login to the system. However, he/she will remain in the system as a person. This implies that his/her contact information will not be lost and that the person can continue to be associated as a contact for experiments.

2.1.19 Create Person

An administrative user may define a new Person. People are associated with experiments. They are not used to control access to data.

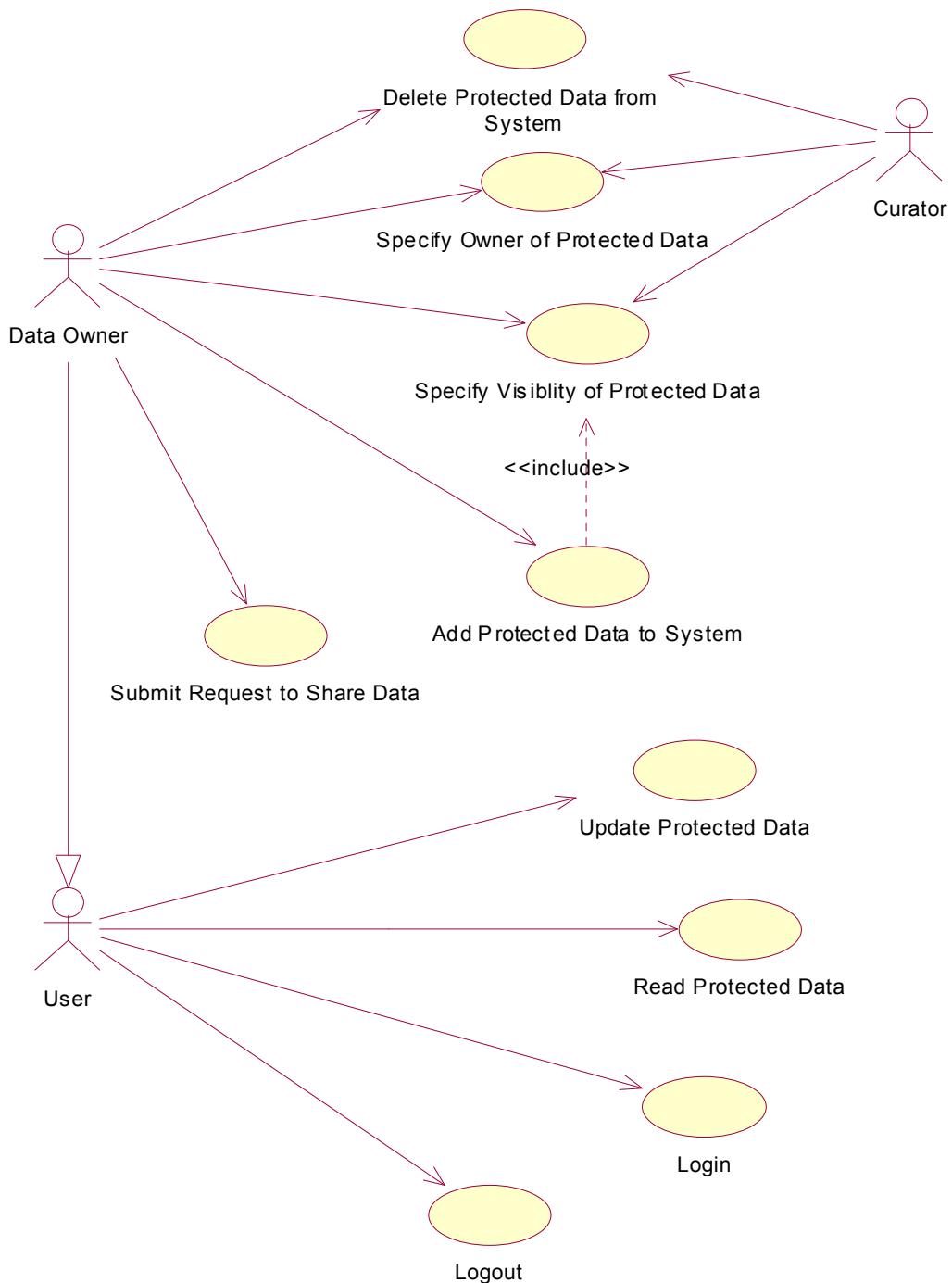
2.1.20 Register as New Person

A user visiting the site may register as a new person. When this action is performed, the person will specify a user name, password, and contact information. The user account will not be created at this time. Instead, the Person will be created and an email will be sent to the support address. A UserManager will then promote the new person to a user and an email will be sent notifying the user that their account is available for access.

2.1.21 Change Own Password

A user can change his/her own password. In order to do this the user must specify their existing password, a valid new password and a verification of the new password.

2.2 ManageDataAccessDetails



This diagram shows the general data management concepts in the caArray system. Protected Data refers to any type of data that is considered "protected" in the caArray system. This list currently includes the following: Experiment, Protocol, Hardware, Software, Array Design, BioSource, BioSample, and Labeled Extracts. Only the owner of a protected data item, or a curator for a protection group that item belongs to, may delete the item, change its visibility, or transfer its ownership.

2.2.1 Update Protected Data

A user with sufficient privileges may update a protected data element. This is done via other use cases such as Modify Experiment and Modify Array Design.

2.2.2 Read Protected Data

A user with sufficient privileges may read/view protected data. This is done via other use cases such as Search Experiments, Search Protocols and Search Array Designs.

2.2.3 Login

A user may login to the system. Users that are not logged in may view only public data elements. Once a user is logged in his/her roles and consortium assignments are used to determine which protected data elements he/she should be able to access.

2.2.4 Logout

A user may logout of the system.

2.2.5 Add Protected Data to System

A user may add protected data to the system. This is done via other use cases such as Submit Experiment, Add Protocol and Add Array Design.

2.2.6 Submit Request to Share Data

The user that is specified as the owner of an existing experiment may request that his/her data be shared with a group of users. Note that this is not necessary if a consortium already exists for the desired users. In this case, the data owner may use the "Specify Visibility of Protected Data" to allow this consortium to view his/her data.

2.2.7 Specify Visibility of Protected Data

The user that is specified as the owner of protected data may specify the visibility of that data. Visibility may be private (visible only to the owner), public (visible to all), or may be one or more consortiums.

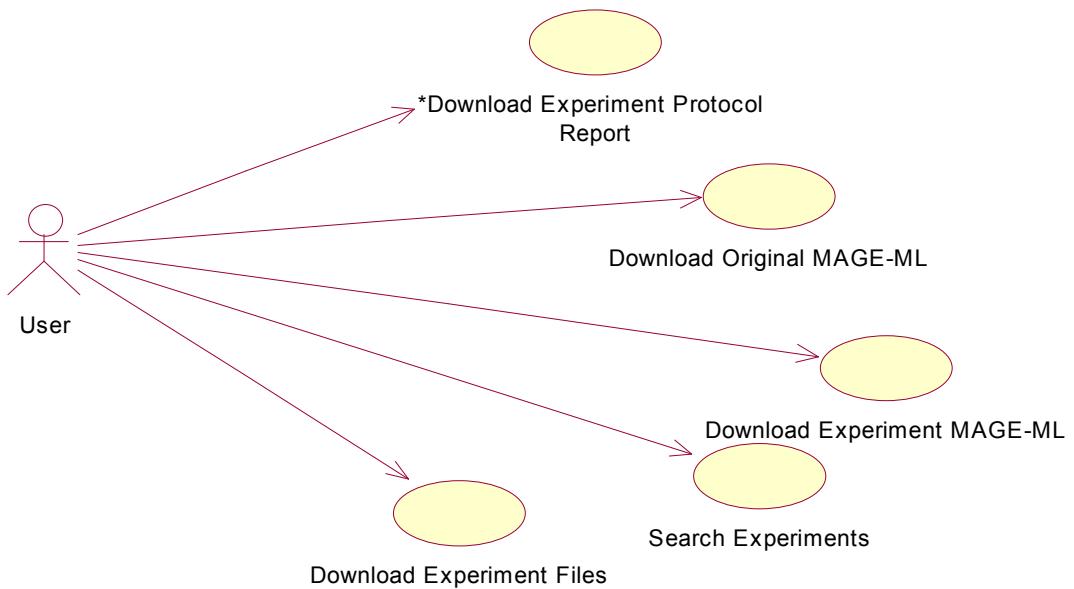
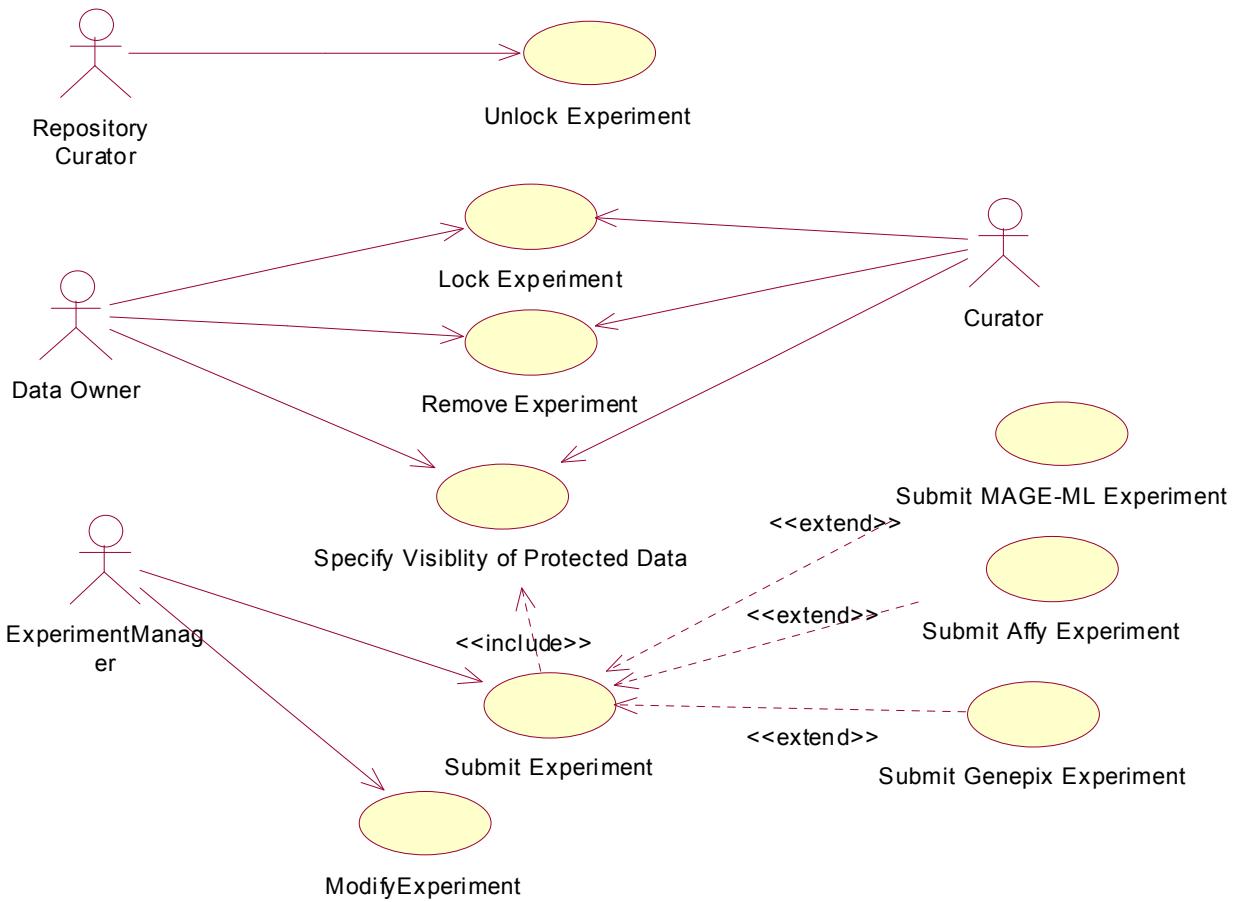
2.2.8 Delete Protected Data from System

The user that is specified as the owner of a protected data element may choose to remove it from the system. This is done via other use cases such as Remove Experiment, Remove Protocol and Remove Array Design.

2.2.9 Specify Owner of Protected Data

The owner of a protected data element may specify a new owner for that element. The new owner may be any user of the system.

2.3 ManageExperimentDetails



This diagram shows the actions that users may perform on an existing experiment.

2.3.1 Submit MAGE-ML Experiment

A user may submit an experiment as MAGE-ML that has been exported from another system. In this case it is expected that the MAGE-ML will conform to the latest MGED DTD. The system will be tested with sample MAGE-ML from the MGED site and with MAGE-ML that has been exported from the MIAMExpress system.

2.3.2 Submit Affy Experiment

A user may submit an experiment in Affymetrix native file formats. This type of experiment must include .cel files for each hybridization at a minimum.

2.3.3 Submit Genepix Experiment

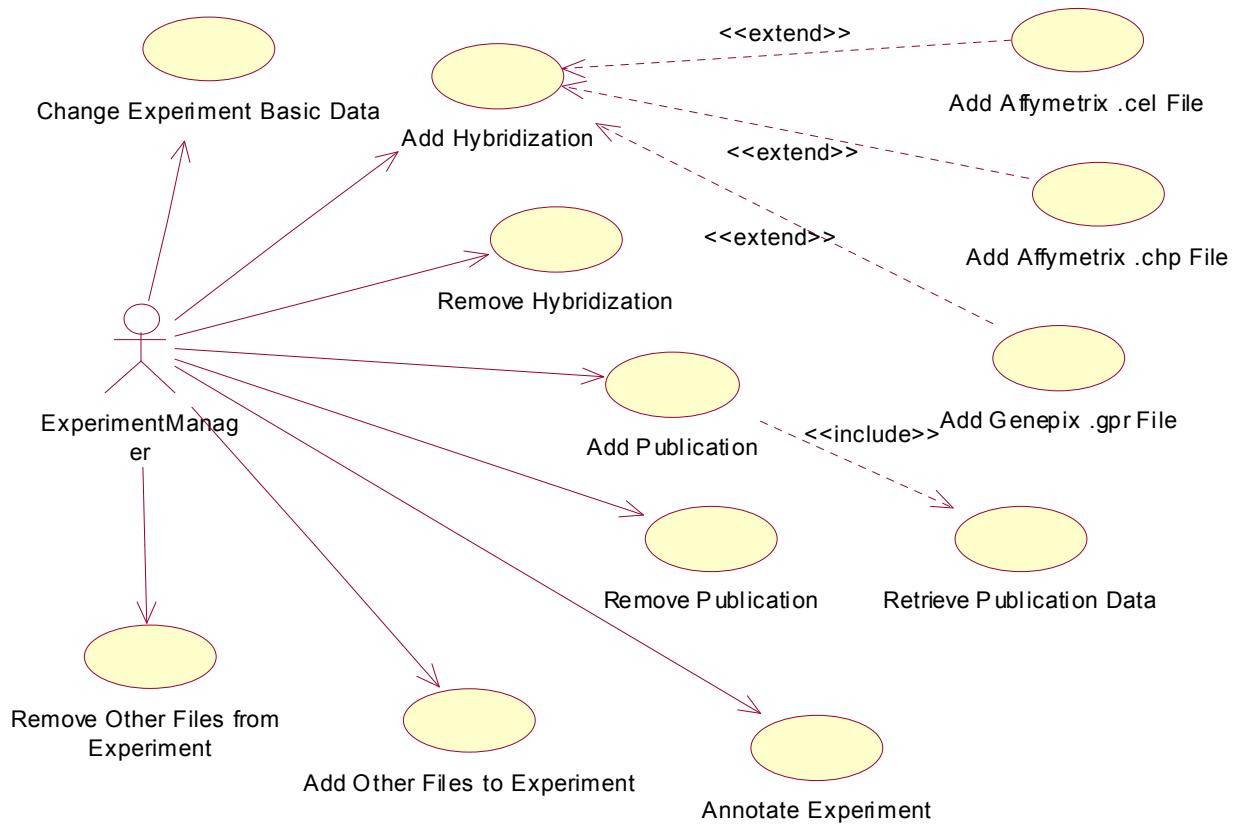
A user may submit an experiment in Genepix native file format. In this case a .gpr file is required for each hybridization.

2.3.4 Submit Experiment

A user may submit a new experiment. Refer to the extending use cases for details about the types of experiment submissions the system supports.

2.3.5 ModifyExperiment

A user may modify a previously submitted experiment. Refer to the ModifyExperimentDetails diagram for details.



2.3.5.1 Add Affymetrix .cel File

A user with sufficient privileges may add a new Affymetrix .cel file to an existing Affymetrix experiment. This will result in an additional MeasureBioAssay and associated elements being added to the experiment.

2.3.5.2 Add Affymetrix .chp File

A user with sufficient privileges may add a new Affymetrix .chp file to an existing Affymetrix experiment. This will result in an additional DerivedBioAssay and associated elements being added to the experiment.

2.3.5.3 Add Genepix .gpr File

A user with sufficient privileges may add a new GenePix .gpr file to an existing GenePix experiment. This will result in additional MeasureBioAssay and DerivedBioAssay elements being added to the

experiment.

2.3.5.4 Retrieve Publication Data

The system will be capable of retrieving information from the PubMed database given a PubMed ID.

2.3.5.5 Lock Experiment

A user with sufficient privileges may lock an experiment so that no further modifications can be made to it. Performing this action will transfer ownership of the experiment to the user that locks it.

2.3.5.6 Unlock Experiment

A user with sufficient privileges may unlock an experiment so that further modifications can be made to it.

2.3.5.7 Change Experiment Basic Data

A user may change the basic attributes of an experiment including its description, private investigators name and species.

2.3.5.8 Add Hybridization

A user with sufficient privileges may add a new hybridization to an existing experiment. See extending use cases to determine what types of hybridizations may be added.

2.3.5.9 Remove Hybridization

A user with sufficient privileges may remove a hybridization from an existing experiment. Doing so will remove all data for that hybridization.

2.3.5.10 Add Publication

A user with sufficient privileges may add publication data to an existing experiment. Information may be manually entered, or may be retrieved from the PubMed database if the user supplies a PubMed identifier.

2.3.5.11 Remove Publication

A user may remove a publication from an experiment.

2.3.5.12 Annotate Experiment

A user with sufficient privileges may annotate an existing experiment. Refer to the AnnotateExperimentDetails use case diagram for more details.

2.3.5.13 Add Other Files to Experiment

A user with sufficient privileges may add files of type "other" to an experiment. These files will not be interpreted by the system in any way. They will simply be stored with the experiment and made available to users for download.

2.3.5.14 Remove Other Files from Experiment

A user with sufficient privileges may remove "other" files associated with an experiment. The removed files will no longer be available for users to download.

2.3.6 Specify Visibility of Protected Data

The user that is specified as the owner of protected data may specify the visibility of that data. Visibility may be private (visible only to the owner), public (visible to all), or may be one or more consortiums.

2.3.7 Remove Experiment

The owner of an experiment may remove it from the system. Doing so will also remove any protocol applications for the experiment, but will not remove the protocols themselves.

2.3.8 Lock Experiment

A user with sufficient privileges may lock an experiment so that no further modifications can be made to it. Performing this action will transfer ownership of the experiment to the user that locks it.

2.3.9 Unlock Experiment

A user with sufficient privileges may unlock an experiment so that further modifications can be made to it.

2.3.10 Search Experiments

A user may search the existing experiments in the system. If no search criteria are specified, all experiments that the user has permission to see will be returned.

2.3.11 Download Experiment Files

A user may download any files that were uploaded in association with an experiment.

2.3.12 Download Experiment MAGE-ML

The user may request that the system export MAGE-ML for an entire experiment. The MAGE-ML document that is generated will be downloadable to the users computer as a .zip file.

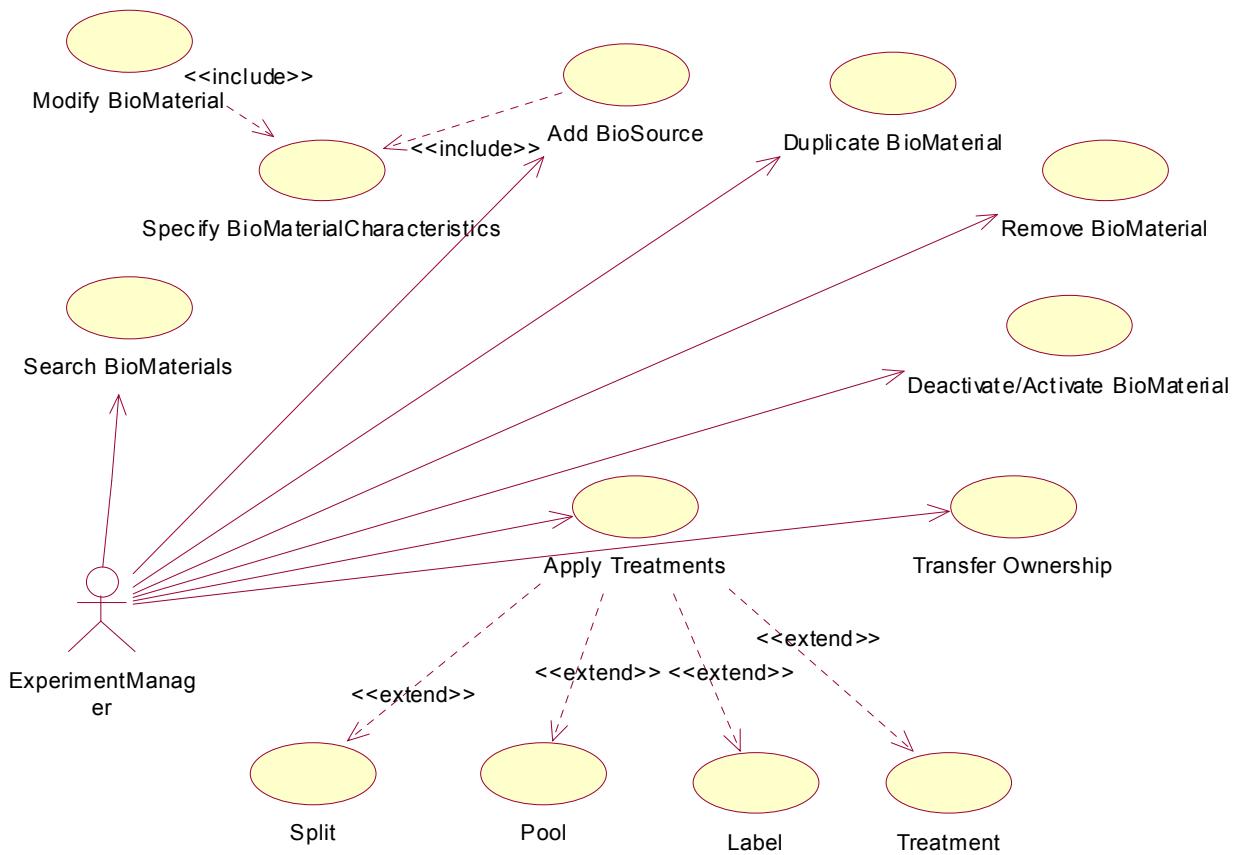
2.3.13 Download Original MAGE-ML

If an experiment was created by uploading MAGE-ML then a user may opt to download the original MAGE-ML that was submitted. This will differ from the current MAGE-ML for the experiment, if any modifications were made to the experiment after submission.

2.3.14 *Download Experiment Protocol Report

A user may download a report of all protocols that were applied in the processing of a particular experiment.

2.4 ManageBioMaterialsDetails



This diagram shows the actions that a user may perform related to BioMaterials.

2.4.1 Split

Split is a type of bio-event when a biomaterial is treated to produce multiple biosamples.

2.4.2 Pool

Pool is a type of bio-event when several biomaterials are pooled together to produce one biomaterial. This is a batch operation by definition.

2.4.3 Label

Label is a type of bio-event when a biosample is labeled to produce Labeled Extract. Labeling of biosamples can be annotated in a batch mode.

2.4.4 Treatment

All types of bio-event treatments (other than split, pool, and label) can be annotated using this option. Treatment of biomaterials can be annotated in a batch mode.

2.4.5 Specify BioMaterialCharacteristics

A user may specify/modify BioMaterial Characteristics according to MGED Ontologies specifications. A user will have an option to select which characteristics to specify; specification of characteristics will be

customized according to the corresponding MGED definitions.

2.4.6 Modify BioMaterial

A user with the correct privileges may modify BioMaterial (biosource, biosample, or labeled extract) information.

2.4.7 Search BioMaterials

A user may search the biomaterials (biosources, biosamples, or labeled extracts) that exist in the system. Specifying no search criteria will return a list of all biomaterials (biosources, biosamples, or labeled extracts) that the searching user is permitted to see.

2.4.8 Add BioSource

The BioSource is the original source material before any treatment events. Two other types of biomaterials (biosamples and labeled extracts) are not entered anew; they are created as a result of one or more bio-events (treatments).

2.4.9 Duplicate BioMaterial

A user may copy a biomaterial (biosources, biosamples, or labeled extracts) under a different name to streamline the annotation of biomaterials (biosources, biosamples, or labeled extracts).

2.4.10 Remove BioMaterial

The user that is currently the owner of a biomaterial (biosource, biosample, or labeled extract) may remove it from the system. If any object exist in the system that reference the biomaterial then the system will inform the user of the objects that are preventing the removal and the operations will not be permitted.

2.4.11 Deactivate/Activate BioMaterial

The user that is currently the owner of a biomaterial (biosource, biosample, or labeled extract) may deactivate it from showing the system; the biomaterial is not deleted though and can be re-activated if necessary.

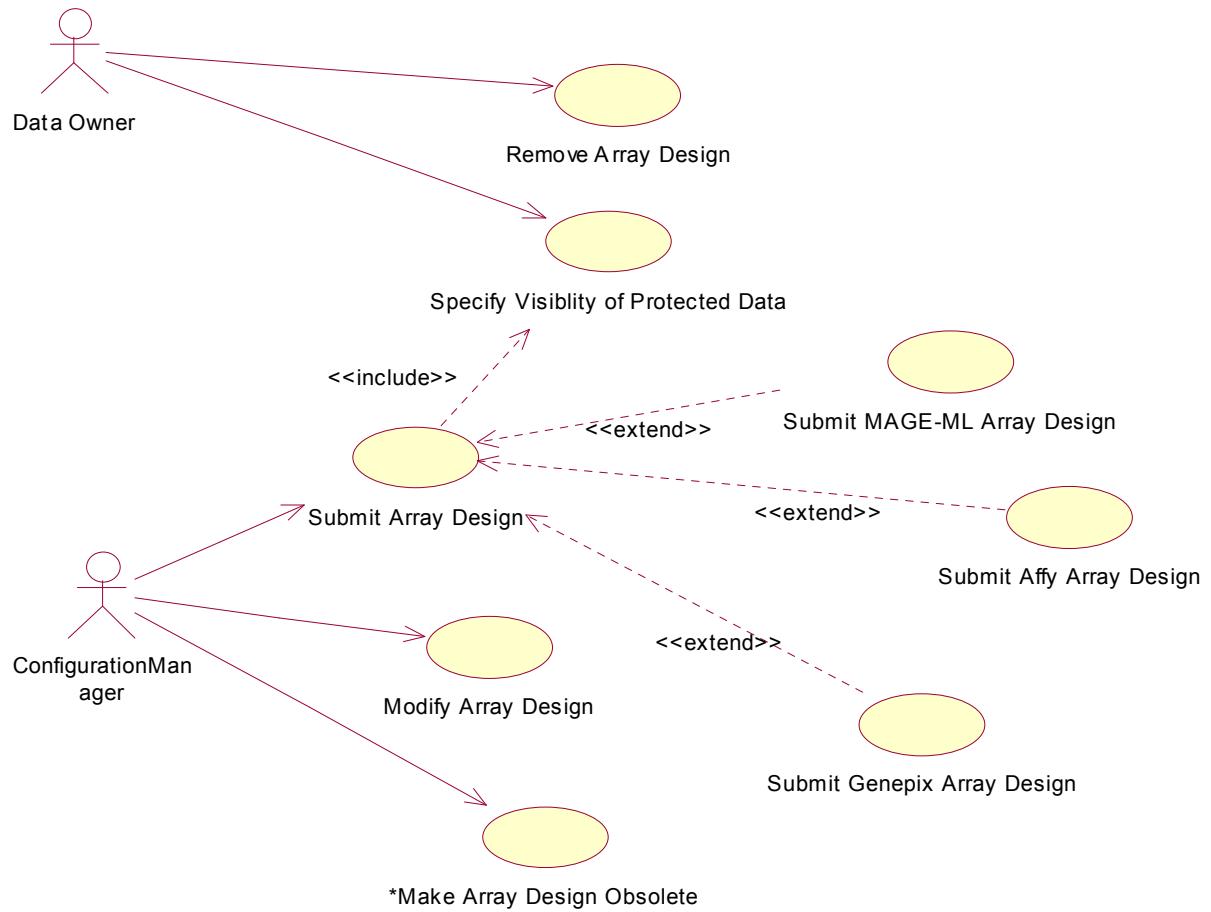
2.4.12 Apply Treatments

A treatment is a bio-event that results in creation of new biosamples. If multiple biomaterials are treated in a similar way the treatment of those can be annotated in a batch then.

2.4.13 Transfer Ownership

A user with the correct privileges may transfer ownership to another user.

2.5 ManageArrayDesignsDetails



* Indicates that the use case will be implemented in a future release of the caArray system.

This diagram shows the actions that a user may perform related to array designs.

2.5.1 Submit MAGE-ML Array Design

A user may submit a new array design by uploading the MAGE-ML file that describes the design.

2.5.2 Submit Affy Array Design

A user may submit a new array design by uploading the MAGE-ML file(s) that describe the design.

2.5.3 Submit Genepix Array Design

A user may submit a new array design by uploading the Genepix .GAL file that describes the design.

2.5.4 Remove Array Design

The user that is currently the owner of an array design may remove it from the system. If any experiments exist in the system that reference the array design then the system will inform the user of the experiments that are preventing the removal and the operations will not be permitted.

2.5.5 Specify Visibility of Protected Data

The user that is specified as the owner of protected data may specify the visibility of that data. Visibility may be private (visible only to the owner), public (visible to all), or may be one or more consortiums.

2.5.6 Search Array Designs

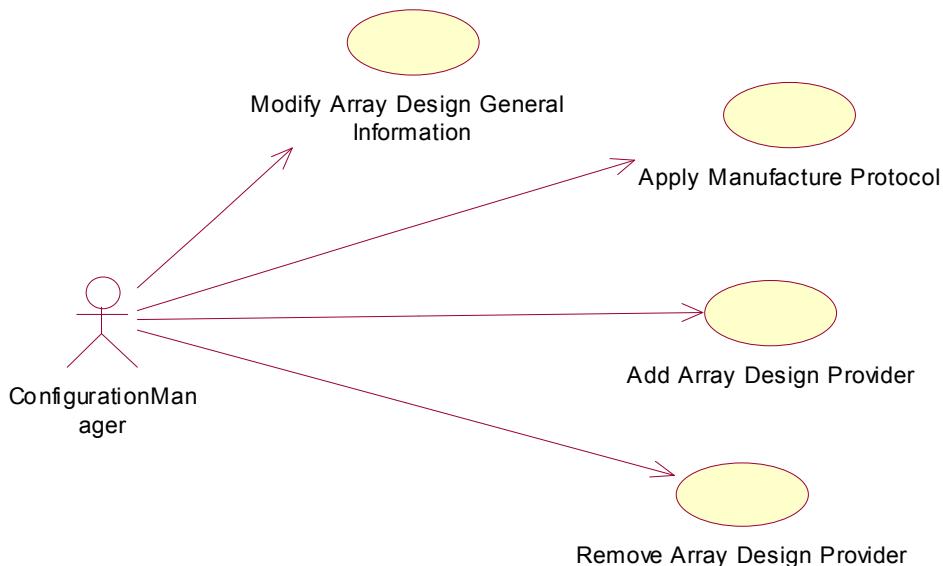
A user may search the array designs available in the system. The user may search by species, technology type, visibility, substrate type, service type, attachment type, strand type and array design name. Specifying none of these criteria will return all array designs that the user has rights to view.

2.5.7 Submit Array Design

A user may submit a new array design to the system. If an array design with the specified name already exists, the user will be notified that the array design cannot be stored. The user may then either submit the array design with a new name, or may remove the existing array design if he/she has appropriate privilege to do so, and then attempt the submission again.

2.5.8 Modify Array Design

A user with the correct privileges may modify an array design that has been previously submitted. Refer to the *ModifyArrayDesigns* use case diagram for details.



This diagram shows the actions that a user may perform to modify an existing array design in the system.

2.5.8.1 Apply Manufacture Protocol

A user may apply a manufacture protocol to an array design. The application of the protocol to the array

design involves choosing a previously defined protocol from an available list and providing values for all parameters defined in the protocol.

2.5.8.2 Add Array Design Provider

A user with sufficient privileges may add a provider to an array design. The user will be prompted to select the provider from a list of known people in the system and will also be asked to specify the role that the provider played.

2.5.8.3 Remove Array Design Provider

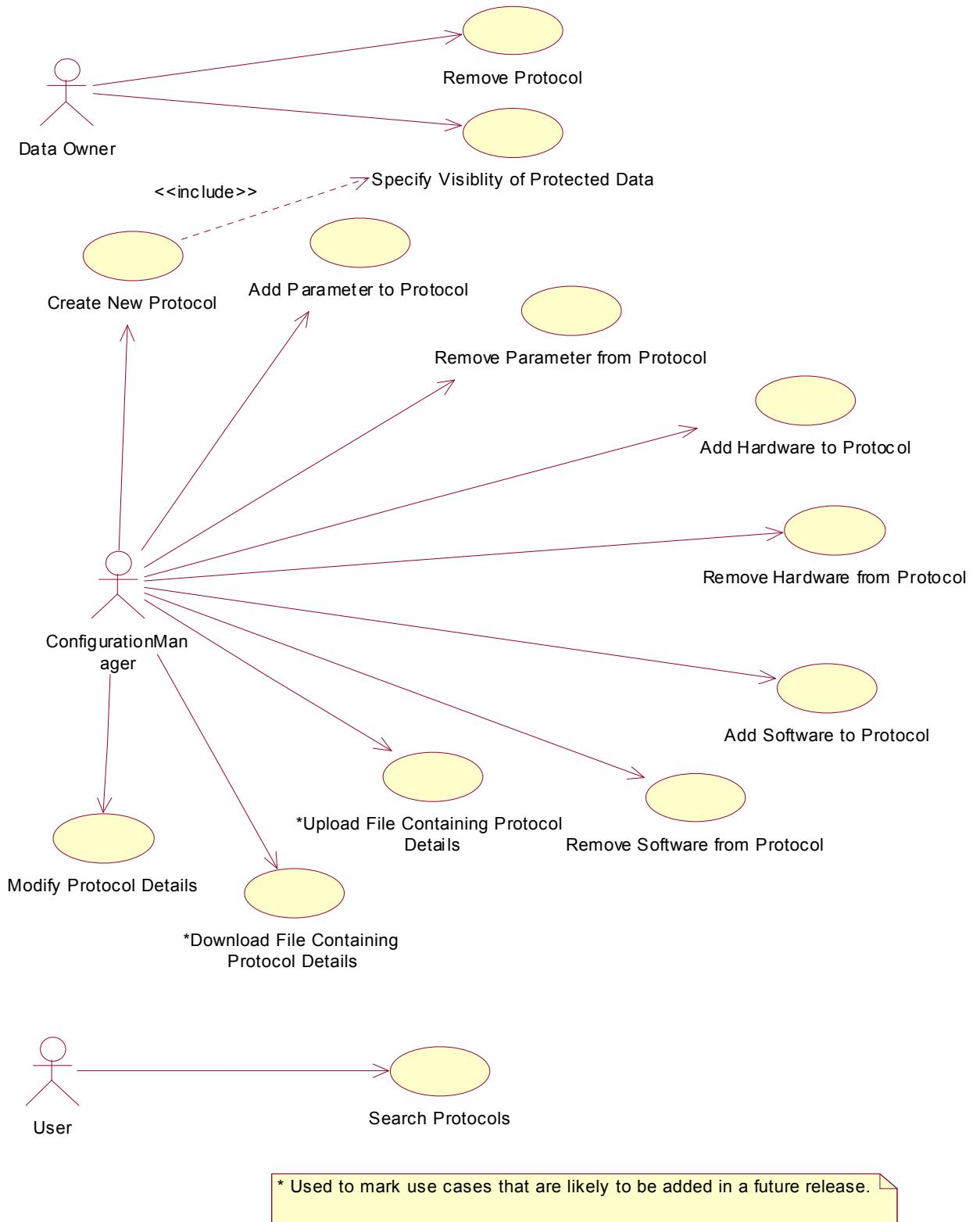
A user with sufficient privileges may remove a provider from an array design.

2.5.8.4 Modify Array Design General Information

2.5.9 *Make Array Design Obsolete

A user with sufficient privileges may make an array design obsolete. Doing so will allow the array design to remain in the system, but will keep it from being used in the future.

2.6 ManageProtocolsDetails



This diagram shows the actions that a user may perform related to protocol management and definition.

2.6.1 Specify Visibility of Protected Data

The user that is specified as the owner of protected data may specify the visibility of that data. Visibility may be private (visible only to the owner), public (visible to all), or may be one or more consortiums.

2.6.2 Remove Protocol

The owner of a protocol may remove it from the system. This operation will not be permitted if there are experiments or array designs that are related to the protocol via a protocol application. If this is the case, the user will be given a list of protocol applications that are preventing the removal of the protocol.

2.6.3 Search Protocols

A user may search the existing protocols that exist in the system. Specifying no search criteria will return a list of all protocols that the searching user is permitted to see.

2.6.4 Create New Protocol

A user may create a new protocol for use in the system.

2.6.5 Add Parameter to Protocol

A user with appropriate privileges may add a parameter to an existing protocol. Adding a parameter includes setting the name of the parameter and the type of data that is expected.

2.6.6 Remove Parameter from Protocol

A user with sufficient privileges may remove a parameter from a protocol. After removal, all future applications of the protocol will no longer prompt for the parameter that was removed.

2.6.7 Add Hardware to Protocol

A user with sufficient privileges may add hardware information to a protocol. This action will involve selecting the hardware to add from a list of existing hardware definitions.

2.6.8 Remove Hardware from Protocol

A user with sufficient privileges may remove hardware information from a protocol. This action will remove the association between the hardware and the protocol.

2.6.9 Add Software to Protocol

A user with sufficient privileges may add software information to a protocol. This action will involve selecting the software to add from a list of existing software definitions.

2.6.10 Remove Software from Protocol

A user with sufficient privileges may remove software information from a protocol. This action will remove the association between the software and the protocol.

2.6.11 *Upload File Containing Protocol Details

A user with sufficient privileges may upload a file that contains detailed information pertinent to the protocol. Each protocol may have exactly one file associated with it. If there is already a file for this protocol, the user will be warned and the uploaded file will replace the existing one.

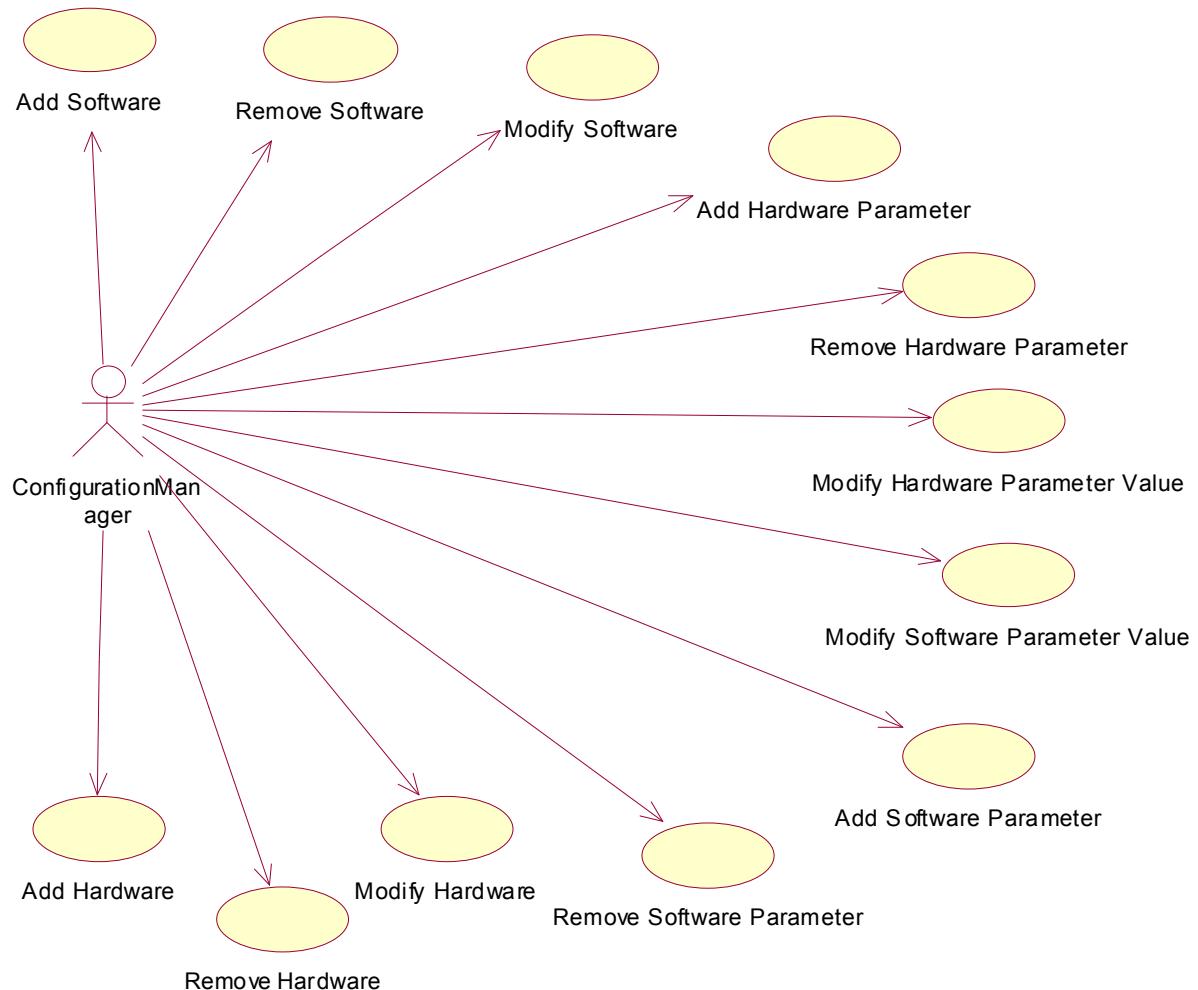
2.6.12 *Download File Containing Protocol Details

A user with sufficient privileges may download the previously uploaded file associated with a protocol.

2.6.13 Modify Protocol Details

A user with sufficient privileges may modify the attributes of a protocol including the type, description and URI.

2.7 ManageSoftwareAndHardwareDetails



This diagram shows the actions that a user may perform related to software/hardware management and definition.

2.7.1 Add Software

A user with sufficient rights may add a software definition to the system.

2.7.2 Remove Software

A user with sufficient privileges may remove a software definition from the system. If the software is referenced by another entity such as a protocol, then it will not be possible to remove it. In this case, the

user will receive an error message indicating which entities are using the software.

2.7.3 Modify Software

A user with sufficient privileges may modify a software definition.

2.7.4 Add Hardware Parameter

A user with sufficient privileges may add a parameter to a hardware definition.

2.7.5 Remove Hardware Parameter

A user with sufficient privileges may remove a parameter from a hardware definition.

2.7.6 Modify Hardware Parameter Value

A user with sufficient privileges may modify the value of a hardware parameter.

2.7.7 Modify Software Parameter Value

A user with sufficient privileges may modify the value of a software parameter.

2.7.8 Add Software Parameter

A user with sufficient privileges may add a parameter to a software definition.

2.7.9 Remove Software Parameter

A user with sufficient privileges may remove a parameter from a software definition.

2.7.10 Modify Hardware

A user with sufficient privileges may modify a hardware definition.

2.7.11 Remove Hardware

A user with sufficient privileges may remove a hardware definition from the system. If the hardware is referenced by another entity such as a protocol, then it will not be possible to remove it. In this case, the user will receive an error message indicating which entities are using the hardware.

2.7.12 Add Hardware

A user with sufficient privileges may add a new hardware definition.