*(Edited in March 23, 2006)*

# CODDE Access Control interface

The CODDE Access Control interface manages content *access rights*, *user names*, *passwords* and *user groups*. This interface includes two web pages that are accessed only by the CODDE *access rights manager*.

User identification is performed by the assigned user name and password, unless the user chooses to access the system as an *anonymous user*. A new user account (*user name*, *password*) is created for each one of the *MedWet authorized user roles*. Example *MedWet authorized user roles*:

- user name: `ekbyDP1` - user role corresponding to an EKBY employee with specific **d**ata **p**roviding and data processing responsibilities
- user name: `unBarcCA1` - user role corresponding to a University of Barcelona researcher with specific **c**ontent **a**ccess rights

User responsibilities are inherited from an abdicated employee to his relief, without need for user account suppresion and creation of a new one. It is a responsibility of the MedWet authorized user organizations to issue a *personal info update request* for one of the owned user accounts. Personal contact info updates are performed by the CODDE *access rights manager*, within a limited number of days. The updated user's name and contact info will be automatically used for the corresponding data fields (e.g. compiler's name), in all subsequent data providing tasks.

Users are assigned to one or more *user groups* based on their organizational role and attributes. Example *user groups*:

- user group: `acGroup1` - user group of **ac**ademic users
- user group: `govGroup1` - user group of **gov**ernment authorities
- user group: `ItaGroup1` - user group of **ita**lian users

Each *user group* is assigned a set of content *access rights*. Each user account eventually owns the union of the sets of *access rights* that come from the *user name*'s assigned *group memberships*. As an example, an Italian user from the University of Rome owns the content *access rights* of both the

`acGroup2` and `ItaGroup1` *user groups*. By default, each new user is declared as member of `anonGroup`, that is, the group of *anonymous users*.

*User group access rights* will be assigned on the basis of individual *data sheets* and will include or not include the following access types:

- **browse**: by default, each user has the right to browse all data provided by himself and if his *group membership* gives him the *browse right* to some *data sheet*, he can also browse this data sheet, even if data was provided by another user
- **create**: this right to some *data sheet* corresponds to the right to create a new empty datasheet with the user's contact info data; this right is always accompanied by the *browse access right* for the same *data sheet* and by default gives to the user the *update* and *erase access rights* to all data provided by himself
- **update**: this right to some *data sheet* corresponds to the right to update its data, including the possibility to insert, delete and update the records shown in the *data sheet*'s subforms; this right is always accompanied by the *browse access right* for the same *data sheet*
- **erase**: this right to some *data sheet* corresponds to the right to delete all data included in the *data sheet*; this right is always accompanied by the *browse access right* for the same *data sheet*

If a user's *group membership* gives him the *create right* to some *data sheet*, he is able to *hide the contents* of the created *data sheets* or *unhide*, in order to make them available to all other group users, when the *data sheets* are completed.

## A CODDE Access Control policy example

The CODDE Access Control mechanism is an *access policy* making framework with minimal administration requirements (refer to the duties of the CODDE *access rights manager*). The described interface provides support to develop and refine the *access control policy* that best fits to the MedWet organizational procedures. The implemented mechanism constitutes a viable solution to the following key problems:

- access control scalability: *access rights* are managed by means of *user groups* and not by defining, for each new user, a new *access rights* collection (with *acces rights* specified for all content items). This feature allows the CODDE *access rights manager* to control hundreds or thousands of users by having classified them according to their organizational roles, to *user groups* with well defined access rights.

- access control flexibility: an *access control policy* for the MedWet transnational inventory system is also subject to local legislative frameworks, as well as to local publicity and access control policies. The CODDE Access Control interface provides the required level of flexibility that allows taking into account many diverse access control constraints and makes possible to combine them into one complex access control policy. This is achieved by having allowed users to combine *access rights* coming from their memberships to more than one *user groups*.

- access traceability: it is easier to detect existing access policy design oversights, since the CODDE *access control manager* will have to examine a limited number of *user groups* (those that own or do not own the questionable *access right*) and will not have to examine a possibly large number of individual users.

Tables 1, 2, 3, 4 specify an example *access control policy*. Table 1 specifies that an *anonymous user*, that is, any user with no *user name* identification can only browse datasheets A and B. By default, all users are declared as members of *anonGroup*, which means that they own at least the set of *access rights* specified in Table 1.

| | browse | create | update | erase |
|---|---|---|---|---|
| datasheet A | $\vee$ | | | |
| datasheet B | $\vee$ | | | |
| datasheet C | | | | |
| datasheet D | | | | |
| datasheet E | | | | |

Table 1: `anonGroup` access rights

Table 2 shows the *access rights* of all users of `ItaGroup1` (data providers in Italy) to browse and create new datasheets, for wetlands located in Italy.

By default, these users also own the update and erase *access rights* to all data provided by themselves. Regarding, their *access rights* to wetlands outside Italy, they are given by `anonGroup` and possibly other group memberships.

| "Italy" | browse | create | update | erase |
|---|---|---|---|---|
| datasheet A | ∨ | ∨ | | |
| datasheet B | ∨ | ∨ | | |
| datasheet C | ∨ | ∨ | | |
| datasheet D | | | | |
| datasheet E | | | | |

Table 2: `ItaGroup1` access rights

Table 2 defines the *access rights* of the group `ItaGroup2` of all users that play a data validation role, for the wetlands located in Italy. They all have the right to update datasheets A, B, C, in order to correct them, but they can not create new ones, unless they also possess an appropriate *group membership*. We also consider goups `GrGroup1` and `GrGroup2` with similar *access rights* to those of `ItaGroup1` and `ItaGroup2`, but only for the wetlands located in Greece.

| "Italy" | browse | create | update | erase |
|---|---|---|---|---|
| datasheet A | ∨ | | ∨ | |
| datasheet B | ∨ | | ∨ | |
| datasheet C | ∨ | | ∨ | |
| datasheet D | | | | |
| datasheet E | | | | |

Table 3: `ItaGroup2` access rights

The example access control scenario is complete with the specification of `medWetGroup` (Table 4), a *user group* with trans-national data *access rights*. This group's users can browse all datasheets irrespective of where the wetland is located and also have the update and erase *access rights* for dtasheets C, D and E.

Next, we outline three different cases of users, with different *access rights* combinations, due to their role in MedWet.

| | browse | create | update | erase |
|---|---|---|---|---|
| datasheet A | ∨ | | | |
| datasheet B | ∨ | | | |
| datasheet C | ∨ | | ∨ | ∨ |
| datasheet D | ∨ | | ∨ | ∨ |
| datasheet E | ∨ | | ∨ | ∨ |

Table 4: `medWetGroup` access rights

Let us suppose that Spyros X. is the MedWet coordinator. He is given the *user name* `medWetCord` and one *password* and for this *user name* the CODDE *access rights manager* will assign a set of *group memberships* that will provide to the user the *access rights* need to play his/her role.

| |
|---|
| user name: `medWetCord`<br>password: `******` |
| group memberships: `anonGroup`<br>`medWetGroup`<br>`GrGroup2` |
| - the user has browse access right to all datasheets (`medWetGroup`)<br>- the user has the update access right to datasheets A and B, only for the wetlands located in Greece (`GrGroup2`)<br>- the user has the update and erase access rights to datasheets C, D and E, irrespective of where the wetland is located (`medWetGroup`) |

Table 5: user's `medWetCord` access rights

We also consider the cases of two employees of TdV. The first one plays in his organization a role associated with data providing responsibilities for the wetlands located in Italy. He is declared as member of `ItaGroup1` and this membership gives him the *access rights* shown in Table 6.

The second TdV employee is in charge of validating the data provided for the wetlands located in Italy, but his organizational role does not give him the right to provide new data. He is declared as member of `ItaGroup2` and this membership gives him the *access rights* shown in Table 7.

Many different access control constraints can be taken into account, by creating the appropriate *user groups* and by defining the required *group memberships* for each new user.

| |
|---|
| user name: `tdvDP1`<br>password: `******` |
| group memberships: `anonGroup`<br>`ItaGroup1` |
| - the user has the browse access right to datasheets A and B irrespective of where the wetland is located (`anonGroup`)<br>- the user has browse access to datasheet C, only for the wetlands located in Italy (`ItaGroup1`)<br>- the user has the create access right to datasheets A, B and C, only for the wetlands that are located in Italy (`ItaGroup1`)<br>- the user has the update and erase access rights to all datasheets created by him (by default) |

Table 6: user's `tdvDP1` access rights

| |
|---|
| user name: `tdvDV1`<br>password: `******` |
| group memberships: `anonGroup`<br>`ItaGroup2` |
| - the user has the browse access right to datasheets A and B irrespective of where the wetland is located (`anonGroup`)<br>- the user has browse access to datasheet C, only for the wetlands located in Italy (`ItaGroup2`)<br>- the user has the update access right to datasheets A, B and C, only for the wetlands that are located in Italy (`ItaGroup2`) |

Table 7: user's `tdvDV1` access rights

## UserToGroupAssignment Web Page

This page allows the CODDE *access rights manager* to create new user accounts. Provided functionality:

- browse existing user accounts
- create a new user account
- assign a *user name*
- assign a *password*
- assign user's *group memberships*: by default, each user is declared as member of `anonGroup`, that is, the group of *anonymous users*
- edit the user's contact info data

## GroupToRightsAssignment Web Page

This page allows the CODDE *access rights manager* to create new *user groups*, assign them the required content *access rights* or delete an existing *user group*. Provided functionality:

- browse existing *user groups*
- create a new *user group*
- assign a *user group* name
- assign/edit the *user group access rights* to the individual *data sheets*
- delete an existing *user group*: user accounts that belong to the deleted *user group* loose the *access rights* of this specific *group membership*

*By the CODDE system development team:*
Dr. Panagiotis Katsaros
Dr. Savvas Nikolaidis
Mr. Anakreon Mentis
Dept. of Informatics
Aristotle University of Thessaloniki
54124 Thessaloniki, GREECE