Protecting DDMs On UNIX, OpenVMS And Windows

As explained in the section *Natural Security On Different Platforms*, the protection of DDMs with Natural Security is different on mainframe computers from that on other platforms. This section describes how to control the use of DDMs under *UNIX, OpenVMS* and *Windows*. The control of DDMs on mainframe computers is described in the section *Protecting DDMs On Mainframes*.

This section covers the following topics:

- Status of a DDM

- DDM Security Profiles

- Creating and Maintaining DDM Security Profiles

- Add DDM Profile

- Copy DDM Profile

- Modify DDM Profile

- Delete DDM Profile

- Display DDM Profile

- Copy Link to All Special Links

- Linking a Library to a Protected DDM

FDDM Profile Parameter

With the Natural profile parameter FDDM, you can specify a system file as central location on which DDMs are to be stored (outside of libraries). If the FDDM parameter is set, DDM security profiles can only be created and maintained for DDMs contained in the library SYSTEM on that system file. Existing security profiles/settings/links for DDMs contained in other libraries are not lost, but they will not be visible within Natural Security and will have no effect.

If a central system file for DDMs is specified with the FDDM parameter, the protection of UNIX, OpenVMS and Windows DDMs and the maintenance of their security profiles is performed in the same way as with the File Maintenance functions for mainframe DDMs described in the section *Protecting DDMs On Mainframes*.

Status of a DDM

Before a DDM can be used under Natural Security, its *status* must be defined in Natural Security. This status determines if the DDM can be used, that is, referenced in a database access statement (for example, READ, FIND, HISTOGRAM, STORE, UPDATE, DELETE) within a program.

Note:
Program in this context means any type of Natural programming object that can contain database access statements; that is, programs, subprograms, subroutines etc.

A DDM whose status is not defined, cannot be referenced.

For every DDM that is to be used, two status classifications have to be made in Natural Security:

- an *internal status* and

- an *external status*.

Internal Status

The internal status controls the use of the DDM *within* the library in which it is contained.

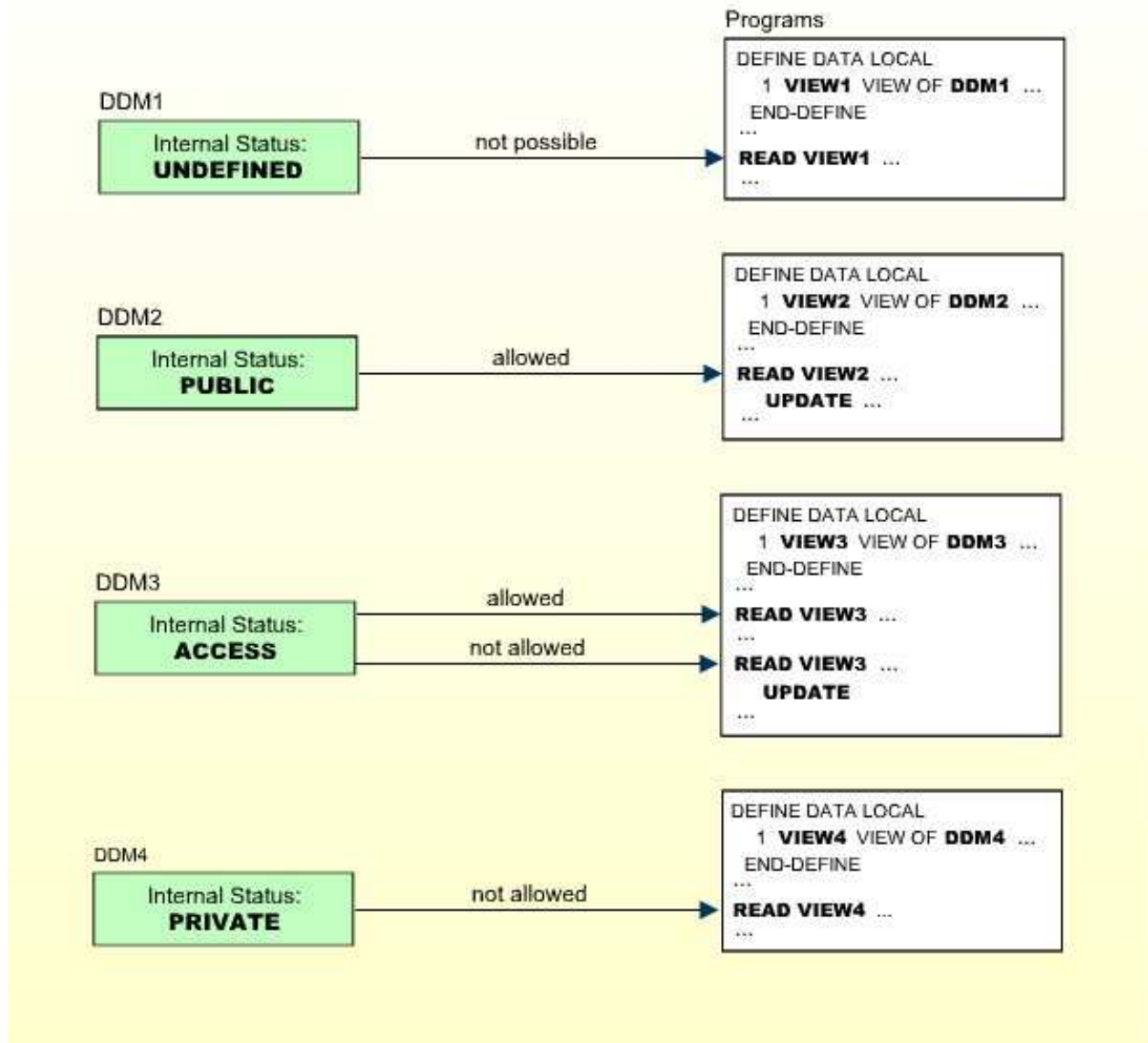The internal status of a DDM may be one of the following:

PUBLIC	The DDM can be read and updated by all programs within the library.
ACCESS	The DDM can be read, but not updated, by all programs within the library.
PRIVATE	The DDM cannot be used by any program within the library.

The internal status only applies within the library in which the DDM is contained.

The check whether a program may use a DDM is made when the program is *compiled*.

The following diagram shows how the internal status affects the use of a DDM within a library:

Library XYZ

Programs

DDM1

Internal Status: **UNDEFINED**	→ not possible →

```
DEFINE DATA LOCAL
    1 VIEW1 VIEW OF DDM1 ...
  END-DEFINE
...
READ VIEW1 ...
...
```

DDM2

Internal Status: **PUBLIC**	→ allowed →

```
DEFINE DATA LOCAL
    1 VIEW2 VIEW OF DDM2 ...
  END-DEFINE
...
READ VIEW2 ...
    UPDATE ...
...
```

DDM3

Internal Status: **ACCESS**	→ allowed → / → not allowed →

```
DEFINE DATA LOCAL
    1 VIEW3 VIEW OF DDM3 ...
  END-DEFINE
...
READ VIEW3 ...
...
READ VIEW3 ...
    UPDATE
...
```

DDM4

Internal Status: **PRIVATE**	→ not allowed →

```
DEFINE DATA LOCAL
    1 VIEW4 VIEW OF DDM4 ...
  END-DEFINE
...
READ VIEW4 ...
...
```

External Status

The external status controls the use of the DDM *by other libraries*.

This requires that the library containing the DDM is used as a steplib by these other libraries. Libraries for which the library containing the DDM is not a steplib, cannot use the DDM anyhow.

The external status of a DDM may be one of the following:

PUBLIC	The DDM is *not* protected. It can be used - that is, read and updated - by any library.
ACCESS	The DDM is protected as far as update is concerned. It can be read by any library. It may, however, be updated only by libraries which have been *linked* to it.
PRIVATE	The DDM is protected. It can be used only by libraries which have been *linked* to it. This *link* may be defined as "read" (that is, read only) or "update" (which implies read).

The external status of a DDM is only relevant if the library that contains the DDM is used as steplib by other libraries.

To allow a library to use a protected DDM in one of the library's steplibs, you have to define a *link* between the library and the DDM.

A link to a DDM whose external status is PRIVATE can be defined as "read link" or "update link". A link to a DDM whose external status is ACCESS can only be an "update link".

The possible relationships between libraries and DDMs in a steplib are shown in the following diagram:
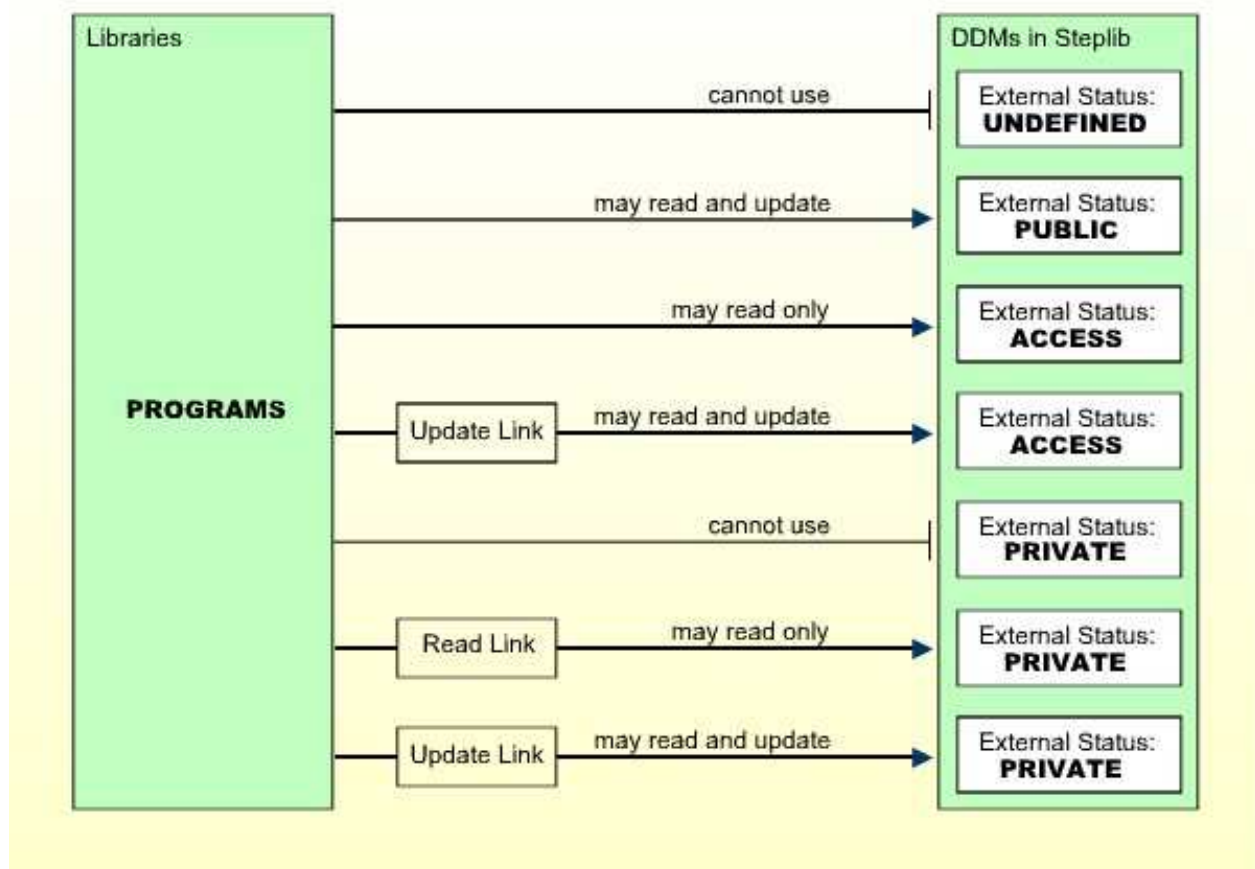
Note:
A link can only be established to a DDM whose external status is ACCESS or PRIVATE, because no link is required to read or update a DDM whose external status is PUBLIC.

The check whether a program may use a DDM in a steplib is made when the program is *compiled*.

For information on how to link a library to a DDM, see Linking a Library to a Protected DDM below.

The Initial Status of a DDM

The initial internal and external status of a newly generated DDM depends on the option "Set Status of DDMs", which is set in the Restrictions window of the library profile (see Components of a Library Profile in the section *Library Maintenance*).

This option affects all DDMs in the library for which no security profiles have been defined.

By default, this option is set to "UNDF"; that is, both the internal and the external status of a new DDM are undefined to start with. Before a new DDM can be used by any program, you have to create a security profile for it and define its internal and external status in the profile.

If you set the option to "PUBL", both the internal and external status of all newly generated DDMs are automatically set to PUBLIC. This means that new DDMs can be used by any program within the same library and in libraries that use the library as steplib. If you do not wish to restrict the use of these DDMs, you need not create security profiles for them or make any further security specifications. If you wish to restrict the use of one of these DDMs, you have to define a security profile for it, and in the profile, change the internal and external status as desired.

If you reset the option "Set status of DDMs" from "PUBL" to "UNDF", the internal and external status of all PUBLIC DDMs without security profiles will be reset to being undefined.
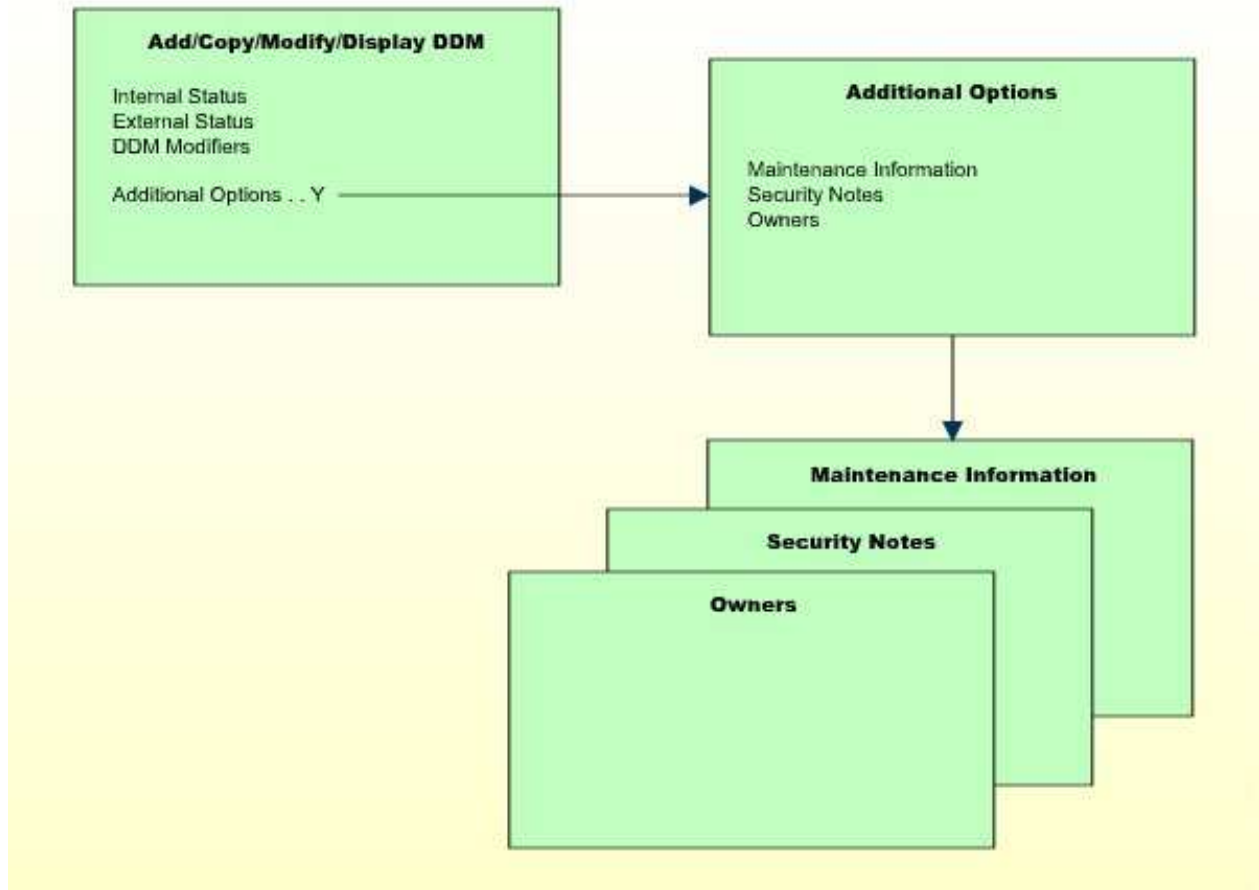
DDM Security Profiles

Unless the *initial status* of a DDM is automatically set to PUBLIC (see above), you have to define a security profile for every DDM that is to be used.

Apart from the internal and external status of a DDM, you can also specify some other options in a DDM security profile:

- You can restrict maintenance of the DDM itself to specific users (DDM modifiers).

- You can restrict maintenance of the DDM security profile to specific users (owners).

- You can enter notes on the security profile.

These options are explained below.

Components of a DDM Security Profile

Add/Copy/Modify/Display DDM

Internal Status
External Status
DDM Modifiers

Additional Options . . Y

Additional Options

Maintenance Information
Security Notes
Owners

Maintenance Information

Security Notes

Owners

Field	Explanation
DDM Name (display only)	The name under which the DDM was generated.
DBID / FNR (display only)	The database ID and file number of the database file referenced by the DDM.
Internal Status / External Status	See Status of a DDM above for an explanation. Possible values are: PUBL PUBLIC ACCE ACCESS PRIV PRIVATE When you create a DDM security profile, the internal and external status will, by default, be set to "PUBL".
DDM Modifiers	You may enter up to eight IDs of users; only these users will then be allowed to maintain the DDM in Predict (or with Natural's DDM Services). If you do not specify any DDM modifier, the owners of the security profile (see Additional Options below) may maintain the DDM. If neither DDM modifiers nor owners are specified, maintenance of the DDM is not restricted. Next to the ID of each DDM modifier, you may optionally specify a number from 1 to 3; this number determines how many of the other DDM modifiers specified must countersign for maintenance permission (the countersignature logic which applies to DDM maintenance permission is analogous to that of owners and co-owners; see the section *Countersignatures*).

Additional Options

If you mark the field "Additional Options" on the basic security profile screen with "Y", a window will be displayed from which you can select the following options:

- Maintenance Information

- Security Notes

- Owners

The options for which something has already been specified or defined are marked with a plus sign (+). You can select one or more items from the window by marking them with any character. For each item selected, an additional window will be displayed:

Additional Option	Explanation
Maintenance Information (display only)	In this window, the following information is displayed: • the date and time when the security profile was created, the ID of the ADMINISTRATOR who created it, and (if applicable) the IDs of the co-owners who countersigned for the creation; • the date and time when the security profile was last modified, the ID of the ADMINISTRATOR who made the last modification, and (if applicable) the IDs of the co-owners who countersigned for the modification.
Security Notes	In this window, you may enter your notes on the security profile.
Owners	In this window, you may enter up to eight IDs of ADMINISTRATORs. Only the ADMINISTRATORs specified here will be allowed to maintain this DDM security profile or link libraries to it. If no owner is specified, any user of type ADMINISTRATOR may maintain and link the security profile. For each owner, the number of co-owners whose countersignatures will be required for maintenance/link permission may optionally be specified in the field after the ID. For an explanation of owner and co-owners, see the section *Countersignatures*.

Creating and Maintaining DDM Security Profiles

Note:
If the Natural profile parameter FDDM is set, DDM security profiles can only be created and maintained for DDMs contained in the library SYSTEM.

On the Library Maintenance selection list, you mark a library with the code "MD" (or, in the case of a private library - if private libraries are used in private mode - you mark the user with the same ID on the User Maintenance selection list with the code "MD").

A window will be displayed, in which you can enter a start value for the list of DDMs (as described in the section *Finding Your Way In Natural Security*).

Then a list of the DDMs contained in the library will be displayed.

For each DDM, the DDM name, the library ID, and the internal and external status are displayed. If a security profile exists for a DDM, this will be indicated in Column P.

The list can be scrolled as described in the section *Finding Your Way In Natural Security*.

External Status as Selection Criterion

If you wish to list only DDMs of a specific status, you can specify one of the following selection criteria in the External Status field above the list:

PUBL	All DDMs of status PUBLIC.
ACCE	All DDMs of status ACCESS.
PRIV	All DDMs of status PRIVATE.
DEFI	Defined; that is, all DDMs of status PRIV, ACCE, and PUBL (*).
UNDF	Undefined; that is, all DDMs whose status is not PRIV, ACCE or PUBL (*).
DDM	All defined and undefined DDMs (*).
NDDM	DDM security profiles for which no corresponding DDMs exist (*).

* This is not an actual DDM status, but for selection purposes only.

The default status for selection is "DDM"; that is, *all* DDMs will be listed.

Selecting a Function

From the DDM list, you invoke all functions for creating and maintaining DDM security profiles. The following functions are available (possible code abbreviations are underlined):

Code	Function
AD	Add DDM Profile
CO	Copy DDM Profile
MO	Modify DDM Profile
DE	Delete DDM Profile
DI	Display DDM Profile
CU	Copy Link to All Special Links

To invoke a specific function for a DDM, mark the DDM with the appropriate function code in column "Co".

You may select various DDMs for various functions at the same time; that is, you can mark several DDMs on the screen with a function code. For each DDM marked, the appropriate processing screen will be displayed, and you can perform for one DDM after another the selected functions.

Add DDM Profile

With this function, you define a DDM to Natural Security, that is, create a new DDM security profile.

On the DDM selection list, enter "UNDF" in the field "Ext. Status".

Only those DDMs in the library which have not yet been defined to Natural Security will be listed. (The list can be scrolled as described in the section *Finding Your Way In Natural Security*).

On the list, mark the DDM for which you wish to create a security profile with function code "AD". The Add DDM screen will be displayed.

The individual items you may define on this screen and any additional windows that may be part of a DDM security profile are described under *Components of a DDM Security Profile* above.

When you add a DDM, the owners specified in the security profile of the library in which the DDM is contained will automatically be copied into the DDM security profile you are creating.

Copy DDM Profile

With this function, you can define a DDM to Natural Security by creating a security profile which is identical to an already existing DDM security profile in the same library.

What is Copied?

All components of the existing DDM security profile will be copied into the new DDM security profile - except the file number and database ID, and the owners (the owners will be copied from your own user security profile into the new DDM security profile you are creating).

Any links existing to the "old" DDM will *not* be copied.

How to Copy

On the DDM selection list, mark the DDM whose security profile you wish to duplicate with function code "CO".

A window will be displayed. In this window, enter the name of the "new" DDM.

The new DDM security profile will be displayed. The individual items you may define or modify in the profile are described under *Components of a DDM Security Profile* above.

Modify DDM Profile

With this function, you can change an existing DDM security profile.

On the DDM selection list, mark the DDM whose security profile you wish to change with function code "MO". The DDM security profile will then be displayed. The individual items you may define or modify are described under *Components of a DDM Security Profile* above.

Delete DDM Profile

With this function, you can delete an existing DDM security profile.

On the DDM Maintenance selection list, mark the DDM you wish to delete with function code "DE". A window will be displayed.

- If you have invoked the Delete DDM function and should then decide against deleting the given DDM security profile, leave the window by pressing ENTER without having typed in anything.

- If you wish to delete the given DDM security profile, enter the DDM name in the window to confirm the deletion.

When you delete a DDM security profile, all existing links to it will also be deleted.

When you delete a DDM security profile, the DDM itself will not be deleted. The DDM name will remain in the DDM selection list with the internal status set to either "UNDF" (undefined) or "PUBL" (public), depending on the option "Set Status of DDMs" in the library profile (this option is described in the section *Library Maintenance*).

Note:
When a DDM itself is deleted (in Predict, or with Natural's DDM Services or SYSMAIN utility), the corresponding DDM security profile will not be deleted. To list the DDM profiles without DDMs in a library, you enter "NDDM" as selection criterion for the list of DDM profiles.

If you mark more than one DDM with "DE", a window will appear in which you are asked whether you wish to confirm the deletion of each DDM security profile by entering the DDM name, or whether all DDM profiles selected for deletion are to be deleted without this individual confirmation. Be careful not to delete a DDM profile accidentally.

Display DDM Profile

With this function, you can display an existing DDM security profile.

On the DDM selection list, mark the DDM whose security profile you wish to view with function code "DI". The DDM security profile will then be displayed. The individual items that are part of the profile are described under *Components of a DDM Security Profile* above.

Copy Link to All Special Links

With this function, you can copy an existing link between a DDM and a people-protected library, so that the same kind of link (read-link or update-link) is simultaneously established between the DDM and all users who have a special link to that library.

On the DDM selection list, mark the DDM whose link you wish to copy with function code "CU". A message will then be displayed stating that the link has been copied.

Linking a Library to a Protected DDM

If the Natural profile parameter FDDM is not set, you link a library to protected DDMs in a steplib as follows:

1. Invoke the DDM selection list of that library (as described under *Creating and Maintaining DDM Security Profiles* above).

2. In the Library field above the list, enter an asterisk (*). A window will be displayed listing all steplibs defined for the library.

3. Mark the steplib which contains the DDM(s) to which you wish to link the library. A list of all DDMs in the selected steplib with external status ACCESS and PRIVATE will be displayed. The list can be scrolled as described in the section *Finding Your Way In Natural Security* .

4. In the "Co" column of the list, you mark one or more DDMs with one of the following function codes listed below.

If the Natural profile parameter FDDM is set, a library can only be linked to protected DDMs contained in the steplib SYSTEM. This is done as follows:

1. Invoke the DDM selection list of that library (as described under *Creating and Maintaining DDM Security Profiles* above).

2. A list of all DDMs in the steplib SYSTEM with external status ACCESS and PRIVATE will be displayed. The list can be scrolled as described in the section *Finding Your Way In Natural Security*.

3. In the "Co" column of the list, you mark one or more DDMs with one of the following function codes:

Code	Function
RE	Read-Link - The library thus linked may only read the DDM, but not update it.
UP	Update-Link - The library thus linked may read and update the DDM.
CL	Cancel - An existing link will be cancelled.
CU	Copy - An existing link between a DDM and a people-protected library will be copied, so that the same kind of link (read-link or update-link) is simultaneously established between the DDM and all users who have a special link to that library.

A link to a PRIVATE DDM can be specified as read-link (RE) or update-link (UP). A link to an ACCESS DDMs can only be specified as update-link (UP), because no link is required to read an ACCESS DDM.