
I-0442: Restrictive Is Not Fully Defined Without Specification Of Attributes

TYPE: NIAP Interpretation
NUMBER: I-0442
STATUS: Ready for External Review

TITLE: Restrictive Is Not Fully Defined Without Specification Of Attributes

COMMENTS DUE BY: Tuesday, October 28, 2003 to cc-cmt@nist.gov

SOURCE REFERENCE: CC v2.1 Part 2 Subclause 8.2 FMT_MSA.3
CC v2.1 Part 2 Subclause H.2 FMT_MSA.3

RELATED TO: <None>

ISSUE:

In FMT_MSA.3.1, the notion of restrictive is not fully defined without describing the attributes that need to be restricted, and the nature of that restriction.

STATEMENT

In FMT_MSA.3.1, the PP/ST author should specify the attributes that are to have values with a particular property.

RECOMMENDED CRITERIA CHANGES

To address this interpretation, the following changes should be made to CC v2.1, Part 2:

- FMT_MSA.3 is relabeled as FMT_MSA.3-NIAP-0442. Unless otherwise noted in these changes, all normative and informative material associated with FMT_MSA.3 is incorporated unchanged into FMT_MSA.3-NIAP-0442, and all references to FMT_MSA.3 in the CC, CEM, or other Common Criteria documentation are changed to refer to FMT_MSA.3-NIAP-0442.
- In Subclause 8.2, the components of FMT_MSA.3 are changed as follows (additions marked thusly; deletions marked ~~thusly~~):

FMT_MSA.3.1-NIAP-0442. The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to provide [selection: restrictive, permissive, other property] default values for the following security attributes that are used to enforce the SFP: [assignment: list of security attributes in the scope of the identified SFP to which the restrictive, permissive, other default value property should apply].

FMT_MSA.3.2-NIAP-0442. The TSF shall allow the [assignment: the authorised identified roles] to specify alternative initial values to override the default values for these attributes when an object or information is created.

- In Subclause H.2, the following is added after Paragraph 1032:

Assignment:

In FMT_MSA.3.1, the PP/ST author should list the attributes under the control of the indicated SFP to

which the designed property chosen in the selection should apply.

Iteration:

The entire FMT_MSA.3 component should be iterated, as appropriate, to cover all of the attributes under the control of SFPs for which static attribute initialisation is appropriate.

SUPPORT:

As currently written, the FMT_MSA.3.1 elements do not provide a way to have some attributes of an SFP to be permissive, and others restrictive. However, such combinations are often desired (for example, permissive permissions for the owner, and restrictive for everyone else). By changing this to an assignment, the needed flexibility is provided.