

---

# I-0352: Rules Governing Binding Should Be Specifiable

---

NUMBER: I-0352  
STATUS: Reposted for External Review  
TYPE: NIAP Interpretation

TITLE: Rules Governing Binding Should Be Specifiable  
COMMENTS DUE BY: Friday, December 1, 2000 to [IWG@gibraltar.ncsc.mil](mailto:IWG@gibraltar.ncsc.mil)

SOURCE REFERENCE: CC v2.1 Part 2 Subclause 7.6 FIA\_USB  
CC v2.1 Part 2 Subclause G.6 FIA\_USB

RELATED TO: <None>

## ISSUE:

The current FIA\_USB component provides the ability to associate "appropriate" user security attributes with subjects. It provides no mechanism to specify any rules governing the association, and it requires that the attributes to be mapped be provided through refinement.

However, in many cases it must be possible to specify how user attributes are mapped into subject attributes. An example would be the requirement that the label assigned to a subject is within the clearance range of the user. This is not expressible under the existing components.

## STATEMENT OF INTERPRETATION:

A new component is added to the FIA\_USB family that provides the ability to specify the rules governing the binding of user attributes to subjects.

## SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CC v2.1, Part 2: (additions marked thusly; deletions marked ~~thusly~~)

- The following component is added to FIA\_USB:

FIA\_USB.NIAP-0352-1: Expanded user-subject binding

Hierarchical To: FIA\_USB.1

FIA\_USB.NIAP-0352-1.1: The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].

FIA\_USB.NIAP-0352-1.2: The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *initial association rules*].

FIA\_USB.NIAP-0352-1.3: The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *changing of attributes rules*].

Dependencies: FIA\_ATD.1 User Attribute Definition

- In Clause 7, Figure 7.1 is modified to show a new component, FIA\_USB.NIAP-0352-1, that is immediately hierarchical to the existing FIA\_USB.1.
- In Subclause 7.6, "Component Levelling" is modified to show a new component, FIA\_USB.NIAP-0352-1, that is immediately hierarchical to the existing FIA\_USB.1.
- In Subclause 7.6, the following paragraph is added after paragraph 295:

FIA\_USB.NIAP-0352-1 Expanded user-subject binding requires the specification of any rules governing the association between user attributes and the subject attributes into which they are mapped.

- In Subclause 7.6, the following Management section is added after paragraph 296:

Management: FIA\_USB.NIAP-0352-1

The following actions could be considered for the management functions in FMT:

- a) an authorised administrator can define default subject security attributes.
- b) an authorised administrator can change subject security attributes.

- In Subclause 7.6, the following Audit section is added after paragraph 297:

Audit: FIA\_USB.NIAP-0352-1

The following actions could be auditable if FAU\_GEN Security audit data generation is included in the PP/ST:

- a) Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject).
- b) Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).

- In Clause G, Figure G.1 is modified to show a new component, FIA\_USB.NIAP-0352-1, that is immediately hierarchical to the existing FIA\_USB.1.
- In Subclause G.6, the following is added after paragraph 1006:

FIA\_USB.NIAP-0352-1 Expanded user-subject binding

User application notes

The phrase "acting on behalf of" has proven to be a contentious issue in source criteria. It is intended that a subject is acting on behalf of the user who caused the subject to come into being or to be activated to perform a certain task. Therefore, when a subject is created, that subject is acting on behalf of the user who initiated the creation. In case anonymity is used, the subject is still acting on behalf of a user, but the identity of the user is unknown. A special category are the subjects that serve multiple users (e.g. a server process). In such cases the user that created this subject is assumed to be the "owner".

Operations

Assignment:

In FIA\_USB.NIAP-0352-1.1, the PP/ST author should specify a list of the user security attributes that are to be bound to subjects.

**Assignment:**

In FIA\_USB.NIAP-0352-1.2, the PP/ST author should specify any rules that are to apply upon initial association of attributes with subjects, or "none".

**Assignment:**

In FIA\_USB.NIAP-0352-1.3, the PP/ST author should specify any rules that are to apply when changes are made to the user security attributes associated with subjects acting on behalf of users, or "none".

**PROJECTED IMPACT:**

Negligible impact anticipated.

**SUPPORT:**

This interpretation addresses the problem described in the Issue statement. It provides the ability to extend FIA\_USB with a new component that provides the ability to specify the rules that govern attribute inheritance between users and subjects. It also makes explicit the listing of attributes to be inherited.