
I-0413: Assurance Of RVM Is By Testing And Design Analysis

NUMBER: I-0413
STATUS: Reputed for External Review
TYPE: NIAP Interpretation

TITLE: Assurance Of RVM Is By Testing And Design Analysis
WOULD SUPERSEDE: [I-0339](#) Assurance Of RVM Is By Testing And Design Analysis
COMMENTS DUE BY: Monday, February 5, 2001 to IWG@gibraltar.ncsc.mil

SOURCE REFERENCE: CC v2.1 Part 2 Subclause 10.10 FPT_RVM
CC v2.1 Part 2 Subclause J.10 FPT_RVM

RELATED TO: [I-0339](#) Assurance Of RVM Is By Testing And Design Analysis
[I-0382](#) TSF Architectural Protections Are Really Assurances

ISSUE:

Most of the CC functional requirements are completely testable through the TSF interface. However, that is not always true for FPT_RVM.1. Determining the internal invocation sequence underlying a call is difficult to assure solely through testing. In such a case, examination of the design must come into play.

STATEMENT OF INTERPRETATION:

Assurance that FPT_RVM.1 is satisfied is achieved through a combination of testing and design analysis.

SPECIFIC INTERPRETATION:

To address this interpretation, the following text is added to CC v2.1, in the Part 2 Annex for FPT_RVM, after paragraph 1263 in Annex J.10:

Evaluator Application Notes

In order to provide assurance that this element is satisfied, the design documentation (functional specification, high-level design, and low-level design, as appropriate) provided by the developer, as part of their descriptions of the TSF, should include sufficient information to enable the evaluator to be convinced that the design provides the enforcement, with this argument verified through testing. Foundations of such argument generally revolve around the construction of the interface to the TSF (e.g., call gates, network cards) and the limitations placed on those interfaces.

FURTHER CONSIDERATIONS:

Corresponding methodology changes are needed to address this interpretation. In particular, informative text must be added to the appropriate ADV work units that call out, for situations where FPT_RVM is included in an ST, the appropriate information (based on EAL) to be included in the design descriptions (functional specification, high-level design, and low-level design, as appropriate).

Note that this interpretation moves some of the verification burden from developer interface testing to evaluator analysis.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

In order to provide assurance that this element is satisfied, the evaluators must be convinced that the design provides the enforcement, with this being verified through testing. In coming to their conclusion, evaluators should consider the construction of the interface to the TSF (e.g., call gates, network cards) and the limitations placed on those interfaces. In addition, the conclusion should take into account the assurance package that has been chosen to be associated with the functional requirements. The depth (i.e., how much detail is involved) is dependent on the nature of assurance being pursued (i.e., the lower the level of assurance the less detail required).

Note: This interpretation is superseding a previously-approved formal interpretation primarily to reflect modifications to the interpretation format. The intent of the interpretation has not been changed, although some specifics of the criteria changes or the support may have been clarified or corrected.