

---

# I-0461: Definition Of TSF: Relied Upon For The Correct Enforcement

---

TYPE: Guidance  
NUMBER: I-0461  
STATUS: Ready for External Repost after Interpretations Board Rework/Review

TITLE: Definition Of TSF: Relied Upon For The Correct Enforcement

FIRST POST: [cc-cmt TBD]  
COMMENTS DUE BY: Tuesday, July 1, 2003 to [cc-cmt@nist.gov](mailto:cc-cmt@nist.gov)

SOURCE REFERENCE: CC v2.1 Part 1 Subclause 2.3  
RELATED TO: <None>

## ISSUE:

In the definition of TSF, what does the phrase "relied upon for the correct enforcement of the TSP" mean? What is the interaction of this phrase with respect to FPT\_SEP and FPT\_RVM: in particular, does "relied upon" have any implications with respect to tamperproof-ness or benign-ness.

## STATEMENT

A TOE component is relied upon for the correct enforcement of the TSP if accidental or intentional failure of that component could result in the TSP not being enforced, based on the knowledge available at the time of evaluation.

## SUPPORT:

There are two aspects of this question. The first revolves around the definition of the term "TSP". The second revolves around the definition of reliance.

The TSP is defined as the "set of rules that regulate how assets are managed, protected, and distributed within a TOE." Asset management rules are covered under FMT; and asset protection under classes such as FAU, FIA, FDP, FCS, FPR, FTA, and FTP. FPT is a mixed bag: whether a particular rule falls under the protection category varies. Distribution rules are unclear.

Turning to the question of reliance. Websters' has two definitions for "rely": to be dependent, and to have confidence based on experience. Although the latter might apply to the assurance aspects of a system, the former appears to be more applicable.

It is clear that the enforcement of rules depends on the correct implementation of those mechanisms that underlie classes such as FDP, FAU, or FIA. Again, FPT is unclear.

The components in FPT can be divided into three groups:

1. Those that explicitly provide a protection function for TSF data. Examples of these are FPT\_ITT or FPT\_ITC. This class is clearly part of the TSF.
2. Those that verify the TSF or its platform is operating correctly. FPT\_TST and FPT\_AMT are examples of these. Some elements of this class may fall into "support" code, and is explored in I-0453. Note that the components in this category, at the time of evaluation, can be analyzed to be working correctly. However, they may identify an unanticipated hardware or software failure later during operation.
3. That that ensure the enforcement of functions "behind the scenes". FPT\_SEP and FPT\_RVM are examples of these.

This class is the source of problems.

To explore the issue further: If FPT\_SEP or FPT\_RVM failed, would the protection mechanisms be enforced? After all, if their failure would cause enforcement to fail or to be otherwise enforced incorrectly, then said enforcement is dependent on the function.

In the case of FPT\_RVM, enforcement would fail, for the failure of FPT\_RVM would imply there are circumstances where the enforcement function is not invoked, indicating that enforcement mechanism is bypassed. If the enforcement function was access control, this could result in either too much or too little access being provided.

If the case of FPT\_SEP, whether or not enforcement fails depends on whether software takes advantage of the vulnerability in the TSF's protection to bypass it. Hence, if FPT\_SEP is present, one needs to have confidence that either the mechanism is working, or none of the software in the TOE is malicious.

To know that the FPT\_SEP mechanism is working means knowing that no software can go around or disable the mechanism. If analysis can show that the design of the TSF precludes any ability to go around the FPT\_SEP mechanism, there is no requirement to show non-maliciousness in the code. However, if the design of the TSF is such that the potential exists to violate FPT\_SEP, then it must be shown that any code with the potential is non-malicious and performs correctly with respect to SFRs.