

IEEE P2600 Hardcopy Device and System Security comments

Cl 01 SC 1 P 1 L 1 # 4

Steinhagen, Jennie M

Comment Type ER Comment Status A

Meets all editorial requirements.

SuggestedRemedy

Response Response Status C

ACCEPT.

Cl 05 SC 5.3.2.3 P 8 L 2 # 5

Chen, Nancy

Comment Type T Comment Status A

TOE functions are defined as a type of TOE asset here, but the PP has no threat/objective for the asset. Later in Section 10.4 there are SFRs that enforce the TOE Function Access Control SFP. These SFRs are used for supporting the objectives for protecting user data and TSF data. If TOE functions are assets, shouldn't they be protected? This seems an inconsistency.

Note: This applies to all other PPs.

SuggestedRemedy

Either

- (1) Remove TOE functions from asset category, or
- (2) Add a threat from unauthorized access to TOE functions as TOE assets, and add the corresponding objective, or
- (3) Clarify in the existing objectives for protecting user data and TSF data that access to TOE functions also need to be protected.

The security objective fulfillment table need to be adjusted accordingly.

(1) or (2) seem more appropriate for environment C, because of the possible need for adding objectives if Normal User authorization mechanism is implemented. (see my comment on section 7.3 of PP-C.)

Response Response Status C

ACCEPT IN PRINCIPLE.

See solution for comment #6

Cl 07 SC 7.3 P 12 L 1 # 6

Chen, Nancy

Comment Type T Comment Status A

Application note recommend ST to add appropriate objectives if an authorization function for Normal Users is provided by the TOE, IT environment, or non-IT environment. I agree that for demonstrable conformance, ST may add more security objectives to the TOE.

However ST is not allowed to pull requirements for the TOE into environments. This leave ST only possible to add objectives to the TOE. It's not possible to add more objectives to IT or non-IT environment. Therefore the Application Note's recommendation is inconsistent with ""demonstrable conformance"" requirement.

Also the PP requires TOE Function Access Control SFP and management SFRs to enforce the SFP. I think the Normal User authorization function (such as Coin Box) by the TOE, or IT environment (e.g. an external pay-per-use mechanism) or non-IT environment (permission for physical access to the TOE) can be considered as example implementations for TOE Function Access Control SFP. No additional objectives need to be added.

SuggestedRemedy

Possible resolutions:

Resolution #1 -

(1) Remove the App Note here.

(2) Add App Note to the SFRs for enforcing TOE Function Access Control SFP to explain that example implementations for TOE Function Access Control in the environment are Normal User authorization by the TOE via Coin Box control, by IT environment by providing an external pay-per-use mechanism, or by non-IT environment by manual permission for physical access to the TOE.

Resolution #2 -

(1) Add a threat from unauthorized access to TOE functions as TOE assets, and add the corresponding objective as an organizational security policy. This way the ST has the choice to add the normal user authorization objective to the TOE, or IT or non-IT environment if it is implemented.

Response Response Status C

ACCEPT IN PRINCIPLE.

In PP-C:

- \* 5.3.2 change "three" to "two"
- \* 5.3.2.3 remove this clause
- \* 10.4 remove FDP\_ACC.1 and FDP\_ACF.1
- \* 10.6 remove FMT\_MSA.1 and FMT\_MSA.3
- \* 10.12 adjust rationale tables accordingly
- \* remove app notes associated with the above SFRs

Change PP APPLICATION NOTE 5 from:

In this environment, a Normal User may be authorized by the TOE, by the IT environment

IEEE P2600 Hardcopy Device and System Security comments

(for example an external pay-per-use mechanism), or by the non-IT environment (for example, by being permitted to physically access the TOE). The ST Author should identify which mechanism or mechanisms are supported by the conforming TOE and add appropriate objectives for the TOE, IT environment or non-IT environment, and also add appropriate SFRs if there is an objective for the TOE.

to:

This Protection Profile does not specify or require any authorization for Normal Users to perform non-administrative functions of the TOE. However, in this operational environment, it may be desired for Normal Users to be authorized by the TOE, by the IT environment (for example an external pay-per-use mechanism), or by the non-IT environment (for example, by being permitted to physically access the TOE). If such authorization is desired, then the ST Author should identify which mechanism or mechanisms are supported by the conforming TOE, add appropriate threats or OSPs, and add appropriate objectives for the TOE, IT environment or non-IT environment. If there is an authorization objective for the TOE, the ST Author should also add appropriate SFRs (e.g., FDP\_ACC.1, FDP\_ACF.1, FMT\_MSA.1, and FMT\_MSA.3).

In PP-D, also change the following:

- \* 5.3.2 change "three" to "two"
- \* 5.3.2.3 remove this clause

|                 |               |             |            |            |
|-----------------|---------------|-------------|------------|------------|
| <b>Cl 08</b>    | <b>SC 8.1</b> | <b>P 13</b> | <b>L 4</b> | <b># 2</b> |
| Smithson, Brian |               | Individual  |            |            |

*Comment Type* **T** *Comment Status* **R**

The objective O.AUDIT.LOGGED currently says ""The TOE shall create and maintain a log of TOE use and security-relevant events, and prevent its unauthorized disclosure or alteration"". However, the PP does not assume by default that the TOE will maintain or protect the log of audit events. Instead, it relies by default on external audit storage and protection (OE.AUDIT\_STORAGE.PROTECTED and OE.AUDIT\_ACECSS.AUTHORIZED). In app note 5, the ST Author is instructed to add appropriate objectives and SFRs for local storage and protection. Consequently, none of the SFRs that fulfill O.AUDIT.LOGGED (FAU\_GEN.1, FAU\_GEN.2, and FIA\_UID.1) actually deal with storage or protection.

*SuggestedRemedy*

Change the definition of O.AUDIT.LOGGED from ""The TOE shall create and maintain a log of TOE use and security-relevant events, and prevent its unauthorized disclosure or alteration"" to ""The TOE shall create a log of TOE use and security-relevant events"". In app note 6, change ""an internal capability to provide access"" to ""an internal capability to store and provide access"" (consistent with app note 8). In app note 6, add ""The ST Author should add to the security objectives rationale tables that P.AUDIT.LOGGING is additionally enforced by additionally enforced by O.ADMIN.AUTHORIZED and OE.ADMIN.AUTHORIZED"". Alternatively, make note of this in the PP Guide.

*Response* *Response Status* **C**

REJECT.

This comment was WITHDRAWN by the commenter.

However, an explanation similar to what is in the suggested remedy will be added to the Guide.

|                 |               |             |             |            |
|-----------------|---------------|-------------|-------------|------------|
| <b>Cl 09</b>    | <b>SC 9.1</b> | <b>P 18</b> | <b>L 10</b> | <b># 1</b> |
| Smithson, Brian |               | Individual  |             |            |

*Comment Type* **E** *Comment Status* **A**

[Nevo] Sharp asked for an application note clarifying the meaning of ""further processing by the TSF"".

*SuggestedRemedy*

Add an app note after FPT\_FDI\_EXP.1.1: The intention of ""further processing by the TSF"" is to ensure that the data being forwarded between interfaces is a normal function of the TOE and does not violate the security policies of the TOE. Alternatively, make a note about this in the PP Guide.

*Response* *Response Status* **C**

ACCEPT IN PRINCIPLE.

This will be added to the Guide.

IEEE P2600 Hardcopy Device and System Security comments

CI 13 SC 13.3 P 35 L 11 # 3  
Smithson, Brian Individual

Comment Type T Comment Status R

PP app note 66 refers to defining roles, but the SFR no longer deals directly with roles but instead depends on FMT\_SMR.1.

*SuggestedRemedy*

Remove PP app note 66.  
Alternatively, make a note about it in the PP Guide.

Response Response Status C

REJECT.

This comment was WITHDRAWN by the commenter.