

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP Guid** SC **5.4.2** P**35** L**40** # **8**
 Aubrey, Carmen

Comment Type **T** Comment Status **D**

Based on the discussions Carmen Aubry had with Helmut, some clarifications are needed to address the scenario where the "user" is the print server (the HCD is going to authenticate the print server in this case)

SuggestedRemedy

"The author of a ST that specifies a print server as an (IT) user that submits jobs to the TOE on behalf of other (human) users needs to define the method used to authenticate the print server "user". In addition the ST needs to define the assumptions made about the print server (basically: a "remote trusted IT product" that preserves the integrity and confidentiality of all the user and TSF data (like a PIN code) related to the job). Adding such an assumption does not break the compliance to the PP as long as the assumption is completely related to a function that is additional to the ones mentioned in the PP (which is the case for an assumption that only relates to the print server). IEEE Std 2600.1 and IEEE Std 2600.2 compliant TOEs also require that the user proves job ownership on the Operator Panel of the TOE before he retrieves the hardcopy output. A possible way to achieve this is via a pin code selected by the end-user before sending the job to the print server."

Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Will add the wording proposed by Carmen to subclause 5.4.2.

Cl **PP Guid** SC **6.2.1** P **38** L **5** # **7**
 Chen, Nancy Oki Data

Comment Type **T** Comment Status **D**

The sentence: "This demonstrable compliance must also encompass whether it is necessary to conform to any of the common SFRs or one or more of the SFR Packages in the applicable PP from the IEEE Std 2600 Series of Protection Profiles." could be mistaken that a demonstrable conforming ST does not need to comply to all common SFRs in the PP it is to conform. However, a conforming ST MUST DEMONSTRATE that it complies to ALL Common SFRs specified by the PP to which it is to conform. This may encompass determining whether the ST is necessary to specify a more restrictive SFR from the SFR family hierarchy in place of any of the common SFRs. The same rule applies for the SFRs in one or more of the SFR Packages for which the HCD function exists in the TOE.

SuggestedRemedy

Reword the sentence in accordance with the comment to avoid possible misinterpretation.

Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.

Agreed to the change. Alan will confirm the new text with Nancy before inclusion in the document.

Cl **PP Guid** SC **6.2.1.2** P **38** L **37** # **1**
 Chen, Nancy Oki Data

Comment Type **T** Comment Status **D**

It's not true that "the ST Author can always claim conformance to the NVS SFR package if desired.", because a HCD might not have a NVS at all to implement the NVS SFR package.

SuggestedRemedy

Two alternatives are recommended:

- 1) Delete the sentence "However, the ST Author can always claim conformance to the NVS SFR package if desired." Or,
- 2) Change the sentence to something like - "However, if the product has a nonvolatile storage but is not designed to be removed by authorized personnel, the ST Author can always claim conformance to the NVS SFR package if desired."

Also change "'i.e.'" to "'e.g.'" in ().

Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.

Use a version of #2:

"However, if the product has a nonvolatile storage but is not designed to be removed by authorized personnel, the ST Author can still claim conformance to the NVS SFR package if desired."

Cl **PP Guid** SC **6.2.1.2** P **39** L **15** # **2**
 Chen, Nancy Oki Data

Comment Type **T** Comment Status **D**

If the TOE uses a 3rd-party NVS product that has not been CC certified, but the 3rd-party is willing to provide all documents and evidences required for the CC certification of the TOE with the NVS product, then the conformance to the NVS Package can still be claimed.

SuggestedRemedy

Add another condition to the "if" statement of the sentence/paragraph:

Something like -
 "and if the documents and evidences required for the CC certification of the TOE with the NVS product cannot be provided by the 3rd-party"

Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.

"and if the documents and artifacts required for the CC certification of the TOE with the NVS product cannot be provided by the 3rd-party"

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP Guid** SC **6.4.1** P **44** L **8** # **3**
 Chen, Nancy Oki Data

Comment Type **T** Comment Status **D**

Only P2600.4 does not have the O.AUDIT.LOGGED security objective for the TOE. P2600.3 still has this objective, but the audit log only requires logging of security violations, not for individual accountability.

SuggestedRemedy

Please fix in accordance with the comment.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Alan will confirm the new text with Nancy before inclusion in the document.

Cl **PP Guid** SC **6.5.8** P **53** L **42** # **4**
 Chen, Nancy Oki Data

Comment Type **T** Comment Status **D**

P2600.2 for environment B only requires that TSF data be protected for confidentiality and integrity when the data is transmitted over a SMI.

SuggestedRemedy

Remove "User and" and the word "both" from the sentence.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP Guid** SC **6.5.8** P **54** L **10** # **5**
 Chen, Nancy Oki Data

Comment Type **T** Comment Status **D**

Kerberos infrastructure establishes assured identification of participating end points. Once two end points are authenticated using Kerberos, they have a trusted path to communicate any data they wish, not just for authentication data, as long as the data are protected for confidentiality and integrity. One can provide the protection by signing and encrypting the data with a key for each connection.

SuggestedRemedy

Please revise the sentence in accordance with the comment, or simply remove the "If" condition statement.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Will revise the sentence and will confirm the new text with Nancy before inclusion in the document.

Cl **PP Guid** SC **6.6** P **54** L **40** # **9**
 Farrell, Lee

Comment Type **T** Comment Status **D**

Subject of Common Access Control SFP in Table 17 referred by FDP_ACC.1 and FDP_ACF.1 is "U.NORMAL". FMT_MSA.3 is a dependency of FDP_ACF.1 Including "U.NORMAL" (Subject of Common Access Control SFP) itself as a role in FMT_MSA.3 will make Access Control useless because FDP_ACF.1 depends on FMT_MSA.3 security management. Therefore concerning example text "Page 54,Line 40-42", it is not appropriate that "U.NORMAL" can change the default value.

SuggestedRemedy

None provided

Proposed Response Response Status **W**

Work on 6.6 to make sure it is right and conveys what was intended. Also, try to get more information from Canon Japan about possible text changes.

Cl **PP Guid** SC **6.7.4** P **59** L **10** # **6**
 Chen, Nancy Oki Data

Comment Type **T** Comment Status **D**

In the statement "the ST should be either the same as, or more than those defined by Protection Profile selected", it is not clear that whether it's referring to the number of security objectives or the strength of security objective. For demonstrable conformance, it's the latter is correct.

SuggestedRemedy

Change to " the ST should be either equivalent, or more restrictive than".

Proposed Response Response Status **W**

PROPOSED ACCEPT.