

IEEE P2600 Hardcopy Device and System Security comments

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

Comment Type T Comment Status X

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 O

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

Comment Type T Comment Status X

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 O

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

Comment Type T Comment Status X

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 O

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

Comment Type T Comment Status X

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 O

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

Comment Type T Comment Status X

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 O

IEEE P2600 Hardcopy Device and System Security comments

---

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

Comment Type **T** Comment Status **X**

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 **O**

---

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

Comment Type **T** Comment Status **X**

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 **O**