

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC 3.1 P 3 L 11 # 75
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

The clause number reference pointer on this line didn't work properly - points to clause 0.
 It appears most of the clause number references in this PP-B draft for some reason didn't work.

SuggestedRemedy

Make sure the clause number reference points to the proper clause throughout the PP-B document.

Proposed Response Response Status **O**

Cl **PP-A** SC 3.1 P 3 L 11 # 50
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

The clause number reference pointer on this line didn't work properly - points to clause 0.
 It appears most of the clause number references in this PP-A draft for some reason didn't work.

SuggestedRemedy

Make sure the clause number reference points to the proper clause throughout the PP-A document.

Proposed Response Response Status **O**

Cl **PP-C** SC 5.1 P 5 L 6 # 101
 Sukert, Alan Xerox

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

The definition of shared-medium interface is not consistent between the description of TOE functions in subclause 5.1 and Annex A. In subclause 5.1 a shared-medium interface is defined as ""transmit and receive documents and data"" between the HCD and external devices over communications media that ""are or can be shared by other users"" while Annex A (page 59, line 36) defines a shared-medium interface as a mechanism for ""exchanging data""...over a communications medium which, in conventional practice ""is or can be simultaneously accessed by multiple users"".

Also, in PP-A and PP-B the definitions of the SMI function in their corresponding subclause 5.1 mentioned transmit and receive of User Data and TSF Data; that was not mentioned in PP-D.

SuggestedRemedy

Make sure the definition of shared-medium interface is consistent between subclause 5.1 and Annex A in terms of what is being transmitted and received and who can share the communications.

Proposed Response Response Status **O**

Cl **PP-D** SC 5.1 P 5 L 6 # 117
 Sukert, Alan Xerox

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

The definition of shared-medium interface is not consistent between the description of TOE functions in subclause 5.1 and Annex A. In subclause 5.1 a shared-medium interface is defined as ""transmit and receive documents and data"" between the HCD and external devices over communications media that ""are or can be shared by other users"" while Annex A (page 27, line 39) defines a shared-medium interface as a mechanism for ""exchanging data""...over a communications medium which, in conventional practice ""is or can be simultaneously accessed by multiple users"".

Also, in PP-A and PP-B the definitions of the SMI function in their corresponding subclause 5.1 mentioned transmit and receive of User Data and TSF Data; that was not mentioned in PP-C.

SuggestedRemedy

Make sure the definition of shared-medium interface is consistent between subclause 5.1 and Annex A in terms of what is being transmitted and received and who can share the communications.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-C** SC 5.2 P 5 L 18 # 102
 Sukert, Alan Xerox

Comment Type T Comment Status X

I understand why this text was changed from Users == Subjects to its current text, but I had to read this new sentence at least three times before it made sense to me. I'm concerned readers of this standard will have to do the same thing. I think if you used wording similar to the preceding text in this sentence will become easier to understand.

SuggestedRemedy

Change this sentence to read something like "...and therefore, it can be assumed that the security attributes of a Subject used in access control decisions are identical to the security attributes of the User that requests the access unless..."

Proposed Response Response Status O

Cl **PP-D** SC 5.2 P 5 L 18 # 118
 Sukert, Alan Xerox

Comment Type T Comment Status X

I understand why this text was changed from Users == Subjects to its current text, but I had to read this new sentence at least three times before it made sense to me. I'm concerned readers of this standard will have to do the same thing. I think if you used wording similar to the preceding text in this sentence will become easier to understand.

SuggestedRemedy

Change this sentence to read something like "...and therefore, it can be assumed that the security attributes of a Subject used in access control decisions are identical to the security attributes of the User that requests the access unless..."

Proposed Response Response Status O

Cl **PP-B** SC 5.1 P 5 L 21 # 74
 Sukert, Alan Xerox

Comment Type T Comment Status X

The definition for removable nonvolatile storage in clause 5.1 does not agree with the corresponding definition for removable nonvolatile storage in Annex A. Specifically, in clause 5.1 nonvolatile storage is defined as User or TSF Data that is designed to be removed from the TOE by ""authorized non-service personnel""; Annex A (page 58, line 29) states that removable nonvolatile storage is designed to be removed from the TOE by ""authorized personnel"".

SuggestedRemedy

Make sure the definition of removable nonvolatile storage is consistent between subclause 5.1 and Annex A.

Proposed Response Response Status O

Cl **PP-B** SC 5.1 P 5 L 22 # 76
 Sukert, Alan Xerox

Comment Type T Comment Status X

The definition of shared-medium interface is not consistent between subclause 5.1 and Annex A. In subclause 5.1 a shared-medium interface is defined as ""transmitting and receiving User or TSF Data"" between the HCD and external devices over communications media that ""are or can be shared by other users"" while Annex A (page 58, line 29) defines a shared-medium interface as a mechanism for ""exchanging data""...over a communications medium which, in conventional practice ""is or can be simultaneously accessed by multiple users"".

SuggestedRemedy

Make sure the definition of shared-medium interface is consistent between subclause 5.1 and Annex A.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC 5.2 P 5 L 34 # 77
 Sukert, Alan Xerox

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

I understand why this text was changed from Users == Subjects to its current text, but I had to read this new sentence at least three times before it made sense to me. I'm concerned readers of this standard will have to do the same thing. I think if you used wording similar to the preceding text in this sentence will become easier to understand.

SuggestedRemedy

Change this sentence to read something like ""...and therefore, it can be assumed that the security attributes of a Subject used in access control decisions are identical to the security attributes of the User that requests the access unless...""

Proposed Response Response Status **O**

Cl **PP-C** SC 5.2 P 6 L 1 # 109
 Sukert, Alan Xerox

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

Figure 1 on the TOE Model still uses the symbology 'USER == Subject' even though based on comments from last month's meeting that symbology was removed from PP-C (see the change in subclause 5.2, page 5, line 18). Figure 1 also uses the TOE==TSF symbology that was also removed from PP-C (see subclause 5.2, page 5, line 25).

SuggestedRemedy

Use a different symbology or terminology in Figure 1 to show that you can't distinguish between Users and Subjects in the context of the TOE model and that the TSF and TOE are equivalent.

Proposed Response Response Status **O**

Cl **PP-D** SC 5.2 P 6 L 1 # 122
 Sukert, Alan Xerox

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

Figure 1 on the TOE Model still uses the symbology 'USER == Subject' even though based on comments from last month's meeting that symbology was removed from PP-D (see the change in subclause 5.2, page 5, line 18). Figure 1 also uses the TOE==TSF symbology that was also removed from PP-D (see subclause 5.2, page 5, line 25).

SuggestedRemedy

Use a different symbology or terminology in Figure 1 to show that you can't distinguish between Users and Subjects in the context of the TOE model and that the TSF and TOE are equivalent.

Proposed Response Response Status **O**

Cl **PP-B** SC 5.2 P 6 L 6 # 85
 Sukert, Alan Xerox

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

Figure 1 on the TOE Model still uses the symbology 'USER == Subject' even though based on comments from last month's meeting that symbology was removed from PP-B (see the change in subclause 5.2, page 5, line 34). Figure 1 also uses the TOE==TSF symbology that was also removed from PP-B (see subclause 5.2, page 5, line 41).

SuggestedRemedy

Use a different symbology or terminology in Figure 1 to show that you can't distinguish between Users and Subjects in the context of the TOE model and that the TSF and TOE are equivalent.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

CI **PP-A** SC 5.1 P 6 L 21 # 49
 Sukert, Alan Xerox

Comment Type T Comment Status X

The definition for removable nonvolatile storage in clause 5.1 does not agree with the corresponding definition for removable nonvolatile storage in Annex A. Specifically, in clause 5.1 nonvolatile storage is defined as User or TSF Data that is designed to be removed from the TOE by ""authorized non-service personnel""; Annex A (page 59, line 24) states that removable nonvolatile storage is designed to be removed from the TOE by ""authorized personnel"".

SuggestedRemedy

Make sure the definition of removable nonvolatile storage is consistent between subclause 5.1 and Annex A.

Proposed Response Response Status O

CI **PP-A** SC 5.1 P 6 L 23 # 51
 Sukert, Alan Xerox

Comment Type T Comment Status X

The definition of shared-medium interface is not consistent between subclause 5.1 and Annex A. In subclause 5.1 a shared-medium interface is defined as ""transmitting and receiving User or TSF Data"" between the HCD and external devices over communications media that ""are or can be shared by other users"" while Annex A (page 59, line 36) defines a shared-medium interface as a mechanism for ""exchanging data""...over a communications medium which, in conventional practice ""is or can be simultaneously accessed by multiple users"".

SuggestedRemedy

Make sure the definition of shared-medium interface is consistent between subclause 5.1 and Annex A.

Proposed Response Response Status O

CI **PP-A** SC 5.2 P 6 L 34 # 52
 Sukert, Alan Xerox

Comment Type T Comment Status X

I understand why this text was changed from Users == Subjects to its current text, but I had to read this new sentence at least three times before it made sense to me. I'm concerned readers of this standard will have to do the same thing. I think if you used wording similar to the preceding text in this sentence will become easier to understand.

SuggestedRemedy

Change this sentence to read something like ""...and therefore, it can be assumed that the security attributes of a Subject used in access control decisions are identical to the security attributes of the User that requests the access unless...""

Proposed Response Response Status O

CI **PP-A** SC 5.2 P 7 L 6 # 60
 Sukert, Alan Xerox

Comment Type T Comment Status X

Figure 1 on the TOE Model still uses the symbology 'USER == Subject' even though based on comments from last month's meeting that symbology was removed from PP-A (see the change in subclause 5.2, page 6, line 34). Figure 1 also uses the TOE==TSF symbology that was also removed from PP-A (see subclause 5.2, page 6, line 41).

SuggestedRemedy

Use a different symbology or terminology in Figure 1 to show that you can't distinguish between Users and Subjects in the context of the TOE model and that the TSF and TOE are equivalent.

Proposed Response Response Status O

CI **PP-D** SC 6.4 P 9 L 30 # 121
 Sukert, Alan Xerox

Comment Type T Comment Status X

This line references the PRT and SMI SFR Packages. However, PP-D only has the SMI SFR Package

SuggestedRemedy

Revise this line to read ""...and the SFR Package for the SMI (Shared-medium Interface) function,...""

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-D** SC **7.2** P **10** L **10** # **119**
 Sukert, Alan Xerox

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

In Table 6, given the discussion at the Aug 08 meeting that software verification can only be done for accidental, non-deliberate modification of the executable software. That aspect doesn't seem to appear in the revised definition of P.SOFTWARE.VERIFICATION since, for example, a ""malfunction"" can be both deliberately and accidentally caused (and the current definition doesn't distinguish the two).

A similar comment applies to the PP App Note in subclause 10.8, page 17, line 13.

SuggestedRemedy

Suggest (1) the definition of P.SOFTWARE.VERIFICATION be changed to read something like ""To detect accidental, non-deliberate malfunction of the TOE, procedures will exist to self-verify executable code in the TOE"" and (2) the PP APP Note in subclause 10.8, page 17, line 13 to read something like ""FPT_TST.1 is intended to verify that the TSF executable code has not been modified by accidental, non-deliberate malfunction.""

Proposed Response Response Status **O**

Cl **PP-D** SC **7.2** P **10** L **10** # **120**
 Sukert, Alan Xerox

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

In Table 8, the new definition of P.CHANNEL.MANAGEMENT indicates that operation of channels will be controlled by the TOE or its ""operating environment"". I noted that the CC and clauses 8.3 and 8.4 of this document, for example, talk about the ""operational environment"" as opposed to the operating environment. I think our definitions should be consistent with the terminology used in the CC and in the rest of the document.

SuggestedRemedy

Suggest changing the definition of P.CHANNEL.MANAGEMENT to read ""...will be controlled by the TOE or its operational environment.""

Proposed Response Response Status **O**

Cl **PP-C** SC **6.4** P **10** L **23** # **105**
 Sukert, Alan Xerox

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

This line references the PRT and SMI SFR Packages. However, PP-C only has the SMI SFR Package

SuggestedRemedy

Revise this line to read ""...and the SFR Package for the SMI (Shared-medium Interface) function,...""

Proposed Response Response Status **O**

Cl **PP-C** SC **7.2** P **11** L **11** # **37**
 Chen, Nancy Oki Data

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

In environment C, only Administrators are identified, authenticated, and authorized. Currently Table 8 - Organizational Security Policies for the TOE : P.USER.AUTHORIZATION states that all users will be authorized.

Are you proposing to change the previously agreed objectives for environment C?

SuggestedRemedy

If not proposing a change of environment C security objectives, then -

Change the ""user"" to ""Administrator"" in the policy. Make corresponding change to Table 13 on page 14.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC 7.2 P 11 L 11 # 79
 Sukert, Alan Xerox

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

In Table 8, the new definition of P.CHANNEL.MANAGEMENT indicates that operation of channels will be controlled by the TOE or its "operating environment". I noted that the CC and clauses 8.3 and 8.4 of this document, for example, talk about the "operational environment" as opposed to the operating environment. I think our definitions should be consistent with the terminology used in the CC and in the rest of the document.

Note: A similar comment applies to subclause 17.1, page 49, line 7.

SuggestedRemedy

Suggest changing the definition of P.CHANNEL.MANAGEMENT to read "...will be controlled by the TOE or its operational environment." Change subclause 17.1, page 49, line 7 to read "...when such devices are removed from the operational environment".

Proposed Response Response Status

Cl **PP-C** SC 7.2 P 11 L 11 # 104
 Sukert, Alan Xerox

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

In Table 8, the new definition of P.CHANNEL.MANAGEMENT indicates that operation of channels will be controlled by the TOE or its "operating environment". I noted that the CC and clauses 8.3 and 8.4 of this document, for example, talk about the "operational environment" as opposed to the operating environment. I think our definitions should be consistent with the terminology used in the CC and in the rest of the document.

SuggestedRemedy

Suggest changing the definition of P.CHANNEL.MANAGEMENT to read "...will be controlled by the TOE or its operational environment."

Proposed Response Response Status

Cl **PP-C** SC 7.2 P 11 L 11 # 103
 Sukert, Alan Xerox

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

In Table 8, given the discussion at the Aug 08 meeting that software verification can only be done for accidental, non-deliberate modification of the executable software. That aspect doesn't seem to appear in the revised definition of P.SOFTWARE.VERIFICATION since, for example, a "malfunction" can be both deliberately and accidentally caused (and the current definition doesn't distinguish the two).

A similar comment applies to the PP App Note in subclause 10.8, page 25, line 13.

SuggestedRemedy

Suggest (1) the definition of P.SOFTWARE.VERIFICATION be changed to read something like "To detect accidental, non-deliberate malfunction of the TOE, procedures will exist to self-verify executable code in the TOE" and (2) the PP APP Note in subclause 10.8, page 25, line 13 to read something like "FPT_TST.1 is intended to verify that the TSF executable code has not been modified by accidental, non-deliberate malfunction."

Proposed Response Response Status

Cl **PP-B** SC 7.2 P 11 L 11 # 78
 Sukert, Alan Xerox

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

In Table 8, given the discussion at the Aug 08 meeting that software verification can only be done for accidental, non-deliberate modification of the executable software. That aspect doesn't seem to appear in the revised definition of P.SOFTWARE.VERIFICATION since, for example, a "malfunction" can be both deliberately and accidentally caused (and the current definition doesn't distinguish the two).

A similar comment applies to the PP App Note in subclause 10.8, page 27, line 30.

SuggestedRemedy

Suggest (1) the definition of P.SOFTWARE.VERIFICATION be changed to read something like "To detect accidental, non-deliberate malfunction of the TOE, procedures will exist to self-verify executable code in the TOE" and (2) the PP APP Note in subclause 10.8, page 27, line 30 to read something like "FPT_TST.1.3 is intended to verify that the TSF executable code has not been modified by accidental, non-deliberate malfunction."

Proposed Response Response Status

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-C** SC **7.3** P **12** L **1** # **38**

Chen, Nancy Oki Data

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

In environment C, there is no way the Assumption can be made that users are aware of the security policies and procedures of their organization, and have the training and competence to follow those policies and procedures.

SuggestedRemedy

Remove A.USER.TRAINED and OE.USER.TRAINED.
Make corresponding change to Table 13 on page 15.

Proposed Response Response Status **O**

Cl **PP-A** SC **7.1** P **12** L **4** # **3**

Farrell, Lee Canon

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

The threats T.DOC.DIS and T.DOC.ALT as currently defined are too generalized -- and therefore difficult to address appropriately -- especially when applied to removable NVS.

The cases for the NVS being on-line and operational vs. offline and non-operational should be handled and identified separately.

SuggestedRemedy

Replace T.DOC.DIS and T.DOC.ALT with the following four threats, all affecting D.DOC:

T.DOC.UAC A user may gain access to User Document Data for which they are not authorized according to the TOE security policy when operational.

T.DOC.REMOVAL (or .REMOVAL_NV?) An attacker may get hold of removable nonvolatile mass-storage device and analyze it off-line to obtain original content of User Document Data.

T.DOC.TAMPER (or .TAMPER_NV?) An attacker may tamper with the original content of User Document Data in the removable nonvolatile mass-storage device off-line by modifying it.

T.DOC.RESIDUAL An attacker may gain unauthorized access to User Document Data through reallocation of TOE resources on retirement or ownership transfer.

Also add the following comment:

It should be noted that T.DOC.REMOVAL and T.DOC.TAMPER are additional threats only applicable when NVS SFR package is present in the target of evaluation. For a description of the NVS SFR package, see clause 11.3.

Also, modify Table 13 to include these four new threats and delete the replaced two threats.

Also in Table 13, map T.DOC.UAC to both O.USER.AUTHORIZED and OE.USER.AUTHORIZED

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC 7.1 P 12 L 4 # 25
 Farrell, Lee Canon

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

Similar to T.DOC.ALT, the threats T.FUNC.ALT and T.PROT.ALT as currently defined are too generalized -- and therefore difficult to address appropriately -- especially when applied to removable NVS.

The cases for the NVS being on-line and operational vs. offline and non-operational should be handled and identified separately.

SuggestedRemedy

Replace T.FUNC.ALT and T.PROT.ALT with corresponding two threats (as suggested with T.DOC.ALT):

T.*.UAC, T.*.TAMPER

Also add the following comment:

It should be noted that T.*.TAMPER is an additional threat only applicable when NVS SFR package is present in the target of evaluation. For a description of the NVS SFR package, see clause 11.3.ö

Also, modify lots of affected Tables and any Application Notes that contain references to these replaced two threats.

[This remedy would be more detailed, but I/Em running up against the comment submission deadline.]

Proposed Response Response Status

Cl **PP-A** SC 7.1 P 12 L 5 # 4
 Farrell, Lee Canon

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

The threats T.CONF.DIS and T.CONF.ALT as currently defined are too generalized -- and therefore difficult to address appropriately -- especially when applied to removable NVS.

The cases for the NVS being on-line and operational vs. offline and non-operational should be handled and identified separately.

SuggestedRemedy

Replace T.CONF.DIS and T.CONF.ALT with the following three threats, all affecting D.CONF:

T.CONF.UAC A user may gain access to TSF Confidential Data for which they are not authorized according to the TOE security policy when operational.

T.CONF.REMOVAL (or .REMOVAL_NVS?) An attacker may get hold of removable nonvolatile mass-storage device and analyze it off-line to obtain original content of TSF Confidential Data.

T.CONF.TAMPER (or .TAMPER_NVS?) An attacker may tamper with the original content of TSF Confidential Data in the removable nonvolatile mass-storage device off-line by modifying it.

Also add the following comment:

It should be noted that T.CONF.REMOVAL and T.CONF.TAMPER are additional threats only applicable when NVS SFR package is present in the target of evaluation. For a description of the NVS SFR package, see clause 11.3.ö

Also, modify Table 13 to include these three new threats and delete the replaced two threats.

Proposed Response Response Status

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC 7.2 P 12 L 11 # 23
Farrell, Lee Canon

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

The definition of P.SOFTWARE.VERIFICATION should not apply to all software in the TOE, but be limited to the executable software that is critical to the security functionality of the TOE.

SuggestedRemedy

Change the definition of P.SOFTWARE.VERIFICATION to:
 ôTo detect malfunction of the TOE security functions, procedures will exist to self-verify the executable code in the TOE that is critical to the security functionality of the TOE.ö

Proposed Response Response Status **O**

Cl **PP-A** SC 7.2 P 12 L 11 # 54
Sukert, Alan Xerox

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

In Table 8, the new definition of P.CHANNEL.MANAGEMENT indicates that operation of channels will be controlled by the TOE or its ""operating environment"". I noted that the CC and clauses 8.3 and 8.4 of this document, for example, talk about the ""operational environment"" as opposed to the operating environment. I think our definitions should be consistent with the terminology used in the CC and in the rest of the document.

Note: A similar comment applies to subclause 17.1, page 50, line 7.

SuggestedRemedy

Suggest changing the definition of P.CHANNEL.MANAGEMENT to read ""...will be controlled by the TOE or its operational environment."" Change subclause 17.1, page 50, line 7 to read ""...when such devices are removed from the operational environment"".

Proposed Response Response Status **O**

Cl **PP-A** SC 7.2 P 12 L 11 # 53
Sukert, Alan Xerox

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

In Table 8, given the discussion at the Aug 08 meeting that software verification can only be done for accidental, non-deliberate modification of the executable software. That aspect doesn't seem to appear in the revised definition of P.SOFTWARE.VERIFICATION since, for example, a ""malfunction"" can be both deliberately and accidentally caused (and the current definition doesn't distinguish the two).

A similar comment applies to the PP App Note in subclause 10.8, page 28, line 30.

SuggestedRemedy

Suggest (1) the definition of P.SOFTWARE.VERIFICATION be changed to read something like ""To detect accidental, non-deliberate malfunction of the TOE, procedures will exist to self-verify executable code in the TOE"" and (2) the PP APP Note in subclause 10.8, page 28, line 30 to read something like ""FPT_TST.1.3 is intended to verify that the TSF executable code has not been modified by accidental, non-deliberate malfunction.""

Proposed Response Response Status **O**

Cl **PP-C** SC 8.1 P 13 L 4 # 39
Chen, Nancy Oki Data

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

In environment C, only Administrators are identified, authenticated, and authorized. Currently Table 10 - Security objectives for the TOE : O.USER.AUTHORIZATION states that all users will be IA&A'd.

Are you proposing to change what we have agreed on environment C security objectives?

SuggestedRemedy

If not proposing to change the agreed environment C security objectives, then -

Change the ""user"" to ""Administrator"" in the objective.
 Make corresponding change to Table 13 on page 14.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **8.1** P **14** L **4** # **5**
 Farrell, Lee Canon

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

The objectives O.DOC.NO_DIS and O.DOC.NO_ALT as currently defined are too generalized -- and therefore difficult to address appropriately -- especially when applied to removable NVS.

The cases for the NVS being on-line and operational vs. offline and non-operational should be handled and identified separately.

SuggestedRemedy

Replace O.DOC.NO_DIS and O.DOC.NO_ALT with the following four objectives:

O.DOC.ACCESS The TOE shall provide mechanisms that control a user/Es logical access to the User Document Data when operational.

O.DOC.CONFIDENT The TOE shall provide functions to maintain the confidentiality of User Document Data that is stored in removable nonvolatile mass-storage device when device is removed from the TOE.

O.DOC.MOUNT The TOE shall provide mechanisms that prevent, diminish or detect successful tampering of User Document Data that is stored in removable nonvolatile mass-storage device when device is removed from the TOE.

O.DOC.RESIDUAL The TOE shall provide functions to ensure that any information contained in User Document Data is not released when resource is reallocated.

Also add the following comment:

ôIt should be noted that O.DOC.CONFIDENT and O.DOC.MOUNT are additional objectives only applicable when NVS SFR package is present in the target of evaluation. For a description of the NVS SFR package, see clause 11.3.ö

Also, modify Table 13 to include these four new objectives mapped to T.DOC.UAC, T.DOC.REMOVAL, T.DOC.TAMPER, T.DOC.RESIDUAL, respectively -- and delete the replaced two objectives.

Proposed Response Response Status

Cl **PP-A** SC **8.1** P **14** L **4** # **6**
 Farrell, Lee Canon

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

The objectives O.CONF.NO_DIS and O.CONF.NO_ALT as currently defined are too generalized -- and therefore difficult to address appropriately -- especially when applied to removable NVS.

The cases for the NVS being on-line and operational vs. offline and non-operational should be handled and identified separately.

SuggestedRemedy

Replace O.CONF.NO_DIS and O.CONF.NO_ALT with the following three objectives:

O.CONF.ACCESS The TOE shall provide mechanisms that control a user/Es logical access to the TSF Confidential Data when operational.

O.CONF.CONFIDENT The TOE shall provide functions to maintain the confidentiality of TSF Confidential Data that is stored in removable nonvolatile mass-storage device when device is removed from the TOE.

O.CONF.MOUNT The TOE shall provide mechanisms that prevent, diminish or detect successful tampering of TSF Confidential Data that is stored in removable nonvolatile mass-storage device when device is removed from the TOE.

Also add the following comment:

ôIt should be noted that O.CONF.CONFIDENT and O.CONF.MOUNT are additional objectives only applicable when NVS SFR package is present in the target of evaluation. For a description of the NVS SFR package, see clause 11.3.ö

Also, modify Table 13 to include these three new objectives mapped to T.CONF.UAC, T.CONF.REMOVAL, T.CONF.TAMPER, respectively -- and delete the replaced two objectives.

Proposed Response Response Status

IEEE P2600 Hardcopy Device and System Security Comments

CI **PP-A** SC **8.1** P **14** L **4** # **26**
 Farrell, Lee Canon

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

Similar to O.DOC.NO_ALT, the objectives O.FUNC.NO_ALT and O.PROT.NO_ALT as currently defined are too generalized -- and therefore difficult to address appropriately -- especially when applied to removable NVS.

The cases for the NVS being on-line and operational vs. offline and non-operational should be handled and identified separately.

SuggestedRemedy

Replace O.FUNC.NO_ALT and O.PROT.NO_ALT with corresponding two objectives (as suggested with O.DOC.NO_ALT):

O.*.ACCESS, O.*.MOUNT

Also add the following comment:

It should be noted that O.*.MOUNT is an additional objective only applicable when NVS SFR package is present in the target of evaluation. For a description of the NVS SFR package, see clause 11.3.0

Also, modify lots of affected Tables and any Application Notes that contain references to these replaced two objectives.

[This remedy would be more detailed, but I'm running up against the comment submission deadline.]

Proposed Response Response Status **O**

CI **PP-D** SC **10.6** P **15** L **29** # **123**
 Sukert, Alan Xerox

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

Since the use of the term 'Nobody' has been standardized in the document now, I was wondering why on line 29 the term 'no one' instead of nobody is used.

SuggestedRemedy

Suggest changing subclause 10.6 - page 15, line 29 to use nobody instead of 'no one'.

Proposed Response Response Status **O**

CI **PP-B** SC **10.4** P **18** L **9** # **81**
 Sukert, Alan Xerox

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

Since the concept of ""owning"" a document, as stated in this PP App Note is different from the usual concept of owning a document, I think the definition of ownership as used in this document needs to go into Annex A.

SuggestedRemedy

Include the following definition (or something like it) in Annex A:

Ownership: A User creating or submitting his/her own document to the TOE.

Proposed Response Response Status **O**

CI **PP-C** SC **10.4** P **18** L **18** # **107**
 Sukert, Alan Xerox

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

In the new PP App Note on page 18, line 11 I think that an additional clarification is needed. The App Note states that the rules that determine access may be the same or may be different for each function; what the note doesn't say is where the ST Author should specify these access rules, especially if they are different for each function - in the SFR Package for each applicable function, in FDP_ACC.1, in an App Note or somewhere else.

SuggestedRemedy

Please clarify in the new PP App Note on page 18, line 18 where the ST Author should specify the access rules, especially if they are different for each function.

Proposed Response Response Status **O**

CI **PP-C** SC **10.4** P **18** L **19** # **106**
 Sukert, Alan Xerox

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

The new PP App Note on page 18, line 19 is a little confusing to me. Is it saying that the TOE Function Access Control SFP may be defined as a policy between users and subjects, or is it saying that the TOE Function Access Control SFP may be defined as a policy that is either between users or between subjects - I couldn't tell.

SuggestedRemedy

Clarify in the PP APP Note in page 18, line 19 what the policy is - between users and subjects, or between users or between subjects.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC **10.4** P **18** L **22** # **80**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

This is a nit - the insertion of the Table 16 reference on page 19, line 22 is missing a space before the next word 'and'.

SuggestedRemedy

Include the missing space after the Table 16 reference in the indicated line.

Proposed Response Response Status **O**

Cl **PP-C** SC **10.4** P **19** L **1** # **108**
 Sukert, Alan Xerox

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

Given the comment I made in the pre-review of this latest PP-A draft about the case where the TOE Function Access Control SFP was that all users were allowed to access all of the applicable TOE functions for that TOE (this would be allowable under the new SFRs in PP-A) I noted it really isn't addressed in this new App Note. Since this case will definitely happen for TOEs that are to apply to PP-C I think it needs to be explicitly discussed in this App Note.

This same comment applies to the PP App Note for the FMT_MSA.1(b) SFR in subclause 10.6, page 22, line 16.

SuggestedRemedy

Add a statement to the App Note in subclause 10.4 page 19, line 1 and in subclause 10.6, page 22, line 16 that deals with the case where all users were allowed to access all of the applicable TOE functions for that TOE.

Proposed Response Response Status **O**

Cl **PP-A** SC **10.4, 10.6** P **19** L **5** # **43**
 Nevo, Ron Sharp

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

FDP_ACC.1(b), FDP_ACF.1(b), FMT_MSA.1(b), and FMT_MSA.3(b)
 These are the specifications of access control functions, etc. that is required in each function specified in 11.3 SFR Package functions. Including them in the PP means these security functions shall be implemented.
 Whether implementing these security functions or not should not be specified since it is different by ST Authors (i.e. TOEs).
 If you want to include all access control functions, etc. into ST, you should add a description into subclause 6.4.

SuggestedRemedy

Remove FDP_ACC.1(b), FDP_ACF.1(b), FMT_MSA.1(b), and FMT_MSA.3(b).

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **10.4** P **19** L **8** # **27**
 Chen, Nancy Oki Data

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

(1) According to CC, assumption on the function of the TOE may not be used to achieve the security objectives. Since "Create" D.DOC is a common operation (and thus a function) of the TOE (=TSF by our definition), there should not be assumption made about the operation as stated in the App. Note that says "Access control rules for the Create Operation are not specified because it is assumed that any authorized U.NORMAL can create his/her own documents and cannot create documents that are owned by another User."

(2) It's unclear that by the Common Access Control SFP, whether those write operations not listed in Table 16 are allowed or denied and for what roles.

SuggestedRemedy

Define the Common Access Control SFP as:

- (1) All operations to D.DOC and D.FUNC are "Denied, except for his/her own documents or function data.
- (2) The write operations include Create, Modify, Delete. We need to add this definition for "write operation" in 5.3.3 where all operations are defined.
- (3) Add an App. Note to clarify that all other operations not specified here are "allowed".
- (4) Add an App. Note for ST authors to understand that they can add stricter access control rules. An example of a stricter rule is that "no implementation of an operation" is the same as "The operation is Denied for All Users". If this is the case, the ST author can then add this stricter access control rule to the SFP and the TOE can still claim demonstrable compliance to the PP. Another example is when the Modify operation is implemented for D.FUNC but only Administrator is allowed to do so for all users, then the ST author can add this rule which is stricter than the standard Common Access Control SFP, and the TOE still can claim compliance to the PP.

This way we don't have to repetively adding App. Notes for the SCN, CPY, FAX, and DSR SFR packages to require ST authors to add access control rules for Modify operation if it's implemented.

Also by doing so, we can remove the CPY SFR package.

Proposed Response Response Status

Cl **PP-B** SC **10.4** P **19** L **8** # **32**
 Chen, Nancy Oki Data

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

(1) Since "Create" D.DOC is a common operation (and thus a function) of the TOE (=TSF by our definition), there should not be assumption made about the operation as stated in the App. Note that says "Access control rules for the Create Operation are not specified because it is assumed that any authorized U.NORMAL can create his/her own documents and cannot create documents that are owned by another User." According to CC, assumption on the function of the TOE may not be used to achieve the security objectives.

(2) It's unclear that by the Common Access Control SFP, whether those write operations not listed in Table 16 are allowed or denied and for what roles.

SuggestedRemedy

Define the Common Access Control SFP as:

- (1) All operations to D.DOC and D.FUNC are "Denied, except for his/her own documents or function data.
- (2) The write operations include Create, Modify, Delete. We need to add this definition for "write operation" in 5.3.3 where all operations are defined.
- (3) Add an App. Note to clarify that all other operations not specified here are "allowed".
- (4) Add an App. Note for ST authors to understand that they can add stricter access control rules. An example of a stricter rule is that "no implementation of an operation" is the same as "The operation is Denied for All Users". If this is the case, the ST author can then add this stricter access control rule to the SFP and the TOE can still claim demonstrable compliance to the PP. Another example is when the Modify operation is implemented for D.FUNC but only Administrator is allowed to do so for all users, then the ST author can add this rule which is stricter than the standard Common Access Control SFP, and the TOE still can claim compliance to the PP.

This way we don't have to repetively adding App. Notes for the SCN, CPY, FAX, and DSR SFR packages to require ST authors to add access control rules for Modify operation if it's implemented.

Also by doing so, we can remove the CPY SFR package.

Proposed Response Response Status

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC 10.4 P 19 L 9 # 56
 Sukert, Alan Xerox

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

Since the concept of ""owning"" a document, as stated in this PP App Note is different from the usual concept of owning a document, I think the definition of ownership as used in this document needs to go into Annex A.

SuggestedRemedy

Include the following definition (or something like it) in Annex A:

Ownership: A User creating or submitting his/her own document to the TOE.

Proposed Response Response Status **O**

Cl **PP-B** SC 10.4 P 19 L 11 # 83
 Sukert, Alan Xerox

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

In the new PP App Note on page 19, line 11 I think that an additional clarification is needed. The App Note states that the rules that determine access may be the same or may be different for each function; what the note doesn't say is where the ST Author should specify these access rules, especially if they are different for each function - in the SFR Package for each applicable function, in FDP_ACC.1(b), in an App Note or somewhere else.

SuggestedRemedy

Please clarify in the new PP App Note on page 19, line 11 where the ST Author should specify the access rules, especially if they are different for each function.

Proposed Response Response Status **O**

Cl **PP-C** SC 10.4 P 19 L 11 # 110
 Sukert, Alan Xerox

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

In the new FDP_ACF.1.2 SFR you indicate that the selection is that the user is explicitly authorized by an administrator to use a function plus some other choices. I note that in the new FDP_ACF.1.3 SFR on line 21 on the same page the SFR refers to the role of U.ADMINISTRATOR.

I have two issues:

1. Why in the FDP_ACF.1.2 SFR do you refer to the administrator while in the FDP_ACF.1.3 SFR do you refer to U.ADMINISTRATOR when both seem to be referring to the same user type or role.
2. The TOE model in subclause 5.3.1, page 6 indicates that U.ADMINISTRATOR is a user type. Why in the FDP_ACF.1.3 SFR is this user type referred to as a user role - aren't a user type and a user role two different (but certainly related) things.

SuggestedRemedy

Clarify the use of administrator vs. U.ADMINISTRATOR in subclause 10.4, discussion of the FDP_ACF.1.2 and FDP_ACF.1.3 SFRs on page 19.

Proposed Response Response Status **O**

Cl **PP-B** SC 10.4 P 19 L 15 # 82
 Sukert, Alan Xerox

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

The new PP App Note on page 19, line 15 is a little confusing to me. Is it saying that the TOE Function Access Control SFP may be defined as a policy between users and subjects, or is it saying that the TOE Function Access Control SFP may be defined as a policy that is either between users or between subjects - I couldn't tell.

SuggestedRemedy

Clarify in the PP APP Note in page 19, line 15 what the policy is - between users and subjects, or between users or between subjects.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **10.4** P **19** L **16** # **55**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

This is a nit - the insertion of the Table 16 reference on page 19, lines 16 and 22 is missing a space before the next word 'and'.

SuggestedRemedy

Include the missing space after the Table 16 reference in the two indicated lines.

Proposed Response Response Status **O**

Cl **PP-A** SC **10.4** P **19** L **32** # **7**
 Farrell, Lee Canon

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

If O.DOC.NO_DIS and O.DOC.NO_ALT are replaced with new proposed objectives (see clause 8.1 comment), then this application note needs modification.

SuggestedRemedy

Replace ôO.DOC.NO_DIS, O.DOC.NO_ALTö with ôO.DOC.ACCESSö.

Proposed Response Response Status **O**

Cl **PP-A** SC **10.4** P **20** L **11** # **58**
 Sukert, Alan Xerox

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

In the new PP App Note on page 20, line 11 I think that an additional clarification is needed. The App Note states that the rules that determine access may be the same or may be different for each function; what the note doesn't say is where the ST Author should specify these access rules, especially if they are different for each function - in the SFR Package for each applicable function, in FDP_ACC.1(b), in an App Note or somewhere else.

SuggestedRemedy

Please clarify in the new PP App Note on page 20, line 11 where the ST Author should specify the access rules, especially if they are different for each function.

Proposed Response Response Status **O**

Cl **PP-A** SC **10.4** P **20** L **15** # **57**
 Sukert, Alan Xerox

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

The new PP App Note on page 20, line 15 is a little confusing to me. Is it saying that the TOE Function Access Control SFP may be defined as a policy between users and subjects, or is it saying that the TOE Function Access Control SFP may be defined as a policy that is either between users or between subjects - I couldn't tell.

SuggestedRemedy

Clarify in the PP APP Note in page 20, line 15 what the policy is - between users and subjects, or between users or between subjects.

Proposed Response Response Status **O**

Cl **PP-B** SC **10.4** P **20** L **20** # **84**
 Sukert, Alan Xerox

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

Given the comment I made in the pre-review of this latest PP-A draft about the case where the TOE Function Access Control SFP was that all users were allowed to access all of the applicable TOE functions for that TOE (this would be allowable under the new SFRs in PP-B) I noted it really isn't addressed in this new App Note. Since this case will happen even in TOEs that are to apply to PP-B I think it needs to be explicitly discussed in this App Note.

This same comment applies to the PP App Note for the FMT_MSA.1(b) SFR in subclause 10.6, page 24, line 18.

SuggestedRemedy

Add a statement to the App Note in subclause 10.4 page 20, line 20 and in subclause 10.6, page 24, line 18 that deals with the case where all users were allowed to access all of the applicable TOE functions for that TOE.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC **10.4** P **20** L **30** # **86**
 Sukert, Alan Xerox

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

In the new FDP_ACF.1.2(b) SFR you indicate that the selection is that the user is explicitly authorized by an administrator to use a function plus some other choices. I note that in the new FDP_ACF.1.3(b) SFR on line 41 on the same page the SFR refers to the role of U.ADMINISTRATOR.

I have two issues:

1. Why in the FDP_ACF.1.2(b) SFR do you refer to the administrator while in the FDP_ACF.1.3(b) SFR do you refer to U.ADMINISTRATOR when both seem to be referring to the same user type or role.
2. The TOE model in subclause 5.3.1, page 7 indicates that U.ADMINISTRATOR is a user type. Why in the FDP_ACF.1.3(b) SFR is this user type referred to as a user role - aren't a user type and a user role two different (but certainly related) things.

SuggestedRemedy

Clarify the use of administrator vs. U.ADMINISTRATOR in subclause 10.4, discussion of the FDP_ACF.1.2(b) and FDP_ACF.1.3(b) SFRs on page 20.

Proposed Response Response Status

Cl **PP-A** SC **10.4** P **21** L **20** # **59**
 Sukert, Alan Xerox

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

Given the comment I made in the pre-review of this latest PP-A draft about the case where the TOE Function Access Control SFP was that all users were allowed to access all of the applicable TOE functions for that TOE (this would be allowable under the new SFRs in PP-A) I noted it really isn't addressed in this new App Note. Since this case will happen even in TOEs that are to apply to PP-A I think it needs to be explicitly discussed in this App Note.

This same comment applies to the PP App Note for the FMT_MSA.1(b) SFR in subclause 10.6, page 25, line 18.

SuggestedRemedy

Add a statement to the App Note in subclause 10.4 page 21, line 20 and in subclause 10.6, page 25, line 18 that deals with the case where all users were allowed to access all of the applicable TOE functions for that TOE.

Proposed Response Response Status

Cl **PP-A** SC **10.4** P **21** L **30** # **61**
 Sukert, Alan Xerox

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

In the new FDP_ACF.1.2(b) SFR you indicate that the selection is that the user is explicitly authorized by an administrator to use a function plus some other choices. I note that in the new FDP_ACF.1.3(b) SFR on line 40 on the same page the SFR refers to the role of U.ADMINISTRATOR.

I have two issues:

1. Why in the FDP_ACF.1.2(b) SFR do you refer to the administrator while in the FDP_ACF.1.3(b) SFR do you refer to U.ADMINISTRATOR when both seem to be referring to the same user type or role.
2. The TOE model in subclause 5.3.1, page 8 indicates that U.ADMINISTRATOR is a user type. Why in the FDP_ACF.1.3(b) SFR is this user type referred to as a user role - aren't a user type and a user role two different (but certainly related) things.

SuggestedRemedy

Clarify the use of administrator vs. U.ADMINISTRATOR in subclause 10.4, discussion of the FDP_ACF.1.2(b) and FDP_ACF.1.3(b) SFRs on page 21.

Proposed Response Response Status

Cl **PP-A** SC **10.4** P **22** L **13** # **44**
 Nevo, Ron Sharp

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

FDP_RIP.1
 FDP_RIP.1 is a fulfillment of O.DOC.NO_DIS. O.DOC.NO_DIS is an objective to T.DOC.DIS against D.DOC.
 If D.DOC is stored into NVS, attackers who are assumed in EAL3 do not have a capability to attack this asset. That means the threat does not exist.
 (The current descriptions indicate that D.DOC shall be stored into NVS.)

SuggestedRemedy

- Either of the two below:
- 1) NVS
 Move FDP_RIP.1 to NVS package (remove from PP)
 - 2) OSP
 Derive O.DOC.NO_DIS from Objective Security Policies

Proposed Response Response Status

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-C** SC **10.6** P **22** L **20** # **111**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

Three grammatical errors on line 20 - now says that "...a ST author has check if all those security attributes..." (note the PP now appears to consistently use 'ST Author')

SuggestedRemedy

Revise subclause 10.6, page 22, line 20 to read "...an ST Author has to check if all those security attributes..."

Proposed Response Response Status **O**

Cl **PP-A** SC **10.4** P **22** L **22** # **8**
 Farrell, Lee Canon

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

If O.DOC.NO_DIS and O.DOC.NO_ALT are replaced with new proposed objectives (see clause 8.1 comment), then this application note needs modification.

SuggestedRemedy

Replace δO.DOC.NO_DIS with δO.DOC.RESIDUAL.

Proposed Response Response Status **O**

Cl **PP-D** SC **12.4** P **22** L **29** # **125**
 Sukert, Alan Xerox

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

The changes made to the PP App Note in PP-A, subclause 18.4, page 55, line 1 were not made in the corresponding PP App Note in PP-D, subclause 12.4, page 22, line 29.

SuggestedRemedy

Make sure the changes made to the PP App Note in PP-A, subclause 18.4, page 55, line 1 are made in the corresponding PP App Note in PP-D, subclause 12.4, page 22, line 29

Proposed Response Response Status **O**

Cl **PP-C** SC **10.6** P **23** L **6** # **112**
 Sukert, Alan Xerox

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

The PP App Note on this line states ""This SFR is used to define the default values for the access to TOE function a user gets assigned...". Since a user could be assigned access to more than one TOE function depending on which TOE functions applied to the TOE and which ones the user might be given access to, this statement needs to encompass this possibility.

SuggestedRemedy

Suggest revising this line to read ""This SFR is used to define the default values for the access to one or more TOE functions a user gets assigned..."

Proposed Response Response Status **O**

Cl **PP-C** SC **10.6** P **23** L **21** # **113**
 Sukert, Alan Xerox

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

There appears to be an inconsistency between the change made to the PP APP Note on line 21 of this page and to the FMT_MTD.1.1(b) SFR on line 29 of this page. The PP App Note states that FMT_MTD.1.1 iteration (b) applies to 'TSF Data that is associated with a Normal User' while FMT_MTD.1.1(b) states that it applies to 'TSF Data associated with documents...owned by a U.NORMAL' (i.e., a Normal User).

SuggestedRemedy

Resolve in subclause 10.6 the inconsistency between the the PP APP Note on line 21 and the FMT_MTD.1.1(b) SFR on line 29 of page 23.

Proposed Response Response Status **O**

Cl **PP-C** SC **10.6** P **23** L **22** # **116**
 Sukert, Alan Xerox

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

Since the use of the term 'Nobody' has been standardized in the document now, I was wondering why on line 22 the term 'no one' instead of nobody is used.

SuggestedRemedy

Suggest changing subclause 10.6 - page 23, line 22 to use nobody instead of 'no one'.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC 10.6 P 24 L 22 # 87
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**
 Three grammatical errors on line 22 - now says that ""...a ST author has check if all those security attributes..."" (note the PP now appears to consistently use 'ST Author')

SuggestedRemedy
 Revise subclause 10.6, page 24, line 22 to read ""...an ST Author has to check if all those security attributes..."".

Proposed Response Response Status **O**

Cl **PP-A** SC 10.6 P 25 L 22 # 62
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**
 Three grammatical errors on line 22 - now says that ""...a ST author has check if all those security attributes..."" (note the PP now appears to consistently use 'ST Author')

SuggestedRemedy
 Revise subclause 10.6, page 25, line 22 to read ""...an ST Author has to check if all those security attributes..."".

Proposed Response Response Status **O**

Cl **PP-B** SC 10.6 P 25 L 26 # 88
 Sukert, Alan Xerox

Comment Type **T** Comment Status **X**
 The PP App Note on this line states ""This SFR is used to define the default values for the access to TOE function a user gets assigned..."". Since a user could be assigned access to more than one TOE function depending on which TOE functions applied to the TOE and which ones the user might be given access to, this statement needs to encompass this possibility.

SuggestedRemedy
 Suggest revising this line to read ""This SFR is used to define the default values for the access to one or more TOE functions a user gets assigned...""

Proposed Response Response Status **O**

Cl **PP-B** SC 10.6 P 26 L 2 # 89
 Sukert, Alan Xerox

Comment Type **T** Comment Status **X**
 Since the use of the term 'Nobody' has been standardized in the document now, I was wondering why on line 2 the term 'no one' instead of nobody is used.

Same comment applies to page 26, line 4.

SuggestedRemedy
 Suggest changing subclause 10.6 - page 26, lines 2 and 4 to use nobody instead of 'no one'.

Proposed Response Response Status **O**

Cl **PP-B** SC 10.6 P 26 L 11 # 90
 Sukert, Alan Xerox

Comment Type **T** Comment Status **X**
 There appears to be an inconsistency between the change made to the PP APP Note on line 1 of this page and to the FMT_MTD.1.1(b) SFR on line 11 of this page. The PP App Note states that FMT_MTD.1.1 iteration (b) applies to 'TSF Data that is associated with a Normal User' while FMT_MTD.1.1(b) states that it applies to 'TSF Data associated with documents...owned by a U.NORMAL' (i.e., a Normal User).

SuggestedRemedy
 Resolve in subclause 10.6 the inconsistency between the the PP APP Note on line 1 and the FMT_MTD.1.1(b) SFR on line 11 of page 26.

Proposed Response Response Status **O**

Cl **PP-A** SC 10.6 P 26 L 26 # 63
 Sukert, Alan Xerox

Comment Type **T** Comment Status **X**
 The PP App Note on this line states ""This SFR is used to define the default values for the access to TOE function a user gets assigned..."". Since a user could be assigned access to more than one TOE function depending on which TOE functions applied to the TOE and which ones the user might be given access to, this statement needs to encompass this possibility.

SuggestedRemedy
 Suggest revising this line to read ""This SFR is used to define the default values for the access to one or more TOE functions a user gets assigned...""

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **10.6** P **27** L **2** # **64**
 Sukert, Alan Xerox

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

Since the use of the term 'Nobody' has been standardized in the document now, I was wondering why on line 2 the term 'no one' instead of nobody is used.

Same comment applies to page 27, line 4.

SuggestedRemedy

Suggest changing subclause 10.6 - page 27, lines 2 and 4 to use nobody instead of 'no one'.

Proposed Response Response Status **O**

Cl **PP-A** SC **10.6** P **27** L **11** # **65**
 Sukert, Alan Xerox

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

There appears to be an inconsistency between the change made to the PP APP Note on line 1 of this page and to the FMT_MTD.1.1(b) SFR on line 11 of this page. The PP App Note states that FMT_MTD.1.1 iteration (b) applies to 'TSF Data that is associated with a Normal User' while FMT_MTD.1.1(b) states that it applies to 'TSF Data associated with documents...owned by a U.NORMAL' (i.e., a Normal User).

SuggestedRemedy

Resolve in subclause 10.6 the inconsistency between the the PP APP Note on line 1 and the FMT_MTD.1.1(b) SFR on line 11 of page 27.

Proposed Response Response Status **O**

Cl **PP-A** SC **10.6** P **28** L **3** # **48**
 Smithson, Brian Ricoh

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

FMT_SMR.1 should be a supporting SFR for O.USER.AUTHORIZED (O.ADMIN.AUTHORIZED in PP-D). This had not been needed in the previous drafts because user authorization for TOE usage was distributed among the packages, but now it is in the common PP.

SuggestedRemedy

Add that to the FMT_SMR.1 app note, and also to the rationale tables in 10.12.

Same for PP-B, PP-C, PP-D.

Proposed Response Response Status **O**

Cl **PP-A** SC **10.12** P **29** L **15** # **9**
 Farrell, Lee Canon

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

If O.DOC.NO_DIS and O.DOC.NO_ALT are replaced with new proposed objectives (see clause 8.1 comment), then table 18 needs modification.

SuggestedRemedy

Map FDP_ACC.1(a) to δPö for O.DOC.ACCESS.
 Map FDP_ACF.1(a), FIA_UID.1, FMT_MSA.1(a), and FMT_MSA.3(a) to δSö for O.DOC.ACCESS.

Map FDP_RIP.1 to δPö for O.DOC.RESIDUAL.

Proposed Response Response Status **O**

Cl **PP-A** SC **10.12** P **30** L **1** # **10**
 Farrell, Lee Canon

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

If O.DOC.NO_DIS and O.DOC.NO_ALT are replaced with new proposed objectives (see clause 8.1 comment), then table 19 needs modification.

SuggestedRemedy

Replace δO.DOC.NO_DIS, O.DOC.NO_ALTö with δO.DOC.ACCESSö in first row.

Replace ""O.DOC.NO_DIS"" with ""O.DOC.RESIDUAL"" in second row.

Proposed Response Response Status **O**

Cl **PP-C** SC **12.1** P **30** L **6** # **114**
 Sukert, Alan Xerox

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

The revised purpose for the SMI SFR package in subclause 12.1 appears to be inconsistent with subclause 11.3. In subclause 11.3 the definition of the F.SMI function in Table 19 is that it is a function that ""transmits and receives User Data and TSF Data"" over a shared-medium interface; subclause 12.1 indicates that the SMI SFR package applies to protection of ""data"" that is ""transmitted"" over a shared-medium interface.

SuggestedRemedy

Resolve the inconsistencies between subclauses 11.3 and 12.1 as to what data is being protected and whether the protection covers just transmission or both transmission and receipt of the data.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC 11.1 P 31 L 17 # 91
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

There is an ""Error! Reference source not found' error message for the clause reference on this line. I noted that in PP-A the clause reference on the corresponding line was clause 10.4

SuggestedRemedy

Correct the clause reference on subclause 11.1, page 31, line 17.

Proposed Response Response Status **O**

Cl **PP-C** SC 12.4 P 32 L 1 # 115
 Sukert, Alan Xerox

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

The changes made to the PP App Note in PP-A, subclause 18.4, page 55, line 1 were not made in the corresponding PP App Note in PP-c, subclause 12.4, page 32, line 1.

SuggestedRemedy

Make sure the changes made to the PP App Note in PP-A, subclause 18.4, page 55, line 1 are made in the corresponding PP App Note in PP-C, subclause 12.4, page 32, line 1

Proposed Response Response Status **O**

Cl **PP-B** SC 12.2 P 34 L 14 # 92
 Sukert, Alan Xerox

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

The PP App Note on lines 14, 15 & 17 talks about the user needing to authenticate using 'operator controls'. This term isn't defined anywhere in PP-A so it is not clear what this is really referring to - is this controls located physically on the machine itself or does it apply to controls . I did note that the IEEE 2600 Standard in discussing the generic TOE architecture does refer in subclause 3.2.3.2 to an ""Operator Interface"" which is what I think is meant in this case. Since the IEEE 2600 Standard is a normative reference in PP-B the use of terms from the IEEE 2600 Standard in PP-B should be allowed without having to define them in the PP standard.

SuggestedRemedy

Change subclause 12.2, page 34 line 14 to read ""A User will need to authenticate using the Operator Interface on the TOE to perform ""Read"" operations. If the User authenticated using an Operator Interface when submitting a print job...then the User will need to authenticate using an Operator Interface in order to establish...""

Proposed Response Response Status **O**

Cl **PP-A** SC 12.2 P 35 L 14 # 66
 Sukert, Alan Xerox

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

The PP App Note on lines 14, 15 & 17 talks about the user needing to authenticate using 'operator controls'. This term isn't defined anywhere in PP-A so it is not clear what this is really referring to - is this controls located physically on the machine itself or does it apply to controls . I did note that the IEEE 2600 Standard in discussing the generic TOE architecture does refer in subclause 3.2.3.2 to an ""Operator Interface"" which is what I think is meant in this case. Since the IEEE 2600 Standard is a normative reference in PP-A the use of terms from the IEEE 2600 Standard in PP-A should be allowed without having to define them in the PP standard.

SuggestedRemedy

Change subclause 12.2, page 35 line 14 to read ""A User will need to authenticate using the Operator Interface on the TOE to perform ""Read"" operations. If the User authenticated using an Operator Interface when submitting a print job...then the User will need to authenticate using an Operator Interface in order to establish...""

Proposed Response Response Status **O**

Cl **PP-A** SC 12.2 P 35 L 28 # 11
 Farrell, Lee Canon

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

If O.DOC.NO_DIS and O.DOC.NO_ALT are replaced with new proposed objectives (see clause 8.1 comment), then this application note needs modification.

SuggestedRemedy

Replace ôO.DOC.NO_DISô with ôO.DOC.ACCESSô.

Proposed Response Response Status **O**

Cl **PP-A** SC 12.2 P 36 L 29 # 1
 Farrell, Lee Canon

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

If O.DOC.NO_DIS and O.DOC.NO_ALT are replaced with new proposed objectives (see clause 8.1 comment), then table 23 needs modification.

SuggestedRemedy

Replace ôO.DOC.NO_DISô with ôO.DOC.ACCESSô.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **12.2** P **37** L **1** # **12**
 Farrell, Lee Canon

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

If O.DOC.NO_DIS and O.DOC.NO_ALT are replaced with new proposed objectives (see clause 8.1 comment), then tables 24, 26, 27, 29, 30, 32, 33, 35, 36 need modification.

SuggestedRemedy

Replace δO.DOC.NO_DISö with δO.DOC.ACCESSö.

Proposed Response Response Status **O**

Cl **PP-B** SC **13.2** P **38** L **11** # **33**
 Chen, Nancy Oki Data

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

(1) It's not clear that whether all other operations not listed in the SCN Access Control SFP is ""allowed"" or ""denied"" and for what roles.

If the assumption for ""not listed"" operations"" are ""denied for all users"", then the App. Note on line 15-16 that states ""If a conforming TOE provides a feature for modifying a scanned document before transmission, then the ST Author should add additional rules for D.DOC (+SCN) using the Modify operation."" must be deleted, because there is no stricter rule than ""denied for all"" can be added.

(2) Shouldn't U.ADMINSTRATOR be allowed to read his own and others' D.DOC(+SCN)?

Note: these comments apply to SCN, FAX, and DSR packages.

SuggestedRemedy

See previous proposal for Common Access Control SFP.

Proposed Response Response Status **O**

Cl **PP-A** SC **13.2** P **38** L **11** # **28**
 Chen, Nancy Oki Data

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

(1) It's not clear that whether all other operations not listed in the SCN Access Control SFP is ""allowed"" or ""denied"" and for what roles.

If the assumption for ""not listed"" operations"" are ""denied for all users"", then the App. Note on line 15-16 that states ""If a conforming TOE provides a feature for modifying a scanned document before transmission, then the ST Author should add additional rules for D.DOC (+SCN) using the Modify operation."" must be deleted, because there is no stricter rule than ""denied for all"" can be added.

(2) Shouldn't U.ADMINSTRATOR be allowed to read his own and others' D.DOC(+SCN)?

Note: these comments apply to SCN, FAX, and DSR packages.

SuggestedRemedy

See previous proposal for Common Access Control SFP.

Proposed Response Response Status **O**

Cl **PP-A** SC **13.2** P **38** L **24** # **13**
 Farrell, Lee Canon

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

If O.DOC.NO_DIS and O.DOC.NO_ALT are replaced with new proposed objectives (see clause 8.1 comment), then this app note needs modification.

SuggestedRemedy

Replace δO.DOC.NO_DISö with δO.DOC.ACCESSö.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC 14.2 P 40 L 12 # 93
 Sukert, Alan Xerox

Comment Type T Comment Status X

There appears to be an inconsistency between subclause 14.1 and subclause 14.2. Specifically, subclause 14.1 now states that the CPY SFR Package can be used to specify additional rules for modifying documents before printing while subclause 14.2, line 12 in the updated PP App Note states talks about previewing documents on a display device which isn't mentioned or even hinted at in subclause 14.2.

A couple of additional points:

1. Subclause 14.1 on line 7 talks about printing a copy job. This contradicts what is in line 6 and, more importantly, what is in subclause 11.3 where F.CPY is defined as the function that takes physical documents input and duplicates it to a physical document output; there is no mention of printing in the definition of F.CPY.
2. If F.CPY only deals with taking physical documents input and duplicating it to a physical document output as stated in subclause 11.3, the new sentence added in subclause 14.2, line 12 doesn't make sense because there is no document in electronic form to be viewed by any type of display device.

SuggestedRemedy

Clarify and correct as necessary the purpose of the CPY SFR Package and associated operations in subclauses 14.1 and 14.2.

Proposed Response Response Status O

Cl **PP-A** SC 14.2 P 41 L 12 # 67
 Sukert, Alan Xerox

Comment Type T Comment Status X

There appears to be an inconsistency between subclause 14.1 and subclause 14.2. Specifically, subclause 14.1 now states that the CPY SFR Package can be used to specify additional rules for modifying documents before printing while subclause 14.2, line 12 in the updated PP App Note states talks about previewing documents on a display device which isn't mentioned or even hinted at in subclause 14.2.

A couple of additional points:

1. Subclause 14.1 on line 7 talks about printing a copy job. This contradicts what is in line 6 and, more importantly, what is in subclause 11.3 where F.CPY is defined as the function that takes physical documents input and duplicates it to a physical document output; there is no mention of printing in the definition of F.CPY.
2. If F.CPY only deals with taking physical documents input and duplicating it to a physical document output as stated in subclause 11.3, the new sentence added in subclause 14.2, line 12 doesn't make sense because there is no document in electronic form to be viewed by any type of display device.

SuggestedRemedy

Clarify and correct as necessary the purpose of the CPY SFR Package and associated operations in subclauses 14.1 and 14.2.

Proposed Response Response Status O

Cl **PP-A** SC 14.2 P 41 L 27 # 2
 Farrell, Lee Canon

Comment Type T Comment Status X

If O.DOC.NO_DIS and O.DOC.NO_ALT are replaced with new proposed objectives (see clause 8.1 comment), then this application note needs modification.

SuggestedRemedy

Replace ðO.DOC.NO_DISð with ðO.DOC.ACCESSð.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC 15.2 P 43 L 12 # 96
 Sukert, Alan Xerox

Comment Type T Comment Status X

In subclause 16.1 in discussing the DSR package it states that this package may be used for specifying roles, mechanisms or rules for authorizing a user or users to access documents that have been stored by another user. Then in the DSR Access Control Table in Table 34 it states that access is denied to everyone except for the Normal Users own documents and if authorized by another role or mechanism if the TOE provides such a function.

I contrast this with the FAX SFR Package. The FAX SFR Package description in subclause 15.1 makes a similar statement as the DSR SFR package does that the FAX SFR package may be used for specifying roles, mechanisms or rules for authorizing a user or users to transfer ownership of a received document to one or more intended recipients. However, in the FAX Access Control SFP for +FAXIN there is no corresponding access provided to a User if receipt is authorized by another role or mechanism if the TOE provides such a function.

It would seem the DSR SFR Package and FAX SFR Packages are similar in this respect, so it is not clear why the corresponding Access Control Lists are so different.

SuggestedRemedy

Clarify whether in the FAX Access Control SFP in Table 31 an access control rule should be added for +FAXIN worded something like "(2) if authorized to accept receipt by another role or mechanism if such functions are provided by a conforming TOE."

Proposed Response Response Status O

Cl **PP-B** SC 15.2 P 43 L 27 # 94
 Sukert, Alan Xerox

Comment Type T Comment Status X

Given the changes in Table 31 made in this PP-B draft, does the reference to D.DOC(+FAX) in line 27 refer to +FAXIN, +FAXOUT or both.

SuggestedRemedy

Clarify what attributes from Table 31 are included in the D.DOC(+FAX) reference on page 44, line 27.

Proposed Response Response Status O

Cl **PP-B** SC 15.2 P 44 L 12 # 35
 Chen, Nancy Oki Data

Comment Type T Comment Status X

- (1) It's not clear that whether other roles other than U.NORMAL is "allowed" or "denied" the access control for D.DOC(+FAXOUT).
- (2) Shouldn't the U.ADMINISTRATOR be allowed to transmit D.DOC (of his own and others') to a FAXOUT interface?

SuggestedRemedy

Add an App.Note to clarify.

Proposed Response Response Status O

Cl **PP-A** SC 15.2 P 44 L 12 # 29
 Chen, Nancy Oki Data

Comment Type T Comment Status X

- (1) The FAX Access Control SFP for D.DOC(+FAXIN) first denies "read" for all users other than the "owner" who is the U.Administrator" here, then allows ST to add a "less strict" access rule such as "+FAXIN Read U.NORMAL æAllowed if this User is authorized by U.ADMINISTRATOR/Æö, violates "Demonstrable Conformance" rule in CC. An ST may only add a stricter SFP to a TOE in order to claim "demonstrable conformance" to the PP.

SuggestedRemedy

- (1) Combine the access control rule for D.DOC(+FAXIN) read operation in Table 31, the App. Note in line (17-19), and the App. Note in line (20-25) to define the access control rule as follows:
 "D.DOC +FAXIN Read U.USER 'Denied, except for the owner (= U.ADMINISTRATOR) and those whom have been authorized by the owner for their own documents".
- (2) Add an App. Note for ST author that states that if a TOE does not allow U.ADMINISTRATOR to transfer ownership to one or more intended FAX recipients, then the ST author should change to rule to 'Denied, except for the owner (=U.ADMINISTRATOR)'. Since the rule is changed to stricter than what the PP requires, the TOE can still claim "demonstrable conformance" to the PP.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC 15.2 P 44 L 12 # 30
 Chen, Nancy Oki Data

Comment Type T Comment Status X

(1) It's not clear that whether other roles other than U.NORMAL is ""allowed"" or ""denied"" the access control for D.DOC(+FAXOUT).
 (2) Shouldn't the U.ADMINSTRATOR be allowed to transmit D.DOC (of his own and others') to a FAXOUT interface?

SuggestedRemedy

Add an App.Note to clarify.

Proposed Response Response Status O

Cl **PP-A** SC 15.2 P 44 L 12 # 73
 Sukert, Alan Xerox

Comment Type T Comment Status X

In subclause 16.1 in discussing the DSR package it states that this package may be used for specifying roles, mechanisms or rules for authorizing a user or users to access documents that have been stored by another user. Then in the DSR Access Control Table in Table 34 it states that access is denied to everyone except for the Normal Users own documents and if authorized by another role or mechanism if the TOE provides such a function.

I contrast this with the FAX SFR Package. The FAX SFR Package description in subclause 15.1 makes a similar statement as the DSR SFR package does that the FAX SFR package may be used for specifying roles, mechanisms or rules for authorizing a user or users to transfer ownership of a received document to one or more intended recipients. However, in the FAX Access Control SFP for +FAXIN there is no corresponding access provided to a User if receipt is authorized by another role or mechanism if the TOE provides such a function.

It would seem the DSR SFR Package and FAX SFR Packages are similar in this respect, so it is not clear why the corresponding Access Control Lists are so different.

SuggestedRemedy

Clarify whether in the FAX Access Control SFP in Table 31 an access control rule should be added for +FAXIN worded something like ""(2) if authorized to accept receipt by another role or mechanism if such functions are provided by a conforming TOE.""

Proposed Response Response Status O

Cl **PP-B** SC 15.2 P 44 L 12 # 34
 Chen, Nancy Oki Data

Comment Type T Comment Status X

(1) The FAX Access Control SFP for D.DOC(+FAXIN) first denies ""read"" for all users other than the ""owner"" who is the U.Administrator"" here, then allows ST to add a ""less strict"" access rule such as ""ô+FAXIN Read U.NORMAL æAllowed if this User is authorized by U.ADMINISTRATORÆö, violates ""Demonstrable Conformance"" rule in CC. An ST may only add a stricter SFP to a TOE in order to claim ""demonstrable conformance"" to the PP.

SuggestedRemedy

(1) Combine the access control rule for D.DOC(+FAXIN) read operation in Table 31, the App. Note in line (17-19), and the App. Note in line (20-25) to define the access control rule as follows:

""D.DOC +FAXIN Read U.USER 'Denied, except for the owner (= U.ADMINISTRATOR) and those whom have been authorized by the owner for their own documents"".

(2) Add an App. Note for ST author that states that if a TOE does not allow U.ADMINISTRATOR to transfer ownership to one or more intended FAX recipients, then the ST author should change to rule to 'Denied, except for the owner (=U.ADMINISTRATOR)'. Since the rule is changed to stricter than what the PP requires, the TOE can still claim ""demonstrable conformance"" to the PP.

Proposed Response Response Status O

Cl **PP-A** SC 15.2 P 44 L 27 # 68
 Sukert, Alan Xerox

Comment Type T Comment Status X

Given the changes in Table 31 made in this PP-A draft, does the reference to D.DOC(+FAX) in line 27 refer to +FAXIN, +FAXOUT or both.

SuggestedRemedy

Clarify what attributes from Table 31 are included in the D.DOC(+FAX) reference on page 44, line 27.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **15.2** P **45** L **1** # **14**
 Farrell, Lee Canon
 Comment Type **T** Comment Status **X**
 If O.DOC.NO_DIS and O.DOC.NO_ALT are replaced with new proposed objectives (see clause 8.1 comment), then this application note needs modification.
 SuggestedRemedy
 Replace δO.DOC.NO_DISö with δO.DOC.ACCESSö.
 Proposed Response Response Status **O**

Cl **PP-B** SC **16.2** P **46** L **11** # **95**
 Sukert, Alan Xerox
 Comment Type **T** Comment Status **X**
 In Table 34, the access control rule says to 'see Application Note below'. Since there are four PP APP Notes immediately following Table 34 on page 47, it is not clear which one (or more) of the four APP Notes is being referred to here.
 SuggestedRemedy
 Clarify which of the four PP APP Notes immediately following Table 34 on page 46 the note in Table 34 applies to.
 Proposed Response Response Status **O**

Cl **PP-A** SC **16.2** P **47** L **11** # **69**
 Sukert, Alan Xerox
 Comment Type **T** Comment Status **X**
 In Table 34, the access control rule says to 'see Application Note below'. Since there are four PP APP Notes immediately following Table 34 on page 47, it is not clear which one (or more) of the four APP Notes is being referred to here.
 SuggestedRemedy
 Clarify which of the four PP APP Notes immediately following Table 34 on page 47 the note in Table 34 applies to.
 Proposed Response Response Status **O**

Cl **PP-A** SC **16.2** P **47** L **11** # **31**
 Chen, Nancy Oki Data
 Comment Type **T** Comment Status **X**
 (1) It's not clear that whether other roles other than U.NORMAL is ""allowed"" or ""denied"" the access control for D.DOC(+DSR).
 (2) Shouldn't the U.ADMINSTRATOR be allowed to transmit D.DOC (of his own and others') to a FAXOUT interface?
 SuggestedRemedy
 Add an App.Note to clarify.
 Proposed Response Response Status **O**

Cl **PP-B** SC **16.2** P **47** L **11** # **36**
 Chen, Nancy Oki Data
 Comment Type **T** Comment Status **X**
 (1) It's not clear that whether other roles other than U.NORMAL is ""allowed"" or ""denied"" the access control for D.DOC(+DSR).
 (2) Shouldn't the U.ADMINSTRATOR be allowed to transmit D.DOC (of his own and others') to a FAXOUT interface?
 SuggestedRemedy
 Add an App.Note to clarify.
 Proposed Response Response Status **O**

Cl **PP-A** SC **16.2** P **47** L **29** # **15**
 Farrell, Lee Canon
 Comment Type **T** Comment Status **X**
 If O.DOC.NO_DIS and O.DOC.NO_ALT are replaced with new proposed objectives (see clause 8.1 comment), then this application note needs modification.
 SuggestedRemedy
 Replace δO.DOC.NO_DISö with δO.DOC.ACCESSö.
 Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC 17.1 P 49 L 6 # 97
 Sukert, Alan Xerox

Comment Type **T** Comment Status **X**
 Subclause 17.1, page 49, line 17 as well as the definition of F.NVS in subclause 11.3, page 33, Table 20 clarifies that the F.NVS function applies to User Data and TSF Data. This distinction, however, isn't made in subclause 17.1, line 6 where it only refers to protection of data that is stored in removable NVS.

SuggestedRemedy
 Change subclause 17.1, page 49, line 6 to read ""the package provides protection of User Data and TSF Data that is stored..."".

Proposed Response Response Status **O**

Cl **PP-A** SC 17.2 P 50 L # 45
 Nevo, Ron Sharp

Comment Type **T** Comment Status **X**
 #43 for the previous meeting:
 Though it was δProposed accepted,δ it is not reflected in the PP.
 (Description regarding appropriateness of FTP_CIP_EXP.1 and FMT_FDI_EXP.1)
 1)□There is no description corresponding to APE_ECD.1-3.
 (Regarding APE_ECD.1-6 and APE_ECD.1-7, they depend on evaluation of APE_ECD.1-3)
 2)□There are no descriptions corresponding to APE_ECD.1-12 and APE_ECD.1-13.
 If nothing is done, ST Author has to explain the validity of expanded components. If you use expanded components, you have to get evaluation including their validity.

SuggestedRemedy

Proposed Response Response Status **O**

Cl **PP-A** SC 17.1 P 50 L 6 # 70
 Sukert, Alan Xerox

Comment Type **T** Comment Status **X**
 Subclause 17.1, page 50, line 17 as well as the definition of F.NVS in subclause 11.3, page 34, Table 20 clarifies that the F.NVS function applies to User Data and TSF Data. This distinction, however, isn't made in subclause 17.1, line 6 where it only refers to protection of data that is stored in removable NVS.

SuggestedRemedy
 Change subclause 17.1, page 50, line 6 to read ""the package provides protection of User Data and TSF Data that is stored..."".

Proposed Response Response Status **O**

Cl **PP-B** SC 17.3 P 50 L 9 # 98
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**
 Note that in subclause 17.3, page 50, line 9 in the definition of the FTP_CIP_EXP.1.1 SFR, the text refers to 'user and TSF data'. I am not familiar with the conventions used in documenting SFRs, but it appears here the text is being inconsistent on capitalization since both User Data and TSF Data are clearly defined proper terms in the document so I would suspect that the text should read ""...integrity of User and TSF Data when either are..."".

Same comment applies to line 18.

SuggestedRemedy
 Change subclause 17.3, page 50, lines 9 and 18 to read ""...integrity of User and TSF Data when either are...""

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC 17.1 P 50 L 10 # 24
 Farrell, Lee Canon

Comment Type T Comment Status X

Introduction of removable NVS device should be enhanced to support clarification of threats.

SuggestedRemedy

Change phrase "is designed to be removed from the TOE" to "is designed to be removed from and re-inserted into the TOE"

And add a second sentence to paragraph on line 14 to result in the following:
 "Removing and transporting such a device outside the operational environment of the TOE would potentially allow an attacker to get hold of the device and analyze its content off-line. Also, inserting the device from outside the operational environment of the TOE would potentially allow an attacker to mount malicious content and result in further disclosure of original content."

Proposed Response Response Status O

Cl **PP-A** SC 17.2 P 50 L 21 # 42
 Nevo, Ron Sharp

Comment Type T Comment Status X

Related to comment No.54,
 if you describe that ST Author shall define what is "designed to be removable," Also necessity of integrity of "data" should be defined by the ST Author.
 It is no doubt that confidentiality of asset shall be ensured since it is "removable."
 1) Failure
 There exist some devices that their MTTF (Mean Time To Failure) are sufficiently long. For example, most SSDs (Solid State Drives) have a million hour MMTF. That is, if removable devices are chosen, integrity infringement by failure can be mitigated.
 2) Integrity infringement by attack
 Since confidentiality is ensured, integrity cannot be infringed unless attacker infringes confidentiality first. That means integrity infringement by attack is practically impossible. For example, there is a mail address NevoR@sharpsec.com as one of D.FUNC. The mail address is encrypted to ensure confidentiality and stored into a removable device. If you want to falsify it to don@lexmark.com, at first you have to decrypt it properly. It is impossible.
 There is another way. You can write some strings into all part of the removable device. However, it is no longer falsification but destruction. Destruction means infringement of availability rather than integrity, since HCD may not work normally.
 From them, to infringe integrity you have to infringe confidentiality first, but it is practically impossible. That is, ensuring confidentiality can mitigate integrity infringement by falsification.

SuggestedRemedy

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC 17.2 P 50 L 25 # 46
 Nevo, Ron Sharp

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

In FTP_CIP_EXP.1.1, FTP_CIP_EXP.1.2 and FTP_CIP_EXP.1.3, confidentiality and integrity are required regarding user and TSF data. That is, you have to store both user data and TSF data into NVS. This defines a basic function of HCD. You described that ST Author shall define what is designed to be removable. There can be a case that user data is stored in removable but TSF data is stored in non-removable.

SuggestedRemedy

Treat user and TSF data simply as data.

Proposed Response Response Status **O**

Cl **PP-A** SC 17.2 P 50 L 25 # 16
 Farrell, Lee Canon

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

The method for requiring integrity relative to the removable NVS device is too restrictive, and limits possible alternatives in achieving the desired goal.

SuggestedRemedy

Change the phrase
 ""The TSF shall provide a function that ensures the confidentiality and integrity of user and TSF data..."" to:
 ""The TSF shall provide a function that ensures the confidentiality and a capability to [selection: detect, diminish, prevent] off-line alteration of user and TSF data...""

Also delete FTP_CIP_EXP.1.2 and and FTP_CIP_EXP.1.3 (in lines 28 and 31).

Proposed Response Response Status **O**

Cl **PP-A** SC 17.1 P 50 L 28 # 47
 Smithson, Brian Ricoh

Comment Type **E** Comment Status **X**

The statement ""obtain the original unencrypted data and validate the integrity"" implies an implementation requirement for encryption. The same intention should be expressed without referring to encryption.

SuggestedRemedy

Change:
 The TSF shall provide functions that obtain the original unencrypted data and validate the integrity of user and TSF data when reading data back that had previously been stored using the confidentiality and integrity protection function.

To:
 The TSF shall provide a function that validates the integrity of user and TSF data when reading data back that had previously been stored using the confidentiality and integrity protection function.

This also applies to PP-B.

Proposed Response Response Status **O**

Cl **PP-A** SC 17.3 P 51 L 8 # 17
 Farrell, Lee Canon

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

The method for requiring integrity relative to the removable NVS device is too restrictive, and limits possible alternatives in achieving the desired goal.

SuggestedRemedy

Change the phrase
 ""The TSF shall provide a function that ensures the confidentiality and integrity of user and TSF data..."" to:
 ""The TSF shall provide a function that ensures the confidentiality and a capability to [selection: detect, diminish, prevent] off-line alteration of user and TSF data...""

Also delete FTP_CIP_EXP.1.2 and and FTP_CIP_EXP.1.3 (in lines 28 and 31).

Also replace the Application Note on line 19 with:
 δPP APPLICATION NOTEù The ST Author should define a list of actions to be taken if ædetectÆ is selected.δ

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl PP-A SC 17.3 P 51 L 9 # 71
Sukert, Alan Xerox

Comment Type E Comment Status X

Note that in subclause 17.3, page 51, line 9 in the definition of the FTP_CIP_EXP.1.1 SFR, the text refers to 'user and TSF data'. I am not familiar with the conventions used in documenting SFRs, but it appears here the text is being inconsistent on capitalization since both User Data and TSF Data are clearly defined proper terms in the document so I would suspect that the text should read "...integrity of User and TSF Data when either are..."

Same comment applies to line 18.

SuggestedRemedy

Change subclause 17.3, page 51, lines 9 and 18 to read "...integrity of User and TSF Data when either are..."

Proposed Response Response Status O

Cl PP-A SC 17.3 P 51 L 22 # 18
Farrell, Lee Canon

Comment Type T Comment Status X

If O.DOC.NO_DIS and O.DOC.NO_ALT are replaced with new proposed objectives (see clause 8.1 comment), then this application note needs modification.

SuggestedRemedy

Replace δO.DOC.NO_DISö with δO.DOC.CONFIDENTö and replace δO.DOC.NO_ALTö with δO.DOC.MOUNTö.

Proposed Response Response Status O

Cl PP-A SC 17.4 P 51 L 28 # 19
Farrell, Lee Canon

Comment Type T Comment Status X

If O.DOC.NO_DIS and O.DOC.NO_ALT are replaced with new proposed objectives (see clause 8.1 comment), then tables 37 and 38 need modification.

SuggestedRemedy

Replace δO.DOC.NO_DISö with δO.DOC.CONFIDENTö and replace δO.DOC.NO_ALTö with δO.DOC.MOUNTö.

Proposed Response Response Status O

Cl PP-B SC 18.1 P 52 L 6 # 99
Sukert, Alan Xerox

Comment Type T Comment Status X

The revised purpose for the SMI SFR package in subclause 18.1 appears to be inconsistent with subclause 11.3. In subclause 11.3 the definition of the F.SMI function in Table 20 is that it is a function that ""transmits and receives"" both User Data or TSF Data over a shared-medium interface; subclause 18.1 indicates that the SMI SFR package applies to protection of ""data"" that is ""tarnsmitted"" over a shared-medium interface.

SuggestedRemedy

Resolve the inconsistencies between subclauses 11.3 and 18.1 as to what data the SMI function/package applies to and whether the protection covers just transmission or both transmission and receipt of the data.

Proposed Response Response Status O

Cl PP-A SC 18.1 P 53 L 6 # 72
Sukert, Alan Xerox

Comment Type T Comment Status X

The revised purpose for the SMI SFR package in subclause 18.1 appears to be inconsistent with subclause 11.3. In subclause 11.3 the definition of the F.SMI function in Table 20 is that it is a function that ""transmits and receives"" both User Data or TSF Data over a shared-medium interface; subclause 18.1 indicates that the SMI SFR package applies to protection of ""data"" that is ""tarnsmitted"" over a shared-medium interface.

SuggestedRemedy

Resolve the inconsistencies between subclauses 11.3 and 18.1 as to what data the SMI function/package applies to and whether the protection covers just transmission or both transmission and receipt of the data.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **18.2** P **53** L **12** # **22**
 Farrell, Lee Canon

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

The definition of FMT_FDI_EXP.1.1 is too restrictive. It should be expanded to cover control/restriction of data being forwarded both with *and* without further processing. As currently worded, it does not include forwarding *with* further processing.

SuggestedRemedy

Change definition of FMT_FDI_EXP.1.1 to:
 FMT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on any Interface from being from being forwarded [selection: with, without] further processing by the TSF to any Shared-medium Interface.
 [This change should also apply on page 54, lines 27 and 30.]

Also remove the word direct in the definition of FMT_FDI_EXP.1.2 in clauses 18.2 and 18.4 to: The TSF shall restrict the ability to permit such forwarding.

Proposed Response Response Status **O**

Cl **PP-B** SC **18.4** P **54** L **1** # **100**
 Sukert, Alan Xerox

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

The changes made to the PP App Note in PP-A, subclause 18.4, page 55, line 1 were not made in the corresponding PP App Note in PP-B, subclause 18.4, page 54, line 1.

SuggestedRemedy

Make sure the changes made to the PP App Note in PP-A, subclause 18.4, page 55, line 1 are made in the corresponding PP App Note in PP-B, subclause 18.4, page 54, line 1

Proposed Response Response Status **O**

Cl **PP-A** SC **18.5** P **55** L **23** # **20**
 Farrell, Lee Canon

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

If O.DOC.NO_DIS and O.DOC.NO_ALT are replaced with new proposed objectives (see clause 8.1 comment), then this application note needs modification.

SuggestedRemedy

Replace O.DOC.NO_DIS, O.DOC.NO_ALT with O.DOC.ACCESS.

Proposed Response Response Status **O**

Cl **PP-A** SC **18.6** P **56** L **1** # **21**
 Farrell, Lee Canon

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

If O.DOC.NO_DIS and O.DOC.NO_ALT are replaced with new proposed objectives (see clause 8.1 comment), then tables 40 and 41 need modification.

SuggestedRemedy

Replace O.DOC.NO_DIS with O.DOC.ACCESS and delete column for O.DOC.NO_ALT in table 40.
 Also replace O.DOC.NO_DIS, O.DOC.NO_ALT with O.DOC.ACCESS in table 41.

Proposed Response Response Status **O**

Cl **PP-D** SC **12.1** P **220** L **6** # **124**
 Sukert, Alan Xerox

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

The revised purpose for the SMI SFR package in subclause 12.1 appears to be inconsistent with subclause 11.3. In subclause 11.3 the definition of the F.SMI function in Table 15 is that it is a function that "transmits or receives User Data and TSF Data" over a shared-medium interface; subclause 12.1 indicates that the SMI SFR package applies to protection of "data" that is "transmitted" over a shared-medium interface.

SuggestedRemedy

Resolve the inconsistencies between subclauses 11.3 and 12.1 as to what data is being protected and whether the protection covers just transmission or both transmission and receipt of the data.

Proposed Response Response Status **O**

Cl **PP-C** SC **14** P **8.4** L **6** # **40**
 Chen, Nancy Oki Data

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

In environment C, only Administrators are identified, authenticated, and authorized. Currently Table 12 - Non-IT objectives for the operational environment : OE.USER.AUTHORIZED states that all users to be authorized.

SuggestedRemedy

If not proposing to change the previously agree security objectives for environment C, then -

Change the "user" to "Administrator" in the objective.
 Make corresponding change to Table 13 on page 14.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-C** SC **14** P **8.5** L **10** #

Chen, Nancy Oki Data

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

Table 13. The threat T.DOC_DELETED.DIS can not be countered by the objectives O.USER.AUTHORIZED or OE.USER.AUTHORIZED.

(Note: USER will be changed to ADMINISTRATOR after previous comments are accepted.)

SuggestedRemedy

remove the check marks for O.USER.AUTHORIZED and OE.USER.AUTHORIZED that are against T.DOC_DELETED.DIS.

(Note: USER will be changed to ADMINISTRATOR if the previous comments are accepted.)

Proposed Response Response Status