

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **10.4 table 16** P L # **51**
 Nevo, Ron Sharp

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

'Modify' operation to object D.FUNC
 Regarding print, copy and FAX (receiving) functions (obtaining paper output), there are many devices that can allow 'Modify' operation. However, regarding scan and FAX (sending) functions there are very few.
 This means that there yields unnecessary requirement of new HCD functions, beyond IEEE 2600.1 security function specifications.
 Therefore, 'modify' operation to object D.FUNC should be left to ST authors/E own choices (i.e. TOE that claims conformance to PP).

Suggested Remedy

Remove the operation "Modify" to object D.FUNC.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Re-write the access control policies using the proper "deny" and "allow" rules. The editor will work with atsec to get these correctly stated. The editor will work with the PP editors to get an early assessment of this new text.

Cl **PP-A** SC **10.8** P L # **40**
 Nevo, Ron Sharp

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

FPT_TST.1
 1) In 36c, we made the comment regarding the necessity of FPT_TEE.1, but we seemed to misunderstand. What is necessary we think is not FPT_TST.1, but FPT_TEE.1.
 As we pointed out in 36c, though the issue "what is the TOE" still remains (according to Fig.1, we can read that the part which provides the TSF is the TOE), what FPT_TST.1 provides is a self verification function of a TOE, not a verification function of external entities that are newly installed. That means there is a possibility that a valid TOE can install a firmware without verifying validity of external entities.
 External entities, in other words "parts of an HCD" can be hardware or firmware, and properties of the TOE "parts of the HCD" shall be validated by FPT_TEE.1.
 2) Regarding FPT_TST.1, we think that self verification is not always necessary.

Suggested Remedy

Remove FPT_TST.1 and add FPT_TEE.1.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Continue to use FPT.TST.1; FTP_TEE.1 is used for device test and may be included by the ST author (in addition to FTP_TST.1) is appropriate for the HCD.

This will protect against inadvertant changes to the code.

Clarify APP NOTE to reflect the above.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC 17.1 P L # 41
 Nevo, Ron Sharp

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

A removable nonvolatile storage device is a nonvolatile storage device that is part of the evaluated TOE but is designed to be removed from the TOE by authorized non-service personnel.

If the TOE has the capability to store user document data or critical TSF data on such a device, the security objective of protecting this data can only be achieved when the confidentiality and integrity of the data is preserved even in the case of an attacker that analyzes this the content of the removable storage device using a system capable of reading the content of the device.

Definitions of "removed" and "removable" are not clear. For example, is a flash memory mounted on a board applicable?

It may be appropriate that we leave this to ST authors, however in PP that is security requirement specification, the definitions should be clarified.

SuggestedRemedy

Either of the followings:

1)Some tools are necessary for attackers to read the asset by removing a non-volatile storage device. That is, they must know the interface to the device to read the asset from it. However, we can obviously imagine that they can easily know the device interface except the case the device is full-customized.

Therefore, a hard disk drive (ATA/Serial ATA interface) is supposed as a non-volatile storage device that the tool is easily prepared.

For this reason, the content of the device should be removed from a removable nonvolatile storage device. This means the asset that is stored in a flash memory mounted on a board should be protected.

2)Modify the description of "A removable nonvolatile storage device . . . the content of the device." to the one that intends a hard disk drive(ATA/Serial ATA interface).

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Add an APPNOTE that says that the ST author will have to identify the nonvolatile storage devices that are removable and non-removable. The lab evaluating the product against the ST will have to assess whether those assertions of removability are accurate.

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

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

FTP_CIP_EXP.1

This requirement is excessive since this requires confidentiality and integrity. Originally FCS_CKM.1, FCS_CKM.4, and FCS_COP.1 require only confidentiality, so FTP_CIP_EXP.1 as the alternative should also require only confidentiality.

SuggestedRemedy

Modify that this only requires confidentiality.

Proposed Response Response Status **W**

PROPOSED REJECT.

see #35

Cl **PP-A** SC 17.2 P L # 43
 Nevo, Ron Sharp

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

FTP_CIP_EXP.1

1)There is no description that corresponds to APE_ECD.1-3. (Regarding APE_ECD.1-6 and APE_ECD.1-7, they depend on the evaluation of APE_ECD.1-3)

2)There is no description that corresponds to APE_ECD.1-12 and APE_ECD.1-13. If we leave them as they are, ST authors shall explain the validity of the expanded component. To utilize expanded components, we shall ask the evaluation body to evaluate the PP including validity of the expanded components.

SuggestedRemedy

Please add description or app notes

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

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

Comment Type **T** Comment Status **D**
 FTP_CIP_EXP.1 Confidentiality and Integrity of Stored Data
 This expanded component requires both confidentiality and integrity regarding user data and TSF data.

Is identification of user data and TSF data necessary in order to read data from non-volatile storage device?

If yes, this requirement should be divided into that for user data and that for TSF data.

SuggestedRemedy

- Either of the followings:
- 1)This requirement should be defined so as not to identify user data and TSF data for the data stored to or read from non-volatile storage device.
 - 2)In the above, if the identification is necessary, the requirement should be divided into that for user data and that for TSF data.
 - 3)You need to consider not utilizing the expanded component, but FCS_COP.1 and FMT_MTD.3 again.

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

Change 17.2 and 17.3 to state:

The TSF shall provide a function that ensures the confidentiality and integrity of User Data and TSF data when either are written to a removable nonvolatile storage device.

Cl **PP-A** SC **18.2** P L # **46**
 Nevo, Ron Sharp

Comment Type **T** Comment Status **D**
 FMT_ITP_EXP.1

Same comment as No.43

SuggestedRemedy

Same as comment No 43.

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

Cl **PP-A** SC **18.4** P L # **47**
 Nevo, Ron Sharp

Comment Type **T** Comment Status **D**
 Does FMT_ITP_EXP.1 belong to Class FMT: Security management?

Security management is not appropriate since it intends to specify the management of several aspects of the TSF: security attributes, TSF data and functions.

SuggestedRemedy

We cannot find any appropriate classes.

Proposed Response Response Status **W**
 PROPOSED REJECT.

As per HK, this is in the right class.

Cl **PP-A** SC **18.2** P L # **48**
 Nevo, Ron Sharp

Comment Type **T** Comment Status **D**
 FMT_ITP_EXP.1

1)This requires for user data and TSF data. For the connection with external entities (using external interfaces), the identification of user data and TSF data is not necessary.

If the identification is necessary, this requirement should be divided into that for user data and that for TSF data.

2)For the requirements to TSF data, you should consider carefully. There exist some HCDs that forward user data (for example forwarding received FAX data inside internal network). However, forwarding TSF data has little meaning regarding using HCD, so it may be considered that HCDs that have this kind of function does not exist. Therefore, we have to develop the TSF data forwarding feature, which may not be used, in order to conform to the PP

SuggestedRemedy

1)The function that forwards TSF data should be removed.

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

Change text in 18.2 and 18.4 to read:

The TSF shall protect User Data and TSF Data if either is received on [assignment: list of external interfaces] to be directly forwarded to [assignment: list of external interfaces].

Rewrite with better terms for "directly," "protect, and "forward." The intention is to protect against accessing the network from the FAX line, another network, etc.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **12.3** P L # **50**
 Nevo, Ron Sharp

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

FIA_UAU.6
 [re-comment]

Though the response to the comment we made in 36c was "Accept in principle," this was not deleted yet.

As we commented in 36c, FIA_UAU.6 is not for widely-used secure print (PIN print), but for the one that requires new authentication function/mechanism. If you think today's secure print is not enough from the viewpoint of threats and vulnerabilities, we understand that new authentication mechanism is required. However, currently there seems that no issues were found regarding the authentication mechanism of the secure print.

SuggestedRemedy

Specification using secure print (FIA_UID.1 and FIA_UAU.1)

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

see resolution of #64

Cl **PP-A** SC **13.2 table 25** P L # **52**
 Nevo, Ron Sharp

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

"Read" operation by subject U.ADMINISTRATOR to object D.DOC
 On what case does "read" operation by subject U.ADMINISTRATOR to object D.DOC occur regarding scanner function?
 Regarding the subject which sends the scanned image to external entity (IT product), we cannot think of the subject (related with the user: e.g. U.ADMINISTRATOR) other than the subject (related with the user) which generated the scan job.
 Regarding scanner function, the subject that operated "read" to object D.DOC should be restricted only to the subject (related with user: U.NORMAL) which generates the job.

SuggestedRemedy

The only subject that operates "Read" to object D.DOC should be U.NORMAL.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

This will be addressed by the rewriting of the access rules.

Cl **PP-A** SC **15.2 table 31** P L # **53**
 Nevo, Ron Sharp

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

"Read" operation by U.ADMINISTRATOR to object D.DOC
 Regarding FAX sending, there is an issue same as No.38.
 (However, regarding FAX receiving, object U.ADMINISTRATOR can operate "read" to object D.DOC.)

SuggestedRemedy

The "read" operation by U.ADMINISTRATOR to object D.DOC should be restricted to FAX receiving.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

see #65

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **19.6** P L # **54**
 Nevo, Ron Sharp

Comment Type T Comment Status D

FMT_MTD.1
 FMT_MTD.1.1(a)
 The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [selection: Nobody, [selection: U.ADMINISTRATOR, [assignment: the authorized identified roles except U.NORMAL]]].
 FMT_MTD.1.1(b)
 The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data associated with a U.NORMAL or documents or jobs owned by a U.NORMAL] to [selection: Nobody, [selection: U.ADMINISTRATOR, the U.NORMAL to whom such TSF data is associated]].
 What is "Nobody" in the above description? What is the role of "Nobody" that is different from that of U.ADMINISTRATOR or U.NORMAL?
 FMT_SMR.1
 FMT_SMR.1.1 The TSF shall maintain the roles U.ADMINISTRATOR, U.NORMAL, nobody, [assignment: the authorised identified roles].
 FMT_SMR.1.2 The TSF shall be able to associate users with roles, except for the role "nobody" to which no user shall be associated.
 What is "nobody" in the above description? The meaning of "nobody" is not clear.

SuggestedRemedy

"Nobody" should be removed since it seems to be unnecessary.

Proposed Response Response Status W

PROPOSED REJECT.

"Nobody" makes it possible for the ST author to state that no role is authorized to perform some kinds of management some kinds of TSF data. For example, you may not want to allow a username to be modified, it can only be created, queried, or deleted.

Definition of "Nobody" will be added.

Cl **PP-A** SC **10.6** P L # **55**
 Nevo, Ron Sharp

Comment Type T Comment Status D

Regarding No.39 and No.40, we guess "Nobody" is defined according to the definition of FMT_ITP_EXP.1 in section 18.4
 We guess that the role "Nobody" seems to be created for the case "TSF shall restrict the capability to override the above rule and allow such forwarding to [assignment: the authorized identified roles]" in FMT_ITP_EXP.1.2 is not enforced.
 Though we will not consider the issue of appropriateness (whether originally intended function is described or not) of FMT_ITP_EXP.1, we think the approach using FMT_ITP_EXP.1 does not seem to be appropriate. That is, it describes "In FMT_ITP_EXP.1.1, forwarding is allowed and in FMT_ITP_EXP.1.2, overriding that rule is allowed to the authorized identified role." We recommend the opposite "In FMT_ITP_EXP.1.1, forwarding is not allowed, and in FMT_ITP_EXP.1.2, overriding that rule is allowed to the authorized identified role."

Considering that way, we tend to think SMI can be described more straightforward by using information flow control (FDP_IFC.1 and FDP_IFF.1) than using expanded component.

SuggestedRemedy

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

It is a misunderstanding that 1.1 allows forwarding, it does not. It protects data to be directly forwarded. I think there is a better way to write 1.1 it so that the intention is more clear.

Rewrite SFR to clarify

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **14.2 table 28** P L # **56**

Nevo, Ron Sharp

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

The subject "any" that operates "read" to object D.DOC
 This may be U.ADMINISTRATOR and U.NORMAL, not "any."
 (Though U.ADMINISTRATOR and U.NORMAL indicate user, not the subject that
 FDP_ACC.1 requires)

SuggestedRemedy

At least this should be modified to U.ADMINISTRATOR and U.NORMAL.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

if we agree to remove FIA_UAU.6 and re-authentication concept for PRT, then it should be
 OK to modify this to U.NORMAL for his/her own documents (not U.ADMINISTRATOR)
 because we assume that U.NORMAL has authenticated when starting the copy job.

Cl **PP-A** SC **17.4 table 37** P L # **57**

Nevo, Ron Sharp

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

1)Though nonvolatile storage is defined as "a function that stores data on a nonvolatile
 storage device" in section 11.3, the explanation in section 5.1 describes that nonvolatile
 storage is "persistent or temporary document storage." It is inconsistent.

2)FTP_CIP_EXP.1 is defined as an SFR for O.DOC.NO_DIS, O.DOC.NO_ALT,
 O.FUNC.NO_ALT, O.PROT.NO_ALT, O.CONF.NO_DIS, and O.CONF.NO_ALT.
 This requires a function (basic function as an HCD) to store user data (D.DOC/D.FUNC)
 and TSF data (D.PROT and D.CONF) to non-volatile storage device.

From the above comments, it should be the objective for the threat to integrity of D.DOC,
 following the PP from the past.

(As pointed out in No.2, what is non-volatile storage device is not clear. Therefore, storing
 D.FUNC, D. PROT or D.CONF into "removed" or "non-removable" device does not
 conform to the PP. Though such HCD must be more secure than the HCD defined in the PP

SuggestedRemedy

Most HCDs that have "removed" or "removable" non-volatile storage device stores D.DOC
 into it, however, storing D.FUNC, D.PROT or D.CONF into it is uncommon. Therefore, this
 should be the objective for the threat to integrity of D.DOC.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

(1) 5.1 and 11.3 (and 11.2) should be revised to be consistent with the definition of NVS as
 stated in 17.1.

However, (2) The SFR does not require any particular kind of data to be stored on NVS, it
 says only that the function ensures C&I of User and TSF Data _when_ written to NVS.]

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **18.6 table 40** P L # **58**
 Nevo, Ron Sharp

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

The same issue as No.44 exists in SMI. It requires the functions (basic function as an HCD) that send and receive user data (D.DOC and D.FUNC) and TSF data (D.PROT and D.CONF) to/from external entity. Regarding user data (D.DOC and D.FUNC), almost all HCD can send/receive them to/from external entities, however, regarding TSF data (D.PROT and D.CONF), there is a question about how many HCDs can send/receive them. In addition, the HCD that cannot send/receive TSF data is more secure than the one that can do it, from the viewpoint of communication with external entities. Remove O.PROT.NO_ALT, O.CONF.NO_DIS, and O.CONF.NO_ALT from Table 40.

SuggestedRemedy

Remove O.PROT.NO_ALT, O.CONF.NO_DIS, and O.CONF.NO_ALT from Table 40.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

If you are sending/receiving user data, then you are probably doing I&A as well

This was also addressed similar to resolution of comment #45

Cl **PP-A** SC **13.2 table 25** P L # **59**
 Nevo, Ron Sharp

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

"Read" operation to object D.DOC by subject U.NORMAL and U.ADMINISTRATOR is an objective to the threat T.DOC.NO_DIS. As we wrote in No.42, U.NORMAL/U.ADMINISTRATOR does not stand for user, not for subject. That is, even if you read U.NORMAL/U.ADMINISTRATOR as subject, oreado operation to the object D.DOC by the other people than U.NORMAL/U.ADMINISTRATOR (or subject) cannot be an objective to T.DOC.NO_DIS.

For HCDs that make O.DOC.NO_DIS (FDP_ACC.1 and FDP_ACF.1) objective to T.DOC.NO_DIS, they shall implement the function of displaying and outputting D.DOC (data) on HCD. It defines a basic function of HCD.

SuggestedRemedy

As written in left, it is uncommon that HCD displays or outputs scanned image on HCD scanner function.

Therefore, since D.DOC cannot exist on general HCD scanner function, SCN package is not needed (no SFRs remain if FDP_ACC.1 and FDP_ACF.1 are removed).

Proposed Response Response Status **W**

PROPOSED REJECT.

The app note explains that "Read" in this case refers to transmission of D.DOC through an interface, and may be used for display]

Cl **All P** SC P L # **1**
 Chen, Nancy Oki Data

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

We have one single set of overall security problem description as assets, threats, assumptions, objectives, OSPs that cover the security problems for the common SRF package, and PRT, SCN, CPY, FAX, DSR, NVS, SMI SFR packages. Would like to have a brief description of the security problems covered by each of the rest of individual packages, so as to clarify the relationship of the partitioned security problems between the common SFR package and the rest of individual SFR packages. This applies to P2600.1, P2600.2, P2600.3, and P2600.4.

SuggestedRemedy

Before the descriptions of SFRs, add a brief description of the security problems covered by each individual optional SFR packages, with clarification of the relationship between the common security problems and those added by the individual optional SFR packages.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Add some clarification as to what each package adds.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **All P** SC P L # 62
 Petrie, Glen Epson

Comment Type **G** Comment Status **D**

PP use original TSF

Who describes why PP use original TSF instead of TSF in CC part2. ?
 This is responsibility of PP, not of ST author.

SuggestedRemedy

Proposed Response Response Status **W**

PROPOSED REJECT.

[do not understand]

Cl **Globa** SC **FIA_UAU.6** P L # 63
 Petrie, Glen Epson

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

FIA_UAU.6 in P2600.x-PRT SFT package. (x=1 or 2)
 FIA_UAU.6(Re-authenticating) is not good for this purpose .
 For Example .
 PIN code authentication.
 Add PIN code to print JOB by printer driver UI.
 Enter PIN code printer panel UI then start printing .
 Add PIN code is not authenticate action.
 Enter PIN code is authenticate action.
 By the way , FIA_UAU.6 requires that the authentication which is the trigger of printing is second authentication.
 FIA_UAU.6(Re-authenticating) is not good for this purpose .
 FIA_UAU.1 or FIA_UAU.2 is good .
 The selection of FIA_UAU1. or FIA_UAU.2 is depend of implementation of application. (*1)

(*1) PIN code authentication
 User select PIN code authentication function on printer panel
 Printer panel UI displays "Enter PIN code" and user enter PIN code, and then start printing .
 This type authentication, ST author select FIA_UAU.1.
 ID card authentication
 User swipe ID card at printer, and then start printing .
 (Before authentication , there is No other user action)
 This type authentication , ST author select FIA_UAU.2.

SuggestedRemedy

Epson recommend that "If a TOE provide a feature for authentication before printing , then the ST author should add FIA_UAU.1 or FIA_UAU.2." in PP APPLICATION NOTE.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

see resolution of #64.

Since they (UAU.1 and UAU.2) are hierarchical, use of UAU.2 in the ST exceeds the requirements of UAU.1 and can be substituted.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **18.2** P L # **49**
 Nevo, Ron Sharp

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

FMT_ITP_EXP.1
 FMT_ITP_EXP.1.1: The TSF shall protect user and TSF data received on [assignment: list of external interfaces] to be directly forwarded to [assignment: list of external interfaces].
 FMT_ITP_EXP.1.2: The TSF shall restrict the capability to override the above rule and allow such forwarding to [assignment: the authorized identified roles].
 1) What does "protect" mean?
 A mechanism that accordingly "protects" something is a security function. This does not explain the mechanism, so this element is not appropriate.
 2) We think they can not explain the function that is originally intended.
 The intention is to define the impossibility to access (attack) from public telephone line to internal network resource. This means HCD does not behave as gateway, or controls the information flow on connection with external entities.

SuggestedRemedy

Either of the followings:

- 1) Since it is considered that they can not explain the function that is originally intended, you need to consider intended SFR. Due to shortage of time, we cannot find any recommendation.
- 2) May need to reconsider utilizing FDP_IFC.1 and FDP_IFF.1 instead of expanded component.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

[perhaps "protect" is not a good term to use? Also note that "directly forwarded" needs to be clarified]

major rewrite..

see also comment #48

Cl **PP-A** SC **2** P **2** L **20** # **10**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **D**

The title of IEEE Std. 2600 in the Normative References is incorrect. It is stated as 'Information Technology: Hardcopy System and Device Security'; it should be 'Information Technology: Hardcopy Device and System Security'

SuggestedRemedy

Change the title for IEEE Std. 2600 in the Normative References clause as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-A** SC **3.2** P **3** L **14** # **16**
 Sukert, Alan Xerox

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

As an example, the title page lists IEEE P2600.1 as the "Draft Standard for a Protection Profile in Operational Environment A" while page 3, line 14 indicates that P2600.1 is the "Protection Profile for Hardcopy Devices, Operational Environment A". We seem to be overloading the use of the P2600.1 designation.

I am concerned we may be creating some confusion as to what P2600.1 actually refers to because we are using the designation P2600.1 to represent both the Standard for a Protection Profile in Operational Environment A and the actual Protection Profile itself.

SuggestedRemedy

Eliminate the use of the P2600.1 designation to stand for both the Standard for the PP and the actual PP itself.

Note that what we decide to do here can have ripple effects on everywhere in the standard where P2600.1 is referenced. For example, see page 4, line 41.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

The PP should be referenced as P2600.1-PP (somewhat consistent with the references to SFR packages P2600.1-PRT, P2600.1-SCN, etc.).

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC 5.1 P 5 L 20 # 25
 Sukert, Alan Xerox

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

There is an inconsistency between the statement of the nonvolatile storage TOE function between subclause 5.1 and subclause 11.2 (page 29, line 20).

Subclause 5.1 says that nonvolatile storage applies to ""persistent or temporary document storage on devices that could practicably be removed and analyzed when the HCD is powered off""; subclause 11.2 states that the NVS package applies to ""a storage device which can practicably be removed from the HCD by unauthorized people for analysis and recovery of deleted data"". There are two main areas where the two differ:

1. Does NVS apply to both persistent and temporary document storage as indicated in subclause 5.1 or not.
2. Does NVS apply just when the device is powered down as indicated in subclause 5.1 or when the device is powered up or powered down as implied in subclause 11.2.

SuggestedRemedy

Make the statements for the NVS function consistent between subclauses 5.1 and 11.2.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Neither is correct, they should be consistent with 17.1

Cl **PP-A** SC 5.1 P 5 L 21 # 26
 Sukert, Alan Xerox

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

There is an inconsistency between the statement of the shared-medium interface (SMI TOE function between subclause 5.1 and subclause 11.2 (page 29, line 32).

Subclause 5.1 says that SMI applies to ""transmitting and receiving documents and data between the HCD and external devices over communications media that are or can be shared by other users""; subclause 11.2 states that the SMI package applies to HCD products that ""transmit and receive data over a communications medium that are or can be shared by other users"". The key difference is that subclause 5.1 indicates SMI applies to both documents and data while subclause 11.2 indicates SMI applies only to data.

SuggestedRemedy

Make the statements for the SMI function consistent between subclauses 5.1 and 11.2.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

(Should match resolution from PP-D)

Cl **PP-A** SC 5.2 P 5 L 33 # 67
 Smithson, Brian Ricoh

Comment Type **E** Comment Status **D**

[NIAP] ""Users == Subjects"" conflicts with many CC concepts.

SuggestedRemedy

Change ""Users == Subjects"" to ""the Subject security attributes used in access control decisions are identical to the security attributes of the User that requested access"".

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-A** SC 5.2 P 6 L 8 # 11
 Sukert, Alan Xerox

Comment Type **E** Comment Status **D**

Grammatical error -- Lines 8 and 9 have ""There may be cases where User Data and TSF Data is generated outside of the TOE and transmitted to the TOE, as well as cases where User Data and TSF Data is generated and/or processed..."".

It should be ""There may be cases where User Data and TSF Data are generated outside of the TOE and transmitted to the TOE, as well as cases where User Data and TSF Data are generated and/or processed...""

SuggestedRemedy

Correct this sentence as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

(Match resolution in PP-D)

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **5.3.2.1** P **7** L **10** # **17**
 Sukert, Alan Xerox

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

The definition of User Document Data in Table 1 deviates slightly from the corresponding definition of User Document Data in Annex A, page 55, line 13. Subclause 5.3.2.1 has ""information contained in a User's document in hardcopy or electronic form"" while Annex A has ""information contained in a User's document.""

SuggestedRemedy

Make the definition of User Document Data in subclause 5.3.2.1 consistent with the corresponding definition in Annex A.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Use what is in Std-2600

Cl **PP-A** SC **5.4** P **9** L **12** # **65**
 Smithson, Brian Ricoh

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

Some statements in the PP make it impossible for HCDs with fax to receive incoming faxes from unidentified, unauthenticated, unauthorized users. However, this is the typical case for fax systems.

SuggestedRemedy

P9 L12 change bullet item to ""All Users that want to perform an access-controlled function or a management function are identified and authenticated, and are authorized before being granted permission to perform TOE functions other than those allowed for unauthenticated users.""

P13 table 10 change P.USER.AUTHORIZATION to ""The TOE shall require identification and authentication of Users, and shall ensure that Users are authorized in accordance with security policies before allowing them to use the functions of the TOE reserved for identified and authenticates users.""

P30 table 21: Change +FAX into two attributes, +FAXIN ""Indicates data that is associated with a fax job for faxes being received by the TOE"", and +FAXOUT ""Indicates data that is associated with a fax job for faxes being sent by the TOE"".

P40 L8 add an app note for the FAX package that says ""Typical fax systems allow unidentified, unauthenticated users outside of the TOE to send fax documents to the TOE. To allow this, the ST Author should consider adding fax reception to the list of TSF-mediated actions that are allowed in FIA_UAU.1.1 in the Common PP.""

P40 table 31 change the D.DOC rules as follows:

- +FAXIN Read U.ADMINISTRATOR Allowed
- +FAXOUT Create, Delete U.NORMAL Allowed for his/her own documents

P40 L11 add an app note ""For +FAXIN, the ""owner"" of an incoming fax job is considered to be U.ADMINISTRATOR. The ST Author may refine this role if a conforming TOE provides a specific role for fax administration.

P40 L11 add an app note ""If a conforming TOE provides a feature that allows an administrator to transfer ownership of an incoming fax job to one or more normal users -- typically, the intended recipients of the fax documents -- then the ST Author should consider adding a rule to the FAX Access Control SFP such as ""+FAXIN Read U.NORMAL Allowed if this User is authorized by U.ADMINISTRATOR"". Alternatively, the ST Author may define and use attributes for this purpose in the FAX Access Control SFP, provided that the initialization and management of such attributes are specified in such as in FMT_MSA.1 and FMT_MSA.3.""

P40 L11 replace the app note with ""For +FAXIN, ""Read"" refers (as a minimum) to the release of pending hardcopy output to a Hardcopy Output Handler or the retransmission of User Document Data through an Interface for faxes that have been received by the TOE. For +FAXIN and +FAXOUT, ""Read"" may also refer to previewing User Document Data on

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **7.2** P **11** L **11** # **66**
 Farrell, Lee Canon

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

Effectiveness of P.SOFTWARE.VERIFICATION and FPT_TST.1 heavily depends on the implementation, and will NOT be applied to the implementation like the following;

Quote from the CC 3.1 Part 2 Rev. 2

J.7 Trusted recovery (FPT_RCV)
 if the recovery is performed in a manner such that only a secure state can be achieved, else recovery fails, then the dependency to the FPT_TST.1 TSF testing TSF self-test component may be argued away.

SuggestedRemedy

P.SOFTWARE.VERIFICATION should be removed from the Protection Profile.

Proposed Response Response Status **W**

PROPOSED REJECT.

After discussions with Helmut, it was agreed to include protection against inadvertent changes to the code load. See comment #40.

Cl **PP-A** SC **7.3** P **12** L **1** # **72**
 Smithson, Brian Ricoh

Comment Type **E** Comment Status **D**

[NIAP] The administrator should also be trained and implement a secure configuration of these devices.

SuggestedRemedy

Change A.ADMIN.TRAINING from "...documentation to configure..." to "...documentation, and configure..."

Change OE.ADMIN.TRAINED from "...documentation to correctly..." to "...documentation, and correctly..."

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-A** SC **10.4** P **18** L **8** # **74**
 Smithson, Brian Ricoh

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

The access control SFPs give administrators various permissions for accessing user documents. For example, the common AC SFP allows admins to Delete, and the PRT AC SFP allows admin to Read. In practice, some administrative interfaces may not provide such access to admins, but other administrative interfaces may provide more access (e.g., Create or Modify). If an ST does not provide the access that we specify in the SFPs, then it would not be compliant. Administrator permissions for document access is not among the security objectives of the PP, and so it should not be specified.

SuggestedRemedy

(1) Remove D.DOC permissions for U.ADMINISTRATOR in the common AC SFP and in all SFR package AC SFPs.

(2) Change D.DOC permissions for U.NORMAL from ""Allowed for his/her own documents"" to ""Denied for documents that are not owned by that user"". (exception: DSR Read access should be ""Denied for documents that are not owned by that user, unless access to the document is permitted for this user by [assignment: the authorized identified roles]"")

(3) Add an app note which explains that the default rules ensure that a normal user cannot access another's documents, but the ST Author may add a rule that permits access to administrators.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

This is being addressed by the re-writing of the access control tables in terms of "deny" rather than "allow"

Cl **PP-A** SC **10.4** P **18** L **11** # **18**
 Sukert, Alan Xerox

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

The PP Application Note on this line refers to Table 15. Since it is discussing the applicable SFPs I believe the table reference here should be to Table 16 instead.

A similar comment applies to the table reference in the PP Application Note on page 18, line 17.

SuggestedRemedy

Reference the proper table in these two PP Application Notes.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

CI **PP-A** SC **10.4** P **18** L **28** # **19**
 Sukert, Alan Xerox

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

The PP Application Note for FDP_ACC.1 indicates that this SFR is a dependency of FMT_MSA.1. For completeness it should be noted here that this SFR is also a dependency of FDP_ACF.1.

SuggestedRemedy

Indicate in this PP Application Note that FDP_ACC.1is also a dependency of FDP_ACF.1.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-A** SC **10.6** P **22** L **7** # **20**
 Sukert, Alan Xerox

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

In line with the conventions used elsewhere in Clause 10, since FMT_MSA.1.1 has been modified to specifically reference the Common Access Control SFP, you should use here the notational convention indicated for SFRs that have been altered (see clause 1.4, page 1, line 21)

A similar comment applies to FMT_MSA.3.1 (clause 10.6, page 22, line 23).

SuggestedRemedy

Define FMT_MSA.1.1 and FMT_MSA.3.1 as altered SFRs using the appropriate notational convention.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-A** SC **10.6** P **22** L **14** # **69**
 Smithson, Brian Ricoh

Comment Type **E** Comment Status **D**

[NIAP] ""Nobody"" is a special term, but is not defined.

SuggestedRemedy

Add a definition to the glossary: Nobody - a pseudo-role that cannot be assigned to any user.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-A** SC **10.6** P **23** L **6** # **21**
 Sukert, Alan Xerox

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

The PP Application Note for FMT_MTD.1 indicates that FMT_MTD.1.1(b) applies to TSF data that is associated with a Normal User. In reading the actual SFR it indicates that the SFR applies to TSF data that is associated with a Normal User and to jobs owned by a Normal User.

SuggestedRemedy

Revise the PP Application Note for FMT_MTD.1 to indicate that FMT_MTD.1.1(b) applies to both TSF data that is associated with a Normal User and to jobs owned by a Normal User.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-A** SC **10.6** P **23** L **10** # **14**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **D**

Administrator is spelled incorrectly in subclause 10.6, page 23, lines 10 and 15.

SuggestedRemedy

Correct the spelling of administrator in the indicated lines.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-A** SC **10.6** P **23** L **14** # **2**
 Chen, Nancy Oki Data

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

FMT_MTD.1.1 is for the protection of TSF data. The protection of user document data and job data has been covered by FDP_ACC. There is no need to protect user document and job data in this SFR.

SuggestedRemedy

Delete ""or documents or jobs owned by U.NORMAL"" from this SFR.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

clarify the intention by saying "or TSF Data associated with documents or jobs. . ."

IEEE P2600 Hardcopy Device and System Security Comments

CI **PP-A** SC 10.6 P 23 L 17 # 22
 Sukert, Alan Xerox

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

It is not clear why in this PP Application Note it states that FMT_MTD.1 is a principal SFR to ""one or more"" of the three objectives listed. Per Table 18 this SFR is a principal SFR for all three objectives, so why not just state it that way.

SuggestedRemedy

Revise this PP Application Note to read that FMT_MTD.1 is a principal SFR of the three objectives listed.

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

CI **PP-A** SC 10.6 P 23 L 35 # 70
 Smithson, Brian Ricoh

Comment Type **E** Comment Status **D**

The role ""Nobody"" is inconsistently capitalized.

SuggestedRemedy

Capitalize ""Nobody"" (multiple places).

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

CI **PP-A** SC 10.6 P 23 L 35 # 3
 Chen, Nancy Oki Data

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

Depending on implementation, ""nobody"" may not be a role that need to have and maintained.

SuggestedRemedy

Delete ""nobody"" from the SFR.

Proposed Response Response Status **W**
 PROPOSED REJECT.

"nobody" is not a maintained role, it is an indicator that there is no role

We will add a definition of Nobody

CI **PP-A** SC 10.8 P 24 L 21 # 61
 Yami, Sameer Toshiba

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

A PP note needs to be added for FPT_TST.1 TSF testing explaining the kind of tests that are possible.

SuggestedRemedy

Give a list of possible tests:

1. Signature check for known files
 2. Encryption / Decryption of known data ...
- ...more can be added over here

Proposed Response Response Status **W**
 PROPOSED REJECT.

Put this kind of information in the guide.

CI **PP-A** SC 10.11 P 25 L 12 # 23
 Sukert, Alan Xerox

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

It is not clear why the statement used to indicate that there are no FTP SFRs is different than the corresponding statement used for other classes. For FTP the statement is that "There are no Class FTP security functional requirements among the Common Security Functional Requirements" whereas, for example, for class FRU (subclause 10.9, page 25, line 2) the statement used is "There are no Class FRU security functional requirements for this Protection Profile"

SuggestedRemedy

Use a consistent statement when indicating that a class has no SFRs that are used in the PP.

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

Use the statement:

"There are no Class FTP security functional requirements for this Protection Profile."

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **10.12** P **26** L **1** # **24**
 Sukert, Alan Xerox

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

I was curious why the purpose for FIA_UID.1 indicated for the O.DOC.NO_DIS / O.DOC.NO_ALT / O.FUNC.NO_ALT objectives (Supports security roles by requiring user identification) is different from the purpose indicated for the O.CONF.NO_DIS / O.PROT.NO_ALT / O.CONF.NO_ALT objectives (Supports access control and security roles by requiring user identification). I would think that the purpose would be the same in both cases since this SFR deals with user identification which would be needed in the same manner for both sets of objectives that doesn't directly deal with access control.

SuggestedRemedy

Make the purpose for FIA_UID.1 consistent within Table 19 for the NO_DIS and NO_ALT objectives.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Both should mention Access Controls.

Cl **PP-A** SC **11.2** P **29** L **21** # **27**
 Sukert, Alan Xerox

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

I am still concerned that the NVS package only applies to data stored on removable NVS devices. First of all there still is no clear definition of what NVS devices this applies to, especially given the inconsistency between subclauses 5.1 and 11.2 regarding the NVS function defined in an earlier comment. Second, we still don't have a clear definition of what constitutes a ""removable"" NVS device in this context - does it apply only to an NVS device which it is designed to be removed; does it apply to an NVS device which can easily be removed but which is not designed specifically to be removable; etc.

Most importantly the threat to NVS applies equally whether the NVS device is designed to be removable or not - we want to protect data stored in an NVS device whether it is located in the TOE or removed from the TOE from unauthorized disclosure or alteration.

SuggestedRemedy

Change the NVS package to apply to NVS devices whether or not they are a ""removable NVS device"".

Proposed Response Response Status **W**

PROPOSED REJECT.

This comment was WITHDRAWN by the commenter.

Cl **PP-A** SC P **29** L **32** # **9**
 aubry, carmen oce

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

"This package applies for TOEs that provide a trusted channel function allowing for secure and authenticated communication with other IT systems. If such protection is supplied by the TOE environment and not the TOE itself, this package can not be claimed."

This is new, we never said that we allow TOEs that are not providing a trusted path. I thought that if we have a SMI, we need to provide trusted path (with a dependency on the environment for the counterpart on the remote trusted party) in order to claim compliance to this PP? Furthermore, SMI provides also channel management so you can not exclude the SMI package just because the trusted path has been provided by the environment.

SuggestedRemedy

I think that as long we have a product with SMI, the SMI package must be included.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Put an example in the PP Guide.

Cl **PP-A** SC **12.2** P **31** L **9** # **73**
 Smithson, Brian Ricoh

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

(1) Permission to execute functions like PRT, SCN, etc. is distributed among the SFR packages. This results in many redundant SFRs for establishing the access control rules and for managing them. (2) NIAP did not like to see distributed administrative functions in the old family of PPs approach, and we have partially duplicated that here. (3) There may be some implication that all TOEs must provide an administrative function that permits or denies each authorized user to execute each function, but in practice, some products will allow all authorized users to execute all available functions. Function-by-function administrative control is not one of the security objectives of the PP, so it should not be a requirement (even by implication).

SuggestedRemedy

Rewrite the access controls for function execution as proposed by Helmut Kurth (reference document <http://grouper.ieee.org/groups/2600/presentations/Camas2008/Function%20access%20control%20policy.doc>).

Proposed Response Response Status **W**

PROPOSED ACCEPT.

We will use the SFRs to define the policy.

IEEE P2600 Hardcopy Device and System Security Comments

CI **PP-A** SC **12.2** P **31** L **10** # **64**
 Smithson, Brian Ricoh

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

The requirement for local authentication before retrieving hardcopy output ("PIN printing") should not have been made using FIA_UAU.6. FIA_UAU.6 is for re-authentication on the same Interface. The requirement is actually for authentication on a different interface. Therefore, it should be covered by the existing FIA_UAU.1. However, it may not be clear that the requirement local authentication is required when a user has submitted a print job from a non-local interface.

SuggestedRemedy

P31 L13 add an app note "A User will need to authenticate using the operator controls on the TOE to perform "Read" operations. If the User authenticated using operator controls when submitting a print job, and that session is still active, then re-authentication is not necessary. However, if that session is no longer active or the User authenticated and submitted the print job over a different Interface, then the User will need to authenticate using operator controls in order to establish a new session before being permitted to perform the "Read" operation."

Remove FIA_UAU.6 from PRT package.

Remove FIA_UAU.6 from tables 23 and 24.

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

CI **PP-A** SC **12.3** P **32** L **24** # **38**
 Farrell, Lee Canon

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

use of FIA_UAU.6 (re-authentication) is too restrictive for applicability to a PIN Print scenario.

It should not be required that the *same* authentication is used for both job submission and hardcopy retrieval.

For job submission, the user should only need to authenticate that s/he is authorized to use the device for printing. This is not an essential step in assuring O.DOC.NO_DIS.

For hardcopy retrieval, it should only be necessary to authenticate that the "print job secret" (e.g., print job password) is known. Although this *could* be the same as the authentication used for job submission, it should not be restricted to that.

SuggestedRemedy

Instead of using FIA_UAU.6, use FIA_UAU.1 (or FIA_UAU.2?)

If necessary, add an APP NOTE to explain that FIA_UAU.1 is applicable to hardcopy retrieval, but different method(s) could be used for determining authorization for job submission.

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

see #64

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **12.3** P **32** L **24** # **36**
 Farrell, Lee Canon

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

FIA_UAU.6 requires the same authentication method as the first authentication, but the PIN print with other authentication methods (i.e. the methods differ from first one) will also satisfy the objective to avoid unintentional person to pick up the printout. In other words, specifying by FIA_UAU.6 (re-authentication) will be too restrictive to satisfy the objective.

SuggestedRemedy

Replace FIA_UAU.6 with FIA_UAU.1, rename FIA_UAU.1_PRT as iteration operation because FIA_UAU.1 already exists, and add the authentication timing to proceed printing the User Document Data spooled by the user as refinement.

Proposed text:

=====

FIA_UAU.1_PRT Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1_PRT - The TSF shall allow on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2_PRT - The TSF shall require each user to be successfully authenticated [refinement: to proceed to print the User Document Data spooled by the user] before allowing any other TSF-mediated actions on behalf of that user.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

refinement is not necessary, see #64

Cl **PP-A** SC **12.4** P **33** L **7** # **28**
 Sukert, Alan Xerox

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

The description for O.USER.AUTHORIZED in Table 24 is not consistent with the corresponding description for O.USER.AUTHORIZED in Table 19 (subclause 10.12, page 27, line 1). Table 24 states ""Authorization of Users and Administrators to use the TOE"" while Table 19 states ""Authorization of Normal Users and Administrators to use the TOE"". The two should be consistent.

A similar comment applies to Table 27 (subclause 13.4, page 36, line 1); Table 30 (subclause 14.4, page 39, line 1); Table 33 (subclause 15.4, page 42, line 1); Table 36 (subclause 16.4, page 45, line 2)

SuggestedRemedy

Make sure the description for O.USER.AUTHORIZED is consistent between Table 19 and Tables 24, 27, 30, 33, 36.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

table 19 is correct

Cl **PP-A** SC **15.2** P **40** L **10** # **71**
 Smithson, Brian Ricoh

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

[NIAP] transmission through an interface should be a ""write"" operation.

SuggestedRemedy

Modify rules to the FAX SFP as follows:

U.NORMAL: Create, Read, Delete.

Change app note on line 11 to say:

"Read" refers (as a minimum) to the release of pending hardcopy output to a Hardcopy Output Handler for receiving faxes and to the transmission of User Document Data through an Interface for receiving faxes. "Create" refers (as a minimum) to submission of User Document Data to be sent and implies transmission of User Document Dat through an Interface for delivering the fax. "Read" may also be used to refer to previewing documents on a display device, if such a feature is present in a conforming TOE.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

CI **PP-A** SC **16.2** P **43** L **9** # **75**

Smithson, Brian Ricoh

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

The DSR AC SFP does not allow a user to store a document.

SuggestedRemedy

Add a rule D.DOC / +DSR / Create / U.NORMAL / Allowed if this user is authorized to execute the DSR function.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-A** SC **16.2** P **43** L **9** # **4**

Chen, Nancy Oki Data

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

In Table 34 DSR Access Control SFP, the very last D.DOC's ""Read"" rule for U.NORMAL, the statement ""à or by another authorized user for that user's own document"" is redundant."" Because the previous ""Read"" rule for U.NORMAL already states that ""allowed for his/her own document"". The same applies for P2600.2 DSR SFR Package.

SuggestedRemedy

Delete ""or by another authorized user for that user's own document"" from this ""Read"" SFP.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

the rule is unclear, but not redundant. It would be more clear to say "Allowed for another User's document if this user is authorized by . . ."

This will be fixed in the rewrite of the Access Control Tables

CI **PP-A** SC **17** P **46** L **1** # **5**

Chen, Nancy Oki Data

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

Since there is no common baseline requirement for protection of data stored on ""removable non-volatile storage"", it should be ST author's responsibility to describe their customer's specific requirements for protection of data store on removable NVS. The same applies to P2600.2.

SuggestedRemedy

Remove NVS SFR package.

Proposed Response Response Status **W**

PROPOSED REJECT.

As per our previous discussion with Helmut this will remain.

CI **PP-A** SC **17.1** P **46** L **9** # **31**

Sukert, Alan Xerox

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

It is not clear why removable NVS is designed to be removed by only authorized non-service personnel. You would certainly want service personnel to be able to remove any removable NVS which seems to be excluded by the current definition.

SuggestedRemedy

Change the definition to read ""...is designed to be removed from the TOE by authorized personnel."" This would include both service and non-service personnel.

Proposed Response Response Status **W**

PROPOSED REJECT.

it was not the intention to prohibit service personnel from removing devices, but we do not want to include (in NVS protection) devices that are designed for servicing but not for end-user removal. The current definition does not prohibit service personnel from removing devices.

IEEE P2600 Hardcopy Device and System Security Comments

CI **PP-A** SC 17.1 and 17.2 P 46 L 14 # 35
 Farrell, Lee Canon

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

The requirement for "integrity of the data" is not appropriate for the removable non-volatile storage threat. This threat should be limited to data confidentiality only.

The threat identified pertains to the possibility that "an attacker [can] get hold of the device and analyze its content off-line". Such analysis would only result in a loss of data confidentiality -- not data integrity.

Also -- change "FTP" to "FPT" and "CIP" to "CP"

SuggestedRemedy

Remove any references to requirements for assuring data integrity in the context of removable non-volatile storage.

Specifically, change the existing text in 17.2, starting on line 21 to:

FPT_CP_EXP.1.1 The TSF shall provide a function that ensures the confidentiality of user and TSF data when stored on [assignment: media used to store the data].

FPT_CP_EXP.1.2 The TSF shall provide a function that obtains the plaintext of user and TSF data when reading data back that has been previously stored using the confidentiality protection function.

Proposed Response Response Status **W**

PROPOSED REJECT.

Integrity needs to be protected noting that it is sufficient to detect a loss of integrity of the data on the non-volatile storage device. Such loss of integrity should be logged or other action taken.

In regards to changing "FTP" to "FPT", this is rejected as well because we are talking about protecting data outside the protected environment and trust path is the appropriate class.

CI **PP-A** SC 17.1 P 46 L 14 # 76
 Smithson, Brian Ricoh

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

It was not the original intention of the NVS package to protect integrity of data; the driving customer requirement is only to protect confidentiality. However, the common PP has objectives for protecting integrity of user and TSF data.

SuggestedRemedy

- (1) In the common PP:
 - (a) Add an OSP P.OFFLINE.CONFIDENTIALITY ""To preserve data confidentiality, the TOE will protect confidential data from unauthorized disclosure when the TOE is not operating"".
 - (b) In the objectives rationale table, add P.OFFLINE.CONFIDENTIALITY and link it to OE.PHYSICAL.MANAGED.
- (2) In the NVS package:
 - (a) Remove ""and integrity"" from page 46 line 14.
 - (b) Change the name and designation of FTP_CIP_EXP.1 to FTP_CP.EXP.1 ""Confidentiality of Stored Data"".
 - (c) Remove ""and integrity"" from FTP_CIP_EXP.1.1.
 - (d) Remove FTP_CIP_EXP.1.2 and FTP_CIP_EXP.1.3.
 - (e) Remove app note on page 47 line 9.
 - (f) Remove the ""NO_ALT"" objectives from app note on page 47 line 12, and from tables 37 and 38.
 - (g) Remove ""or alteration"" from table 38.

Proposed Response Response Status **W**

PROPOSED REJECT.

This comment was WITHDRAWN by the commenter.

CI **PP-A** SC 17.1 P 46 L 15 # 15
 Sukert, Alan Xerox

Comment Type **E** Comment Status **D**

grammatical error: the line states ""...preserved even in the case of an attacker that analyzes this the content..."". Should be ""...preserved even in the case of an attacker that analyzes the content..."".

SuggestedRemedy

Correct the line as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **17.2** P **46** L **27** # **29**
 Sukert, Alan Xerox

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

Not clear for extended SFR FTP_CIP_EXP.1.3 why the requirement only applies to detecting errors validating just the integrity of user and TSF data; wouldn't you also want to detect errors validating that confidentiality of user and TSF data hasn't been compromised.

Same comment applies to subclause 17.3, page 47, line 8.

SuggestedRemedy

Revise FTP_CIP_EXP.1.3 to read ""The TSF shall perform [assignment: list of actions] when it detects an error when validating the confidentiality and integrity of user and TSF data.""

Proposed Response Response Status **W**

PROPOSED REJECT.

how do you detect that confidentiality has been compromised?

Cl **PP-A** SC **18.2** P **48** L **13** # **39**
 Farrell, Lee Canon

Comment Type **E** Comment Status **D**

The use of the phrase ""directly forwarded"" is not clear, and possibly too restrictive. What exactly is meant by ""directly"" -- and is it relevant?

Are we excluding any possibility of ""indirectly forwarding"" from the scope of concern?

SuggestedRemedy

Choose one:

- 1) remove the word ""directly"" (preferred)
or
- 2) modify the phrase to ""directly or indirectly""

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

See comment #48

Cl **PP-A** SC **18.1** P **48** L **13** # **32**
 Sukert, Alan Xerox

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

My understanding of SFR FMT_ITP_EXP.1.1 was that this was the requirement that will be used for "bridging" issues like assuring one can't use a FAX phone line to access the network.

If that is the case, then it is not clear why this requirement is written as it is. I would think that the requirement should be stated in terms of protecting user and TSF data received from a listed external interface (in the case of the Fax the PSTN) from being forwarded to a listed external interface (in the case of Fax the "network"). Grammatically that doesn't appear to be what the current requirement is saying.

SuggestedRemedy

Revise SFR FMT_ITP_EXP.1.1 to read something like ""The TSF shall protect user and TSF data received on [assignment: list of external interfaces] from being directly forwarded to [assignment: list of external interfaces].""

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

See #48

Cl **PP-A** SC **18.4** P **49** L **23** # **7**
 Chen, Nancy Oki Data

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

Since FMT_ITP_EXP.1.2 requires to restrict the ability to override forwarding rule to authorized identified roles, FMT_ITP_EXP.1 should have dependency on FMT_SMR.1 that requires maintenance of the identified roles if the roles are not specified in the FMT_SMR.1 of the common PP.

SuggestedRemedy

- (1) Add dependency on FMT_SMR.1 to FMT_ITP_EXP.1
- (2) Either Add FMT_SMR.1 in this package so that additional roles identified for FMT_ITP_EXP.1.2 but not in the FMT_SMR.1 of the common PP will be maintained, or Add an App Note in the FMT_SMR.1 of the common PP to require ST to add all roles identified in all packages applicable to the ST.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **17.3** P **50** L # **44**
 Nevo, Ron Sharp

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

Does FTP_CIP_EXP.1 belong to Class FTP: Trusted Paths?
 Though it may fall down to the discussion of what is TOE, basically non-volatile storage device is defined to be installed in HCD.
 Trusted Paths is not appropriate since it is a requirement regarding paths between users/trusted IT device and TSF.

SuggestedRemedy

Need to remove FTP_CIP_EXP.1

Proposed Response Response Status **W**

PROPOSED REJECT.

Helmut has advised us this is in the right place.

Cl **PP-A** SC **18.5** P **50** L **16** # **8**
 Chen, Nancy Oki Data

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

In FTP_ITC.1.3, the communication function does not specify which data (among D.DOC, D.FUNC, D.CONF, D.PROT) must be protected from disclosure, which data must be protected from alteration.

SuggestedRemedy

For consistency with the security objectives, clarify the communication function to state which data must be protected from disclosure, which must be protected from modification.

Proposed Response Response Status **W**

PROPOSED REJECT.

Everything is protected (confidentiality & integrity) and therefore meets the objective. Breaking it up is not possible.

Cl **PP-A** SC **18.6** P **51** L **1** # **33**
 Sukert, Alan Xerox

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

The description for O.CHANNELS.MANAGED in Table 41 is not consistent with the corresponding description for O.CHANNELS.MANAGED in Table 19 (subclause 10.12, page 27, line 1). Table 41 states ""Authorization of Users and Administrators to use the TOE"" while Table 19 states ""Management of input-output channels"". The two should be consistent.

SuggestedRemedy

Make sure the description for O.CHANNELS.MANAGED is consistent between Table 19 and Table 41.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Table 19 is correct

Cl **PP-A** SC **Annex A** P **53** L **1** # **30**
 Sukert, Alan Xerox

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

If the NVS package is going to revolve around removable nonvolatile storage device, the definition of such a device that is included in subclause 17.1 needs to be added to Annex A.

SuggestedRemedy

Add the following definition to Annex A:

Removable nonvolatile storage: nonvolatile storage that is part of an evaluated TOE but is designed to be removed from the TOE by authorized personnel. See also Nonvolatile storage.

Note that this includes resolution of a previous comment about authorized personnel.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **Annex B** P **56** L **5** # **34**
Sukert, Alan Xerox

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

For consistency with the other notational prefix conventions listed in Table 1 (subclause 1.4, page 2, line 8), the prefix 'F' standing for Function is not included in the list of acronyms in Annex B.

SuggestedRemedy

Add 'F' for Function to the list of acronyms in Annex B

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-A** SC **17.2** P **46 & 47** L **234** # **6**
Chen, Nancy Oki Data

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

Not all documents are in the form of plaintext. It may be an image displaying plain readable content.

SuggestedRemedy

Change ""plaintext"" to ""intelligible form"" or something that can represent both.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

It was not intended to refer to ASCII data, it was intended to refer to unencrypted data. Perhaps "clear text" would be a more standard term?

Instead of plaintext, use unencrypted data.