

IEEE P2600 Hardcopy Device and System Security comments

Cl **All P** SC P L # 57
 Chen, Nancy Oki Data
 Comment Type **T** Comment Status **D**
 There is no mandated security attribute in the SMI Access Control SFP for FMT_MSA.1.1 to manage.
SuggestedRemedy
 Remove ""SMI Access Control SFP"" specified in FMT_MSA.1.1
Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.
 It is unclear exactly how this will be fixed but it should be fixed.

Cl **All P** SC P L # 56
 Chen, Nancy Oki Data
 Comment Type **T** Comment Status **D**
 According to the current specification, The 5th information flow control rule (the 5th row of the SMI information flow control SFP table) denies all information flows mediated by the TSF, unless they are specified in FDP_IFF.1.4.
SuggestedRemedy
 Change the rule to: ""Deny the information flow if established by the same or another U.USER(+Remote), unless it does not conflict with other rules specified within this table or it is mediated by the TSF according to other rules specified in FDP_IFF.1.4.""
Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **All P** SC P L # 49
 Chen, Nancy Oki Data
 Comment Type **T** Comment Status **D**
 P.AUDIT.LOGGING states that "records that provide an audit trail of TOE use and security-relevant events will be maintained and protected from unauthorized disclosure or alteration by the TOE,..." The alteration of log records could be by the TOE, but also by others such as Administrators too. This comment applies to the definition of P.AUDIT.LOGGING in all TOEs of all PPs.
SuggestedRemedy
 Delete the statement ""by the TOE"", or change that to ""in the TOE"".
Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.

"records that provide an audit trail of TOE use and security-relevant events will be maintained in the TOE and protected from unauthorized disclosure or alteration..."
 (delete "by the TOE")

Cl **All P** SC P L # 58
 Chen, Nancy Oki Data
 Comment Type **E** Comment Status **D**
 For clarity and consistency, would like the original text of the following SFRs that have been modified from CC be provided in grey text: FAU_SAR.1.1, FAU_STG.1.2, FAU_STG.4.1, FDP_ACF.1.2, FAU_UAU.1.1, FIA_UID.1.1, FMT_MSA.3.2 (only for P2600.1 & .2), FMT_MTD.1.1, FTP_TRP.1.1, FTP_TRP.1.2, FTP_TRP.1.3.
SuggestedRemedy
 Provide the original text of the listed SFRs in grey text.
Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.
 If we decide to leave the original CC text throughout the document we will add these in grey.

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC 7.5.2 P 23 L 23 # 8
 Smithson, Brian Ricoh

Comment Type T Comment Status D

In the SFR descriptions, some SFRs are described (in app notes) as performing only a supporting role when in fact they perform a principal role in support of some objectives.

SuggestedRemedy

Make the following changes to SFR descriptions for all PPs and TOEs in which these SFRs (and objectives) occur:

FAU_GEN.1: change app note to ""FAU_GEN.1 is a principal SFR that directly fulfills O.AUDIT.LOGGED, and one of the dependencies of FAU_GEN.2 and FAU_SAR.1"".

FIA_UAU.1: change app note to ""FIA_UAU.1 is a principal SFR that directly fulfills O.USER.AUTHORIZED and O.ADMIN.AUTHORIZED, and one of the dependencies of FIA_AFL.1 and FIA_UAU.7"".

FIA_UID.1: change app note to ""FIA_UID.1 is a principal SFR that directly fulfills O.USER.AUTHORIZED and O.ADMIN.AUTHORIZED, and one of the dependencies of FIA_UAU.1, FIA_UAU.7, FAU_GEN.2, and FMT_SMR.1"".

Proposed Response Response Status W

PROPOSED ACCEPT.

(Using changed suggested remedy)

Cl All P SC 7.5.6 P L # 46
 Volkoff, Brian Hewlett-Packard Co.

Comment Type T Comment Status D

[MULTIPLE INSTANCES, REFERS TO ALL FIA_UAU.1 and FIA_UID.1]

1.2 Identification & Authentication (I&A)

1.2.1 Problem Statement

In the referenced draft standard, the PP requires that identification and authentication (I&A) be performed by the TOE. It doesn't allow for other trusted IT products to perform user I&A.

Problem: Large enterprises commonly use centralized account repositories such as LDAP and Kerberos to maintain user account data and configure their TOEs to use these mechanisms to perform user I&A.

SuggestedRemedy

1.2.2 Proposal

Extend FIA_UAU.1 and FIA_UID.1 to allow either the TOE and/or another trusted IT product (e.g. LDAP, Kerberos) to provide I&A functionality. An example of an extended FIA_UAU.1 is provided in section 1.2.2.2. An example of an extended FIA_UID.1 is provided in section 1.2.2.3.

Additional SFR dependency rationale would need to be added to the PP to explain how these extended components replace and satisfy the dependencies of other PP SFRs on FIA_UAU.1 and FIA_UID.1.

1.2.2.1 Rationale

What's important from a security perspective is that the TOE uses trusted I&A mechanisms, not that I&A mechanisms are in the TOE. Extended component definitions which allow for both the TOE and IT environment to perform I&A provide the needed flexibility within the PP without sacrificing security.

1.2.2.2 Example Extended Component Definition for FIA_UAU.1

1.2.2.2.1 FIA_UAU.8-EXT

The Protection Profile defines the extended component FIA_UAU.8-EXT as part of the FIA_UAU family in CC part 2 for usage within this PP and instantiating ST.

This extended component is identical to FIA_UAU.1 except it allows the TOE and/or other trusted IT products to authenticate users and it has a dependency on FIA_UID.3-EXT instead of FIA_UID.1.

1.2.2.2.1.1 Component leveling

Allows a user to perform certain actions prior to authentication of the user's identity and allows the TOE and/or other trusted IT products to perform the authentication.

IEEE P2600 Hardcopy Device and System Security comments

1.2.2.2.1.2 Management: FIA_UAU.8-EXT

The following actions could be considered for the management functions in FMT:

- a) management of the authentication data by an administrator;
- b) management of the authentication data by the associated user;
- c) managing the list of actions that can be taken before the user is authenticated.

1.2.2.2.1.3 Audit: FIA_UAU.8-EXT

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- a) Minimal: Unsuccessful use of the authentication mechanism;
- b) Basic: All use of the authentication mechanism;
- c) Detailed: All TSF mediated actions performed before authentication of the user.

1.2.2.2.1.4 FIA_UAU.8-EXT Timing of trusted authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.3-EXT Timing of trusted identification

<bold>

FIA_UAU.8-EXT.1 The TSF shall allow [assignment: list of TSF-mediated actions] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.8-EXT.2 The TSF shall require each user to be successfully authenticated by [selection: the TOE, another trusted IT product] before allowing any other TSF-mediated actions on behalf of that user.

</bold>

1.2.2.3 Example Extended Component Definition for FIA_UID.1

1.2.2.3.1 FIA_UID.3-EXT

The Protection Profile defines the extended component FIA_UID.3-EXT as part of the FIA_UID family in CC part 2 for usage within this PP and instantiating ST.

This extended component is identical to FIA_UID.1 except it allows the TOE and/or other trusted IT products to identify users.

1.2.2.3.1.1 Component leveling

Allows users to perform certain actions before being identified by the TSF and allows the TOE and/or other trusted IT products to perform the identification.

1.2.2.3.1.2 Management: FIA_UID.3-EXT

The following actions could be considered for the management functions in FMT:

- a) the management of the user identities;
- b) if an authorised administrator can change the actions allowed before identification, the managing of the action lists.

1.2.2.3.1.3 Audit: FIA_UID.3-EXT

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.

- a) Minimal: Unsuccessful use of the user identification mechanism, including the user

identity provided;

- b) Basic: All use of the user identification mechanism, including the user identity provided.

1.2.2.3.1.4 FIA_UID.3-EXT Timing of trusted identification

Hierarchical to: No other components.

Dependencies: No dependencies.

<bold>

FIA_UID.3-EXT.1 The TSF shall allow [assignment: list of TSF-mediated actions] on behalf of the user to be performed before the user is identified.

FIA_UID.3-EXT.2 The TSF shall require each user to be successfully identified by [selection: the TOE, another trusted IT product] before allowing any other TSF-mediated actions on behalf of that user.

</bold>

Proposed Response *Response Status* **W**

PROPOSED REJECT.

Based on conversations with Helmut Kurth of ATSEC:

There are ways to structure the authentication process such that the HCD takes advantage of the external environment in certain ways to accomplish the identification and authentication functions. We will investigate existing PPs and STs that do this as well as "prototype" various alternatives for review.

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC 7.5.6 P 27 L 2 # 6
 Smithson, Brian Ricoh

Comment Type T Comment Status D

FIA_UAU.7 cannot be fulfilled within the TOE scope in the cases of (1) network authentication and (2) when external authentication servers are used. It does not apply in cases where credentials are not supplied by manual input (e.g. if smartcards are used for authentication). Even in the case of manual input of credentials on a local device console, feedback could be protected from view by means other than ****s (e.g. physical shield that limits observation to line-of-sight).

SuggestedRemedy

Remove FIA_UAU.7 from all four PPs:

P2600.1 7.5.6 P27 L2, 8.5.6 P46 L27, 9.5.6 P64 L27, 10.5.6 P83 L1, 11.5.6 P103 L2, 12.5.6 P122 L7, 13.5.6 P143 L16, and search also to remove references in app notes and in completeness and sufficiency tables

P2600.2 7.5.6 P27 L1, 8.5.6 P46 L15, 9.5.6 P64 L15, 10.5.6 P83 L15, 11.5.6 P103 L2, 12.5.6 P122 L7, 13.5.6 P142 L15, and search also to remove references in app notes and in completeness and sufficiency tables

P2600.3 7.5.6 P23 L7, 8.5.6 P37 L26, 9.5.6 P52 L7, 10.5.6 P66 L26, 11.5.6 P81 L26, 12.5.6 P96 L16, 13.5.6 P115 L15, and search also to remove references in app notes and in completeness and sufficiency tables

P2600.4 7.5.6 P19 L2, 8.5.6 P29 L1, 9.5.6 P39 L1, 10.5.6 P49 L16, 11.5.6 P59 L1, 12.5.6 P73 L17, and search also to remove references in app notes and in completeness and sufficiency tables

Proposed Response Response Status W

PROPOSED REJECT.

This comment was WITHDRAWN by the commenter.

Cl All P SC 7.5.7 P 28 L 3 # 1
 aubry, carmen oce

Comment Type T Comment Status D

We have agreed that it is not mandatory to offer the possibility for U.ADMINISTRATOR to modify the +Owner. Nevertheless, it is still mandatory to have the +Delegates modifiable by U.ADMINISTRATOR and I don't understand why.
 This remark concerns FMT_MSA.1.1(b) and FMT_MSA.1.1(d) and applies to Printer, Fax and DSR models for PP-A and PP-B.

SuggestedRemedy

Replace ""U.ADMINISTRATOR"" with ""[selection: U.ADMINISTRATOR, nobody]""

Proposed Response Response Status W

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC 7.5.9 P L # 47
Volkoff, Brian Hewlett-Packard Co.

Comment Type T Comment Status D
[MULTIPLE INSTANCE OF FPT_STM.1, COMMENT APPLIES TO ALL.]

1.1 Reliable Time Stamps

1.1.1 Problem Statement

In the referenced draft standard, the TOE contains the FPT_STM.1 Reliable Time Stamps security functional requirement (SFR) which requires the TOE to provide the reliable time stamp functionality. The draft standard does not allow this functionality to be supplied by a trusted component of the IT environment.

Problem 1:It's difficult for software products to comply with FPT_STM.1 since it's often the hardware (which is typically in the IT environment) or an operating system that contains the reliable time stamp functionality, not the software being evaluated. The TOE typically uses the time function provided by the IT environment.

Problem 2: Some enterprises use trusted NTP servers to obtain/maintain their system clocks across the enterprise. Here, the reliable time stamps are generated by the NTP server which typically would be part of the enterprise environment, not the TOE, unless the TOE includes the NTP server.

Problem 3: Though the PP allows demonstrable conformance, the Common Criteria will not allow ST authors to replace FPT_STM.1 with an Assumption on the environment and remain compliant with the PP.

SuggestedRemedy

1.1.2 Proposal 1

Replace FPT_STM.1 with an Assumption in the PP allowing either the TOE and/or another trusted IT product (e.g. operating system, hardware clock, NTP server) to provide the reliable time stamp functionality.

The Assumption could be as simple as:

A.TIMESTAMPS The IT environment provides reliable time stamp functionality to the TOE. (This assumption may be removed if FPT_STM.1 "Reliable time stamps" can be claimed for all TOE time stamp functionality.)

Additional SFR dependency rationale would need to be added to the PP to explain how this Assumption replaces and satisfies the dependencies of other PP SFRs on FPT_STM.1.

1.1.2.1 Rationale

What's important from a security perspective is that the TOE uses reliable time stamp functionality, not that it generates its own reliable time stamps. Since the PP claims

demonstrable conformance, ST authors can replace the assumption with FPT_STM.1 in cases where their TOE provides reliable time stamps.

=====

1.1.3 Proposal 2

Replace FPT_STM.1 with an extended component definition which extends FPT_STM.1 to allow the TOE and/or another trusted IT product to provide the reliable time stamps functionality. An example of this is provided in section 1.1.3.2.

Additional SFR dependency rationale would need to be added to the PP to explain how this extended component replaces and satisfies the dependencies of other PP SFRs on FPT_STM.1.

1.1.3.1 Rationale

What's important from a security perspective is that the TOE uses reliable time stamp functionality, not that it generates its own reliable time stamps. An extended component definition which allows for both the TOE and IT environment to generate reliable time stamps provides the needed flexibility within a TOE SFR without sacrificing security.

1.1.3.2 Example Extended Component Definition for FPT_STM.1

1.1.3.2.1 FPT_STM.2-EXT

The Protection Profile defines the extended component FPT_STM.2-EXT as part of the FPT_STM family in CC part 2 for usage within this PP and instantiating ST.

This extended component is identical to FPT_STM.1 except it allows the TOE and/or other trusted IT products to provide reliable time stamps.

1.1.3.2.1.1 Component leveling

Allows the TSF and/or other trusted IT products to provide reliable time stamps to TSF functions.

1.1.3.2.1.2 Management: FPT_STM.2-EXT

The following actions could be considered for the management functions in FMT:

a) management of the time.

1.1.3.2.1.3 Audit: FPT_STM.2-EXT

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- a) Minimal: changes to the time;
- b) Detailed: providing a timestamp.

1.1.3.2.1.4 FPT_STM.2-EXT Extended reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-A** SC P L # 54
 Chen, Nancy Oki Data

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

U.ADMINISTRATOR shall also be authorized for ""read"" operation on D.CONF.REST in SMI, NVS, DSR Access Control SFPs. Both U.ORIGINATOR and U.ADMINISTRATOR shall also be authorized for ""read"" operation on D.CONF.REST in PRT, SCN, CPY, and FAX Access Control SFPs.

The same applies to PP-B.

SuggestedRemedy

Add the missing read operation at places as indicated.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

U.ORIGINATOR should only have access to their own confidential data.

CI **PP-A** SC **11.5.5** P **103** L **14** # 24
 Sukert, Alan Xerox

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

In the FDP_ACF.1.2 AFR on line 14, it states ""...SFP governing access among subjects.DSR and controlled..."". This should be ""...SFP governing access among S.DSR and controlled...""

SuggestedRemedy

Correct this line as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-A** SC **13.5.1.2** P **137** L **11** # 26
 Sukert, Alan Xerox

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

Table 115 mentions the D.DOC.TRANSIT and D.FUNCT.TRANSIT entities. There are no such entities listed in Table 103 on page 130.

SuggestedRemedy

Resolve the inconsistency between Tables 103 and 115 as to the existence of the D.DOC.TRANSIT and D.FUNCT.TRANSIT entities.

Proposed Response Response Status **W**

PROPOSED REJECT.

It is in table 103 on page 129 intentionally presented differently, i.e. combining the information and the attribute.

CI **PP-A** SC **4** P **3** L **4** # 13
 Sukert, Alan Xerox

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

For consistency purposes, the phrase 'family of Protection Profiles' should either be stated as 'Family of Protection Profiles' or 'family of Protection Profiles'. Note that page 3, line 4 has it as 'family of Protection Profiles' while page 3, line 14 has it as 'Family of Protection Profiles'.

SuggestedRemedy

Be consistent in how the phrase 'Family of Protection Profiles' is stated within the document. I note that in the majority of the document 'Family of Protection Profiles' is used.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Use "Family"

CI **PP-A** SC **5.3** P **7** L **22** # 14
 Sukert, Alan Xerox

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

I noted that the acronym TOE is first used in this line without having been defined in the text.

SuggestedRemedy

Define the acronym TOE on this line or define it on page 7, line 7 where the term 'target of evaluation' is used.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-A** SC **5.5.1** P **8** L **9** # 15
 Sukert, Alan Xerox

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

The acronym TSP is first used in Table 1 without being defined.

SuggestedRemedy

Define the acronym TSP in Table 1

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **5.5.3** P **11** L **1** # **16**
 Sukert, Alan Xerox

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

In Table 4, there is an extra ',' after TOE in the definition of D.PROT.REST.

SuggestedRemedy

Change '...in the TOE,...' to '...in the TOE, ...' in the definition of D.PROT.REST in Table 4.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-A** SC **6.4** P **14** L **23** # **17**
 Sukert, Alan Xerox

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

I think the wording on this line is incorrect. It states "...be a suitable solution to the generic security problems described in this Protection Profile." Shouldn't it read "...be a suitable solution to the generic security problems described in this Family of Protection Profile."

SuggestedRemedy

Correct this line as indicated in the comment above.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

"...be a suitable solution to the generic security problems described in this Family of Protection Profiles."

Cl **PP-A** SC **7.5.1** P **22** L **1** # **18**
 Sukert, Alan Xerox

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

In the new Table 17 you use the term 'Delegates' several times. Did you mean that term or should this have been 'Delegates'?"

SuggestedRemedy

Resolve whether the term 'Delegates' is correct in Table 17.

Proposed Response Response Status **W**

PROPOSED REJECT.

This is correct. A delegatee is the object of a delegation.

Cl **PP-A** SC **7.5.1.1** P **22** L **1** # **25**
 Sukert, Alan Xerox

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

In the new Table 17, in the D.DOC.OUTPUT entry for +Delegates, the access control rule is missing the '=='; i.e., the rule should be ""Authorized for U.DELEGATE if D.DOC.OUTPUT(+Delegates) == U.DELEGATE(+Identifier).

The same comment applies to subclause 8.5.1.1, Table 33, page 43, line 9; subclause 9.5.1.1, Table 49, page 60, line 9; subclause 10.5.1.1, Table 65, page 79, line 1; subclause 11.5.1.1, Table 81, page 99, line 1.

SuggestedRemedy

Correct the access control rules indicated above.

Proposed Response Response Status **W**

PROPOSED REJECT.

The rule uses "▷" and is correct. It means it is contained in the set.

Cl **PP-A** SC **7.5.2** P **24** L **4** # **19**
 Sukert, Alan Xerox

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

Table 19 on page 23 indicates that there are audit recommendations for both FDP_ACF.1 and FIA_AFL.1. However, in the associated PP APP Note on page 24 only FDP_AFL.1 is listed as an optional SFR.

This same comment applies to subclause 8.5.2, page 44, line 13; subclause 9.5.2, page 62, line 13; subclause 10.5.2, page 81, line 4; subclause 11.5.2, page 101, line 4.

SuggestedRemedy

Revise the PP APP Note on the pages and lines listed above to read "...and FTA_SSL3, and optionally, FDP_ACF.1 and FIA_AFL.1."

Proposed Response Response Status **W**

PROPOSED REJECT.

The APPNOTE is correct as is because there are two auditable events (Job Completion is required and Job Initiation is recommended) for FDP_ACF.1, but the required event takes precedence in the APPNOTE.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **7.5.6** P **26** L **29** # **2**
 aubry, carmen oce

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

FIA_UAU.1.1 - The TSF shall allow [assignment: list of TSF-mediated actions that do not conflict with the essential processing elements of the PRT TOE as stated in clause 7.1.1] on behalf of the user to be performed before the user is authenticated.

FIA_UIA.1 is referencing the clause x.1.1 (which is the TOE model) but there is no requirement for user authentication in the model (these requirements are in clause x.1.2: Major security features of the TOE).

If I interpret this SFR, I can say that submitting a print job without user authentication is allowed (it is not in contradiction with 7.1.1).
 It applies to PP-A and PP-B for all the models.

SuggestedRemedy

Is it on purpose or should 7.1.2 (x.1.2) be mentioned in the SFR?

Proposed Response Response Status **W**

PROPOSED ACCEPT.

The statement needs to be revised to include x.1.1 and x.1.2

Cl **PP-A** SC **7.5.7** P **27** L **24** # **50**
 Chen, Nancy Oki Data

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

The PRT Access Control SFP rule for D.PROT.REST and D.CONF.REST depends on the security attributes +Owner, which shall be managed. Therefore, the FMT_MSA.1.1 of PRT TOE is missing the specification for the security attribute +Owner of D.PROT.REST and D.CONF.REST; not consistent with Access Control SFP. Although in CC only User Data access control SFRs depend on FMT_MSA, but if we requires some security attribute for the access control of TSF data, we should add management SFRs for the required security attribute. The same also applies to SCN, CPY, FAX, DSR TOEs.

SuggestedRemedy

Add the missed specification for management of security attribute +Owner of D.PROT.REST and D.CONF.REST in FMT_MSA.1.1 for being consistent with the Access Control SFP in each applicable TOE.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Probably will need an new attribute name for the "owner" of TSF data that is different from OWNER of document and function data.

Cl **PP-A** SC **7.5.7** P **29** L **8** # **20**
 Sukert, Alan Xerox

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

In the new FMT_MSA.1.1(c), reference to 'T.FUNCT.REST' should be to 'D.FUNC.REST'. The same comment applies to subclause 7.5.7, page 29, lines 25 & 26; subclause 10.5.7, page 86, lines 8, 25 & 26.

SuggestedRemedy

Correct this reference in the subcaluses indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-A** SC **7.5.7** P **29** L **9** # **21**
 Sukert, Alan Xerox

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

The new FMT_MSA.1.1(c) SFR states that the ability to modify the security attribute +Owner for any instance of D.FUNC.REST (see previous comment) to [selection: U.ADMINISTRATOR, nobody]. However, in Table 17 that describes the PRT Access Control SFP U.ADMINISTRATOR is not discussed at all for D.FUNC.REST like it was, for example, for D.DOC.OUTPUT. If that is the case how can you assign the ability for D.FUNC.REST to U.ADMINISTRATOR if that entity doesn't apply to D.FUNCT.REST.

The same comment applies to subclause 10.5.7, page 86, line 9 vs. Table 65; subclause 11.5.7, page 106, line 9 vs. Table 81.

SuggestedRemedy

Resolve the inconsistency between the applicable Access Control SFPs and the corresponding FMT_MSA.1.1(c) SFR as to whether U.ADMINISTRATOR can be assigned the ability to monitor the +Owner attribute.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Table 17 needs to permit the administrator to read and to delete D.FUNC.REST

Cl **PP-A** SC **8.5.6** P **47** L **17** # **22**
 Sukert, Alan Xerox

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

The reference to clause 8.1.17.1.1 here should be to 8.1.1.

SuggestedRemedy

Correct the clause reference to 8.1.1 as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **8.5.7** P **47** L **16** # **52**
 Chen, Nancy Oki Data

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

In PRT TOE, the FMT_MSA.1.1 specification expands what's specified in the PRT Access Control SFP. But here in SCN TOE, the SFR is specified to only reference the SCN Access Control SFP. For clarity, would like to see the consistency in expanding Access control SFP into SFRs. The same applies to CPY TOE, and the Information Flow Control SFP in SMI TOE.

SuggestedRemedy

Expand what's specified in the SCN Access Control SFP table, CPY Access Control SFP table and SMI Information Flow Control Table into their respective FMT_MSA.1.1

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

Cl **PP-A** SC **8.5.7** P **50** L **4** # **23**
 Sukert, Alan Xerox

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

The FMT_SMR.1.1 SFR indicates that the roles U.ADMINISTRATOR and U.ORIGINATOR shall be maintained by the TSF. Since U.DELEGATE is also included in the SCN Access Control SFR in Table 33, why isn't U.DELEGATE also maintained by the TSF?

The same comment applies to subclause 9.5.7, page 68, line 4.

SuggestedRemedy

Include the U.DELEGATE role in the list of roles maintained by the TSF for the FMT_SMR.1.1 SFR in the subclauses listed above.

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

The real problem is there shouldn't be a DELEGATE function in SCN; it will be removed.

Cl **PP-B** SC P L # **3**
 aubry, carmen oce

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

Table 113 in PP-B, SMI Information Flow Control SFP: I think that we should authorize O.DOC(+OtherTOE).TRANSIT flow (otherwise our network printers or scanners are useless). Same for D.FUNC(+OtherTOE).TRANSIT.

SuggestedRemedy

Authorize O.DOC(+OtherTOE).TRANSIT flow. Same for D.FUNC(+OtherTOE).TRANSIT.

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

Cl **PP-B** SC **11.5.5** P **102** L **6** # **37**
 Sukert, Alan Xerox

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

In the FDP_ACF.1.2 AFR on line 14, it states "...SFP governing access among subjects.DSR and controlled...". This should be "...SFP governing access among S.DSR and controlled..."

SuggestedRemedy

Correct this line as indicated above.

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

Cl **PP-B** SC **4** P **3** L **4** # **27**
 Sukert, Alan Xerox

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

For consistency purposes, the phrase 'family of Protection Profiles' should either be stated as 'Family of Protection Profiles' or 'family of Protection Profiles'. Note that page 3, line 4 has it as 'family of Protection Profiles' while page 3, line 14 has it as 'Family of Protection Profiles'.

SuggestedRemedy

Be consistent in how the phrase 'Family of Protection Profiles' is stated within the document. I note that in the majority of the document 'Family of Protection Profiles' is used.

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

Use "Family"

Cl **PP-B** SC **5.3** P **7** L **21** # **28**
 Sukert, Alan Xerox

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

I noted that the acronym TOE is first used in this line without having been defined in the text.

SuggestedRemedy

Define the acronym TOE on this line or define it on page 7, line 7 where the term 'target of evaluation' is used.

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

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-B** SC **5.5.1** P **8** L **9** # **29**
 Sukert, Alan Xerox
 Comment Type **E** Comment Status **D**
 The acronym TSP is first used in Table 1 without being defined.
 SuggestedRemedy
 Define the acronym TSP in Table 1
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **PP-B** SC **5.5.3** P **11** L **1** # **30**
 Sukert, Alan Xerox
 Comment Type **E** Comment Status **D**
 In Table 4, there is an extra ',' after TOE in the definition of D.PROT.REST.
 SuggestedRemedy
 Change '...in the TOE,,' to '...in the TOE, ...' in the definition of D.PROT.REST in Table 4.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **PP-B** SC **6.4** P **14** L **23** # **31**
 Sukert, Alan Xerox
 Comment Type **E** Comment Status **D**
 I think the wording on this line is incorrect. It states "...be a suitable solution to the generic security problems described in this Protection Profile." Shouldn't it read "...be a suitable solution to the generic security problems described in this Family of Protection Profile."
 SuggestedRemedy
 Correct this line as indicated in the comment above.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.
 "...be a suitable solution to the generic security problems described in this Family of Protection Profile."

Cl **PP-B** SC **7.5.1.1** P **21** L **9** # **32**
 Sukert, Alan Xerox
 Comment Type **E** Comment Status **D**
 In the new Table 17, in the D.DOC.OUTPUT entry for +Delegatees, the access control rule is missing the '=='; i.e., the rule should be ""Authorized for U.DELEGATE if D.DOC.OUTPUT(+Delegatees) == U.DELEGATE(+Identifier).
 The same comment applies to subclause 8.5.1.1, Table 33, page 41 line 9; subclause 9.5.1.1, Table 49, page 59 line 9; subclause 10.5.1.1, Table 65, page 78, line 2; subclause 11.5.1.1, Table 81, page 98, line 1.

SuggestedRemedy
 Correct the access control rules indicated above.
 Proposed Response Response Status **W**
 PROPOSED REJECT.
 The rule uses "⊃" and is correct. It means it is contained in the set.
 Add an APPNOTE that explains what the symbols mean.

Cl **PP-B** SC **7.5.2** P **23** L **19** # **33**
 Sukert, Alan Xerox
 Comment Type **T** Comment Status **D**
 Table 19 on page 23 indicates that there are audit recommendations for both FDP_ACF.1 and FIA_AFL.1. However, in the associated PP APP Note on page 24 only FDP_AFL.1 is listed as an optional SFR.
 This same comment applies to subclause 8.5.2, page 43, line 5; subclause 9.5.2, page 61, line 5; subclause 10.5.2, page 80, line 4; subclause 11.5.2, page 100, line 3.
 SuggestedRemedy
 Revise the PP APP Note on the pages and lines listed above to read "...and FTA_SSL3, and optionally, FDP_ACF.1 and FIA_AFL.1."
 Proposed Response Response Status **W**
 PROPOSED REJECT.
 The APPNOTE is correct as is because there are two auditable events (Job Completion is required and Job Initiation is recommended) for FDP_ACF.1, but the required event takes precedence in the APPNOTE.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-B** SC **7.5.7** P **27** L **23** # **51**
 Chen, Nancy Oki Data

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

The PRT Access Control SFP rule for D.PROT.REST and D.CONF.REST depends on the security attributes +Owner, which shall be managed. Therefore, the FMT_MSA.1.1 of PRT TOE is missing the specification for the security attribute +Owner of D.PROT.REST and D.CONF.REST; not consistent with Access Control SFP. Although in CC only User Data access control SFRs depend on FMT_MSA, but if we requires some security attribute for the access control of TSF data, we should add management SFRs for the required security attribute. The same also applies to SCN, CPY, FAX, DSR TOEs.

SuggestedRemedy

Add the missed specification for management of security attribute +Owner of D.PROT.REST and D.CONF.REST in FMT_MSA.1.1 for being consistent with the Access Control SFP in each applicable TOE.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Probably will need an new attribute name for the "owner" of TSF data that is different from OWNER of document and function data.

Cl **PP-B** SC **7.5.7** P **28** L **29** # **34**
 Sukert, Alan Xerox

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

In the new FMT_MSA.1.1(c), reference to 'T.FUNCT.REST' should be to 'D.FUNC.REST'. The same comment applies to subclause 7.5.7, page 29, lines 6 & 8; subclause 10.5.7, page 85, lines 6, 21 & 23.

SuggestedRemedy

Correct this reference in the subcaluses indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-B** SC **7.5.7** P **28** L **30** # **36**
 Sukert, Alan Xerox

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

The new FMT_MSA.1.1(c) SFR states that the ability to modify the security attribute +Owner for any instance of D.FUNC.REST (see previous comment) to [selection: U.ADMINISTRATOR, nobody]. However, in Table 17 that describes the PRT Access Control SFP U.ADMINISTRATOR is not discussed at all for D.FUNC.REST like it was, for example, for D.DOC.OUTPUT. If that is the case how can you assign the ability for D.FUNC.REST to U.ADMINISTRATOR if that entity doesn't apply to D.FUNC.REST.

The same comment applies to subclause 10.5.7, page 85, line 7 vs. Table 65; subclause 11.5.7, page 104, line 31 vs. Table 81.

SuggestedRemedy

Resolve the inconsistency between the applicable Access Control SFPs and the corresponding FMT_MSA.1.1(c) SFR as to whether U.ADMINISTRATOR can be assigned the ability to monitor the +Owner attribute.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Table 17 needs to permit the administrator to read and to delete D.FUNC.REST

Cl **PP-B** SC **8.5.7** P **47** L **12** # **53**
 Chen, Nancy Oki Data

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

In PRT TOE, the FMT_MSA.1.1 specification expands what's specified in the PRT Access Control SFP. But here in SCN TOE, the SFR is specified to only reference the SCN Access Control SFP. For clarity, would like to see the consistency in expanding Access control SFP into SFRs. The same applies to CPY TOE, and the Information Flow Control SFP in SMI TOE.

SuggestedRemedy

Expand what's specified in the SCN Access Control SFP table, CPY Access Control SFP table and SMI Information Flow Control Table into their respective FMT_MSA.1.1

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-B** SC **8.5.7** P **48** L **24** # **35**
 Sukert, Alan Xerox

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

The FMT_SMR.1.1 SFR indicates that the roles U.ADMINISTRATOR and U.ORIGINATOR shall be maintained by the TSF. Since U.DELEGATE is also included in the SCN Access Control SFR in Table 33, why isn't U.DELEGATE also maintained by the TSF?

The same comment applies to subclause 9.5.7, age 65, line 28.

SuggestedRemedy

Include the U.DELEGATE role in the list of roles maintained by the TSF for the FMT_SMR.1.1 SFR in the subclauses listed above.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

The real problem is there shouldn't be a DELEGATE function in SCN; it will be removed.

Cl **PP-C** SC P L # **55**
 Chen, Nancy Oki Data

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

U.ADMINISTRATOR shall also be authorized for ""read"" operation on D.CONF.REST in the Access Control SFPs of all TOEs.

The same applies to PP-D

SuggestedRemedy

Add the missing read operation at places as indicated.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-C** SC P L # **4**
 aubry, carmen oce

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

Table 103 in PP-C SMI Information Flow Control SFP: I think that we should authorize O.DOC(+OtherTOE).TRANSIT flow (otherwise our network printers or scanners are useless). Same for D.FUNC(+OtherTOE).TRANSIT.

SuggestedRemedy

Authorize O.DOC(+OtherTOE).TRANSIT flow. Same for D.FUNC(+OtherTOE).TRANSIT.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-C** SC **4** P **3** L **4** # **38**
 Sukert, Alan Xerox

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

For consistency purposes, the phrase 'family of Protection Profiles' should either be stated as 'Family of Protection Profiles' or 'family of Protection Profiles'. Note that page 3, line 4 has it as 'family of Protection Profiles' while page 3, line 14 has it as 'Family of Protection Profiles'.

SuggestedRemedy

Be consistent in how the phrase 'Family of Protection Profiles' is stated within the document. I note that in the majority of the document 'Family of Protection Profiles' is used.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Use "Family"

Cl **PP-C** SC **5.3** P **7** L **21** # **39**
 Sukert, Alan Xerox

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

I noted that the acronym TOE is first used in this line without having been defined in the text.

SuggestedRemedy

Define the acronym TOE on this line or define it on page 7, line 7 where the term 'target of evaluation' is used.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-C** SC **5.5.1** P **8** L **9** # **40**
 Sukert, Alan Xerox

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

The acronym TSP is first used in Table 1 without being defined.

SuggestedRemedy

Define the acronym TSP in Table 1

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-C** SC **5.5.3** P **10** L **11** # **48**
 Chen, Nancy Oki Data

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

Figure 4 Objects(Assets) diagram includes User Function Data which is not an asset for environment C.

SuggestedRemedy

Delete User Function Data from the Objects(Assets) diagram.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-C** SC **7.5.7** P **24** L **23** # **41**
 Sukert, Alan Xerox

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

FMT_SMR.1.1 indicates that the TSF maintains the roles of U.ADMINISTRATOR and U.ANONYMOUS. It is not clear why the TSF has to maintain the U.ANONYMOUS role because it doesn't appear in either the PRT Access Control SFP or in any of the other SFRs except this one.

This same comment applies to subclause 8.5.7, page 39, line 7; subclause 9.5.7, page 53, line 18; subclause 10.5.7, page 68, line 7; subclause 11.5.7, page 83, line 7.

SuggestedRemedy

Consider revising FMT_SMR.1.1 in the indicates subclauses above to only require that the TSF maintain the U.ADMINISTRATOR role.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-D** SC P L # **5**
 aubry, carmen oce

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

Table 76 in PP-Dù SMI Information Flow Control SFP: I think that we should authorize O.DOC(+OtherTOE).TRANSIT flow (otherwise our network printers or scanners are useless). Same for D.FUNC(+OtherTOE).TRANSIT.

SuggestedRemedy

Authorize O.DOC(+OtherTOE).TRANSIT flow. Same for D.FUNC(+OtherTOE).TRANSIT.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-D** SC **4** P **3** L **4** # **42**
 Sukert, Alan Xerox

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

For consistency purposes, the phrase 'family of Protection Profiles' should either be stated as 'Family of Protection Profiles' or 'family of Protection Profiles'. Note that page 3, line 4 has it as 'family of Protection Profiles' while page 3, line 14 has it as 'Family of Protection Profiles'.

SuggestedRemedy

Be consistent in how the phrase 'Family of Protection Profiles' is stated within the document. I note that in the majority of the document 'Family of Protection Profiles' is used.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Use "Family"

Cl **PP-D** SC **5.3** P **7** L **21** # **43**
 Sukert, Alan Xerox

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

I noted that the acronym TOE is first used in this line without having been defined in the text.

SuggestedRemedy

Define the acronym TOE on this line or define it on page 7, line 7 where the term 'target of evaluation' is used.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-D** SC **5.5.1** P **8** L **9** # **44**
 Sukert, Alan Xerox

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

The acronym TSP is first used in Table 1 without being defined.

SuggestedRemedy

Define the acronym TSP in Table 1

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-D** SC **7.5.7** P **20** L **20** # **45**
Sukert, Alan Xerox

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

FMT_SMR.1.1 indicates that the TSF maintains the roles of U.ADMINISTRATOR and U.ANONYMOUS. It is not clear why the TSF has to maintain the U.ANONYMOUS role because it doesn't appear in either the PRT Access Control SFP or in any of the other SFRs except this one.

This same comment applies to subclause 8.5.7, page 30, line 15; subclause 9.5.7, page 40, line 15; subclause 10.5.7, page 50, line 25; subclause 11.5.7, page 60, line 15.

SuggestedRemedy

Consider revising FMT_SMR.1.1 in the indicates subclauses above to only require that the TSF maintain the U.ADMINISTRATOR role.

Proposed Response Response Status **W**

PROPOSED ACCEPT.