

**IEEE P2600 Meeting #38**  
**September 9-10, 2008**  
**Sharp, Arlington, VA**

September 19, 2008

**1. Attendees**

Helmut Kurth*	atsec
Nick Del Re	Canon
Lee Farrell	Canon
Jon Huber	HP
Don Wright	Lexmark
Carmen Aubry*	Océ
Nancy Chen	Oki Data
Jan Walter	Peerless
Brian Smithson*	Ricoh
Shah Bhatti	Samsung
Peter Cybuck	Sharp
Akihiko Iwasaki	Sharp
Ron Nevo	Sharp
Takanori [Tony] Yoshimura	Sharp
Sameer Yami	Toshiba
Alan Sukert	Xerox

\* via telephone

**2. Administrivia**

Don Wright led the meeting and provided the planned agenda topics:

- Welcome & Introductions
- Update and Approve Agenda
- Review and approve August Minutes
- IEEE Patent Policy Review
- 2008 Meeting Schedule
- Update on TCG (Volkoff)
- Update on INCITS CS1 Working Group (Thrasher)
- Update of CC Vendor's Forum (Sukert)
- Review of Action Items from August Meeting
- PP Evaluation ad hoc status (Nevo)
- Protection Profiles version 38 versus version 37
  - \* Comments
- Sponsor ballot Comments
  - \* PP-A
  - \* PP-B
  - \* PP-C
  - \* PP-D
- Issues raised on e-mail
- Guide to P2600 PPs ad hoc status (Sukert)

- Production Printing Profile (Sukert)
- Schedule Review
- Other items
- Posting and Comment deadlines for the October Meeting
- Next meeting details

### **3. Review and approve August Minutes**

There were no objections to the Minutes.

### **4. Review IEEE Patent Policy**

Don presented the “Participants, Patents, and Duty to Inform” slide:

- All participants in this meeting have certain obligations under the IEEE-SA Patent Policy.  
Participants:
  - \* “Shall inform the IEEE (or cause the IEEE to be informed)” of the identity of each “holder of any potential Essential Patent Claims of which they are personally aware” if the claims are owned or controlled by the participant or the entity the participant is from, employed by, or otherwise represents
    - “Personal awareness” means that the participant “is personally aware that the holder may have a potential Essential Patent Claim,” even if the participant is not personally aware of the specific patents or patent claims
  - \* “Should inform the IEEE (or cause the IEEE to be informed)” of the identity of “any other holders of such potential Essential Patent Claims” (that is, third parties that are not affiliated with the participant, with the participant’s employer, or with anyone else that the participant is from or otherwise represents)
  - \* The above does not apply if the patent claim is already the subject of an Accepted Letter of Assurance that applies to the proposed standard(s) under consideration by this group  
*(Quoted text excerpted from IEEE-SA Standards Board Bylaws subclause 6.2)*
- Early identification of holders of potential Essential Patent Claims is strongly encouraged
- No duty to perform a patent search

He provided a few IEEE Patent Policy related links, saying that all participants should be familiar with their obligations under the IEEE-SA Policies & Procedures for standards development:

- Patent Policy is stated in these sources:
  - \* IEEE-SA Standards Boards Bylaws  
<http://standards.ieee.org/guides/bylaws/sect6-7.html#6>
  - \* IEEE-SA Standards Board Operations Manual  
<http://standards.ieee.org/guides/opman/sect6.html#6.3>
  - \* Material about the patent policy is available at  
<http://standards.ieee.org/board/pat/pat-material.html>

### **5. Call for Potentially Essential Patents**

Don provided an opportunity for WG members to identify or disclose patents that any WG member believes may be essential for the use of the P2600 standard. No one responded.

## **6. IEEE Meeting Guidelines**

The list of Other Guidelines for IEEE WG Meetings was presented and reviewed with the group:

- All IEEE-SA standards meetings shall be conducted in compliance with all applicable laws, including antitrust and competition laws
- Don't discuss the interpretation, validity, or essentiality of patents/patent claims
- Don't discuss specific license rates, terms, or conditions
  - \* Relative costs, including licensing costs of essential patent claims, of different technical approaches may be discussed in standards development meetings
  - \* Technical considerations remain primary focus
- Don't discuss or engage in the fixing of product prices, allocation of customers, or division of sales markets
- Don't discuss the status or substance of ongoing or threatened litigation
- Don't be silent if inappropriate topics are discussed ... do formally object

## **7. 2008 Meeting Schedule**

Don listed the remaining dates for P2600 meetings this year:

- Oct 24                                      Lexington, KY [Lexmark]
- Dec 11-12                                  Plantation, Florida [Equitrac]

## **8. Update on Trusted Computing Group (TCG) Hardcopy Working Group (HCWG)**

Jon Huber announced that Brian Volkoff has been reassigned, and will no longer be participating in the IEEE 2600 meetings. Jon will be taking his place at these meetings. However, Jon was not aware of what will happen with regard to Brian's role as the Chair of the TCG HCWG.

Don Wright said that he is not aware of any recent meetings that the TCG HCWG group has had.

There was no activity to report.

## **9. Update on INCITS CS1 Working Group**

Don Wright reported, based on some material provided by Jerry Thrasher. He referenced some of the CS1 topics that might be of interest to P2600:

- CS1 Project -- Small Organization Baseline Information Security Handbook (this project is still in process at INCITS)
- Presentation of the NIST proposal for a new project in CS1 – The Policy Machine
- (no further update, likely to be next discussed at 1st meeting of next year, still discussing how to proceed)

He also mentioned some of the activities related to the Common Criteria:

- ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security – Part 2: Security functional components  
→ published
- ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security – Part 3: Security assurance components  
→ published

- ISO/IEC 15408-1  
(still working through the last steps in ISO process)
- ISO/IEC DTR 15446:2008-06-25 Information technology – Security techniques -- Guide for the production of Protection Profiles and Security Targets  
(CS1 voted to approve without comment)

...and some of the topics at the September meeting that might be of interest to P2600:

- ISO/IEC 1st CD 27033-1, Information technology – Security techniques – Network security – Part 1: Guidelines for network security  
→ Voted to disapprove with comments
- ISO/IEC 3rd WD 27033-2 (18028-2) – Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security  
→ WD sent for review, CS1 provided comments on the draft
- ISO/IEC 2nd WD 27033-3 – Information technology – Security techniques - Network security Part 3: Reference network scenarios Risks, design techniques and control issues  
→ WD sent for review, CS1 provided comments on the draft

## **10. Update of CC Vendor's Forum**

Alan Sukert reported that the e-mail discussions within the Common Criteria Vendor's Forum have been limited to logistical items relating to the upcoming ICCV conference. He said there was nothing of importance to share.

## **11. Review of Action Items from Previous Meeting**

Don Wright led a review of the 2008-09-08 Action Item spreadsheet, which was updated during the meeting to reflect the latest status.

Only two items – 246 and 477 – were not complete.

Item 246, “Find out what copyright license terms could be offered on an IEEE std and what that means for a published Protection Profile” remains partially open.

Item 477, “explain how if trusted path functions are performed by a third-party NIC, it must be evaluated as part of the TOE or it must be a certified product that is composed with the TOE (see P2600A\_2008\_08\_v05.pdf comment #9)” remains open.

## **12. PP Evaluation ad hoc Committee Status**

Ron Nevo indicated that there have been no changes since the previous meeting status.

Peter Cybuck noted that there haven't been any questions or issues submitted to atsec.

Don reminded everyone that each of the 14 company sponsors should have received a copy of the IEEE license agreement for 10 copies of the P2600 standard documents. This agreement will need to be signed by each company and returned to the IEEE.

### **13. Protection Profiles – Comments on version 38 versus version 37**

Don Wright led the review of comments submitted on the latest drafts of the Protection Profile documents. There were many comments requiring changes for consistency of text, clarification, or correcting cut/paste errors. They did not cause notable discussion and were accepted as proposed—or with only slight modification. These and the comments that were withdrawn or did not generate any extensive discussion are not included in the list below.

All responses agreed to by the group were recorded by Don for subsequent publication on the website.

#### **Comment #37**

"In environment C, only Administrators are identified, authenticated, and authorized.

Currently Table 8 - Organizational Security Policies for the TOE:

P.USER.AUTHORIZATION states that all users will be authorized.

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

#### *SuggestedRemedy*

If not proposing a change of environment C security objectives, then -  
Change the 'user' to 'Administrator' in the policy.  
Make corresponding change to Table 13 on page 14."

➔ Nancy Chen was not convinced that every user in environment C requires some sort of authorization. In some cases, the user is only required to "be there". What type of "authorization" is the device required to implement to satisfy this goal? How do we measure it?

Brian Smithson agreed that Nancy had a good point. On the other hand, he noted that in some environments classified as environment, a password, credit card, or some other means (e.g., putting a coin in a coin drop) is required. He suggested that the comment remained unresolved for further consideration.

Helmut Kurth suggested that the authentication and/or authorization *might* be enforced outside the TOE (e.g., by the IT or physical environment or the operating system.) Brian noted that this is [somewhat] mentioned in PP-C.

➔ It was agreed that Normal Users are authorized (but not necessarily identified or authenticated) in environment C. For example, they might be authorized by having put coins in a coin drop, or by virtue of being allowed to join a WiFi network at a hotspot.

Authorization of USERS may be done by the environment (IT or physical). HCDs may choose to provide additional functionality in their corresponding ST. Authorization of ADMINISTRATORS will still need to be done by the TOE itself or by the TOE in conjunction with a trusted IT system.

#### **Comment #104**

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

#### *SuggestedRemedy*

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

→ Accept

During this comment review, Carmen Aubry noted that there is some issue about the interpretation of a “channel” vs. an “interface”. She said that she would submit her concerns as a comment later.

Comments #3, 25, and 4 (and other related comments) were all rejected – based on the discussion and rejection of Comment #5 (below).

#### Comment #23

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

#### *SuggestedRemedy*

Change the definition of P.SOFTWARE.VERIFICATION to:

‘To detect malfunction of the TOE security functions, procedures will exist to self-verify the executable code in the TOE that is critical to the security functionality of the TOE.’”

→ Agree in principle. Change the definition to: “To detect malfunction of the *TSF*, procedures will exist to self-verify executable code in the *TSF*.”

#### Comment #5

“The objectives O.DOC.NO\_DIS and O.DOC.NO\_ALT as currently defined are too generalized -- and therefore difficult to address appropriately -- especially when applied to removable NVS.

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

#### *SuggestedRemedy*

Replace O.DOC.NO\_DIS and O.DOC.NO\_ALT with the following four objectives:

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

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

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

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

Also add the following comment:

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

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

➔ Helmut Kurth explained that he knows of two mechanisms that address the objectives O.DOC.NO\_DIS and O.DOC.NO\_ALT for removable NVS.

Mechanism 1: whole disk encryption. This will protect from modification. However, it won't protect from restoring a previous version.

Mechanism 2 requires a "key" authentication for writing on the disk or retrieving the data.

Lee Farrell tried to explain that the objectives do not address the differences between the NVS being attached and operational to the TOE vs. being outside and not operational.

Brian Smithson said that the current definition, "The TOE shall protect User Document Data from unauthorized alteration" should be adequate to allow the use of both mechanisms/alternatives identified by Helmut as sufficient solutions to meet the objectives.

Brian suggested that if Canon does not like the word "protect", then the group should address that issue specifically. Helmut suggested that the word "protect" is a key word that is understood by the CC evaluators, and can remain in the current objectives. However, he did suggest that the extended SFR for FTP\_CIP\_EXP.1.1 should be written as a selection for "*prevent, detect*".

It was also felt that this approach for re-writing the SFR (with "*prevent, detect*") should be applicable *both* when the NVS is attached to the TOE and when it is not—and therefore the additional objectives proposed by Canon are not necessary. Helmut feels that the existing objectives are written with sufficient precision to adequately cover the security goals for the NVS.

People were not comfortable with the word "diminishing". Helmut advised that the word "diminish" should not be used in the Profile. In response to document references that use the word "diminish" (see Section A.7.3.3 in CC Part I and page 30 of Secure Systems Limited Silicon Data Vault ® Security Target [http://www.niap-ccevs.org/cc-scheme/st/st\\_vid10018-st.pdf](http://www.niap-ccevs.org/cc-scheme/st/st_vid10018-st.pdf)), Helmut explained that Silicon Data uses the term in the Rationale section—but not in an SFR. This is rationale to explain to the evaluator that the TOE makes it too difficult for an attacker to pursue in practice, but not impossible in theory.

➔ The additional objectives proposed (and the additional corresponding threats in comment #3)—and several other related comments—were rejected. However, the group did agree to change the extended SFR FTP\_CIP\_EXP.1.1 to provide a selection for *detect* and *prevent*. It was noted that inside the TOE, access control is used to provide the protection mechanism.

Comments #6 and 26 were accepted in principle, based on the discussion and decision in Comment #5.

#### Comment #43

"FDP\_ACC.1(b), FDP\_ACF.1(b), FMT\_MSA.1(b), and FMT\_MSA.3(b)

These are the specifications of access control functions, etc. that is required in each function specified in 11.3 SFR Package functions. Including them in the PP means these security functions shall be implemented.

Whether implementing these security functions or not should not be specified since it is different by ST Authors (i.e. TOEs).

If you want to include all access control functions, etc. into ST, you should add a description into subclause 6.4.

#### *Suggested Remedy*

Remove FDP\_ACC.1(b), FDP\_ACF.1(b), FMT\_MSA.1(b), and FMT\_MSA.3(b)."

→ ACCEPT IN PRINCIPLE.

The group decided that we cannot remove the SFRs; otherwise there will be no access control for using the TOE!

However, the app note on page 20, line 11 could be refined to say “The *\_allowed\_* functions are those defined in clause 11.3 of this Standard, and the ST Author should include all such functions that are provided by a conforming TOE.”

Comment #27

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

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

*Suggested Remedy*

Define the Common Access Control SFP as:

(1) All operations to D.DOC and D.FUNC are "Denied, except for his/her own documents or function data.

(2) The write operations include Create, Modify, Delete. We need to add this definition for "write operation" in 5.3.3 where all operations are defined.

(3) Add an App. Note to clarify that all other operations not specified here are ‘allowed’.

(4) Add an App. Note for ST authors to understand that they can add stricter access control rules. An example of a stricter rule is that ‘no implementation of an operation’ is the same as ‘The operation is Denied for All Users’. If this is the case, the ST author can then add this stricter access control rule to the SFP and the TOE can still claim demonstrable compliance to the PP. Another example is when the Modify operation is implemented for D.FUNC but only Administrator is allowed to do so for all users, then the ST author can add this rule which is stricter than the standard Common Access Control SFP, and the TOE still can claim compliance to the PP.

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

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

→ Accept in principle.

Helmut explained that if we state any default rule, we have to make sure that all vendors agree that *every* device will be able to implement it. As a [preferred] alternative, Helmut suggests that ST authors should add any default rules that they would like for their device. Of course, any default rules that conflict with the objectives should be noted—and rejected—by the evaluator.

Carmen noted that it should not be possible for one user to modify another user’s documents. Helmut said that as long as it is a *controlled* operation to give a user a modify capability, then it is acceptable.

Originally, Brian wanted to add a Create Rule to the PP. However, given Helmut’s comments, he feels that it should be left to the ST author to add any desired default rules for the specific TOE. It is not true

that "all operations" are denied for non-owners (any user can read FUNC data), so we can't say that. It would be clearer to remove the app note and add the following Create rules to the AC SFP:

D.DOC | none | Create | U.NORMAL | Denied, except for his/her own documents

D.FUNC | none | Create | U.NORMAL | Denied, except for his/her own documents

➔ It is not appropriate for an application note to make an assumption about the function of the TOE. It was agreed to add an application note stating that the ST author should add a create rule appropriate for their product. It was also decided to remove the default option from the default of access control (FMT\_MSA.3).

#### Comment #44

"FDP\_RIP.1

FDP\_RIP.1 is a fulfillment of O.DOC.NO\_DIS. O.DOC.NO\_DIS is an objective to T.DOC.DIS against D.DOC.

If D.DOC is stored into NVS, attackers who are assumed in EAL3 do not have a capability to attack this asset. That means the threat does not exist.

(The current descriptions indicate that D.DOC shall be stored into NVS.)

#### *SuggestedRemedy*

Either of the two below:

1)\_NVS

Move FDP\_RIP.1 to NVS package (remove from PP)

2)\_OSP

Derive O.DOC.NO\_DIS from Objective Security Policies"

➔ Rejected. The comment was explained to mean that if D.DOC is written on external storage, then RIP.1 would not apply. However, Helmut explained that RIP.1 does apply to *any* internal storage (such as temp storage and ram buffers, etc.) on the TOE. Helmut also indicated that NIAP requires RIP.1 for government use.

#### Comment #112

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

#### *SuggestedRemedy*

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

➔ Accept in principle. It was agreed that in general the wording could be a bit more clear, such as: "This SFR is used to define the default values for access to TOE functions that are assigned to a user when that user is defined."

Also, replace "needs to be" with "should be" in two places.

#### Comment #33

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

If the assumption for 'not listed' operations' are 'denied for all users', then the App. Note on line 15-16 that states 'If a conforming TOE provides a feature for

modifying a scanned document before transmission, then the ST Author should add additional rules for D.DOC (+SCN) using the Modify operation.' must be deleted, because there is no stricter rule than 'denied for all' can be added.  
(2) Shouldn't U.ADMINSTRATOR be allowed to read his own and others' D.DOC(+SCN)?  
Note: these comments apply to SCN, FAX, and DSR packages.

*SuggestedRemedy*

See previous proposal for Common Access Control SFP."

➔ Accept in principle (see #27.) If it is desired for Administrators to be able to read others' documents, then that should be stated in the ST.

Operations that are not listed in the AC SFPs are allowable, provided that they do not conflict with operations that are listed as all of the AC SFPs of the conforming ST.

So, for example, +SCN documents cannot be Read by U.NORMAL except by the document owner, AND they cannot be deleted by U.NORMAL except for the document owner. We don't specify what U.ADMINISTRATOR can or cannot do. We also don't specify whether U.NORMAL can or cannot Modify a document (except to say that they non-owners cannot read them) because if we define a rule for Modify, then the TOE must provide a Modify feature.

**Comment #93**

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

A couple of additional points:

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

*SuggestedRemedy*

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

➔ Accept in principle. In 14.1, change last sentence end to "previewing or modifying documents before producing hardcopy output".

On App note on line 19, change the words "printing and copying" to "producing hardcopy output".

**Comment #96**

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

I contrast this with the FAX SFR Package. The FAX SFR Package description in subclause 15.1 makes a similar statement as the DSR SFR package does that the FAX SFR package may be used for specifying roles, mechanisms or rules for authorizing a

user or users to transfer ownership of a received document to one or more intended recipients. However, in the FAX Access Control SFP for +FAXIN there is no corresponding access provided to a User if receipt is authorized by another role or mechanism if the TOE provides such a function. It would seem the DSR SFR Package and FAX SFR Packages are similar in this respect, so it is not clear why the corresponding Access Control Lists are so different.

*SuggestedRemedy*

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

➔ Reject.

Brian said that it is a good point, but there is a difference between DSR and FAX:

In DSR, the originator retains ownership and may authorize others to read or modify.

In FAX, the fax administrator—if one exists—actually assigns ownership to another user, so at that point the other user is an "owner".

**ACTION:** Alan Sukert will add some text in the PP Guide that describes the administration capability to assign ownership to another user. (See comment #96)

**Comment #35**

"(1) It's not clear that whether other roles other than U.NORMAL is 'allowed' or 'denied' the access control for D.DOC(+FAXOUT).

(2) Shouldn't the U.ADMINISTRATOR be allowed to transmit D.DOC (of his own and others') to a FAXOUT interface?

*SuggestedRemedy*

Add an App. Note to clarify."

➔ Accept in principle.

(1) Rules for other roles can be added by the ST author, as long as they do not conflict with those that are in the PP/packages.

(2) If such a feature is provided by a conforming TOE, then the ST author can add D.DOC | +FAXOUT | Read | U.ADMINISTRATOR | Allowed.

An app note would help: "If a conforming TOE provides a feature that allows an administrator to manage transmission of, modify, or delete outgoing fax documents, then the ST Author should consider adding a rule to the FAX Access Control SFP such as 'D.DOC | +FAXOUT | <operations> | U.ADMINISTRATOR | Allowed', specifying Read, Modify, or Delete operations as needed." (Also see comment #27.)

**Comment #29**

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

*SuggestedRemedy*

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

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

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

➔ Nancy was concerned that the text allows the introduction of a less strict rule, if the administrator delegates ownership to a non-trusted user. However, Helmut indicated that this did not seem to be a problem. For example, if "ownership" is defined by the possession of a PIN, then the ownership can be passed without sacrificing security. He believes that the method of assigning ownership should be left up to the ST author—not specified in the PP.

➔ The comment was rejected, with the explanation that in the FAX package, ownership is actually transferred or assigned from the fax administrator to a recipient user.

#### Comment #46

"In FTP\_CIP\_EXP.1.1, FTP\_CIP\_EXP.1.2 and FTP\_CIP\_EXP.1.3, confidentiality and integrity are required regarding 'user and TSF data.'

That is, you have to store both user data and TSF data into NVS. This defines a basic function of HCD.

You described that ST Author shall define what is 'designed to be removable.' There can be a case that user data is stored in 'removable' but TSF data is stored in 'nonremovable.'

#### *SuggestedRemedy*

Treat 'user and TSF data' simply as 'data.'"

➔ Accept in principle.

It was noted that the group already addressed this case by agreeing to write FTP\_CIP\_EXP.1.1 as "user and TSF data when either are written to".

However, we should consider changing "user and TSF data" to "user or TSF data" in FTP\_CIP\_EXP.1.2 and FTP\_CIP\_EXP.1.3.

We should not refer to ALL data, because we are only trying to protect user data and TSF data. A TOE might have other data stored on NVS devices that we do not care about.

#### Comment #16

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

#### *SuggestedRemedy*

Change the phrase 'The TSF shall provide a function that ensures the confidentiality and integrity of user and TSF data...' to:

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

Also delete FTP\_CIP\_EXP.1.2 and FTP\_CIP\_EXP.1.3 (in lines 28 and 31)."

➔ Brian explained that he thinks that “ensuring confidentiality” generally means that you take reasonable steps, consistent with the expected attack level, to prevent disclosure. Similarly, he thinks that “ensuring integrity” generally means that you take reasonable steps, consistent with the expected attack level, to prevent alteration. Since alteration by deletion or random data overwrite cannot really be prevented, we also require detection of integrity violation. Initially, he was not sure that the suggestion to allow a choice of [detect, diminish, prevent] is equivalent. In particular, he pointed out that he does not know how one would evaluate “diminish.”

However, based on the discussion on Comment #5 in which Helmut explained that it is up to the evaluators to determine whether a threat is “diminished” sufficiently, the group agreed to accept in principle. (See #5.)

#### Comment #47

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

#### *SuggestedRemedy*

Change from:

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

To:

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

This also applies to PP-B.”

➔ Accept in principle. [Brian noted that this issue might be overridden by other comments.]

#### Comment #22

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

#### *SuggestedRemedy*

Change definition of FMT\_FDI\_EXP.1.1 to:

‘FMT\_FDI\_EXP.1.1 The TSF shall provide the capability to restrict data received on any Interface from being forwarded [selection: with, without] further processing by the TSF to any Shared-medium Interface.’

[This change should also apply on page 54, lines 27 and 30.]

Also remove the word ‘direct’ in the definition of FMT\_FDI\_EXP.1.2 in clauses 18.2 and 18.4 to: ‘The TSF shall restrict the ability to permit such forwarding...’”

➔ Reject. Brian noted that to require control and restriction for *anything* involving further processing would require the equivalent of an output firewall. Also, using a selection statement would allow the author to avoid using the original intent of the SFR.

Helmut said that an ST Author can add any specific limitation to any forwarding *with further processing*—and that it should *not* be included in the PP as a selection. Although Brian acknowledged

that the phrase “without further processing” is somewhat vague, he notes that this seems to be the best wording we’ve been able to come up with so far.

The suggestion for substituting the words “without human intermediation” for “without further processing” was also rejected, because there should be some automated processing features that do not require human intermediation.

## **14. Sponsor Ballot Comments**

Don Wright led the review of comments submitted for the Sponsor Ballot on the version 37 drafts of the Protection Profile documents. Many of these comments were already addressed by the group at the previous meeting. If so, they are not listed below. Nor are they listed if there was no significant discussion.

All responses agreed to by the group were recorded by Don for subsequent publication on the website.

### **14.1 PP-A**

#### **Comment #90**

“According to CC part 3, APE\_SPD.1.2C says, ‘All threats shall be described in terms of a threat agent, an asset, and an adverse action.’ In Table 6, T.DOC.ALT does not currently meet this mandate, and it should be made more explicit as to the actual threat being considered.

#### *SuggestedRemedy*

Change the definition of T.DOC.ALT from ‘User Document Data may be altered by unauthorized persons’ to ‘A user may gain read/write access to User Document Data for which they are not authorized.’ Similar changes should also be made to the definitions of T.FUNC.ALT, T.PROT.ALT, and T.CONF.ALT.”

➔ Accept in principle. The group was not convinced that the current description of the threat(s) does not meet the “threat agent, asset, adverse action” model. However, it was acknowledged that the distinction of gaining access to the data was a useful clarification.

Helmut suggested that a section of text should be added to the document to explain the threat agents in more detail.

On Wednesday, the group continued the review of the Sponsor Ballot Comments. As before, they skipped the ones that had been addressed at the previous meeting.

#### **Comment #96**

“The definition of FTP\_CIP\_EXP.1.1 uses the word “ensure” when discussing the integrity of data written to a medium. The requirement of “ensuring data integrity” has been interpreted by some to mean that the data must be \*recoverable\* to its original value. However, during discussions, the WG has indicated that the data only needs to be \*detected\* if/when the data is inadvertently or intentionally altered by unauthorized means.

#### *SuggestedRemedy*

Either one of the following:

1) Remove the phrase ‘and integrity’ from the definition of FTP\_CIP\_EXP.1.1. [NOTE: This change would not undermine the goal of integrity, because integrity checking is covered by FTP\_CIP\_EXP.1.2 and 1.3]

-- OR --

2) Modify the definition of FTP\_CIP\_EXP.1.1 to 'The TSF shall provide a function that ensures the confidentiality of and detects any lack of integrity of user and TSF data written to [assignment: media used to store the data].'

➔ It was noted that the WG had agreed yesterday to redefine FTP\_CIP\_EXP.1.1 to “The TSF shall provide a function that ensures the confidentiality and a capability to [selection: detect, prevent] off-line alteration.

However, Brian commented that FTP\_CIP\_EXP.1.2 and 1.3 will not apply if you select “detect”. He would like to reconsider how these three items interact. The “official” response to this item is deferred for further consideration.

Comments #78, 81, 92, 93, 94, 95, 98

➔ Don noted that all these comments seem to make requests that the NVS package should be removed. He said that he does not understand the request to avoid protection of the NVS.

Carmen said that it is not a matter of protection, but a matter of agreement on “sufficient” mechanisms for protection. According to NIAP, “there is wide divergence about what is good enough to protect against offline salvage attacks; some communities accept only physical destruction of the media. That is, no automated mechanism is considered sufficient”. She does not understand why we keep asking for this kind of protection for non-volatile storage “designed to be removed”.

Don pointed out that NIAP’s comment was about *salvage* attacks—and that the goal for protection that the group is attempting to address is not about *salvage*. Brian agreed.

Although some companies are declaring they have customers that are requesting this type of protection, apparently not all companies have the same customer demands. Carmen says Océ customers are not asking for encrypted *removable* NVS.

Don reminded everyone that the group has collectively decided that the whole-disk encryption method (or similar protection) was set as the minimum goal for “designed to be removable” NVS.

Brian said that we couldn’t find an adequate description of “removable” vs. “non-removable” using accepted CC language.

Brian also noted that because removable drives can be locked up in a cabinet and protected by a person with a gun, he would not object to the NVS package being removed. He feels that as currently worded, it really doesn’t apply to the [more significant, in his opinion] threat of attack on NVS that remains in the TOE overnight.

He pointed out that an ST author can also clarify the definition of “removable” to indicate which NVS devices are covered. That could include “physically removable” as well as “designed to be removable”.

Nancy said that we should not require encryption of a removable disk, if customers do not require it. A few others pointed out that because this requirement is intended for environments that are looking for security protection, it is not an unreasonable package to include.

Don suggested that we should leave the NVS package in the PP, and see if any problems arise during the PP evaluation process.

A straw poll vote to leave the package in or remove it was taken. 11 people voted to keep it in, 2 against, 1 abstained (8 to 2 with voting rights.) If during the evaluation process, significant issues arise with the package that can only be solved by the removal of the package, we will reconsider this decision.

## 14.2 PP-B

Many of the comments for PP-B were similar or identical to those in PP-A, and were quickly resolved with the same responses.

### Comment #56

"The NVS SFR Package is unnecessary. It is redundant with the requirements set out by A.ACCESS.MANAGED and OE.PHYSICAL.MANAGED--which collectively address any threat scenario identified for "Confidentiality and Integrity of Stored Data". Because the NVS device is assumed to be under adequate physical security that prevents unauthorized individuals access to the physical components of the TOE \*and\* the NVS device is considered a physical components of the TOE, the necessary protection is already covered without the need for additional SFRs.

#### *Suggested Remedy*

Remove the NVS SFR Package."

➔ It was noted that in environment B, the Profile does not require encryption of user data, but it does require encryption of TSF data. For an NVS package, if a removable NVS device is only used to hold user data—but not TSF data—then the protection requirements do not apply.

The group agreed to have the NVS package requirements only apply to the protection of TSF data stored on removable NVS.

## 14.3 PP-C

Several of the comments for PP-C were similar or identical to those in PP-A and/or -B, and were quickly resolved with the same responses.

## 14.4 PP-D

Several of the comments for PP-D were similar or identical to those in PP-A, -B, and/or -C, and were quickly resolved with the same responses.

## 15. Issues raised on e-mail

None.

## 16. Guide to P2600 PPs ad hoc Status

Alan Sukert reported that PP Guide version 38a has been posted and includes drafts of Sections 5.2.1 and 5.2.2. The current plan is to post PP Guide Version 39a for Oct P2600 Meeting by Oct 10<sup>th</sup>. Alan would also like to have drafts for all of Section 5 plus as many additional sections as are available.

He is also planning to have an initial PP Guide draft ready for final review and approval at the Dec P2600 meeting.

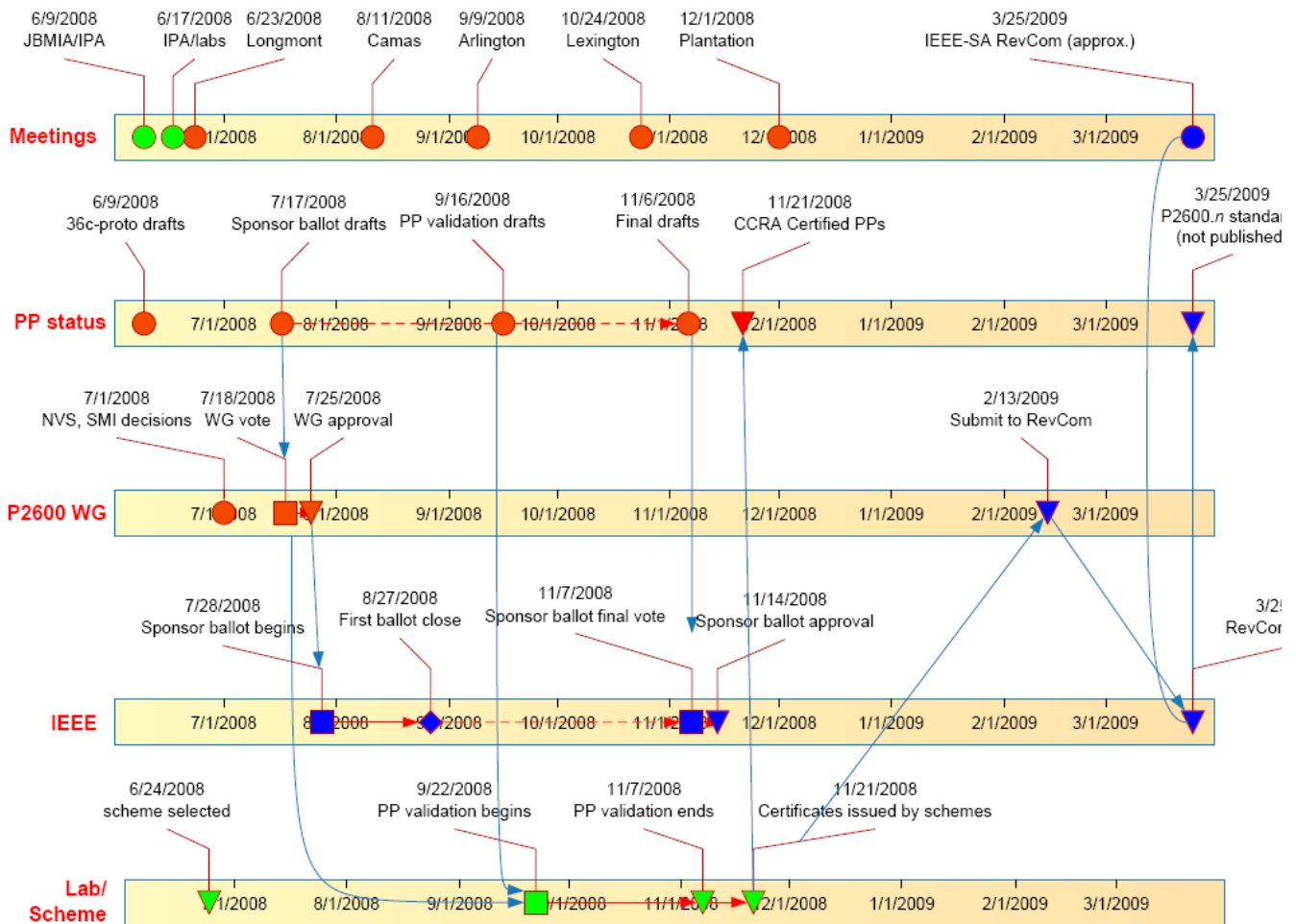
### 17. Production Printing Protection Profile

Harry Lewis was not at the meeting to provide a report. Alan Sukert mentioned that the latest plan he was aware of was to coordinate a session at the next AFP consortium meeting in early October.

### 18. Schedule Review

It was reported that BSI, the German alternative to NIAP, have indicated that based on a high level of review, they have not found any noticeable problems with the Profile documents.

It was noted that PP Validation should begin at the end of September, resulting in the schedule below:



### 19. February Meeting

The group agreed that enough work will remain to justify commitment for a meeting in February. This will be coordinated with the PWG that is also having a meeting that month.

## **20. Posting and Comment deadlines for the October Meeting**

Don reminded everyone of the following guidelines and deadlines for submitting comments:

- All PPs are under change control
  - \* All comments must be in the tool
  - \* The editor may not make changes EXCEPT based on submitted and accepted comments.
- Posting of Documents: October 10, 2008
- Posting of Comments: October 17, 2008

## **21. Next Meeting Details**

Don announced that the next meeting will be held on October 24 at the following location:

Lexmark  
Building 082  
740 W New Circle Rd  
Lexington, KY 40511

He noted that there is no hotel block reserved.

Hardcopy Device and System Security meeting adjourned.