

# IEEE P2600 Meeting #28

## August 21-22, 2007

### Holiday Inn on King, Toronto, ON, CA

#### Attendees

Chair: Don Wright, Lexmark  
Vice Chair: Lee Farrell, Canon  
Secretary / Lead Editor (PPs): Brian Smithson, Ricoh  
Lead Editor (P2600 Std.): Jerry Thrasher, Lexmark

Nancy Chen, Okidata  
Nick Del Re, Canon (day 2)  
Satoshi Fujitani, Ricoh  
Tom Haapanen, Equitrac  
Ron Nevo, Sharp  
Alan Sukert, Xerox  
Shigeru Ueda, Canon  
Brian Volkoff, HP

In the following sections, names of speakers are indicated by [brackets].  
The primary speaker for a session is noted at the beginning of the session  
as a default; others are noted in place. Some comments may appear in  
these minutes, indicated by {braces}, inserted by the Secretary for clarity.

|  |   |
|--|---|
| Attendees.....                                       | 1 |
| Administrivia [Wright] .....                         | 2 |
| Agenda review.....                                   | 2 |
| Minutes and Agenda approvals .....                   | 2 |
| IEEE patent policy .....                             | 2 |
| Inappropriate topics review .....                    | 2 |
| Officers and Editors.....                            | 2 |
| Meeting schedule updates [Wright] .....              | 2 |
| INCITS CS1 update [Thrasher].....                    | 3 |
| TCG update [Volkoff] .....                           | 3 |
| CCVF update [Sukert].....                            | 4 |
| Action items from previous meeting [Wright].....     | 4 |
| PP evaluation Decision ad hoc committee [Nevo] ..... | 4 |
| NIAP fee-for-service [Audrey Dale] .....             | 4 |
| Proposal to remove ALC_FLR.2 [Ueda].....             | 5 |
| Objections to NO_BRIDGE requirements [Ueda].....     | 5 |
| Guide to P2600 PPs [Farrell] .....                   | 5 |
| P2600 review [Thrasher].....                         | 6 |
| Review of P2600.1 (FPP-A) [Smithson] .....           | 6 |
| P2600.2/3/4 preview [Smithson] .....                 | 9 |

|   |    |
|---|----|
| PP-E status [Sukert].....                   | 11 |
| Ballot invitation and process [Wright]..... | 11 |
| Schedule [Wright].....                      | 11 |
| Next meeting [Wright] .....                 | 11 |

**\* Called to order at 9:10 AM 8/21/2007 \***

## **Administrivia [Wright]**

The following administrative items were reviewed:

### ***Agenda review***

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Aug2007.ppt>

### ***Minutes and Agenda approvals***

The July 2007 minutes were approved without changes. The August 2007 agenda was presented and approved without changes.

### ***IEEE patent policy***

Patent policy was reviewed. There were no patent disclosures made by attendees.

### ***Inappropriate topics review***

Inappropriate topics criteria were reviewed. No issues were identified.

Refer to meeting slides for detail:

<http://grouper.ieee.org/groups/2600/presentations/P2600-Aug2007.ppt>

### ***Officers and Editors***

No changes.

Officers:

Chair: Don Wright, Lexmark.

Vice Chair: Lee Farrell, Canon.

Secretary: Brian Smithson, Ricoh.

Lead editors:

Editor (P2600 Std.): Jerry Thrahser, Lexmark.

Editor (PPs): Brian Smithson, Ricoh.

### ***Meeting schedule updates [Wright]***

**Oct 24-25**, at Ricoh in Cupertino, CA

- TCG HCWG will meet there on October 23

### **Dec 6-7 (changed)**

- At Sharp's facility in/near Miami FL
- TCG to meet at same location on Dec 5

### **Tentative dates/hosts/locations for 2008**

- Feb 5-6, Canon, Orange County, with PWG
- Mar 11-12, some Japanese HCD mfr, Tokyo
- Apr 15-16, host TBD, Tucson/Phoenix, or NYC, with PWG
- May 21-22, Xerox, Rochester NY area
- Jun 25-26, InfoPrint or TBD, Boulder/Denver, with PWG

No other schedule conflicts or issues were identified during this meeting. The most current P2600 meeting information is always available at <http://grouper.ieee.org/groups/2600/meetings.html>

## **INCITS CS1 update [Thrasher]**

(INCITS CS1 web site: <http://cs1.incits.org/>)

- met in August at BAH/Washington DC
  - 1831 is still on hold (IP issue with PCI)
    - X9 doing something like PCI for financial industry
    - INCITS study group for deployable best practices for financial and insurance industries
  - 15446 in 2nd working draft
  - 15408 in final committee draft, expect to be standards by end of year
  - 15292 PP registration procedure
    - confirmation of 15292:2001
- next mtg September at Lexmark/Lexington
- TCG is being considered as a PAS submitter for fast-track approval
  - PAS=publicly available specification
  - IrDA, UPnP, are PAS submitters

## **TCG update [Volkoff]**

(TCG web site: <http://www.trustedcomputinggroup.org/>)

- concentrating on TNC because it is getting a lot of traction in the NAC/NAP arena
  - TNC aligned with Microsoft NAP
- 802.1ar working on device ID
- IETF group working on values/parameters for device health (NEA)
- in NAC, hardcopy devices are an "exception" [Thrasher]
- NAC and NAP add to device ID the health of the device to the trustfulness of the device
  - TPM is not required for TNC, but it helps

## **CCVF update [Sukert]**

(No CCVF web site)

- There will be a teleconference with NIAP today to discuss fee-for-service

## **Action items from previous meeting [Wright]**

Main action items were updated on presentation slides:

<http://grouper.ieee.org/groups/2600/presentations/P2600-Aug2007.ppt>

Action item spreadsheet was reviewed and updated:

Pre-meeting: <http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20070820.xls>

During meeting: <http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20070822.xls>

Post-meeting: <http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20070906.xls>

## **PP evaluation Decision ad hoc committee [Nevo]**

Refer to the presentation:

<http://grouper.ieee.org/groups/2600/presentations/Toronto2007/IEEE-PP-Validation-29c.ppt>

- IEEE doesn't have guidance for RFPs
  - will make RFP based on Xerox input
- need to have draft PPs (all envs) for Oct meeting
  - will ask for quotes on AB, ABC, and ABCD
- who are external comments handled and to whom are they distributed? [Ueda]
  - external comments are put in a database by a WG member on behalf of others [Wright]
  - they are distributed to WG members as usual [Wright]
- IEEE considering some kind of logo for VALIDATED products

## **NIAP fee-for-service [Audrey Dale]**

{We participated in a conference call between CCVF members and Audrey Dale of NIAP CCEVS which happened to be taking place during the P2600 meeting. Since the other participants on the conference call were not aware that the call was part of a meeting in which minutes were being taken, details of the call will not be published. If you attended this meeting and are interested in a summary of the call, contact the P2600 WG secretary.}

## Proposal to remove ALC\_FLR.2 [Ueda]

Refer to <http://grouper.ieee.org/groups/2600/email/msg00882.html> and <http://grouper.ieee.org/groups/2600/email/msg00884.html>

- objection #1: is not related to the security of the device
- objection #2: may be OK for OpEnv A, but OpEnv B is for enterprise market, large and small vendors
  - support for small vendors is different
  - may become barrier to vendor to support the PP
- propose instead that it be in the ST, not the PP
- Carmen Aubry's response is that it is important security feature [Wright]
  - CC is not just security, it is assurance [Smithson]
- is ALC\_FLR.2 part of CIM requirements? [Wright]
  - it is in basic robustness [Sukert]
- ALC\_FLR is part of the basis for doing assurance maintenance, which is beneficial and cheaper [Sukert]
- but what do we lose by not having it? or what does it cost us to have it? [Sukert]
  - you could get the benefits by just putting it in the ST, but that may weaken the PP [Smithson]
- resolved: it is only a process requirement, not so much of a burden, we will keep it for A&B [Wright]
- alan and nancy and carmen will look into is it appropriate to C&D [Wright]

## Objections to NO\_BRIDGE requirements [Ueda]

Refer to <http://grouper.ieee.org/groups/2600/email/msg00881.html>

- These objections should be handled by the new policy for SMI mediation [Smithson]

## Guide to P2600 PPs [Farrell]

Refer to

<http://grouper.ieee.org/groups/2600/presentations/Toronto2007/Guide%20to%20P2600%20PPs-29b.doc>

- culled a summary of reasons we thought about having a guide (in section 1) with details in section 3
- do we need this document?
  - I think that an informal document on the p2600 web site that only is needed until some STs have been written and some products have been certified [Smithson]
  - after the first generation of products have been done, will this still be needed? [Thrasher]

- most ST writers aren't familiar with the family structure [Sukert]
- end customer may be confused with what compliance means [Nevo]
- a web-based document that can be updated with real questions might be more useful [Smithson]
  - we could decide later to publish it as an IEEE Guide [Wright]
  - web-only is good, but will everyone be able to find it that needs it? [Sukert]
    - developers should be no problem because we can tell them, but customers would have more trouble [Smithson]
- resolved: put out a call for participants to form an ad hoc subcommittee [Wright]

## **P2600 review [Thrasher]**

Refer to

[http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE\\_P2600\\_v29a.pdf](http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE_P2600_v29a.pdf);  
[http://grouper.ieee.org/groups/2600/comment-tracking/P2600\\_2007\\_08\\_v02.pdf](http://grouper.ieee.org/groups/2600/comment-tracking/P2600_2007_08_v02.pdf);  
<http://grouper.ieee.org/groups/2600/email/msg00908.html>

- miscellaneous changes from Bellevue meeting
  - {accepted all such changes}
- compliance clause update
  - updates were based on decisions/comments from Bellevue meeting
- {various action items recorded in the action items list}

## **Review of P2600.1 (FPP-A) [Smithson]**

Refer to documents:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/P2600.1-29b.pdf>;  
<http://grouper.ieee.org/groups/2600/presentations/Toronto2007/P2600master-29a.xls>;  
<http://grouper.ieee.org/groups/2600/email/msg00899.html>;  
[http://grouper.ieee.org/groups/2600/comment-tracking/P2600-1-2007\\_08\\_v01.pdf](http://grouper.ieee.org/groups/2600/comment-tracking/P2600-1-2007_08_v01.pdf);  
<http://grouper.ieee.org/groups/2600/email/msg00883.html>;  
<http://grouper.ieee.org/groups/2600/email/msg00885.html>;  
<http://grouper.ieee.org/groups/2600/email/msg00886.html>;  
<http://grouper.ieee.org/groups/2600/email/msg00893.html>;  
<http://grouper.ieee.org/groups/2600/email/msg00895.html>;  
<http://grouper.ieee.org/groups/2600/email/msg00901.html>;  
<http://grouper.ieee.org/groups/2600/email/msg00907.html>;  
<http://grouper.ieee.org/groups/2600/comment-tracking/Sukert-Comments-P2600-1-2007-08-22.doc>;  
<http://grouper.ieee.org/groups/2600/comment-tracking/Nevo-Comments-P2600-1-2007-08-22.doc>

- {reviewed all changes implemented after Bellevue meeting}
- customer may not want all security functions, for example CPY and FAX [Ueda]
- customer can turn off those functions, but by doing that, the product is no longer in its certified state [Ueda]
- propose to allow customers to add to "complete TOE rule" that customer can change to their own requirement [Ueda]
  - our default certified configuration has functions that are typically turned off by customers, for example, I never need to authenticate to the printer at my office, but we should not eliminate the requirement to provide that function [Smithson]
  - also, by allowing vendors to certify some but not all functions, we might be opening up threats to those other functions, like if you lock three doors in your car but leave one unlocked for convenience, you have left the car wide open [Smithson]
  - we should clarify the difference between an end user turning off a function and a vendor deciding that because 95% of his customers turn it off then why certify that function [Wright]
  - we had that same issue, and the position that NIAP took for us is that if you certify with print, scan, copy, and fax, and the customer turns off fax, then the product is still considered to be certified [Sukert]
  - that assumes the security functions are independent of the capability [Farrell]
  - however, if you certify with fax turned off, and you turn fax on, then the product is not in a certified configuration [Sukert]
  - NIAP also wants you to certify the whole product [Smithson]
    - They put an addendum on policy 13 [Sukert]
  - IPA says that if you have fax, you must certify it, and if you don't have fax, then don't mention fax [Nevo]
  - There are risks on both sides. If you certify a TOE, and the administrator turns that TOE off, then there is some risk that it exposes vulnerabilities in that TOE which may not have been tested by the vendor. On the other hand, if you don't certify a TOE, there is risk that it exposes vulnerabilities outside of that TOE. I think the risk is generally lower in the first case [Smithson]
  - We originally started this FoPP structure because of this situation. How does a customer tell what certification means if a vendor can choose which functions to certify? [Thrasher]
    - The customer would need to actually read the ST [Smithson]
  - Should we put something at the end of the Complete TOE Rule that says "you can turn these functions off at your own risk"? [Wright]

- That's always true, you can buy a car with seatbelts and not wear them [Smithson]
- 90% of users don't want authentication for copy, so we are saying that 90% of users should take a risk by turning it off [Ueda]
  - We should certify that configuration, with authentication for copy turned off? [Chen]
  - That's the vendor's decision [Sukert]
  - You could define a user "anonymous" and let them use it that way [Thrasher]
  - If we re-wrote the copy PP to not require authentication and certified a product that way, then everything is OK. But if we ignore the copy TOE, that puts the customer at risk. [Smithson]
  - There are other functions that customers may want to turn off, like removing authentication for scan-to-email. Which do you choose? [Nevo]
  - It's a slippery slope, too many combinations [Thrasher]
- A customer may not want any copy security. We are forcing them to have it. [Ueda]
  - It might be possible to ship it with copy security turned off, as long as you provide instructions on how to turn it on in order to get it into the certified configuration, and you could run your own tests or perhaps extend the ST to include that configuration. [Smithson]
- You could certify it both ways, with and without [Sukert]
  - Wouldn't the lab have a problem with that? The PP says you need to have it [Wright]
  - I'll see what the lab says [Sukert]
- Even if we can do it, should we do it? We are trying to establish what amounts to a brand – P2600 – which means that customers need to only see the P2600 brand and not need to know anything else [Smithson]
- If 95% of the customers turn it off, and that exposes vulnerabilities, then we're worse off [Wright]
- The TOEs are supposed to stand alone [Del Re]
- Yes, although in practice, there are too many combinations to test [Smithson]
- Maybe we could require that if a particular vendor wants to market a product with some functions are turned off in the out-of-the-box configuration, then the vendor must test for that configuration [Smithson]
  - Would that be different from stating that the TOEs stand alone? [Wright]

- It would be up to the vendor to select a single out-of-box configuration, so you would not have so many combinations. [Smithson]
  - Another possibility is to write your own ST, maybe use the P2600 PPs as guidance, but you could not claim P2600 conformance. [Smithson]
- comment 1: In the SFPs, what is authorized? [Chen]
  - I will clarify what is authorized (binding to subject to perform ops) and when (before ops) and which (subsequent rules)
- comment 2: is OK based on 29b [Chen]
- comment 3: prot/conf assets need minimum required sets [Chen]
  - should be in the guide, because it may be different depending on the environment and it may imply implementation [Sukert]
  - even the obvious ones, like user credentials need to be CONF, may be a problem if you want to do I&A outside of the TOE and won't store creds in the TOE [Smithson]
  - resolved: send another call for contributions, make a PP app note of examples [Wright]
- {various minor comments} [Sukert]
  - I will make corrections and consider suggestions as per comments file [Smithson]

## **P2600.2/3/4 preview [Smithson]**

Refer to documents:

<http://grouper.ieee.org/groups/2600/email/msg00899.html>;

[http://grouper.ieee.org/groups/2600/presentations/Toronto2007/P2600 masterB-29a.xls](http://grouper.ieee.org/groups/2600/presentations/Toronto2007/P2600%20masterB-29a.xls);

[http://grouper.ieee.org/groups/2600/presentations/Toronto2007/P2600 masterC-29a.xls](http://grouper.ieee.org/groups/2600/presentations/Toronto2007/P2600%20masterC-29a.xls);

<http://grouper.ieee.org/groups/2600/email/msg00902.html>;

<http://grouper.ieee.org/groups/2600/email/msg00906.html>;

<http://grouper.ieee.org/groups/2600/email/msg00911.html>;

[http://grouper.ieee.org/groups/2600/presentations/Toronto2007/P2600 masterD-29a.xls](http://grouper.ieee.org/groups/2600/presentations/Toronto2007/P2600%20masterD-29a.xls)

- The master spreadsheets for B, C, and D were generated by removing rows and columns for assets, threats, policies, objectives, and SFRs that were not applicable to each of the target environments.
- Some additional work was required to remove SFRs that were dependent on primary SFRs that had been removed.
- Additional work was required to weed out audit and management recommendations that were no longer applicable because of the cumulative removal of SFRs

- The resulting security problem definitions and SFRs make sense and correspond well to the informal security requirements that we had established a while ago, which means that this whole process and model is working pretty well
  - In B, relative to A, requirements for protection of user data in transit is removed
  - The set of SFRs remains the same because we still need to protect TSF data in transit
  - In C, relative to B, all protection of user data at rest is removed except for protection of deleted documents
    - D.FUNC still appears in C? [Chen]
    - I will look into that
  - In D, relative to C, requirements for protection of deleted data disappears, and so the entire User Data class is no longer an asset; auditing goes away, and SW verification also goes away in D (but I am not sure if that is correct, I will need to check)
- So it looks like these other profiles could be generated mostly by cutting things out of A [Wright]
  - That was the idea
- We can't wait until one week before the meeting to complete these PPs [Wright]
- I was wondering if the fax-bridge requirement is needed in C, it would not be present in a self-serve environment like Kinkos [Sukert]
  - Where they have fax, it would be behind the counter, which would be environment B [Chen]
  - Fax is present in the example of a business center for environment C [Thrasher]
    - They are not public in the business center [Chen]
    - Yes they are, they are often available [Wright]
  - Does it make sense to certify? [Sukert]
  - Only if you have fax in your product, otherwise you don't need to certify it [Wright]
  - Why would you have a fax in the machine? [Thrasher]
    - Because some of your other customers want it, which means that you would want to certify it [Wright]
  - In the PP, it's covered under SMI mediation, so it's not relevant if you have fax or not [Smithson]
    - But this is in the compliance clause [Chen]
- Why do we audit job initiation? [Nevo]
  - It was requested by others, I don't think we need it [Smithson]
  - I will ask on the mailing list [Nevo]

## PP-E status [Sukert]

- We will have pp-e to review for review at the October meeting
- clause 5 mods for pp-e will or will not go into p2600 out for ballot
  - will require an amendment PAR [Wright]
  - will also ripple into clause 7 tables, and clause 10 [Thrasher]
- who is the attacker in the prod env? [Thrasher]
  - primarily internal users
- you didn't want encryption because you said you trusted users [Nevo]
  - we are working on that issue

## Ballot invitation and process [Wright]

- Sponsor ballot has started, announcements have gone out, the process works (Smithson has signed up), we have 11 people signed up
- When you join IEEE-SA and sign up for notifications, you need to specify your areas of interest and make sure that you have included P2600
- There is a custom list of affiliations? I noticed that "CC Lab" was in there [Smithson]
  - Yes, I added that, and also consultants. Vendors would be "Producers"
- Ballot formation period is 60 days. I don't think we'll be ready before then.

## Schedule [Wright]

See updated schedule on presentation slides:

<http://grouper.ieee.org/groups/2600/presentations/P2600-Aug2007.ppt>

- for next meeting:
  - all PPs, complete docs
  - form p2600 1-2-3-4 bodies (after mtg)
  - send PPs to labs for prelim
  - need par extension request (put on AI list)

## Next meeting [Wright]

- Next meeting is at Ricoh in Cupertino, on October 24-25. There will be a TCG HCWG meeting also at Ricoh on October 23 (for TCG members only). For more information, refer to:  
<http://grouper.ieee.org/groups/2600/meetings.html>.

***\* Entropy resumed at 5:10PM, 8/22/2007 \****