

# Background on the need for IEEE 2600.1 Support Documents

Status: Whitepaper

Author: Brian Smithson

Copyright © 2011 Printer Working Group

<ftp://ftp.pwg.org/pub/pwg/ids/white/2600sd-20110223.pdf>

## Background

In June 2009, IEEE Std 2600.1 was approved as an IEEE standard, certified as a Common Criteria (CC) Protection Profile (PP), and was endorsed by , the National Information Assurance Partnership Common Criteria Evaluation and Validation Service (NIAP) as the US Government Protection Profile (USGPP) for Hardcopy Devices (HCDs).

At that time, NIAP wrote its own USGPPs in a system that overlaid internationally recognized Evaluation Assurance Levels (EALs) with NIAP-specific requirements that were based on NIAP-defined “robustness” categories.

- EALs are named packages of Security Assurance Requirements (SARs), ranging from EAL1 to EAL7, and are defined in the Common Criteria part 3.
- Robustness categories – “basic”, “medium”, and “high” – are based on a two-dimensional model with highest value of resources on one axis and least-trustworthy access on the other axis.
- EALs are tailored to the suit the assurance requirements of the assets of a target of evaluation (TOE).
- Robustness is intended to also tailor the assurance requirements to the threat environment.

Using the conventional CC approach to specify security assurance requirements, IEEE 2600.1 conforms to the EAL3 package with the addition of the ALC\_FLR.2 SAR. When it was endorsed as the USGPP for HCDs, NIAP endorsed it as a PP for “basic robustness environments”.

A different approach has been taken by the Smart Card industry, primarily in Europe. Smart Card PPs use conventional EALs, often at EAL4 or EAL5, and are supplemented by “Supporting Documents” (SDs). SDs have been used by the CC to provide additional information of general interest to the CC community. The Smart Card community has developed SDs that are specific to Smart Card technologies. Some of the SDs are considered to be mandatory, and others are considered to be for guidance. Mandatory SDs can be used in conjunction with a PP to provide and enforce additional requirements for CC evaluation, and they can be applied to a specific technology (like Smart Cards) or even a specific PP (like IEEE 2600.1).

## NIAP’s new policy

In late June 2009, NIAP announced a new policy and approach to USGPPs. NIAP’s new approach employs “tailored assurance” and is intended to achieve greater reliability, consistency, and objectivity in product evaluations across multiple CC labs and CC schemes. Assurance requirements are tailored to the technology and intended use of the TOE. NIAP abandoned its “robustness” concept, and demoted all existing USGPPs to EAL2 with the intention of writing new USGPPs that augment a relatively low (or no) EAL with SARs and guidance that are tailored to the technology.

## Initial reconciliation

The P2600 WG started discussions with NIAP about how to reconcile the IEEE Std. 2600.1 Protection Profile (PP) with NIAP’s new approach to creating US Government Standard PPs.

In September 2009, NIAP agreed to continue to endorse 2600.1 as the US Government PP for Hardcopy Devices, and the vendor community agreed to work with NIAP to develop a new or revised PP using NIAP’s tailored assurance approach at an unspecified future date.

## Endorsement of IEEE 2600.2 “plus”

In June 2010, NIAP started discussions about how it might endorse 2600.2 instead of or in addition to 2600.1, possibly by augmenting 2600.2 with Security Functional Requirements (SFRs) from 2600.1. The P2600 WG expressed many concerns about any such changes::

- P2600 WG members have made substantial investments to develop, promote, and conform to 2600.1.
- Many HCD evaluations conforming to 2600.1 are being performed by a variety of labs in several different CC schemes.
- Customers have been educated about the benefits of certification conforming to 2600.1 at its assurance level, and might be confused by changes of endorsement and downgraded EAL.
- Such changes would only downgrade the EAL, but otherwise would do little to achieve NIAP's objectives for the new Standard PP approach.

Nonetheless, in November 2010, NIAP issued a policy (#20) that removed their endorsement of IEEE 2600.1 as the USGPP for HCDs, and in its place, endorsed IEEE 2600.2 plus a defined set of SFRs (taken from IEEE 2600.1) at EAL2 + ALC\_FLR.2. The policy stated that NIAP would only evaluate HCDs conforming to IEEE 2600.2. However, the policy also recognized that HCDs evaluated conforming to IEEE 2600.1 outside of the US would be acceptable to US government customers as being equivalent to HCDs that have been evaluated conforming to the USGPP.

From the customer's point of view, there are two different kinds of CC certification of HCDs that are acceptable to the US government:

1. HCDs certified to conform to IEEE 2600.2 plus additional SFRs, at EAL2 + ALC\_FLR.2 (evaluation performed anywhere)
2. HCDs certified to conform to IEEE 2600.1, at EAL3 + ALC\_FLR.2 (evaluation performed outside of the US, unless evaluation was underway when policy #20 was introduced)

## The problem

NIAP's new policy has impacted the endorsement of 2600.1, in which HCD vendors invested a great deal of time, money, and promotion. NIAP's new approach to PPs may also have a long term impact on how HCD PPs are developed by the vendor community.

## Counter-proposal

The P2600 WG has proposed to NIAP a way to reinstated endorsement of IEEE 2600.1 as the USGPP for HCDs:

*“Unlike other Standard PPs that are under development, the HCD vendor community has many evaluations that are currently underway. In the next six to nine months we expect 8-10 certificates of conformance to 2600.1, covering 30-40 MFP models, evaluated by 4-5 labs and issued by 3-4 schemes. This provides a unique opportunity to gather input from multiple lab / multiple scheme evaluations, focusing on ATE and AVA, and to work with NIAP to create Supporting Documents for 2600.1 that provide technology-specific evaluation guidance based on real-world evaluation results.*

*“Our objective is that the Supporting Documents will help NIAP achieve its vision of greater reliability, consistency, and objectivity in HCD product evaluations across multiple labs and schemes, while also providing continuity to HCD vendors and customers who see 2600.1 as a useful and practical benchmark for HCD security.”*

NIAP agreed in principle that such SDs could provide the necessary specificity and guidance to evaluators to assure NIAP that evaluations performed by different labs and schemes would have reliable, consistent, objective results. NIAP also agreed to consider reinstating IEEE 2600.1 with mandatory SDs as the USGPP for HCDs.

## **Why PWG? Why IDS?**

The P2600 WG has asked its counterparts in the IEEE-ISTO PWG to establish and perform a project to create the SDs because the PWG can create documents according to policies and procedures that are less time-consuming than those of the IEEE-SA P2600 working group, and the resulting documents can more easily be made available free of charge under PWG's copyright than under IEEE-SA's copyright.

The Imaging Device Security WG was chosen for this project because it is already involved in security-related specifications for HCDs.

## **Appendix:**

### **Acronyms:**

- SD – Supporting Document
- CC – Common Criteria
- PP – Protection Profile
- USGPP – U.S. Government Protection Profile
- HCD – Hard Copy Device
- NIAP – National Information Assurance Partnership
- CCEVS – Common Criteria Evaluation and Validation Service (of NIAP)
- EAL – Evaluation Assurance Level
- SAR – Security Assurance Requirement
- SFR – Security Functional Requirement
- TOE – Target of Evaluation
- ALC\_FLR – an SAR in the lifecycle class related to flaw remediation

### **Relevant documents and links:**

- IEEE 2600.1 – <http://standards.ieee.org/about/get/#get2600>
- Common Criteria – <http://www.commoncriteriaportal.org/cc/>
- Common Criteria supporting documents – <http://www.commoncriteriaportal.org/supporting/>
- NIAP CCEVS Consistency Instruction Manuals (“robustness environments”) – [http://www.niap-ccevs.org/pp/ci\\_manuals.cfm](http://www.niap-ccevs.org/pp/ci_manuals.cfm)
- NIAP CCEVS Policy Letter #20 – <http://www.niap-ccevs.org/policy/ccevs/policy-ltr-20.pdf>