

Hardcopy Device Protection Profiles Technical Community Update 2011

A status report and proposal for achieving the Collaborative PP vision

Brian Smithson
Ricoh Americas Corporation
28 September 2011

An updated version of the presentation may be found on
<http://grouper.ieee.org/groups/2600/presentations/12iccc/smithson-slides.pdf>.

The updated paper for this presentation may be found on
<http://grouper.ieee.org/groups/2600/presentations/12iccc/smithson-paper.pdf>.

Agenda

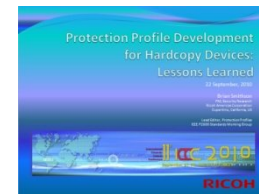
➤ In previous ICCC presentations:

The hardcopy devices PP development approach...

<http://grouper.ieee.org/groups/2600/presentations/8iccc/smithson.pdf>

...and lessons learned about PP development,
and about organizing a technical community.

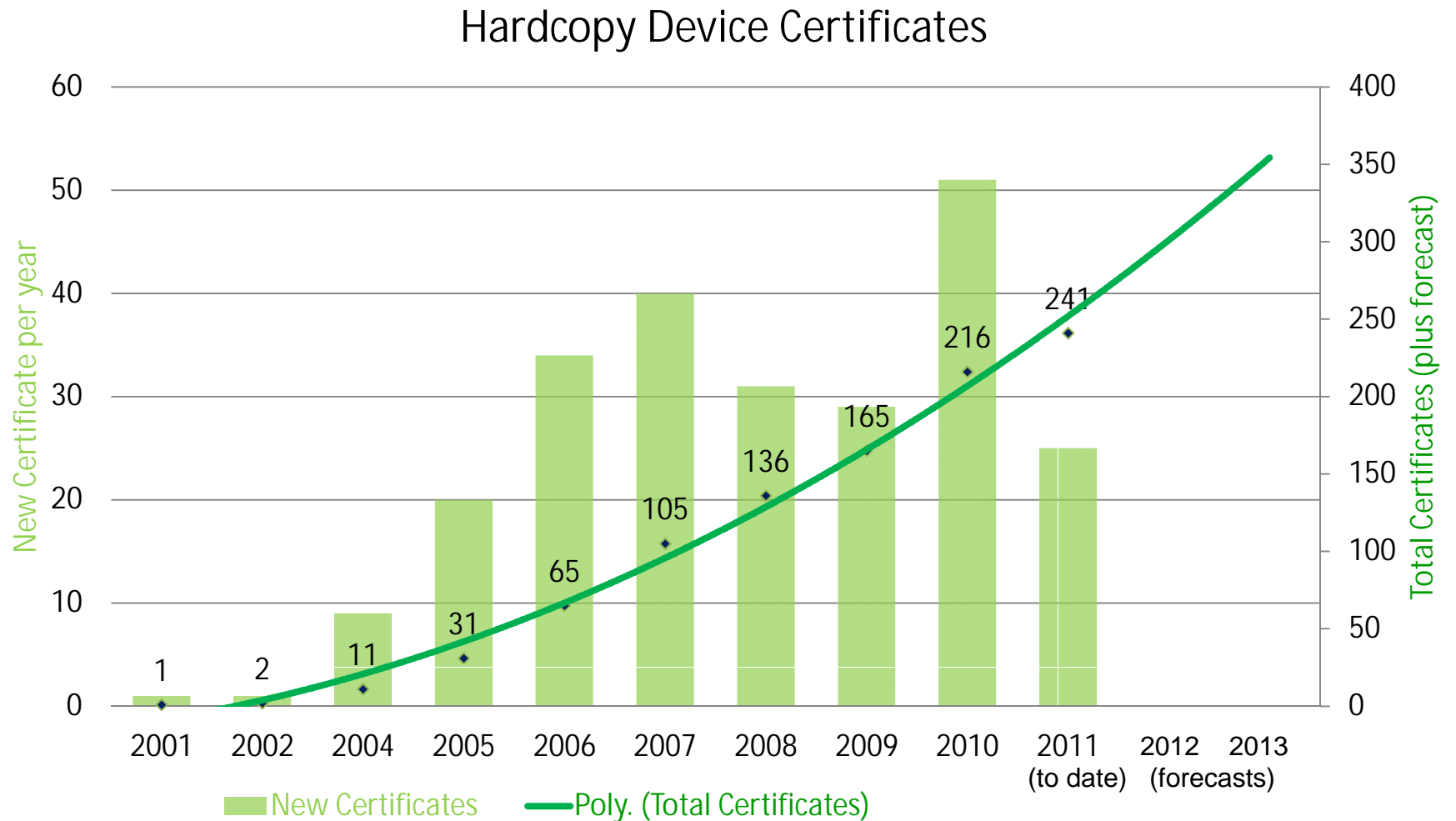
<http://grouper.ieee.org/groups/2600/presentations/11iccc/smithson.pdf>



➤ In today's presentation:

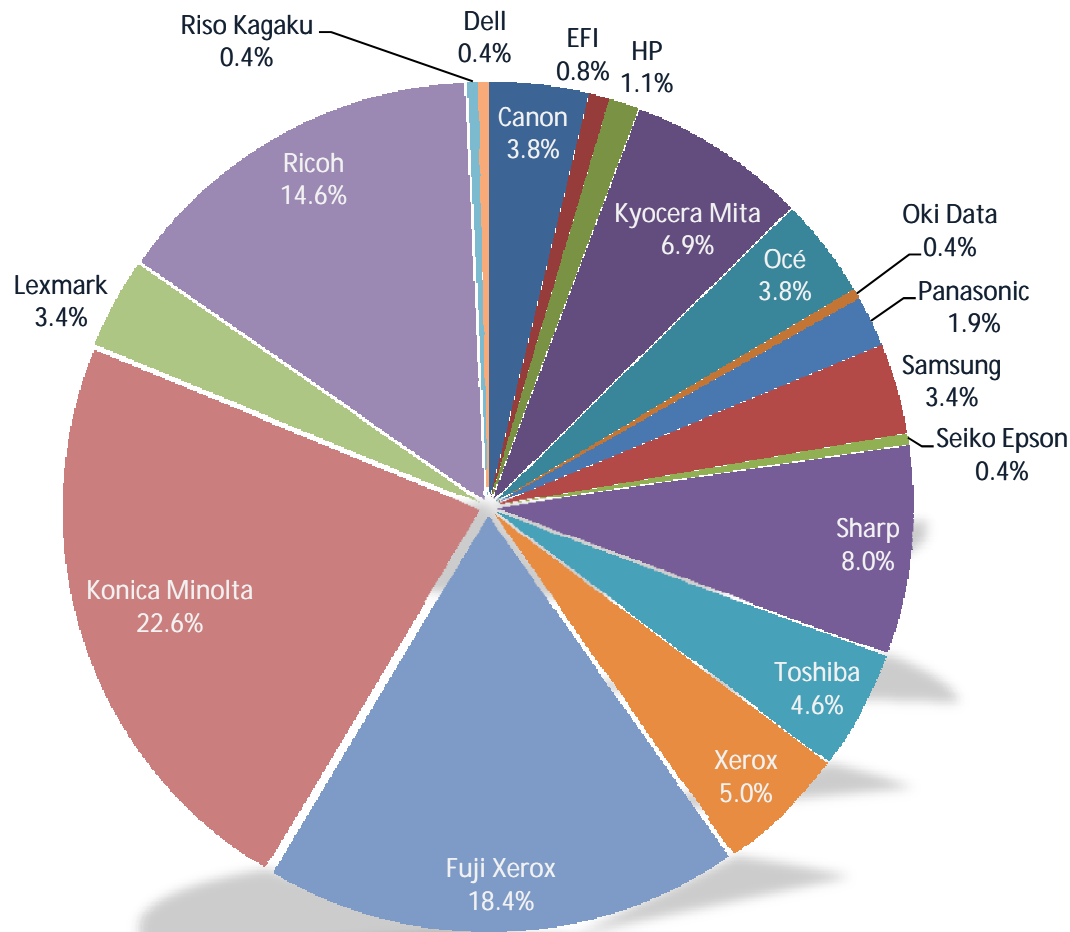
- Hardcopy Device certifications to date
- The IEEE P2600 WG and Hardcopy Device Protection Profiles
- Adoption and revision by the U.S. Government
- Evaluation and recognition issues
- Conformance trends
- What is next for Hardcopy Devices Protection Profiles?
- Concerns about the content and process of new PPs
- Proposal: High-level Protection Profile plus specific Supporting Documents

Hardcopy device certifications

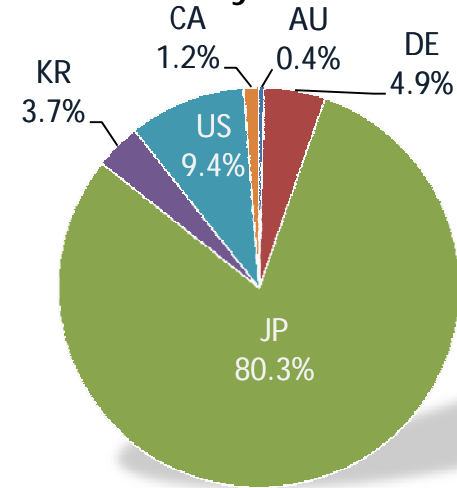


Vendors, Schemes, and EALs, 2001 to date

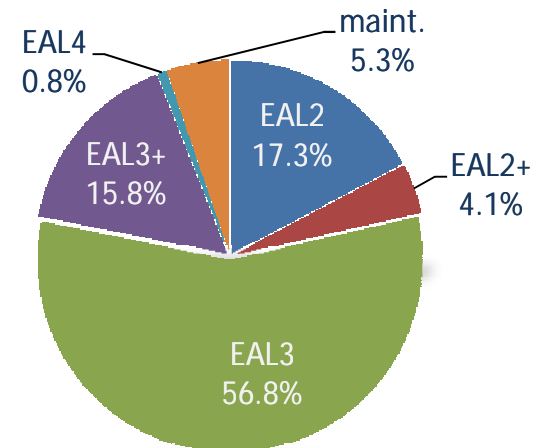
Certificates by Vendor



Certificates by Scheme

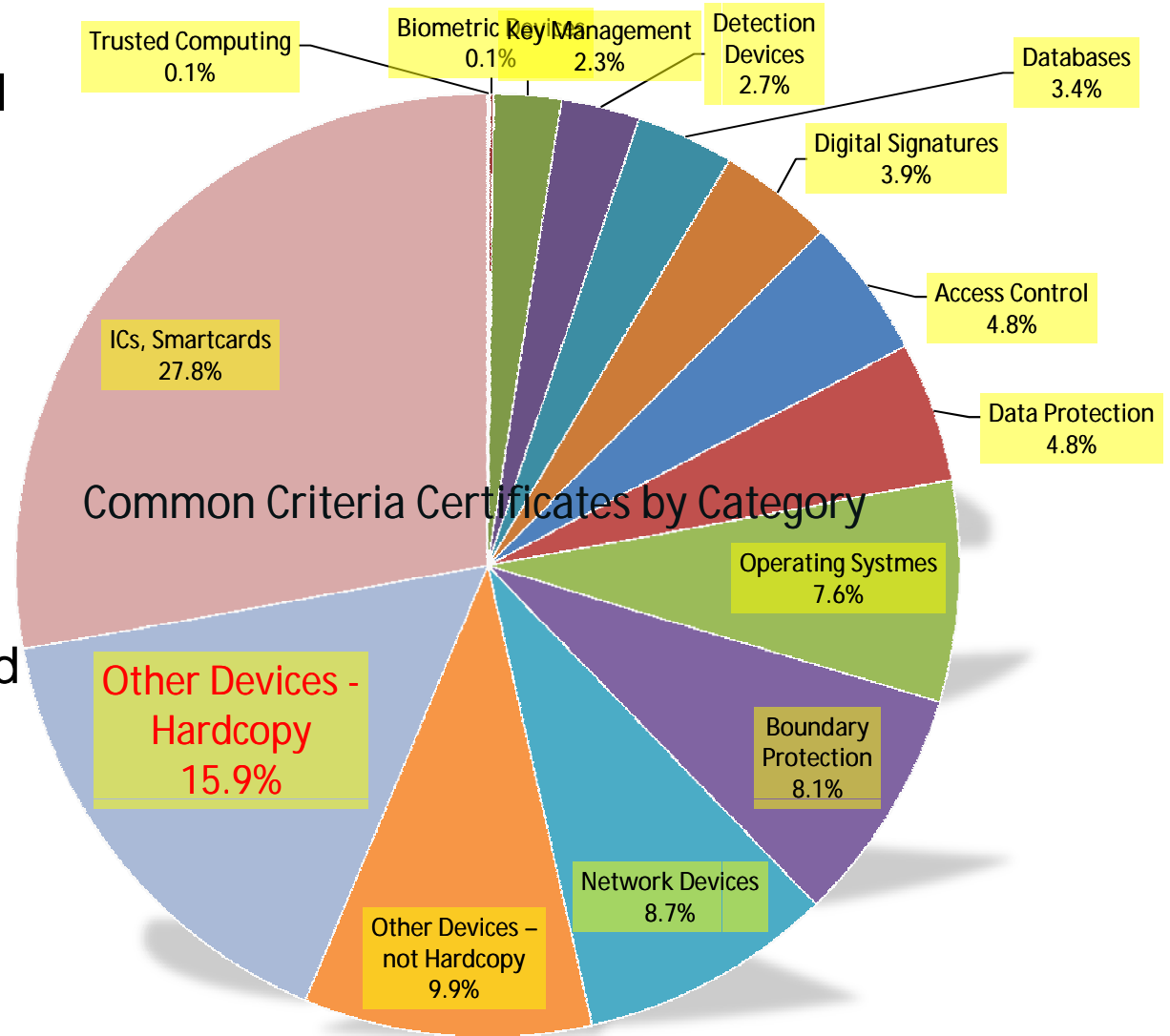


Certificates by EAL



Hardcopy devices as a TOE type

- ▶ Hardcopy devices are listed on the CC portal in the “Other Devices” category.
- ▶ Counted separately, they represent about 16% of the total of certified products.
 - ▶ Second only to smartcards!
- ▶ The CCDB has agreed to give “Hardcopy Devices” its own category.



The IEEE P2600 working group and Hardcopy Device PPs

- Technical community was formed by major hardcopy device vendors.



- IEEE 2600.1

- Issued in June, 2009
- EAL3 + ALC_FLR.2



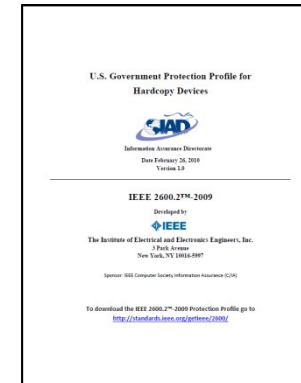
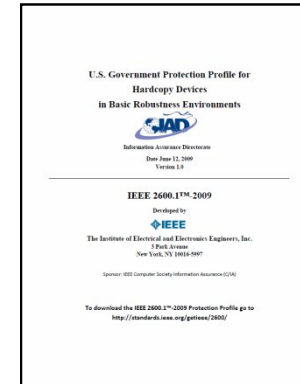
- IEEE 2600.2

- Issued in February, 2010
- EAL2 + ALC_FLR.2



Adoption and revision by the US scheme

- In June, 2009, IEEE 2600.1 was adopted as the “*U.S. Government Protection Profile for Hardcopy Devices in Basic Robustness Environments*”.
- In November, 2010, IEEE 2600.2, augmented by some SFRs from IEEE 2600.1, was adopted as the “*U.S. Government Protection Profile for Hardcopy Devices Version 1.0*”. NIAP Scheme Policy Letter #20 contains the details.

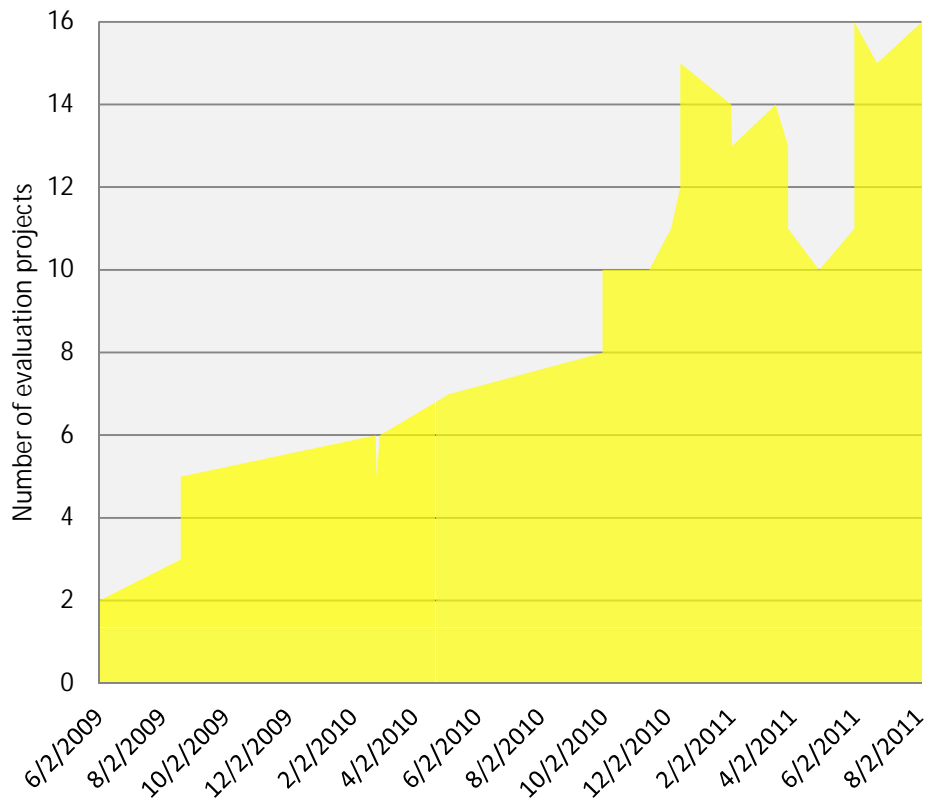


The current confusing recognition arrangement

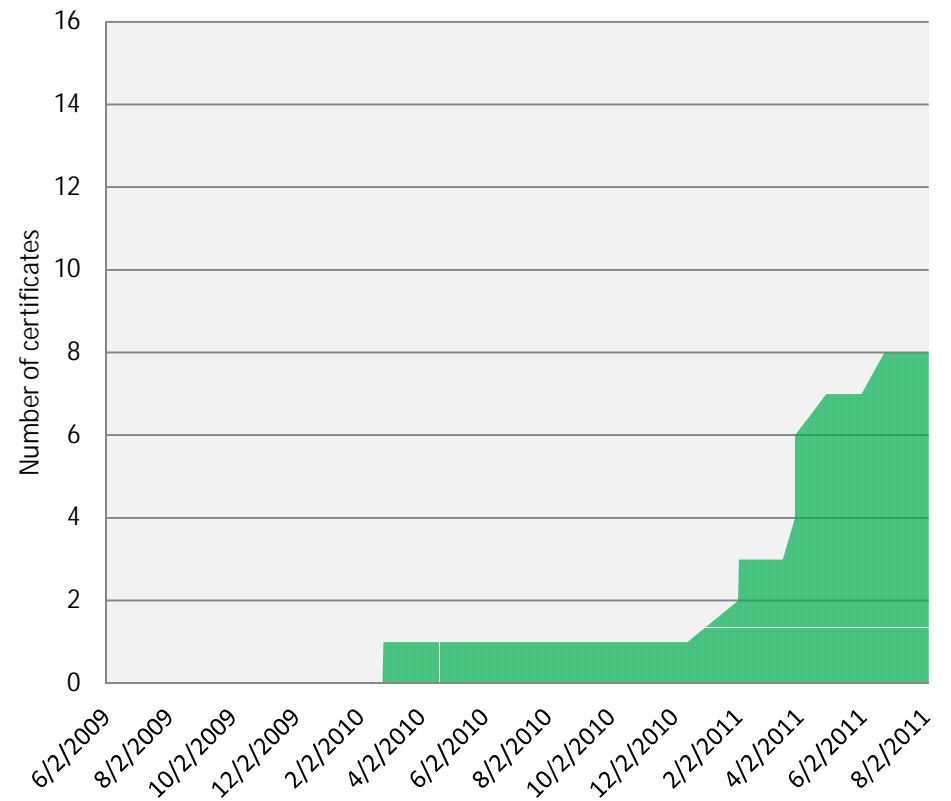
Profile	Evaluation		Recognition	
	In the U.S.	Rest of World	In the U.S.	Rest of World
IEEE 2600.1 (EAL3+)	Not allowed	Allowed	For procurement: US PP for HCDs (EAL2+, current) For CCRA: IEEE 2600.1 (EAL3+)	IEEE 2600.1 (EAL3+)
IEEE 2600.2 (EAL2+)	Allowed	Allowed	IEEE 2600.2 (EAL2+)	IEEE 2600.2 (EAL2+)
US PP for HCDs (EAL3+, archived)	No longer available	No longer available	US PP for HCDs (EAL3+, archived)	US PP for HCDs (EAL3+, archived)
US PP for HCDs (EAL2+, current)	Allowed	Allowed?	US PP for HCDs (EAL2+, current)	IEEE 2600.2 augmented ?

PP-conforming evaluations and certifications

Evaluation projects,
conforming to 2600.1 or 2600.2+P#20

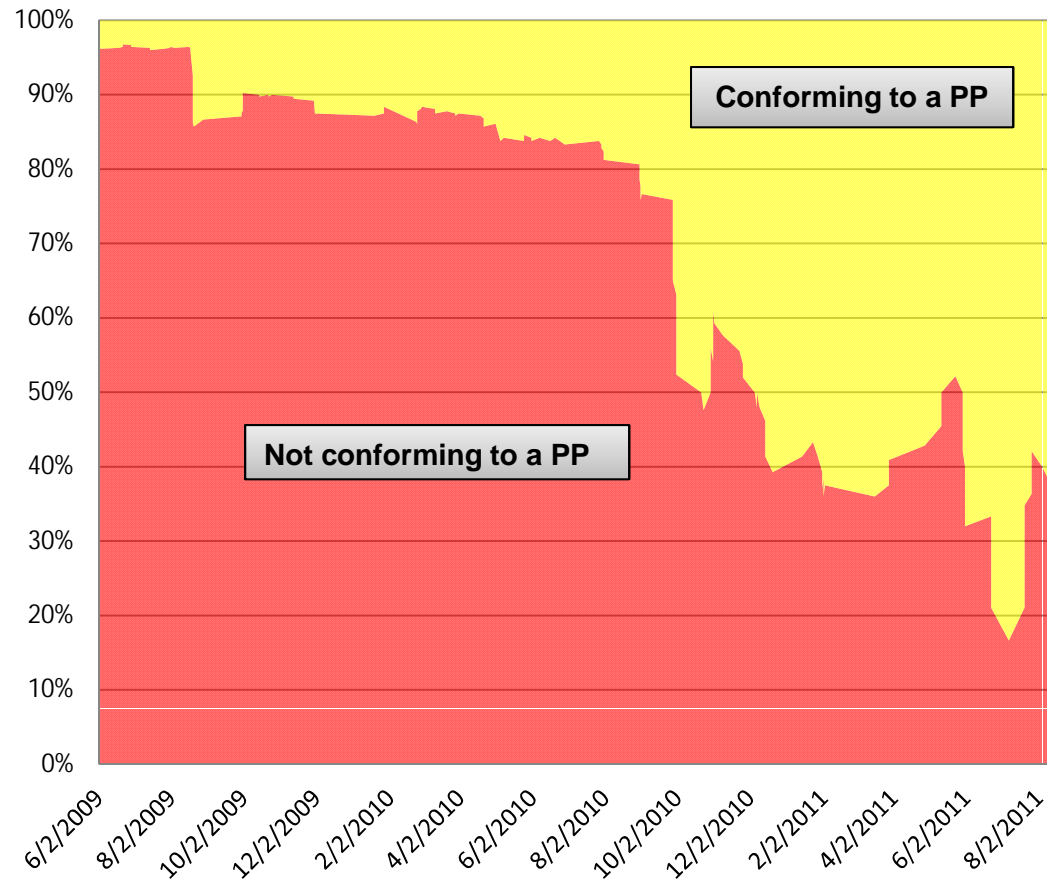


Certificates,
conforming to 2600.1 or 2600.2+P#20



New evaluation projects: PP versus no PP

Evaluation projects



What is next for Hardcopy Device PPs?

- ▶ It is not likely that the HCD technical community will write a “standard PP” for a few years.
 - ▶ The existing PPs seem to be working so far, even though the changes and existence multiple PPs with the same customer target causes some confusion.
 - ▶ It is expensive and time-consuming to create a new PP.

- ▶ Anticipating that a new PP will be written sometime in the future:
 - ✓ We can gain practical experience from using the existing PPs.
 - ✓ We could develop Supporting Documents to enhance the existing HCD PPs and to provide tailored assurance, consistent/reliable/objective evaluation, etc.
 - ✓ We sought to learn from other technical communities as they develop new PPs and Supporting Documents for their respective technologies.

A quick look at new PPs for other technologies

- ▶ Where are the Supporting Documents?
 - ▶ Instead of Supporting Documents we found many things are being incorporated directly in the new PPs.

- ▶ Concerns about the new PPs:
 - ▶ Level of detail
 - ▶ National policies
 - ▶ Vulnerability analysis requirements

- ▶ Concerns about the new PP process:
 - ▶ Evaluation on first use
 - ▶ Frequent updates

Example: FCS_RBG_EXT.1 from the NDPP

➤ This is only one SFR, plus:

- Application Note.
- Assurance Activities.
- Implementation Notes.

- Low level details obfuscate basic requirements.
- Detailed requirements can make it necessary to define extended components.
- Built-in obsolescence means frequent updates.

➤ It is replicated in several draft ESM PPs:

- Replication across multiple PPs invites:
 - Erroneous use.
 - Inconsistent updates.
 - Compatibility issues.

FCS_RBG_EXT.1 Extended: Cryptographic operation (Random Bit Generation)
FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [selection, choose one of: NIST Special Publication 800-90 using [selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES), Dual_EC_DRBG (any)], FIPS Pub 140-2 Annex C, X9.31 Appendix 2.4 using AES] seeded by an entropy source that accumulates entropy from at least one independent TSF-hardware-based noise sources. FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [selection, choose one of: 128 bits, 256 bits] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

Application Note: NIST Special Pub 800-90, Appendix C describes the minimum entropy measurement that will probably be required future versions of FIPS-140. If possible this should be used immediately and will be required in future versions of this PP.
For the first selection in FCS_RBG_(EXT).1.1, the ST author should select the standard to which the RBG services comply (either 800-90 or 140-2 Annex C).
SP 800-90 contains four different methods of generating random numbers; each of these, in turn, depends on underlying cryptographic primitives (hash functions/ciphers). The ST author will select the function used (if 800-90 is selected), and include the specific underlying cryptographic primitives used in the requirement or in the TSS. While any of the identified hash functions (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) are allowed for Hash_DRBG or HMAC_DRBG, only AES-based implementations for CTR_DRBG are allowed. While any of the curves defined in 800-90 are allowed for Dual_EC_DRBG, the ST author not only must include the curve chosen, but also the hash algorithm used.
Note that for FIPS Pub 140-2 Annex C, currently only the method described in NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, Section 3 is valid. If the key length for the AES implementation used here is different than that used to encrypt the user data, then FCS_COP.1 may have to be adjusted or iterated to reflect the different key length. For the selection in FCS_RBG_(EXT).1.2, the ST author selects the minimum number of bits of entropy that is used to seed the RBG. The ST author also ensures that any underlying functions are included in the baseline requirements for the TOE.

Assurance Activity:
The evaluator shall review the TSS section to determine the version number of the product containing the RBG(s) used in the TOE. The evaluator shall also confirm that the TSS describes the hardware-based noise source from which entropy is gathered, and further confirm the location of this noise source. The evaluator will further verify that all of the underlying functions and parameters used in the RBG are listed in the TSS.
The evaluator shall verify that the TSS contains a description of the RBG model, including the method for obtaining entropy input, as well as identifying the entropy source(s) used, how much entropy is produced by each entropy source. The evaluator shall also ensure that the TSS describes known modes of entropy source failure. Finally, the evaluator shall ensure that the TSS contains a description of the RBG outputs in terms of the independence of the outputs and variance with time and/or environmental conditions.
The evaluator shall also perform the following tests, depending on the standard to which the RBG conforms.

Implementations Conforming to FIPS 140-2, Annex C
The reference for the tests contained in this section is The Random Number Generator Validation System (RNGVS) [RNGVS]. The evaluators shall conduct the following two tests. Note that the "expected values" are produced by a reference implementation of the algorithm that is known to be correct. Proof of correctness is left to each Scheme. The evaluators shall perform a Variable Seed Test. The evaluators shall provide a set of 128 (Seed, DT) pairs to the TSF RBG function, each 128 bits. The evaluators shall also provide a key (of the length appropriate to the AES algorithm) that is constant for all 128 (Seed, DT) pairs. The DT value is incremented by 1 for each set. The seed values shall have no repeats within the set. The evaluators ensure that the values returned by the TSF match the expected values.
The evaluators shall perform a Monte Carlo Test. For this test, they supply an initial Seed and DT value to the TSF RBG function; each of these is 128 bits. The evaluators shall also provide a key (of the length appropriate to the AES algorithm) that is constant throughout the test. The evaluators then invoke the TSF RBG 10,000 times, with the DT value being incremented by 1 on each iteration, and the new seed for the subsequent iteration produced as specified in NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, Section 3. The evaluators ensure that the 10,000th value produced matches the expected value.

Implementations Conforming to NIST Special Publication 800-90
The evaluator shall perform 15 trials for the RNG implementation. If the RNG is configurable, the evaluator shall perform 15 trials for each configuration. The evaluator shall also confirm that the operational guidance contains appropriate instructions for configuring the RNG functionality.
If the RNG has prediction resistance enabled, each trial consists of (1) instantiate drbg, (2) generate the first block of random bits (3) generate a second block of random bits (4) unstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. "generate one block of random bits" means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP 800-90).
If the RNG does not have prediction resistance, each trial consists of (1) instantiate drbg, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) unstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call.
The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator.
Entropy input: the length of the entropy input value must equal the seed length.
Nonce: if a nonce is supported (CTR_DRBG with no dr does not use a nonce), the nonce bit length is one-half the seed length.
Personalization string: The length of the personalization string must be <= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is supported, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.
Additional input: the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.

Example: National policy statement in ESM PPs

- ▶ This is a statement about national policy that appears in three draft Enterprise Security Management PPs:

If cryptography is internal to the TOE, the evaluator shall verify that the product has been validated by FIPS 140-2 (if evaluating in the United States or Canada) or an equivalent national standard for the nation in which the evaluation is being conducted.

- What if it isn't being evaluated in the US or CA? What about other nations' standards?
- Why is it the nation in which the product is being evaluated, not the nation in which the it is to be sold?

- What if the product has not yet *completed* FIPS 140-2 validation during CC evaluation?

Example: Itemized vulnerabilities to appear in future PPs?

- ▶ This is a statement about vulnerability analysis from the NDPP:

- Who will collect and collate this information?
- Who will assess and maintain its relevance?

For the first generation of this protection profile, the evaluation lab is expected to survey open sources to discover what vulnerabilities have been discovered in ~~these types of products. ...~~ This information will be used in the development of penetration testing tools and for the development of future protection profiles.

- Vulnerabilities are discovered (and fixed) far more often than PPs need to be updated.
- Overspecifying AVA_VAN means either unnecessary work or frequent updates.

PPs are “living documents” and “frequently updated”?

- Frequent updates would be necessary in order to keep up with current approved implementation practices, national policies, and vulnerability trends.

- However,
 - It creates a moving target for vendors, disrupting routine and reuse.
 - Frequent updates may increase requirements bloat.
 - Common requirements would tend to drift apart, especially among different technology types.
 - Updates that occur more often than the duration of a typical product lifecycle limits the usefulness of the PP as a baseline against which customers can compare multiple products.

PPs are “evaluated and certified when they are first used”?

- Eliminating the formal validation of PPs would be necessary to keep up with frequently updates.

- However,
 - It increases project risk for the first vendor to conform to the PP.
 - It assumes that the first use of the PP is to evaluate a product in the US scheme or another scheme that permits this process.
 - Is it really equivalent to evaluating the PP first?

Proposal: A high-level PP plus specific supporting documents

p.17

- ▶ Use the PP to provide a high-level security *requirements* specification
 - ▶ Include technology-specific tailored assurance activities
 - ▶ Developed using the collaborative PP model by a technical community
 - ▶ Formally evaluated and certified by a lab under a sponsoring scheme

- ▶ Use supporting documents (SDs) to address other issues:
 1. Current best practices for implementation of security functions (mandatory)
 2. Current vulnerability trends (mandatory)
 3. Various national policies (guidance)

Benefits of a high-level PP

- It provides a clear Security Problem Definition for the TOE type.
- It is “a security specification on a relatively high level of abstraction” and “an implementation-independent statement of security needs for a TOE type”
- It is stable.
 - The hardcopy PPs are valid today, 1~2 years after publication.
 - Aside from changes in the CC itself, they could have been valid ten years ago.
 - Aside from CC changes, they might be valid ten years hence.
 - The fundamental Security Problem Definition does not tend to change.

What is missing from a high-level PP

- ▶ There are no details of:
 - ▶ Protocols to use.
 - ▶ Cryptographic algorithms, key sizes, management, random generators.
 - ▶ No mention of cryptography at all!
 - ▶ Vulnerabilities to be analyzed.
 - ▶ Nation-specific requirements.
- ▶ Assurance of appropriate implementation is judged by the evaluators

- ▶ However, it is believed that this may result in evaluations that are:
 - ▶ Too subjective.
 - ▶ Inconsistent among labs and schemes.
 - ▶ Unreliable.

- ▶ To address that, I propose specific Supporting Documents.

- Specifies or recommends current best practices for implementation of common security functional requirements.
- Includes assurance activities for those implementation practices.
- In many cases, these can (and should) span multiple technology types.
- Conditionally-mandatory conformance.

- Specifies or recommends vulnerabilities to be analyzed.
 - Tailored for each technology type.
 - Based on trends from actual vulnerability reports.
- Could recommend tools or techniques to be used.
- Mandatory conformance.

National Policy supporting documents

- Specifies or recommends national procurement requirements.
- Where possible, expressed in the style of Organizational Security Policies but implemented in the form of Application Notes.
- Developed by each nation or group of collaborating nations.
- Guidance (“if you want to sell your product here...”).

Typical conformance scenario

- ▶ A product's ST will conform to the current version of a high-level PP for its technology type.

- ▶ That PP would also require conformance to:
 - ✓ The applicable current Approved Implementation Practices SD(s)
 - ✓ The current Vulnerability Analysis SD for its technology type

- ▶ Optionally, it may conform to:
 - ✓ Optionally, one or more National Policy SDs

Conclusion

- Hardcopy devices are being successfully certified conforming to PPs, but what about the future?
- We are trying to get PPs to serve too many purposes.
- A high-level PP plus SDs is a better way to serve those purposes.
- High-level PPs are international, long-lived, and easier to write.
- Separating other requirements into SDs provides focus on issues and reduces conflicting objectives.
- Applying SDs to multiple technologies ensures uniform updating.
- SDs can be updated independently from PPs and from other SDs.

- It is a shorter path to achieving the CCDB's vision of Collaborative Protection Profile development and potentially reducing the need to adopt interim, national solutions.

Questions? Comments?

Resources

- This presentation:

<http://grouper.ieee.org/groups/2600/presentations/12iccc/smithson-slides.pdf>

- The related paper:

<http://grouper.ieee.org/groups/2600/presentations/12iccc/smithson-paper.pdf>

- IEEE P2600 Working Group: <http://grouper.ieee.org/groups/2600/>

- IEEE 2600.1 and IEEE 2600.2: <http://standards.ieee.org/getieee/2600/>

- NIAP Policy #20: <http://www.niap-ccevs.org/policy/ccevs/policy-ltr-20.pdf>

- Conforming products:

http://grouper.ieee.org/groups/2600/conforming_products.html

Thank you – Terima kasih