
# The Printer Working Group

## Imaging Device Security

November 16, 2017

Virtual Face-to-Face

# Agenda

| When | What |
|---|---|
| | |
| 9:00 – 9:10 | Introductions, Agenda review |
| 9:10 – 10:50 | Review results of Latest MFP TC Meeting |
| 10:50 – 11:00 | Wrap Up / Next Steps |

# Intellectual Property Policy

*"This meeting is conducted under the rules of the PWG IP policy".*

- Refer to the IP statements in the plenary slides

# Officers

- Chair:
  - Alan Sukert (Xerox)
- Vice-Chair:
  - Currently Vacant
- Secretary:
  - Alan Sukert (Xerox)
- Document Editors:
  - Ira McDonald (High North): HCD-TNC

# New HCD Protection Profile

- The new Protection Profile for Hardcopy Devices (PP_HCD_V1.0) was published on September 11.
- You can find it on NIAP's web site … https://www.niap-ccevs.org/pp/PP_HCD_V1.0/
- … and on IPA's (including links to both the original and the Japanese translation) https://www.ipa.go.jp/security/publications/pp-jp/hcd.html
- It is a US/Japan PP, not a "cPP" with broader international support.

# Summary of Oct 25, 2017 MFP Technical Committee Meetings

MFP TECHNICAL COMMITTEE MEETING AGENDA

- Welcome, introductions, logistics, agenda review…
- TC administrivia
- Requirements issues
- Implementation issues
- Plans and processes for updating and maintaining the HCD PP
- Summary and next steps

# Requirements issues:
# RSA key establishment in TLS

- Labgram #106 was issued, put "on hold" after lab meeting
- NIST is revising 800-56A/B/C, perhaps by mid 2018
- NIAP may or may not align with NIST; not decided yet
- Recommend that TOEs be able to disable RSA key exchange ciphersuites in evaluated configuration

# Requirements issues: Password policies

- FIA_PMG_EXT specifies password length/composition requirements
  - Requires capability to compose using upper case, lower case, numeric, and specials
  - It may be updated to require passwords to include all four types
- SP 800-171, SP 800-53, and CNSSI 1253, have more stringent requirements
  - Including password lifetime, re-use
  - These are not required for CC evaluation
- On the other hand, new SP 800-63 tosses out composition, lifetime, re-use
- Password policies could be different for normal versus admin users
  - Admins are more trusted, but admin access is more critical
  - We are looking at other PPs (e.g., GPOS, Mobile Devices) for precedents

# Requirements issues: Audit log servers

- Does FAU_STG_EXT.1 require the use of syslog protocol?
- Network Devices interpretation #1 said that syslog is *not* required
- It was accepted by NIAP, but the TD is now archived
- It should apply to the HCD PP
- A TRRT will be submitted

# Requirements issues:
# NDcPP and FDEcPP updates and TDs


- NDcPP and FDEcPP have been updated since their predecessors were used as the basis for some parts of the HCD PP
- In particular, TLS requirements were separated into TLS server and TLS client SFRs, and X.509 requirements have been added
- Technical Decisions have also been issued for NDcPP, FDEcPP, and other NIAP PPs / cPPs, that may apply to HCDs
- The HCD TC will review these and propose changes to the HCD as appropriate

# Requirements issues:
# Key Transport (FCS_COP.1(i)) AAs

- There are no assurance activities associated with FCS_COP.1(i)
- They have been added to the FDEcPP
- The TC will propose to adopt/adapt those assurance activities

# Requirements issues:
# Wi-Fi support

- HCDs support WiFi, but it is not part of HCD PP v1.0
- The WLAN EP for Mobile Devices covers this, so we may adopt/adapt requirements from that (as an option for HCDs)

# Requirements issues: Other protocols

- HCDs in customer environments use protocols that are not covered by the PP.
- To evaluate using these protocols, they must be encapsulated, but that may not be representative of how customers use them
- We are looking at
  - SNMPv3: There is a TD on this topic for NDcPP v1.0
  - S/MIME: It is covered in the Email Client PP
  - Kerberos: Maybe it would be covered in a directory server PP (not currently in development)
  - SMBv3: Not sure

# Implementation issues:
# Requirements embedded in AAs

- Some of the assurance activities impose security functional requirements that are not present in the associated SFR
- The TC will identify these and propose changes to consolidate those requirements in the SFR

# Implementation issues:
# Inconsistencies in KMD instructions

- There are some inconsistencies between the KMD instructions in the HCD PP annex and KMD-related assurance activities
- The TC will identify these and propose changes to make them consistent

# Implementation issues: Use of 3rd-party entropy sources

- There were some questions about how to describe entropy from 3rd party sources
  - Vendors cannot describe details that are unavailable to them or that would infringe on 3rd party intellectual property
- NIAP has a policy on that topic

# Implementation issues: Key destruction testing

- Key destruction testing by before-after comparison of memory dumps can be onerous
- Alternative testing methods can be proposed to NIAP for consideration
- There is a more information in a key destruction template on github

# Implementation issues:
# Use of TPMs in the HCD TOE

- Some vendors use TPMs in their products
- How can TPM crypto functions be evaluated?
- It was suggested that the DSC cPP (under development) would need to be used
- However, it’s not clear if the DSC cPP has that purpose…

# Plans and processes for updating/maintaining the HCD PP
# Internationalized crypto

- Current SFRs and Assurance Activities for cryptographic functions in HCD PP cannot be evaluated in all nations (in particular, Korea)
- The crypto WG is developing a catalog of crypto functions that we may adopt/adapt

# Plans and processes for updating/maintaining the HCD PP
## EAL claims

- The HCD PP itself is certified (by JISEC) but it does not claim conformance to EAL1
- The PP does not claim conformance to EAL1 but mentions that it contains the SARs necessary for conforming STs to claim EAL1
- We may be able to fix this in a revised PP
- However, this does not solve other EAL-related problems (EU customers if they require either EAL2+ or cPP)

# Plans and processes for updating/maintaining the HCD PP
# Versioning

- An update to HCD_PP_V1.0 that fixes problems, incorporates existing TDs and errata, but which does not add new requirements, would be V1.1
- If new requirements are added, it must be V2.0.

# Plans and processes for updating/maintaining the HCD PP
# Who does what?

- US/JP/KR schemes are resource-limited and cannot lead the effort to update the HCD PP
- The HCD TC will lead the effort and, where possible, submit fully-formed proposals for US and JP approval

# Plans and processes for updating/maintaining the HCD PP
# iTC formation and cPP development

- We will update the HCD PP as a bi-lateral (US/JP) PP, not a cPP
- There is sufficient interest from at least two schemes to start the iTC formation process, perhaps 6~12 months from now

# Wrap Up/ Next Steps

- Some volunteer assignments have been made to work these issues
- If you are interested in working on these or other issues, please contact Brian Smithson brian.smithson@ricoh-usa.com or Alan Sukert Alan.Sukert@xerox.com

# Wrap Up/ Next Steps
# HCD PP Version 1.1 Potential Topics


- Existing Technical Decisions against HCD PP Version 1.0
- Current Errata
- RSA Key Agreement – when NIST enforces NIST SP 800-131A
- Audit Log Server Requirements
- Updated requirements from NDcPP and FDEcPP
- Updated requirements from Technical Decions other than for HCD PP
- Assurance Activities (AAs) for Key Transport SFR (FCS_COP.1(i))
- Additional requirements that show up in Assurance Activities
- Inconsistencies between Key Management Descriptio (KMD) description and KMD AAs
- 3rd Party Entropy Sources
- Key Destruction SFR
- TPMs used in the TOE
- EAL Claim for HCD PP

# Wrap Up/ Next Steps
## HCD PP Version 1.1 Potential Topics

- Password Policies
- Password Policy Applicability (normal vs. admin users)
- Wi-Fi Support
- SNMPv3 Support
- Kerberos Support
- S/MIME Support
- SMBv3 Support
- Internationally-friendly crypto requirements that don't rely on FIPS