The Printer Working Group

Imaging Device Security

April 18, 2019

PWG April 2019 Virtual Face-to-Face

Agenda

When	What
9:00 – 9:05	Introductions, Agenda review
9:05 – 10:40	Discuss results of latest HCD TC Meetings
10:40 – 10:50	HCD Security Guide 1.0 Status
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:
  - Brian Smithson (Ricoh)
- Secretary:
  - Alan Sukert (Xerox)
- Document Editor:
  - Ira McDonald (High North) – HCD Security Guide

HCD PP Version 1.1 Status

HCD PP Version 1.1 Status Comment Disposition

- Final draft (Version 1.0.1) that included the current NIAP Technical Decisions against the HCD PP, Errata #1 changes and other changes previously approved by the HCD TC had a final review by HCD TC members
  - 11 Comments Against HCD PP v1.1 Received Since last HCD TC Face-to-Face in Amsterdam

HCD PP Version 1.1 Status Comment Disposition

- Change previously approved by the HCD Technical Community in Section C.1.1, paragraph 1014 in the TSS Assurance Activity for the FAU_SAR.1 SFR had not been implemented correctly by me:
  - Change the sentence to now read 'The evaluator shall check to ensure that the TSS contains a description that audit records can be viewed only by an Administrator and authorized functions to view audit records' (the added word is in red type font).

Change approved by HCD TC

HCD PP Version 1.1 Status Comment Disposition

- The text for the 'Test 2' Test Assurance activity for SFR FCS_CKM.4 has a minor typo in it, so it does not completely match the required text per NIAP TD0299:
  - Test 2: Applied to each key held in non-volatile memory and subject to destruction by the TOE, except for replacing a key using the selection *[a new value of a key of the same size]*. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to ensure the tests function as intended.

Change approved by HCD TC

HCD PP Version 1.1 Status Comment Disposition

- The current dependency list for FCS_COP.1(g) is incorrect - it does not include FCS_COP.1(c) that was agreed upon by the HCD TC
  - Add FCS_COP.1(c) Cryptographic operation (Hash Algorithm) to the dependency list for FCS_COP.1(g)

Change approved by HCD TC

- The current dependency list for SFR FPT_KYP.1 is incorrect - it does not include SFR FCS_KYC_EXT.1 as agreed upon by the HCD TC
  - Add FCS_KYC_EXT.1 Extended: Key Chaining to the dependency list for FPT_KYP.1

Change approved by HCD TC

HCD PP Version 1.1 Status Comment Disposition

- TD0074 changed FCS_CKM.1(a) Asymmetric Key Generation from a required SFR to a vendor-optional SFR. It was issued by NIAP, but without any rationale.
- Further, FCS_CKM.1(a) is a firm dependency of IPsec, TLS, and SSH, which means that it should be a firm dependency in any conforming TOE.
- Propose that we reverse TD0074 and make FCS_CKM.1(a) a mandatory SFR again

Deferred by HCD TC

HCD PP Version 1.1 Status Comment Disposition

- Per JISEC, need to provide rationale and support for NIAP TD0074 which made FCS_CKM.1(a) optional instead of mandatory, by:
  - Explicitly allowing the operational environment (OE) to satisfy FCS_CKM.1(a)
  - Add specification text to a new security objective for the OE, requiring the same crypto strength as FCS_CKM.1(a) and administrative protection for the keys in the OE
  - Add a new Optional Use Case for this configuration

No decision yet by HCD TC – Still Open

HCD PP Version 1.1 Status Comment Disposition

- TD0074 changed FCS_CKM.1(a) Asymmetric Key Generation from a required SFR to a vendor-optional SFR. It was issued by NIAP, but without any rationale.
  - Further, FCS_CKM.1(a) is a firm dependency of IPsec, TLS, and SSH, which means that it should be a firm dependency in any conforming TOE.
  - I propose that we reverse TD0074 and make FCS_CKM.1(a) a mandatory SFR again

Deferred by HCD TC

- This came up during the Amsterdam TC meeting, during discussion of TD0074. In cases where keys are imported from outside of the TOE, should we have an SFR?

Deferred by HCD TC

HCD PP Version 1.1 Status Comment Disposition

- Believe that some references to Appendixes were broken when Appendix C.4 was added. See it in paragraph 549, 581 and 612 where "C.4.1" is referred (in addition to "Appendix C") and there is no reference to "Appendix D"
  - Change text to read "The Assurance Activities contained in Section 4, Appendix B , Appendix C , and Appendix D should provide the ST authors with sufficient information to determine the appropriate content for the TSS section.

No decision yet by HCD TC – Still Open

HCD PP Version 1.1 Status Comment Disposition

- Editorial error in dependencies of FPT_TUD_EXT.1
  - FPT_TUD_EXT.1 was updated to incorporate v1.0 errata, but the way to update is slightly different from v1.0 errata. In v1.1 draft rev2, "or" is removed, but brackets [] is not.
  - With v1.1 draft rev2, it is not clear enough that both dependencies are mandatory
  - Change dependencies for FPT_TUD_EXT.1 to be

    FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)

    FCS_COP.1(c) Cryptographic operation (Hash Algorithm)

No decision yet by HCD TC – Still Open

HCD PP Version 1.1 Status Comment Disposition

Implementation of NIAP TD0393 (Require FTP_TRP.1(b) only for printing)

NIAP has issued TD0393 against the FTP_TRP.1(b) SFR. Per the TD, "HCDPP allows for one or more of the following functions defined in section 1.3.1.1: printing, scanning, copying. HCDPP also contains FTP_TRP.1(b) which requires the existence of a remote, non-administrative interface to the device regardless of the devices functionality. FTP_TRP.1(b) is an issue for department-level copy-only and scan-only devices containing a control panel, which don't have a need for a remote, non-administrative interface". The justification for the changes was that Remote, non-administrative user access to the device is not required anywhere except for this SFR. The concepts of Local and Network Users are mentioned and used in Section 1 but are not incorporated into the U.NORMAL definition in Section 2.1 and A.1. The use cases for copying and scanning specifically apply to Local Users only.

We need to implement the changes requested in TD0393 into HCD PP v1.1

HCD PP Version 1.1 Status Comment Disposition

Implementation of NIAP TD0393

- Concern about implementing this TD is what is the definition of a "remote, non-administrative interface" in terms of the PP use case "Network communications: sending or receiving documents over a Local Area Network (LAN)"
  - Network communications can also be used for administration and/or for user interaction (monitoring jobs, etc.).
  - "sending or receiving documents" can take place with a user (e.g. submitting a print job) and/or with an IT entity (e.g., scan-to-email).
  - Should have required network communications for admin functions, and made the other network uses conditionally mandatory. But what SFRs go with network communications involving users? It's clear that a user interacting with an MFP's web interface is FTP_TRP.1(b), but what about users submitting prints job from their PCs? Is it TRP or ITC?
  - Is this really a mandatory or optional SFR

Agreed to Implement TD0393 in HCD PP v1.1 as is for now and review by HCD iTC for change in HCD cPP v1.0

HCD PP Version 1.1 Status Comment Disposition

New Proposals from JBMIA

HCD PP Version 1.1 Status
1.Proposal for Modifications to FCS_CKM.4 1/2

- SFR： FCS_CKM.4
- HCD-PP ver1.1 Draft2 (Applied TD0261)

FCS_CKM.4 in the HCD PP is replaced with the following:
FCS_CKM.4.1(a) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [selection:
（snip）
· *For non-volatile memory the destruction shall be executed by a [selection: [selection: single, [assignment: ST author defined multi-pass]] overwrite consisting of [selection: zeroes, ones, pseudo-random pattern, a new value of a key of the same size, [assignment: any value that does not contain any CSP]], block erase];*
]that meets the following: *No Standard*.
Application Note: *In the first selection, the ST Author is presented options for destroying disused cryptographic keys based on whether they are in volatile memory or non-volatile memory within the TOE.*
The selection of block erase for non-volatile memory applies only to flash memory.

- Issue:
  - The meaning of "block erase" in HCD-PP ver1.1 Draft2 is ambiguous.
  - An erase command for controller and erase a block of cells are both so-called "block erase" to flash memory. We concern that may be confusing in the requirement.
- Proposal:
  - To specify the purpose of "block erase", we propose to copy following sentences from FDEcPP into Application Note in HCD-PP ver1.1. It describes a resulting effect of block erase command for controller, and the implementation for erasing a block of cells will be vender-specific.

    "A block erase does not require a read verify, since the mappings of logical addresses to the erased memory locations are erased as well as the data itself."

HCD PP Version 1.1 Status
1.Proposal for Modifications to FCS_CKM.4 2/2

We refers Application Note in cPP_FDE_EEver2.0

In FDEcPP, a "block erase" is described as follows.

"the mappings of logical addresses to the erased memory locations are erased as well as the data itself"

Application Note: *In the first selection, the ST Author is presented options for destroying a key based on the memory or storage technology where keys are stored within the TOE.*
~~*If non-volatile memory is used to store keys, the ST Author selects whether the memory storage algorithm uses wear-leveling or not. Storage technologies or memory types that use wear-leveling are not required to perform a read verify.*~~ *The selection for destruction includes block erase as an option, and this option applies only to flash memory.* ***A block erase does not require a read verify,*** **since the mappings of logical addresses to the erased memory locations are erased as well as the data itself.**

Our proposal:
We propose to copy this sentence from FDEcPP into the next of paragraph 214 in the Application Note.

This sentence is already exist in paragraph 214 in HCD-PP ver1.1 draft2.

This strike out sentence specifies whether wear-leveling algorithm is selected or not in non-volatile memory. This sentence is not needed, since there is no requirement for wear-leveling algorithm in HCD-PP.

Proposal accepted by HCD TC

HCD PP Version 1.1 Status
2.Proposal for Modifications to FPT_KYP_EXT.1 1/2

- O.KEY_MATERIAL in HCD-PP ver1.1 Draft2

> - 3.1.10 **Protection of Key Material (conditionally mandatory)**
> - *¶ 132* The TOE shall protect from unauthorized access any cleartext keys, submasks, random numbers, or other values that contribute to the creation of encryption keys for storage of User Document Data or Confidential TSF Data in Field-Replaceable Nonvolatile Storage Devices; The TOE shall ensure that such key material is not stored in cleartext on the storage device that uses that material [O.KEY_MATERIAL].

- FPT_KYP_EXT.1 in HCD-PP ver1.1 Draft2

> - *¶ 924* **FPT_KYP_EXT.1.1** The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in **any Field-Replaceable Nonvolatile Storage**

- Issue :
  - Compared to the description of that requirement of [O.KEY_MATERIAL], the cleartext key material is not specified in FPT_KYP_EXT.1.1.
  - O.KEY_MATERIAL can not be achieved if FPT_KYP_EXT.1.1 is satisfied.
  - We consider that FPT_KYP_EXT.1.1 is missing “key materials”.

NO.	category		description
1	Security Objective	O.KEY_MATERIAL	Field-Replaceable Nonvolatile Storage Devices; The TOE shall ensure that such key material is not stored in cleartext on the storage device that uses that material
2	SFR	FPT_KYP_EXT.1.1	The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 .

HCD PP Version 1.1 Status
2.Proposal for Modifications to FPT_KYP_EXT.1 2/2

- Modifications :
  - Add the “key materials” to FPT_KYP_EXT.1.1 and Assurance Activity.

- *¶ 924* **FPT_KYP_EXT.1.1** The TSF shall not store plaintext keys and key materials that are part of the keychain specified by FCS_KYC_EXT.1 in **any Field-Replaceable Nonvolatile Storage Device**.

- *¶ 928* The evaluator shall verify the KMD to ensure it describes the storage location of all keys and key materials and the protection of all keys and key materials stored in nonvolatile memory.

Proposal accepted in principle

HCD PP Version 1.1 Status

Current Plan

- Implement TD0393 to create the "final" HCD PP v1.1 text by end of April
- Submit to NIAP and JISEC for their review and approval as soon as possible thereafter
- One question/concern:
  - In announcing TLS Package 1.1 NIAP indicated that "As new and updated PPs/PP-Modules are published, they will make use of this TLS package, where applicable."
  - If we get HCD PP v1.1 approved by NIAP and JISEC, does that mean we automatically include TLS Package 1.1 by reference in place of FCS_TLS_EXT.1 that is currently in the HCD PP?

Note: Per NIAP the answer is "YES"

HCD iTC Status

HCD iTC Status

- CCDB at its Oct 2018 Meeting chartered a CCDB Working Group (WG) containing the Korean and Japanese schemes. Goal was formation of the HCD iTC at the April CCDB meeting in Rome
- HCD WG is creating the following documents to be submitted to the CCDB for review at the April CCRA meeting:
  - Essential Security Requirements (ESR)
  - Terms of Reference (ToR)
- At the same time the HCD TC as creating its own versions of the same two documents plus a "Key Persons" document that will be referenced by the ToR

  Goal is to fold the HCD TC documents into the HCD WG versions that are submitted to the CCDB
- HCD WG submitted ToR to CCDB for approval at its April 2019 Meeting
  - Is currently being voted on by CCDB members; will take 60-90 days to finish
  - If passed will be submitted to CCMC for approval; should take about 1 mo
  - CCMC approval gives official authorization to form HCD iTC

HCD iTC Status - Essential Security Requirements

- The HCD WG is aware of recent work including the draft ESR done by the HCD TC since HCD TC provided the latest resolution of review comments as an input to support the HCD WG's works.
- The HCD WG almost harmonized the ESR and will make a call for participation that goes out all CCRA participants soon.
- HCD WG provided its draft ESR to HCD TC for comment
  - Comments due back to HCD WG by mid-June
  - Should formally submit to CCDB shortly thereafter

HCD iTC Status - Essential Security Requirements

HCD TC ESR Comment Status

#	Comment	Resolution
43	PSTN and Document Storage are Conditionally Mandatory, which is different from Optional. The Conditionally Mandatory functions (according to HCDPP at least) are fax, document storage/retrieval, and field-replaceable nonvolatile storage. Need to clarify in ESR	Accepted in Principle
44	All products should have a means for updating software. It should not be optional.	Accepted
45	There are other reasons for ensuring software integrity, not just to prevent malware distribution	Accepted
46	In addition to not checking User Data for malware, the ESR also does not require checking for other kinds of malicious User Data (for example, PostScript, JPEG)	Accepted

HCD iTC Status - Essential Security Requirements

#	Comment	Resolution
54	Fax should be added to the 'Use Case' discussion	Rejected
55	Under 'Attacker's Resources' there was the statement "There is numerous PC software providing HCD users with a variety of applications delivered by each HCD vendor. "Some rewording of this sentence to make it grammatically correct was suggested. Also, there is also the statement "The tools used for attacks are expected to be tools that are free or non-free according to the knowledge levels of the attackers". Either revise or remove this statement	Accepted
56	It was suggested that we add something about physical attacks to the 'Attacker's Access' section	Rejected
57	Under the 'ESR' section, the statement "HCD shall test some subset of its security functionality to help ensure that subset is operating properly" should add some wording about when this subset is run and be reworded slightly to make this statement clearer	Accepted

HCD iTC Status - Essential Security Requirements

HCD TC ESR Comment Status

#	Comment	Resolution
64	An HCD has firmware (e.g. BIOS) in addition to software. The protection of HCD's firmware is critical to the security of the HCD	Accepted
65	Currently the following bulleted item in the "Attacker's Access" section covers firmware / software: "An attacker may cause the installation of unauthorized software on the HCD." I propose to supplement the attacker's access to firmware / software above by adding the following attacker's access: "An attacker may change (modify or delete) firmware / software in the HCD through one of the HCD's interfaces" The proposed attacker's access covers access to firmware / software outside the firmware / software update process	Accepted

HCD iTC Status - Essential Security Requirements

HCD TC ESR Comment Status

#	Comment	Resolution
66	Execution of corrupted code can degrade the security of the HCD. As such, the HCD should detect corrupted code, and alert when corrupted code is detected, to enable corrective action	Deferred
67	Having a root of trust for the verifying boot firmware provides added assurance of the security mechanism	Deferred
71	HCD shall verify the hardware-anchored integrity of firmware/software, including initial boot, operating system, and applications.	Accepted in Principle

HCD iTC Status - Essential Security Requirements

- Current Set of Essential Requirements in latest draft HCD TC ESR:
  - HCD shall perform authorization of Users in accordance with security policies
  - HCD shall perform identification and authentication of Users for operations that require access control, User authorization, or Administrator roles
  - HCD shall enforce access controls to protect User Data and TSF Data in accordance with security policies.
    - User Document Data can be accessed only by the Document owner or an Administrator.
    - User Job Data can be read by any User but can be modified only by the Job Owner or an Administrator.
    - Protected TSF Data are data that can be read by any User but can be modified only by an Administrator or (in certain cases) a Normal User who is the owner of or otherwise associated with that data.
    - Confidential TSF Data are data that can only be accessed by an Administrator or (in certain cases) a Normal User who is the owner of or otherwise associated with that data.

HCD iTC Status - Essential Security Requirements

- Current Set of Essential Requirements in latest draft HCD TC Version:
  - HCD shall ensure that only authorized Administrators are permitted to perform administrator functions.
  - HCD shall provide mechanisms to verify the authenticity of software updates.
  - HCD shall test some subset of its security functionality to help ensure that subset is operating properly.
  - HCD shall have the capability to protect LAN communications of User Data and TSF Data from Unauthorized Access, replay, and source/destination spoofing.
  - HCD shall generate audit data, and be capable of sending it to a trusted External IT Entity. Optionally, it may store audit data in the HCD.

HCD iTC Status - Essential Security Requirements

- Current Set of Essential Requirements in draft HCD WG Version:
  - The HCD shall perform authorization of users in accordance with security policies
  - The HCD shall perform identification and authentication of users for operations that require access control, user authorization, or administrator roles
  - HCD shall verify the hardware-anchored integrity of firmware/software, including initial boot, operating system, and applications.
  - The HCD shall enforce access controls to protect user data and the HCD critical data in accordance with security policies.
    - User document data can be accessed only by the document owner or an administrator.
    - Shared user document data can be accessed by the authorized users if the HCD has such a capability.
    - User job data can be read by any user but can be modified only by the job owner or an administrator.

HCD iTC Status - Essential Security Requirements

- Current Set of Essential Requirements in draft HCD WG Version:
  - The HCD shall enforce access controls to protect user data and the HCD critical data in accordance with security policies.
    - The HCD critical data (for integrity protection) are data that can be read by any user but can be modified only by an administrator or (in certain cases) a normal user who is the owner of or otherwise associated with that data.
    - The HCD critical data (for confidentiality protection) are data that can only be accessed by an administrator or (in certain cases) a normal user who is the owner of or otherwise associated with that data.
  - The HCD shall ensure that only authorized administrators are permitted to perform administrator functions.
  - The HCD shall provide mechanisms to verify the authenticity of firmware and/or software updates.
  - The HCD shall test some subset of its security functionality to ensure that the security functionality is not compromised by the detectable malfunction.

HCD iTC Status - Essential Security Requirements

- Current Set of Essential Requirements in draft HCD WG Version:
  - The HCD shall have the capability to protect LAN communications of transmitted user data and the HCD critical data from unauthorized access, replay and source/destination spoofing.
  - The HCD shall generate audit data, and be capable of sending it to a trusted external IT entity and store it in the HCD.
  - The HCD shall ensure logical separation of the PSTN and the LAN if it provides a PSTN faxing function.
  - The HCD shall encrypt user document data and/or the HCD critical data (for confidentiality protection) stored on the nonvolatile storage device if it uses nonvolatile storage device for the purpose of storing those data. To support encryption, the HCD shall maintain key chains so that keys and key materials are protected. Note that the initial data of the key chain stored on the nonvolatile storage device without protection do not meet the requirement.

HCD iTC Status – Terms of Reference

- HCD TC shared the draft version of HCD iTC ToR to HCD WG (ITSCC, JISEC). HCD WG reviewed the draft ToR that was provided by HCD TC and had one major comment:
  - Wanted more details on the voting and decision process than the simplified process we borrowed from the OSPP iTC
- HCD TC resolved the comment by including from original draft; HCD WG accepted revised ToR and is submitting it to the CCDB.

HCD iTC Status – Terms of Reference

HCD TC ToR Comment Status

#	Comment	Resolution
39	Most of the ToR refers to the iTC Chair when referencing the Chairperson. However, Lines 171 and 172 (Section 8.2) talks about Chairpersons. The ToR should be consistent in how it refers to the iTC Chair	Accepted
40	Concerned about the process described in Section 7.6.2 for making technical decisions. Specifically, the Core SMEs should determine how to resolve the issue by consensus, and if no consensus is reached the iTC Chair should make the decision how to resolve the issue; then it should be up to the Technical Editor and original issuer on how to implement the resolution that is decided upon. Also, the Technical Editor should not be making the judgement what to do with the proposed solution; the iTC Chair should be doing that	Accepted

HCD iTC Status – Terms of Reference

HCD TC ToR Comment Status

#	Comment	Resolution
41	The ToR does not really talk about how persons are assigned to a given role (are they elected, do they volunteer, is there some other method used) and how long a person such as the iTC Chair stay in that role. I don't want to create a bureaucracy or a complicated process here, but the ToR should at least say something generic about this	Open – will leave to HCD iTC to address in ToR update
42	The ”Hardcopy Devices International Technical Community - Key persons and affiliations” document referenced in the ToR needs to be provided	Accepted
49	There was a discussion at the 1/24 IDS Conference Call of what functions were applicable to an HCD in this context, whether Fax was an optional function or not, and whether the scope should include the ‘Transform’ function. It was agreed to relook at the ‘Scope’ statement in the ToR and revise as needed to address the comments	Rejected

HCD iTC Status – Terms of Reference

HCD TC ToR Comment Status

#	Comment	Resolution
50	One of the comments from the 1/24/19 IDS Conference Call was that instead of referencing Causeway in the ToR we just refer to an "approved collaboration tool" so we don't have to revise the ToR if we change collaboration tools	Accepted
51	At the 1/24/19 IDS Conference Call, there was a long discussion about the rules around 'Technical Decisions' and how they are made. The consensus appeared to be that what was there now wasn't correct, but we didn't have an agreed-upon way to fix it. This will have to be an area the HCD TC will have to address	Accepted
52	It was suggested at the 1/24/19 IDS Conference Call that the ToR include in its 'Voting' discussion some wording around who can participate to vote in terms of meeting attendance; the concern was that we didn't want to allow the case where someone joins the iTC, does not come to any meetings and then comes to a meeting where a vote is to be taken and votes against the proposal in question. No resolution was formulated here – again this will have to be an area the HCD TC will have to address	Open – will leave to HCD iTC to address in ToR update

HCD iTC Status – Terms of Reference

HCD TC ToR Comment Status

#	Comment	Resolution
53	At the 1/24/19 PWG IDS Conference Call it was pointed out all the different types of SMEs mentioned in the TOR, but that only the Core SMEs are included in the technical decisions. We agreed that the whole SME discussion should be simplified in the ToR	Withdrawn
62	Since we may or may not be able to continue indefinitely with the Causeway tool, we shouldn't make specific reference to it in the ToR	Accepted
63	This covers the whole of sections 7.6 and 7.7. Propose that we pretty much copy what is in the OSPP TC ToR section 6.2 to replace our existing sections 7.6 and 7.7	Accepted[1]

[1]This was superseded by need to address HCD WG comment (#70) about decision process; original text was restored

HCD iTC Status – Terms of Reference

HCD TC ToR Comment Status

#	Comment	Resolution
70	Address more specific voting procedures including on-line/off-line voting. For example, there may exist a situation that parts of iTC members are attended at a face-to-face meeting and decisions made by voting. Then the iTC may need a rule for valid ballot. For decisions through Internet voting, the procedure may need the minimum limit date for responding	Accepted

HCD iTC Status – "Key Persons" List

- HCD TC (Kwangwoo Lee) requested several HCD stakeholders to invite the SME(s) list of HCD iTC. According to the feedbacks of each organization, HCD TC created a draft Hardcopy Device International Technical Community – Key persons and affiliations
  - Made key roles 'TBD'
- Document submitted to HCD WG and accepted. Will be forwarded to CCDB.
- The Status of Subject Matter Experts
  - Industry SMEs: 26 members 11 organizations
  - Lab SMEs: 15 members 9 organizations
  - Certification Body SMEs: 3 members 2 schemes (KR, JP)
    - Waiting the official feedback from 2 schemes (US, SE)
  - Other SMEs: 4 members (IEEE-ISTO PWG experts/Biometric iTC expert

HCD TC to HCD iTC Transition

HCD TC → HCD iTC Transition

- Questions that need to be addressed:
  - Leadership
    - Probably the most important question now -- who will take on the following roles defined in the ToR:
      - iTC Chair
      - ITC Deputy Chair
      - Record Manager (aka “Secretary”)
      - Technical Editor(s)
    - How do we determine who takes each role and when will that occur
    - How long the terms of office will be for each of these roles
    - The original thought was that theses roles would be “voluntary” in terms of how they are assigned and the term would be for as long as the volunteers wanted to serve in that role. Do we (or should we) make this more formal?

HCD TC → HCD iTC Transition

- Questions that need to be addressed:
  - What iTC or TC, if any, should we pattern the formation and processes of the HCD iTC after –
    - Network Device
    - Full Drive Encryption
    - OS
    - Some other TC
    - None of the above
  - Should the HCD iTC implement some type of "NIT" process like the ND iTC has where a small team develops any interpretations needed? If so, how soon after formation of the iTC

HCD TC → HCD iTC Transition

- Questions that need to be addressed:
  - How should we handle comments against the cPP drafts?
  - How often should the HCD iTC meet
    - We have the Spring and Fall Face-to-Face Meetings as part of the CCUF now; do we need additional Face-to-Face Meetings beyond these two
      - If so, where would we hold them
    - Should we have monthly Conference Calls, and if so how often
  - iTC participation
    - Should we have some type of minimum participation requirement on the part of a voting entity to allow that entity to vote
    - How do we get as many vendors, labs and schemes as possible to participate in the iTC

HCD TC → HCD iTC Transition

- Questions that need to be addressed:
  - How often should we update the ToR
  - How often should we issue updates to the HCD cPP
    - Major version update (e.g., 1.0 → 2.0) once 1-2 years and minor updates at least once every six months
    - Some other cadence
  - Other questions I haven't thought about

HCD CPP v1.0

HCD cPP v1.0

- When we start making a cPP, we will use HCD PP v1.1 as the starting place, then make changes as necessary:
  - Move assurance activities from HCD PP v1.1 to a supporting document
  - Internationalize references to NIST, FIPS, etc.
  - Include some issues on the HCD PP issues list that we deferred to the cPP
- Our Initial thoughts were that big changes like TLS1.3, use of packages or modules, etc. would likely be included over time in subsequent versions of the cPP. However, that needs to be reconsidered

HCD cPP v1.0

- Issues that should be considered for HCD cPP v1.0
  - HCD PP v1.1 comments that are open or deferred
  - Parking Lot issues from the development of HCD PP v1.0 (see backup slides)
  - Impact of recently approved NIST SP 800-131A and NIST SP 800-56B updates as they relate to:
    - Sunset of cipher suites with SHA1
    - Sunset of cipher suites with RSA Key Generation with keys < 2048 bits
  - Inclusion of requirement to include TLS 1.3 and removal of requirement to include TLS 1.1
  - Implementing the high-level requirements that are in the ESR approved by the CCDB
  - Updating Assurance Activities

HCD cPP v1.0

- Issues that should be considered for HCD cPP v1.0
  - NIAP TLS Package
    - Splitting up of separate requirements for TLS as a client and TLS as a server.
    - Elimination of support for any ‘SHA’ TLS cypher suites except for TLS_RSA_WITH_AES_128_CBC_SHA
    - The selection of TLS supporting ‘mutual authentication’ and ‘session renegotiation and the TLS requirements for each of the two if either is supported.
    - New requirement for TLS as a client if any ECDHE or ECDHA cipher suites are selected in FCS_TLSS_EXT.5.
    - Inclusion by reference of FIA_X509_EXT.1 (X.509 Certificate Validation) and FIA_X509_EXT.2 (X.509 Certificate Authentication) from NDcPP (see backup slides)

HCD cPP v1.0

- Issues that should be considered for HCD cPP v1.0
  - Sync with requirements and assurance activities in NDcPP and FDE cPP updates (e.g., changes for NDcPP v2.1)
  - NDcPP or FDE cPP SFRs that are not currently in HCD PP but could be in HCD cPP v1.0
  - Any new NIAP or JISEC Technical Decisions against the HCD PP
  - Any new NIAP or JISEC policies that impact HCD PP
  - Password policies to comply with the new California "password" law and NIST SP 800-171
  - Internationally-friendly crypto requirements that don't rely on FIPS
  - Proposals from JBMIA

HCD cPP v1.0

California “Password” Law

- As of Jan 1, 2020 each connected device must ensure that either:
  - The preprogrammed (aka “default”) authentication password is unique to each device manufactured or
  - The device contains a security feature that requires a user to generate a new means of authentication (i.e., a new authentication password) before access is granted to the device for the first time

NIST SP 800-171

- As of Jan 1, 2018 requires among other things that we
  - Prohibit password use for a specified number of generations
  - Allow temporary password use for system logons with an immediate change to a permanent password

HCD cPP v1.0

- More Issues that should be considered for HCD cPP v1.0
  - Privacy issues (e.g., GDPR)
  - Use of TPMs
  - Securing the default configuration
  - Integrating the work of the CCDB Cryptographic Working Group's cryptographic catalog
  - Use of ISO 19790 instead of FIPS 140-2
  - Implementing the latest NIST cryptographic algorithms and guidance
  - More specific requirements around the concepts of secure boot, roots of trust, etc. under the umbrella of a "trusted computing environment"
  - Dedicated security components

HCD cPP v1.0

- Changes for NDcPP v2.1 that might be considered
  - Deletion of support for 192-bit TLS cipher suites and addition of two new TLS_DHE_RSA cipher suites
  - New NTP SFR
  - Addition of new encryption algorithms, authentication implementations and key exchange methods for SSH
  - Added additional management functions for possible selection, some of which we might want to look at for inclusion in HCD PP
  - Include requirements for authentication protocols like Kerberos and LDAP

HCD cPP v1.0

- Other Changes for NDcPP v2.1 that might be considered
  - FAU_GEN.1 – add the following requirements
    - • *Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
      • *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
      • *Resetting passwords (name of related user account shall be logged)*
  - Expand FAU_STG.1 to add proposal from JBMIA

HCD cPP v1.0

- Other Changes for NDcPP v2.1 that might be considered
  - FPT_STM.1– add the following requirement
    - **FPT_STM_EXT.1.2** The TSF shall [selection: allow the Security Administrator to set the time, synchronise time with *an NTP server*].
  - Modify FTA_SSL.3 to be like NDcPP:
    - **FTA_SSL.3.1:** The TSF shall terminate a remote interactive session after a Security Administrator-configurable time interval of session inactivity
  - Add the following SSH SFR
    - **FCS_SSHC_EXT.1.9** The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key or [selection: *a list of trusted certification authorities, no other methods*] as described in RFC 4251 section 4.1

HCD cPP v1.0

- Other Changes for NDcPP v2.1 that might be considered
  - Include the following IPsec SFRs
    - **FCS_IPSEC_EXT.1.9** The TSF shall generate the secret value x used in the IKE DiffieHellman key exchange ("x" in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [*assignment: (one or more) number(s) of bits that is at least twice the security strength of the negotiated Diffie-Hellman group*] bits.
    - **FCS_IPSEC_EXT.1.10** The TSF shall generate nonces used in [selection: *IKEv1, IKEv2*] exchanges of length [selection:
      • *according to the security strength associated with the negotiated Diffie-Hellman group];*
      • *at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash*] .
    - **FCS_IPSEC_EXT.1.12** The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [selection: *IKEv1 Phase 1, IKEv2 IKE_SA*] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [selection: *IKEv1 Phase 2, IKEv2 CHILD_SA*] connection.
    - **FCS_IPSEC_EXT.1.14** The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following types: [selection: *SAN: IP address, SAN: Fully Qualified Domain Name (FQDN), SAN: user FQDN, CN: IP Address, CN: Fully Qualified Domain Name (FQDN), CN: user FQDN, CN: Distinguished Name (DN)*] and [*selection: no other reference identifier type, [assignment: other supported reference identifier types]*].

HCD cPP v1.0

- NDcPP v2.1 SFRs not in HCD PP that could be considered for inclusion in HCD cPP v1.0 (full text in backup slides):
  - FAU_GEN.2 User identity association
  - FCS_CKM.2 Cryptographic Key Establishment (Refinement)
  - FIA_UAU_EXT.2 Password-based Authentication Mechanism
  - FIA_X509_EXT.3 X.509 Certificate Requests
  - FPT_APW_EXT.1 Protection of Administrator Passwords (would extend to all authentication passwords)
  - FAU_ STG.3/LocSpace Action in case of possible audit data loss
  - FCS_NTP_EXT.1 NTP Protocol
  - FPT_TST_EXT.2 Self-tests based on certificates
  - FPT_TUD_EXT.2 Trusted Update based on certificates
  - FMT_MOF.1/AutoUpdate Management of security functions behaviour
  - FMT_MOF.1/Functions Management of security functions behaviour
  - FMT_MTD.1/CryptoKeys Management of TSF data

HCD iTC and HCD cPP v1.0

- Potential Schedule for creation of HCD cPP v1.0
  - CCMC approval of creation of HCD iTC – July 2019
  - First HCD iTC F2F Meeting – Sep 2019
  - First draft of HCD cPP v1.0 – Apr 2020
  - Updated draft of HCD cPP v1.0 – Oct 2020
  - HCD cPP v1.0 submitted for approval by HCD iTC membership – Feb 2021
  - HCD cPP v1.0 submitted to CCDB for approval – Mar 2021
  - HCD cPP v1.0 published – Apr 2021

HCD Security Guide Status

Next Steps

- Submit HCD PP v1.1 to NIAP/JISEC and get it approved
- Implement the transition from the HCD TC → HCD iTC
  - Determine and install "officers"
  - Set up meeting cadence, iTC membership, etc.
  - Have the first iTC meeting
- Reconcile any gaps between the HCD WG version and the HCD TC version of the ESR
- Start work on HCD cPP v1.0
  - Develop plan for development, review and release of HCD cPP v1.0
  - Determine content scope
  - Initiate "transition" of HCD PP v1.1 into first draft
  - Update and review drafts as necessary to create "final" version
  - Get iTC review and approval for "final" version
  - Release HCD cPP v1.0