The Printer Working Group

Imaging Device Security

August 29, 2019

PWG August 2019 Virtual Face-to-Face

Agenda

When	What
9:00 – 9:05	Introductions, Agenda review
9:05 – 10:35	Discuss results of latest HCD TC Meetings and potential HCD cPP content
10:35 – 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

- NIAP has indicated that they will not accept any changes to the current bilateral HCD PP v1.0
- NIAP is waiting for international HCD cPP v1.0 which they will adopt upon approval
- As a result, HCD v1.1 will not be published as a new version of the bilateral HCD PP
- However, it will be the basis for international HCD cPP v1.0

HCD iTC Status

HCD iTC Status

- Common Criteria Development Board (CCDB) at its Oct 2018 Meeting chartered an HCD 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 created the following documents which were submitted to the CCDB for review at the April 2019 CCRA meeting:
  - Essential Security Requirements (ESR)
  - Terms of Reference (ToR)

  which incorporated input and comments from the HCD TC
- HCD WG formally submitted ESR and ToR to CCDB for approval at its April 2019 Meeting
  - ESR was approved by CCDB in July
  - ToR was approved on August 12th

HCD iTC Status

- ESR and ToR have been submitted to Common Criteria Management Committee (CCMC) for its approval
  - Once CCMC approves ESR and ToR we can officially form the HCD iTC and start the work to generate an HCD cPP
- Our hope is that the CCMC will approve the ESR and ToR in time to initiate the HCD iTC at the Sep 26th HCD TC Face-to-Face in Singapore
  - HCD WG is working closely with the CCMC to get both documents approved as quickly as possible

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 – "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. Was forwarded to CCDB and approved with the ToR.
- The Status of Subject Matter Experts
    - Industry SMEs: 30 members 14 organizations
    - Lab SMEs: 14 members 9 organizations
    - Certification Body SMEs: 4 members 3 schemes (KR, JP, SE)
        - Waiting the official feedback from 1 scheme (US)
    - 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 (if there is one)
      - Record Manager
      - 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 (most likely “candidate”)
    - 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
- These issues and others will (hopefully) be discussed at the HCD TC Face-to-Face on Sep 26th
  - Meeting is planned for 8 hours
    - First 4 hours will discuss HCD PP issues
    - Last 4 hours will discuss formation of the iTC

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
- Goal is to minimize additional content beyond what is in HCD PP v1.1 to just the content that is “absolutely necessary” for inclusion in the initial cPP version and then provide updates on a regular basis (e.g., every 6 months, once a year, etc.) to reflect changes in NDcPP, FDE cPP and other standards

HCD cPP v1.0

- Content that could 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
  - 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 1.0 and 1.1
  - Implementing the high-level requirements that are in the ESR approved by the CCDB
  - Updating Assurance Activities

HCD cPP v1.0

- Additional content that could be considered for HCD cPP v1.0 (based on the 8/22/19 IDS WG Conference Call)
  - Including FIPS 140-3 and by extension ISO Standard 19790
  - Inclusion of other country-specific crypto requirements
  - What TLS cipher suites should be allowed
  - Sync with requirements and assurance activities in NDcPP and FDE cPP updates (e.g., changes for NDcPP v2.1)
    - What changes to the Network Device cPP should be flowed down to the HCD cPP
  - Secure boot / trusted boot
  - Validated rapid software updates
  - Prohibiting all bridging of network interfaces

HCD cPP v1.0

- Other content that could be considered for HCD cPP v1.0
  - 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
  - Proposals from other Schemes or organizations like JBMIA
  - European Cybersecurity Standards

JBMIA Proposal for FCS_CKM.4.1

Purpose of this Proposal

- We know that the deadline for comments of HCD-PPver1.1 is over, but we would like to share the issue that has got pointed out by JISEC, and amend the Assurance Activity of ver1.1 if possible to suppress variation in the evaluation method in ver1.1.

- There is no test for garbage collection selected in FCS_CKM.4.1, and it is ambiguous. JISEC said, “Except for the case that the test is unnecessary, each selection in SFR should be tested along the instructions in Assurance Activity.
  If there is no test in Assurance Activity, the evaluator should find and evaluate a new suitable test method.”

- We would like to propose the solutions about the above issues. We hope that our proposal will be adopted in HCD-PPver1.1, and we’d like to know opinion from HCD TC members.

Proposal for Modification of FCS_CKM.4.1

- We think there are two issues in FCS_CKM.4 as follows. We’d like to propose solutions described later.

The definition of “garbage collection” seems ambiguous, described as the proposal No.1. If clearing the definition is needed, then add the words “memory management”.

FCS_CKM.4.1 Refinement: The TSF shall destroy cryptographic keys in accordance with a specified c estruction method [**selection:**

***For volatile memory, the destruction shall be executed by a [selection: single overwrite consisting of [selection lo-random pattern using the TSF’s RBG, zeroes, ones, a new value of a key, [assignment: any value that does not contain any P]], removal of power to the memory, destruction of reference to the key directly followed by a request for garbage collection or** memory management];*

(snip)

Test 1: **Applied to each key held as in volatile memory and subject to destruction by overwrite by the TOE** (whether or not the value is subsequently encrypted for storage in volatile or non-volatile memory). **In the case where the ~~only~~ selection made for the destruction method key was removal of power** **or destruction of reference to the key directly followed by a request for garbage collection, then this test is unnecessary.**

There is no test method for destruction of reference to the key, described as the proposal No.2.

Proposal for Modification of FCS_CKM.4.1

- We think there are two issues in FCS_CKM.4 as follows. We'd like to propose solutions described later.

The definition of "garbage collection" seems ambiguous, described as the proposal No.1. If clearing the definition is needed, then add the words "memory management".

FCS_CKM.4.1 Refinement: The TSF shall destroy cryptographic keys in accordance with a specified c estruction method [**selection:**

For volatile memory, the destruction shall be executed by a [selection: single overwrite consisting of [selection lo-random pattern using the TSF's RBG, zeroes, ones, a new value of a key, [assignment: any value that does not contain any C P]], removal of power to the memory, destruction of reference to the key directly followed by a request for garbage collection or memory management];

(snip)

Test 1: **Applied to each key held as in volatile memory and subject to destruction by overwrite by the TOE** (whether or not the value is subsequently encrypted for storage in volatile or non-volatile memory). **In the case where the ~~only~~ selection made for the destruction method key was removal of power or destruction of reference to the key directly followed by a request for garbage collection, then this test is unnecessary.**

There is no test method for destruction of reference to the key, described as the proposal No.2.

Proposal for Modification of FCS_CKM.4.1 1/2

- SFR:FCS_CKM.4.1

FCS_CKM.4.1 Refinement: The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**selection:**

***For volatile memory, the destruction shall be executed by a [selection:** single overwrite consisting of* [**selection:** *a pseudo-random pattern using the TSF's RBG, zeroes, ones, a new value of a key,* [**assignment:** *any value that does not contain any CSP*]*], removal of power to the memory, destruction of reference to the key directly followed by a request for garbage collection*]*;*

- Issue: The definition of "Garbage Collection" seems ambiguous.
  - □ The requirement selection "destruction of reference to the key directly followed by a request for garbage collection" is consist of two instructions.

    Step ①: destruction of reference to the key directly, and

    Step ②: garbage collection accumulates and recycling memory that are no longer used.
  - □ The purpose of the garbage collection in FCS_CKM.4.1 is disposal of freed memory.
  - □ There are two manners for memory management in application. They are different ways. One is automatic memory management such as garbage collection. Another is manual memory management such as malloc() and free() in C language, or new() and delete() in C++ language. Is the destruction with garbage collection selectable for manual memory management in C/C++ or not?

Proposal for Modification of FCS_CKM.4.1 2/2

- Proposal(One of the following two proposals)
  1. Add following description to application note.
     - The selection, “destruction of reference to the key directly followed by a request for garbage collection” mentions implicitly any kind of memory management for releasing the memory for keys and key materials that are allocated and no longer needed.
  2. Add following description to the selection with garbage collection in FCS_CKM.4.1.

FCS_CKM.4.1 Refinement: The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**selection:**
***For volatile memory, the destruction shall be executed by a* [selection: *single overwrite consisting of* [selection: *a pseudo-random pattern using the TSF’s RBG, zeroes, ones, a new value of a key,* [assignment: *any value that does not contain any CSP*]], *removal of power to the memory, destruction of reference to the key directly followed by a request for garbage collection or memory management*];**

Proposal for Modification of FCS_CKM.4.1 1/2

- SFR:FCS_CKM.4.1

FCS_CKM.4.1 Refinement: The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**selection:**

For volatile memory, the destruction shall be executed by a [selection: single overwrite consisting of [selection: a pseudo-random pattern using the TSF's RBG, zeroes, ones, a new value of a key, [assignment: any value that does not contain any CSP]], removal of power to the memory, destruction of reference to the key directly followed by a request for garbage collection];

(snip)

Test 1: **Applied to each key held as in volatile memory and subject to destruction by overwrite by the TOE** (whether or not the value is subsequently encrypted for storage in volatile or non-volatile memory). **In the case where the only selection made for the destruction method key was removal of power, then this test is unnecessary.**

- Issues
  - If we select "destruction of reference to the key directly followed by a request for garbage collection", we can't find what we should test for the case as described in the following table.

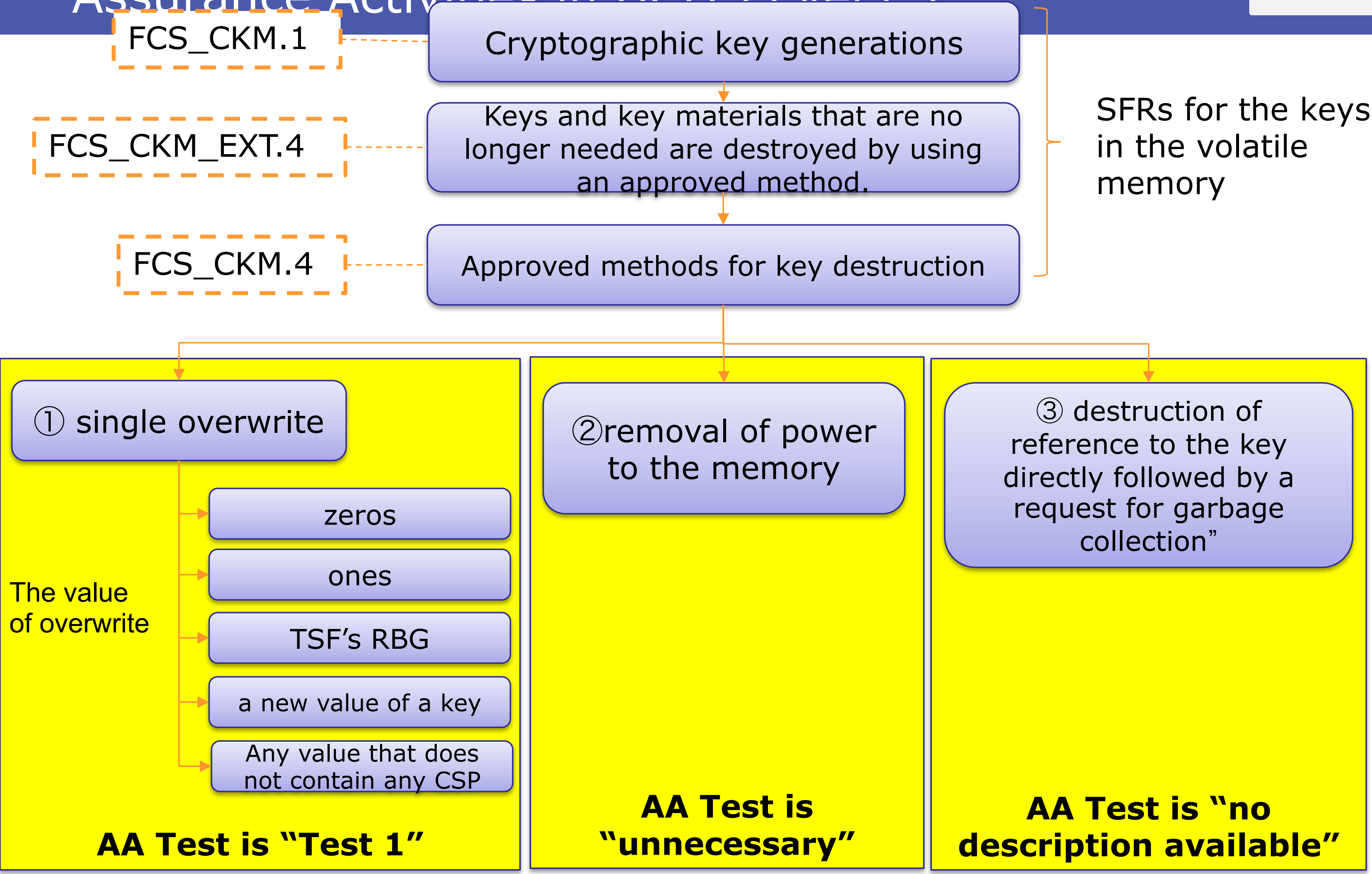
Proposal for Modification of FCS_CKM.4.1 1/2

No.	The selection of SFR	Assurance activity Test	Test
1	single overwrite consisting of a pseudo-random pattern using the TSF’s RBG, zeroes, ones, a new value of a key, [assignment: any value that does not contain any CSP	Test 1: Applied to each key held as in volatile memory and subject to destruction by overwrite by the TOE	Test1
2	removal of power to the memory	In the case where the only selection made for the destruction method key was removal of power, then this test is unnecessary	Unnecessary
3	destruction of reference to the key directly followed by a request for garbage collection	Not documented	N/A

Proposal for Modification of FCS_CKM.4.1 2/2

- Issue:
- Test 1 is the only suitable test for volatile memory.
- If we select “destruction of reference to the key directly followed by a request for garbage collection”, we have to apply Test 1 and confirm the erase of cryptographic keys.
  - □ Any kind of garbage collection mechanism collecting unused memory and recycles them. However, ordinary garbage collection has no function to erase the values in memory.
  - □ So, all tests shall fail with Assurance Activity’s Test 1.
  - □ That implies that destruction with garbage collection shall not be selected, in spite of definition in FCS_CKM.4.1.
- Proposal:
- Add following sentence to the Assurance Activity to avoid previous issue.
  - □ In the case where the only selection made for the destruction method key was removal of power or destruction of reference to the key directly followed by a request for garbage collection, then this test is unnecessary.

(Reference) The lifecycle of keys, the approved methods for key destruction, and Assurance Activities in HCD-PPver1.1



FCS_CKM.1

Cryptographic key generations

FCS_CKM_EXT.4

Keys and key materials that are no longer needed are destroyed by using an approved method.

FCS_CKM.4

Approved methods for key destruction

SFRs for the keys in the volatile memory

① single overwrite

The value of overwrite

- zeros
- ones
- TSF’s RBG
- a new value of a key
- Any value that does not contain any CSP

AA Test is “Test 1”

②removal of power to the memory

AA Test is “unnecessary”

③ destruction of reference to the key directly followed by a request for garbage collection”

AA Test is “no description available”

HCD cPP v1.0

- More content that could 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
  - Dedicated security components
  - Changes in NDcPP
- Key will be determining which of the above potential content are “absolutely necessary” for HCD cPP v1.0 and determining priorities for the other proposed changes.

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
  - Other SFRs that might be applicable

HCD cPP v1.0 Content Discussion

What do IDS WG Members think must go into HCD cPP v1.0:

- Distributed security model with block chains
- Wireless (Wi-Fi, Bluetooth, NFC, Cellular 3G/4G/5G)
- Advanced cryptographic techniques like hash-based signatures
- Mobile (e.g., guest authentication, printing, scanning)
- Integrating differences among national cryptographic requirements – cryptographic agility

HCD iTC and HCD cPP v1.0

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

HCD Security Guide Status

Next Steps – HCD cPP v1.0

- 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
- Start work on HCD cPP v1.0
  - Develop plan for development, review and release of HCD cPP v1.0
  - Determine HCD cPP v1.0 content
  - 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

Next Steps – Security Guide

- Develop Initial Draft Version
  - Review content with IDS WG at Conference Calls and F2F Meetings as it is created
- Develop Final Draft
- Obtain PWG Approval Process

Next Steps – IDS WG

- Next IDS Conference Call – Sep 19
    - Goal is to help me get ready for the HCD TC Face-to-Face on Sep 26th
- IDS Conference Call – Oct 10
    - Will review results from the HCD TC Face-to-Face on Sep 26th
- Start looking at involvement in other HCD standards activities starting Oct 10th
    - Will try to get IDS WG access to the proposed revision to ISO 15408 (the Common Criteria standard) that will be published in 2020 or access to the slides showing what has changed

BACKUP

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