The Printer Working Group

Imaging Device Security

May 17, 2018

PWG May 2018 Face-to-Face

Agenda

When	What
9:00 – 9:05	Introductions, Agenda review
9:05 – 11:50	Review results of Latest MFP TC Meetings
11:50 – 12:00	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

Summary of Apr 25 & May 8 HCD Technical Committee Meetings

April 25, 2018 HCD TECHNICAL COMMITTEE MEETING AGENDA

- Agenda Review and Introductions
- Current HCD PP Status
- Proposed Changes to HCD v1.0
  - Suggested HCD PP v1.1 Updates
  - Areas for Future Updates
- Other Topics “from the room”

Summary of Apr 25 & May 8 HCD Technical Committee Meetings

May 8, 2018 HCD TECHNICAL COMMITTEE MEETING AGENDA

- Welcome, introductions, logistics, agenda setting
- Planning topics:
  - What's should be HCD PP v1.1? Does it need to be evaluated?
  - What's after that? PPv2.0 or **c**PP v1.0?
  - International issues (v. NIST, and v. EALs)
  - Expected timeline
- Technical topics:
  - Establishing a baseline HCDPP+TDs
  - Review items and outcomes from Trondheim meeting
  - Other technical issues
- Causeway intro

Current HCD Protection Profile Status

- Developed by the MFP Technical Committee
- Approved by US and Japanese Schemes in Sep 2015
- Effective immediately in the US; Effectiveness status in Japan is up to individual vendors
  - Have been MFPs certified in both US and Japan against the HCD PP
- PP Certified by Japanese Scheme in July 2017
  - Issued Errata #1 with mostly editorial changes to HCD PP
- NIAP direction on what Assurance Activities in the PP can be met by using FIPS-certified modules (Policy 5) is being updated in July 2018
  - NIAP indicated not to expect any "significant" changes
- Early draft HCD PP v1.1 created that implements the NIAP Technical Decisions against the HCD PP and Errata #1

What should be in HCD PP v1.1?

- We are looking at several sets of changes for future HCD PPs:
  1. Roll-up of NIAP TDs and JISEC Errata
  2. Minor corrections for inconsistencies, misplaced requirements, etc.
  3. NDcPP Version 2.0 – SFRs common with the HCD PP
  4. FDE AA and EE cPP Version 2.0 - SFRs common with the HCD PP
  5. NIAP Technical Decisions for NDcPP, FDE AA cPP and FDE EE cPP
  6. Areas where the HCD PP Assurance Activities may have provided unintended functional requirements
  7. Inconsistencies in Key Management Description (KMD) Requirements
  8. Inconsistencies found by Japanese Labs & Vendors
  9. Internationalization (i.e., replace or augment NIST standards with ISO)
- The general consensus is to:
  - Include #1 and #2 in HCD PP v1.1
  - Defer #3 → #9 to be included in an HCD cPP
- Key decision is that we want to go to an HCD cPP after HCD PP v1.1 rather than develop an HCD PP v2.0

Establishing a Baseline HCD PP + TDs

- A draft HCD PP “v1.0.1” has been prepared, implementing the NIAP TDs and JISEC Errata
- After someone checks the accuracy of the implementation, we can use it as a baseline for proposing further updates
- There is an open question of whether JISEC approved all NIAP TDs

Decisions on Proposed Changes to HCD PP v1.0

- Make FAU_STG.4 Prevention of audit data loss a mandatory SFR rather than an optional SFR
  - SFR indicates what should happen when audit log becomes full
  - Agreed that this should be done
  - Like to include this change in HCD PP v1.1
- Add the following new requirement to FAU_STG.4 as FAU_STG.4.2:

  FAU_STG.4.2 The TSF shall be able to store generated audit data on the TOE itself
  - No resolution reached at either meeting
  - Action to check with JISEC on their view of this proposal
  - If implemented would be in new HCD cPP

Decisions on Proposed Changes to HCD PP v1.0

- Add the following new optional SFR:

  FMT_MTD.1/CryptoKeys Management of TSF data

  FMT_MTD.1.1/CryptoKeys The TSF shall restrict the ability to manage the cryptographic keys to U.ADMIN.

  - Not sure this is always done on MFPs
  - Agreed to the following approach:

    Instead of making a special case for crypto keys, since they are TSF data add the following row to the existing FMT_MTD.1 Management of TSF Data Table 4 --

    [assignment: list of cryptographic keys] | [selection: generate, import, export, modify, delete] | U.ADMIN
  - Will most likely be held till new HCD cPP

Decisions on Proposed Changes to HCD PP v1.0

- Add one or more of 4 new IPsec SFRs with associated Assurance Activities extracted from NDcPP v2.0 to the FCS_IPSEC_EXT.1 SFR
  - 4 SFRs to be added were considered solid IPsec requirements
  - TC felt these new SFRs should deferred to the new HCD cPP
- Split the TLS SFR (FCS_TLS_EXT.1 TLS selected) into separate SFRs for TLS acting as a Client and TLS acting as a Server
  - Agreed it was the right thing to do to be consistent with NDcPP
  - Utilize the TLS package NIAP is creating that does just this
  - Defer this change to the new HCD cPP
- Remove requirement to implement TLS 1.0 from FCS_TLS_EXT.1 as was done in NDcPP v2.0
  - Agreed that this should be done
  - Like to include this change in HCD PP v1.1

Decisions on Proposed Changes to HCD PP v1.0

- Add a new SFR **FPT_APW_EXT.1 Protection of Authentication Passwords**

  FPT_APW_EXT.1.1 The TSF shall store authentication passwords in non-plaintext form.
  - Agreed in principle this should be done, but have to resolve what authentication passwords this should apply to (e.g., should this apply only to user passwords)
  - Need to provide an adequate Assurance Activity for this new SFR
  - Once the new SFR is agreed upon, will be part of new HCD cPP

- Issue raised on whether the mandatory TLS cipher suite TLS_RSA_WITH_AES_128_CBC_SHA in FCS_TLS_EXT.1 should longer be mandated to be consistent with NDcPP v2.0 (which has all optional TLS cipher suites)
  - Agreed that all the TLS cipher suites for FCS_TLS_EXT.1 should be optional and selection-based as is the case in NDcPP
  - Should remove this particular cipher suite as was done for NDcPP
  - Would like this change included in HCD PP v1.1

Decisions on Proposed Changes to HCD PP v1.0

- Proposed Minor Modifications to Existing SFR:

  FCS_COP.1(e) Cryptographic Operation (Key Wrapping)

  FCS_COP.1.1(e) Refinement: The TSF shall perform [*key wrapping*] in accordance with a specified cryptographic algorithm [*AES*] **in the following modes [selection: KW, KWP, GCM, CCM]** and the cryptographic key size [***selection: 128 bits, 256 bits***] that meet the following: [*AES as specified in ISO/IEC 18033-3,* ***[selection: NIST SP 800-38F, ISO/IEC 19772, no other standards]***]

  - Makes this SFR wording consistent with corresponding SFR in NDcPv2.0
  - Agreed to include this change in HCD PP v1.1

Decisions on Proposed Changes to HCD PP v1.0

Proposed Minor Modifications to Existing SFR:

FCS_COP.1(i) Cryptographic Operation (Key Transport)

FCS_COP.1.1(i) Refinement: The TSF shall perform [*key transport*] in accordance with a specified cryptographic algorithm [*RSA in the following modes* ***[selection: KTS-OAEP, KTS-KEM-KWS]***] and the cryptographic key size [***selection: 2048 bits, 3072 bits***] that meet the following: [*NIST SP 800-56B, Revision 1*].

- Agreed to include this change in HCD PP v1.1

Decisions on Proposed Changes to HCD PP v1.0

Proposed Minor Modifications to Existing SFR:

FCS_PCC_EXT.1 Extended: Cryptographic Password Construct and Conditioning

FCS_PCC_EXT.1.1 A password used by the TSF to generate a password authorization factor shall enable up to [*assignment: positive integer of 64 or more*] characters in the set of {upper case characters, lower case characters, numbers, and [*assignment: other supported special characters*]} and shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm HMAC-[selection: SHA-256, SHA-512], with [*assignment: positive integer of 1000 or more*] iterations, and output cryptographic key sizes [selection: 128, 256] bits that meet the following: [*NIST SP 800-13*]

- Make this SFR consistent with the corresponding SFR in NDcPP
- Agreed to include this change in HCD PP v1.1

Decisions on Proposed Changes to HCD PP v1.0

Inconsistencies in the Key Management Description Requirements:

- Appendix F talks about requiring that the KMD is detailed enough to provide assurance that when the user enables encryption, the product encrypts all **hard storage devices**. The assurance activity for FDP_DSK_EXT.1 states that "The evaluator shall verify the KMD provides sufficient instructions to ensure that when the encryption is enabled, the TOE encrypts **all applicable Devices."**
  - Change bolded references to "Field-Replaceable Nonvolatile Storage" to be consistent with terminology in the rest of HCD PP
  - Agreed to include this change in HCD PP v1.1

Decisions on Proposed Changes to HCD PP v1.0

Inconsistencies in the Key Management Description Requirements:

- Appendix F requires that the KMD describe "The process for destroying keys when they are no longer needed by describing the storage location of all keys and the protection of all **keys stored in nonvolatile memory**."; the assurance activities for SFR FCS_CKM.4 states "The evaluator shall check to ensure the KMD lists each type of key material (software-based key storage, BEVs, passwords, etc.) and its origin, storage location, and the method for destruction for each key" which since this SFR covers keys stored in both volatile and non-volatile memory implies that storage has to be discussed for **keys stored in both volatile and non-volatile memory**.
  - Resolution was to clarify paragraph 1280 in Appendix F as to requirement applies to
  - Need to be careful about key destruction in flash memory
  - Agreed to include this change in HCD PP v1.1

Decisions on Proposed Changes to HCD PP v1.0

Areas of Implied Requirements in Assurance Activities:

- Identified 11 possible areas in the following SFRs:

FAU_GEN.1	FMT_SMF.1	FAU_STG.1	FCS_IPSEC_EXT.1.8
FIA_USB.1	FPT_TUD_EXT.1	FAU_STG.4	FCS_IPSEC_EXT.1.10
FIA_UAU.1	FAU_SAR.1	FCS_SMC_EXT.1	

- The ones that the TC agreed should be changed were:
  - **FMT_SMF.1 --** Make Assurance Activity for this SFR consistent with the Assurance Activity for FMT_MOF.1 (in HCD PP v1.1)
  - **FPT_TUD_EXT.1** -- Update to make the test for hash verification contingent on selecting that option in the SFR (in HCD PP v1.1)
  - **FAU_SAR.1** – Make Assurance Activity consistent with the SFR (in HCD PP v1.1)
  - **FAU_STG.4** – Add test to show device performs action as specified in SFR (in HCD PP v1.1)
  - **FCS_IPSEC_EXT.1.8 & FCS_IPSEC_EXT.1.10** – Align with the corresponding SFR in NDcPP v2.0; include any changes here in HCD cPP

Decisions on Proposed Changes to HCD PP v1.0

Inconsistencies Reported by JBMIA (Japanese Vendor Association):

- Inconsistency between FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)] and FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication).

  FCS_COP.1.1(g) requires us to assign the key length, but FCS_CKM.1.1(b) requires us to select 128 bits or 256 bits for the key length. That's why, if we use 160 bit length key for HMAC, we cannot claim the key generation conformance with FCS_CKM.1(b).

  - Do we need another FCS_CKM.1 for HMAC?
  - Is an inconsistency that coukd be addressed by updating FCS_CKM.1(b) to include key sizes up to 512 bits and add an App Note that for AES Keys select bit sizes of 18 and 256.
  - Agreed to address this for HCD PP v1.1

Decisions on Proposed Changes to HCD PP v1.0

Inconsistencies Reported by JBMIA (Japanese Vendor Association):

- Inconsistency of SFR dependencies

  There seem to be a lot of inconsistencies on SFR dependencies in HCD PP v1.0.

  - Agreed we need to go through all the SFRs and correct the SFR dependencies
  - Will address in HCD PP v1.1

Decisions on Proposed Changes to HCD PP v1.0

One Change Predicated on a NIAP TD for NDcPPv2.0:

Based on TD0290: Physical interruption of Trusted Path/Channel, suggesting the following minor change to the Assurance Activity for SFR FTP_ITC.1 Inter-TSF Trusted Channel :

The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each secure communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST. The evaluator shall confirm that the operational guidance contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

- Makes HCD PP would be consistent with NDcPPv2.0
- Agreed to include change in HCD PP v1.1

Other Proposed Changes to HCD PP v1.0

- SFR FCS_CKM.4 Cryptographic key destruction
  - inconsistency between the SFR and Assurance Activities for Testing:
    - Assurance Activity Test 1 has two cases, overwrite or power-cycle; but the SFR has three cases, overwrite, power-cycle, or garbage collection.
    - Result from the Apr 25th Meeting was that it was OK as is; didn't discuss at the May 8th Meeting
- FCS_HTTPS_EXT.1.3 test case is somewhat oddly worded: consider "If a peer cert is presented, the TSF shall [not require client auth] if the peer certificate is deemed invalid".
  - Change not needed so issue withdrawn from consideration at the May 8th Meeting

Other Topics Discussed

- Parking Lot items left over from HCD PP v1.0 development
  - Hopefully most of them have been resolved already
  - Will just have to go thru them off-line
- Inconsistency of SFR dependencies
  - Will address as best we can in HCD PP v1.1
- "Purge Data" may need to change to "Clear Data" to be consistent with terms and requirements from SP 800-88 (and equivalent ISO standard)
  - Will change in HCD PP v1.1

What's next? HCD PP v2.0? Or HCD cPP v1.0?

- We have several CC schemes that will support formation of an iTC
  - Sweden
  - Japan
  - Korea
  - US (support but with limited resources)
  - Canada? (this is a new idea, Canada's DND has begun asking for HCD PP)
- An HCD PP v2.0 will not resolve problems that lead vendors to certify confirming to both HCD PP and 2600.2
- We will seek to form an iTC and develop HCD cPP v1.0

Wrap Up/ Next Steps
Potential Topics for HCD cPP

- RSA Key Agreement – when NIST enforces NIST SP 800-131A
- Audit Log Server Requirements
- Assurance Activities (AAs) for Key Transport SFR (FCS_COP.1(i))
- Key Destruction SFR
- TPMs used in the TOE
- EAL Claim for HCD PP
- Password Policies
- Password Policy Applicability (normal vs. admin users)
- Wi-Fi Support
- SNMPv3 Support
- Kerberos Support
- S/MIME Support
- SMBv3 Support
- Support for TLS 1.3

International issues

- HCD PP has a mixture of references to standards, some refer to NIST SPs and others refer to ISO standards
- We inherited most (all?) of the NIST references from NDPP, so we should be able to look at how they handled it in NDcPP
- We did not discuss these in detail

Formation of an iTC to Generate an HDD cPP

- HDP cPP is needed to address the fact that European countries are requiring "EAL" CC certifications which is forcing some vendors to certify the same MFP twice – once against the HCD PP which has no EAL and once against 2600.2 which is at EAL2
- iTC formation has to be approved by the CCDB (Common Criteria Development Board) which requires two artifacts:
  - An ESR (Essential Requirements) document
  - Terms of References which addresses how the iTC will function
- We will need to establish at some point a "NIT" process for HCDs
  - Means we will set up a subgroup within the TC to address requests for interpretations of the HCD PP.

Expected Timeline for HCD PP v1.1 & Beyond

- Goal for v.1.1 proposal is November 2018
  - Need to understand the process for getting v1.1 update approved by NIAP and JISEC
- Start iTC process now with goal of getting iTC approval at October 2018 CCDB meeting
  - Will have to submit draft ESR and ToRs to the CCDB well ahead of the next CCDB meeting which is the week of Oct 22nd so the CCDB can address the creation of HCD iTC at that meeting

Action items

- Contact Dag Ströman about current iTC formation process and ESR content (Brian)
- Contact Korean CC scheme about iTC support (Kwangwoo)
- Carefully review the draft HCD PP v1.0.1 to make sure it correctly implements the TDs and Errata #1 (Alan, others?)
- Contact JISEC (through JBMIA member) about JISEC's position on NIAP TDs (Alan, through FX)
- Populate new comments database (Brian)
- Review and dispose or renew "parking lot" HCDPPv1.0 issues (Brian)
- Review SFR dependencies (has not been assigned)
- Research Purge versus Clear (Brian)

BACKUP

BACKUP

Current HCD Protection Profile Status

- Seven NIAP Technical Decisions
  - **TD0299:** Update FCS_CKM.4 Assurance Activities (Test 2) to properly address when a TOE replaces a key with another valid key
  - **TD0261:** Replace FCS_CKM.4 in its entirety (including Assurance Activities) to include destruction of keys stored in flash memory.
  - **TD0253:** Provide an Assurance Activity for FCS_COP.1(i) since there were none before
  - **TD0219:** NIAP endorsement of the errata contained in *Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017*
  - **TD0176:** Modified the App Note and Assurance Activities for this SFR so they now applied to Self-Encrypting Drives

Current HCD Protection Profile Status

- Seven Technical Decisions (cont)
  - **TD0157:** Added a new App Note and modified the Assurance Activity to reflect that fact that for some HCDs administrators are not permitted to manually configure or edit the IPsec Security Policy Database (SPD) and that BYPASS operations are not supported.
  - **TD0074:** Makes FCS_CKM.1(a) an optional rather than a mandatory requirement and moves the description of that requirement to Appendix C Optional Requirements.

Current HCD Protection Profile Status – Errata #1

- Notation error corrections
  - **4.3.1 FAU_GEN.1 Audit data generation**
  - **4.5.3 FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction**
  - **4.5.4 FCS_CKM.4 Extended: Cryptographic key destruction**
  - **4.5.6 FCS_COP.1(b) Cryptographic Operation (for signature generation/verification**
  - **4.8.4 FMT_MTD.1 Management of TSF data**
  - **4.8.5 FMT_SMF.1 Specification of Management Functions**
  - **4.13.1 FTP_ITC.1 Inter-TSF trusted channel**
  - **4.13.2 FTP_TRP.1(a) Trusted path (for Administrators)**
  - **4.13.2 FTP_TRP.1(b) Trusted path (for Non-administrators)**
  - **B1.1 FPT_KYP_EXT.1 Extended: Protection of Key and key Material**
  - **D2.5 FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication**
  - **D4.3 FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication**
  - **D4.4 FCS_SNI_EXT.1 Extended: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)** .

Current HCD Protection Profile Status – Errata #1

- Extended Components Definition (ECD) Changes
  - **A.9.4 FCS_IPSEC_EXT.1 Extended: IPsec selected** – Resolve inconsistency between ECD and FCS_IPSEC_EXT.1.5 SFR
  - **A.9.5 FCS_KDF_EXT Extended: Cryptographic Key Derivation** – Add missing rationale
  - **A.9.7 FCS_PCC_EXT Extended: Cryptographic Password Construction and Conditioning** – Add missing rationale
  - **A.9.10 FCS_SNI_EXT Extended: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)** – Add missing rationale

Current HCD Protection Profile Status – Errata #1

Fix SFR Dependencies

- **4.5.1 FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)**
- **4.5.1 FCS_CKM.1(b) Cryptographic Key Generation (Symmetric Keys)**
- **4.5.6 FCS_COP.1(b) Cryptographic Operation (for signature generation/verification**
- **4.10.4 FPT_TUD_EXT. Extended: Trusted Update**
- **D2.1 FCS_IPSEC_EXT.1 Extended: IPsec selected**
- **D2.2 FCS_TLS_EXT.1 Extended: TLS selected**
- **D2.3 FCS_SSH_EXT.1 Extended: SSH selected**
- **D2.4 FCS_HTTPS_EXT.1 Extended: HTTPS selected**

Proposed New IPsec Requirements & Associated Assurance Activities

FCS_IPSEC_EXT.1.11 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.1.12 The TSF shall generate nonces used in [selection: IKEv1, IKEv2] exchanges of length [selection:

- *[assignment: 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

] .

Proposed New IPsec Requirements & Associated Assurance Activities

FCS_IPSEC_EXT.1.13 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: IP address, Fully Qualified Domain Name (FQDN), user FQDN, Distinguished Name (DN)] and [selection: no other reference identifier type, [*assignment: other supported reference identifier types*]].

Implicit Requirements in HCD PP Assurance Activities TC Agreed Needed To Be Addressed

- **FMT_SMF.1 Specification of Management Functions**

  In testing our products against the HCD PP we found that there is an implicit requirement associated with this SFR - **that all of the security management functions listed for this SFR in the Security Target can be performed by the admin and only by the admin**. The question in whether this implicit requirement should be made explicit.

Implicit Requirements in HCD PP Assurance Activities TC Agreed Needed To Be Addressed

- **FPT_TUD_EXT.1 Extended: Trusted Update**

  The evaluator shall check to ensure that the verification of the data for updates of the TOE fails using unauthorized data for updates by means of the operation methods specified by the administrator guidance. (The evaluator shall also check those cases where **hash verification mechanism** and digital signature verification mechanism fail.)

  This isn't a requirement; rather it is an inconsistency in this test assurance activity because testing for hash verification mechanism failure should only be required if 'publish hash' is selected in **FPT_TUD_EXT.1.3**

Implicit Requirements in HCD PP Assurance Activities TC Agreed Needed To Be Addressed

- **FAU_SAR.1 Audit review**

  Check to ensure that no users other than **authorized users** can retrieve audit records.

  This is an inconsistency with the actual SFR that require that only '**an Administrator'** can retrieve the audit records**.**

- **FAU_STG.4 Prevention of audit data loss**

  Perform the following tests:

  - Generates auditable events after the capacity of audit records becomes full by generating auditable events in accordance with the operational guidance.
  - Check to ensure that the processing defined in the SFR is appropriately performed to audit records.

  There is an implicit test assurance activity that should be explicitly stated that you should test that when the audit log gets full the selected action(s) like overwriting the oldest audit log entries stated in the ST for **FAU_STG.4.1** are performed

Implicit Requirements in HCD PP Assurance Activities TC Agreed Needed To Be Addressed

- **FCS_IPSEC_EXT.1.8**

  Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection:

  - (Conditional): Configure a maximum lifetime in terms of the # of packets (or bytes) allowed following the operational guidance. Establish an SA and determine that once the allowed # of packets (or bytes) **through this SA is exceeded, the connection is renegotiated**.

  The fact that when an SA is established and that once the allowed # of packets (or bytes) through this SA is exceeded, the connection is renegotiated may be an implicit requirement for IPsec

Implicit Requirements in HCD PP Assurance Activities TC Agreed Needed To Be Addressed

- **FCS_IPSEC_EXT.1.10**

  For each supported signature algorithm, test that peer authentication using that algorithm can be successfully achieved and **results in the successful establishment of a connection**.

  The fact that peer authentication using a supported algorithm can be successfully achieved and results in the successful establishment of a connection may be an implicit requirement for IPsec