The Printer Working Group

Imaging Device Security

November 4, 2020

PWG November 2020 Virtual Face-to-Face

Agenda

When	What
10:00 – 10:05	Introductions, Agenda review
10:05 – 10:50	Discuss results of latest HCD iTC Meetings and potential HCD cPP v1.0 content
10:50 – 11:10	HCD Security Guidelines 1.0 Status
11:10 – 11:55	CCC and 3D Printing Presentation
11:55 – 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
- Vice-Chair:
  - TBD
- Secretary:
  - Alan Sukert
- Document Editor:
  - Ira McDonald (High North) – HCD Security Guidelines

HCD international Technical Community (iTC) Status

HCD international Technical Community (iTC)

- HCD iTC formally approved by Common Criteria Management Committee in Feb 2020

- Key HCD iTC Officers:
  - Chairperson – Kwangwoo Lee, HP
  - Deputy Chairperson – Alan Sukert
  - CCDB Liaison - Eunkyoung Yi, Korean Scheme
  - Editors – Alan Sukert; Brian Volkoff, Ricoh; Geraldo Colunga, HP
  - Record Manager – TBD (Kwangwoo Lee acting for now)

HCD international Technical Community (iTC)

- Agreed to hold bi-weekly meetings. However, to resolve comments against the draft HCD collaborative PP (cPP) and Supporting Document (SD), went to weekly meeting.
- Since last IDS F2F on August 19th, meetings have been held on:
  - August 24th & 31st
  - September 7th, 14th & 21st
  - October 5th, 12th, 19th & 26th
  - November 2nd

HCD cPP/SD Status

- Released first internal draft of the HCD cPP v1.0 on July 21,2020
  - Received 68 comments against that draft version
  - All comments have been adjudicated by the HCD iTC
  - Final tally:
    - 59 Comments Accepted
    - 4 Comments Accepted in Principle but will be addressed in a later v1.0 draft
    - 5 Comments Deferred to be addressed by the HCD iTC at a later point in time

HCD cPP/SD Status

- Released first internal draft of the HCD SD v1.0 on 8/26/20
  - Received 28 comments against that draft version
  - All comments have been adjudicated by the HCD iTC
  - Final tally:
    - 12 Comments Accepted
    - 9 Comments Accepted in Principle but will be addressed in a later v1.0 draft
    - 6 Comments Deferred to be addressed by the HCD iTC at a later point in time
    - 1 Comment Not Accepted

HCD cPP/SD Status
HCD iTC Network Subgroup

- Is a Network Subgroup of the HCD iTC looking at what to do with the functional and assurance requirements for the four Secure Protocols – IPsec, TLS, SSH and HTTPS – in HCD cPP/SD v1.0
- Key points from the Network Subgroup meetings so far:
  - The Network Device (ND) TLS subgroup is addressing TLS 1.3 and DTLS but there is no ND SSH subgroup.
    - We should include TLS 1.3 in HCD cPP/SD v1.0 if ND does incorporate TLS 1.3 into the next published ND cPP/SD updates within the next year as the ND TLS Subgroup indicates it plans to do
  - SSH requirements are being addressed by the CCUF Crypto Working Group which has released an SSH package
  - The Network SG clearly agrees that both TLS and SSH should split requirements into separate client and server requirements

HCD cPP/SD Status
HCD iTC Network Subgroup

- It is recommended that IPP should be considered from later versions of the HCD cPP/SD beyond v1.0.
- The current Network SG recommendation is that the HCD iTC use the IPsec, TLS, SSH and HTTPS requirements taken from ND cPP/SD v2.2e **as the basis** for the SFRs/assurance activities in HCD cPP/SD v1.0
  - However, in long term goal is to establish cross-functional teams to develop packages for each of the four Secure Protocols that can be referenced by any cPP or SD that needs to use any of the protocols
  - Need to determine if that also includes any of the FIA_X509_EXT.* SFRs/Assurance Activities related to certificate evaluation
- Regarding DTLS, the current Network SG position is that HCD cPP/SD v1.0 will not include requirements for DTLS unless vendors indicate that they need to support it

HCD iTC Status
Key Issues Raised Since August F2F

- Ricoh Proposal on Non-Field Replaceable Non-Volatile Storage that non-field replaceable non-volatile storage be allowed to store key material in clear text rather than encrypted as long as the HCD had some type of "purge" function that would allow the key material to be deleted when the HCD was ready to be decommissioned or moved to another location
  - Issue was that the Essential Security Requirements (ESR) document approved by the Common Criteria Development Board (CCDB) contained the following requirement:

    "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 in such a way 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 Issues Raised Since August F2F

- The bolded text would seem to imply, depending on how you interpreted what "protected" meant, that the ESR would not allow such a proposal, so if we agreed on this proposal the ESR would have to be changed
- Any change to the ESR would have to be approved by the CCDB so ESR changes cannot be taken lightly
- If we are going to make this change, assuming this proposal is eventually accepted, that there will likely be other ESR changes required as we develop the HCD cPP/SD v1.0 so we should submit all the ESR changes at one time
- Are several arguments for and against this proposal. For example, it was pointed out that if the HCD become broken and the purge cannot be performed that the key material is still vulnerable.
- Formed an iTC subcommittee to come up off-line with a recommendation to the full iTC
  - Recommended to 'Defer' proposal because would require an ESR change to implement
  - Need HCD iTC to agree whether to ask HCD WG to change ESR to allow this change

HCD iTC Status
JBMIA Issue on Key Material Collection

HCD cPP ESR v0.7 requires that the initial data of the key chain stored on the nonvolatile storage device should be "protected".

But, since the initial value of the key chain is unquestionably plaintext, depending on the definition of "protection", it is not allowed to store the initial value in TOE. It would force users having a big trouble to get the key for storage encryption.

We have to find a means to get the plaintext initial value of the key chain from outside of the HCD, or to store the initial value protected with some methods in HCD.

HCD iTC Status
JBMIA Issue on Key Material Collection

	Options to get Intial Value	Consideration
1	Define the SFRs(*) so that they require the initial value of the key chain to be provided from the external entities (e.g. the external server, passcode input by the user).	The operation of the SFRs seems not practical for multifunction device. In the case of passcode entry, the entropy acquisition might be a concern.
2	Define a concept of "protected memory", and define the SFRs so that it allows TOE to store the plaintext initial value in the "protected memory".	How to define the "protected memory" which can be evaluated objectively is an issue. Is it acceptable if the protected memory product is CC certificated?

(*) e.g. FPT_KYP_EXT.1

- Data Encryption Key should be reproducible after HCD restarting.

  HCD cPP requires that user document data and HCD critical data stored in the non-volatile storage are encrypted, and that the data encryption key (DEK) is not stored in the non-volatile storage with plaintext format. That’s why, DEK should be derived from some kind of the key materials. It means that the key materials should be the same whenever HCD restarts.

HCD iTC Status
JBMIA Issue on Key Material Collection

Requirements Gap in FDE cPP 2.0e

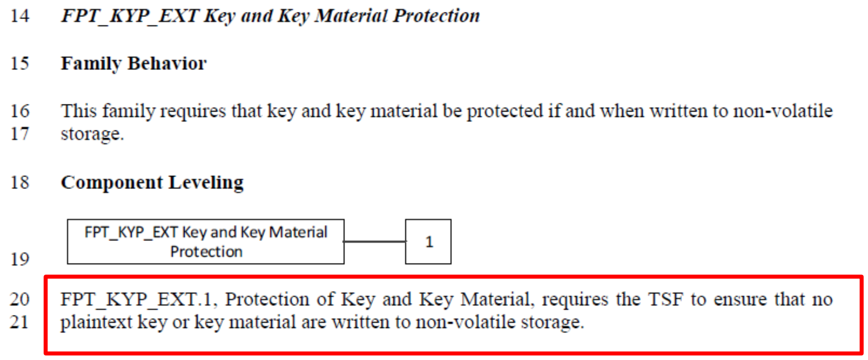
Even in FDE cPP 2.0e, there is a gap between the component definition and the detailed SFR for Key and Key Material Protection.

In the component definition of FPT_KYP_EXT.1, the definition does not allow TSF to store the plaintext key or key material NV storage.
# refer to the next page.

On the other hand, SFR of FPT_KYP_EXT.1.1 does allow TSF to store the plaintext key or key material within some conditions.
# refer to the next page.

HCD iTC Status
JBMIA Issue on Key Material Collection

C.2 Extended Component Definitions



FPT_KYP_EXT Key and Key Material Protection

Family Behavior

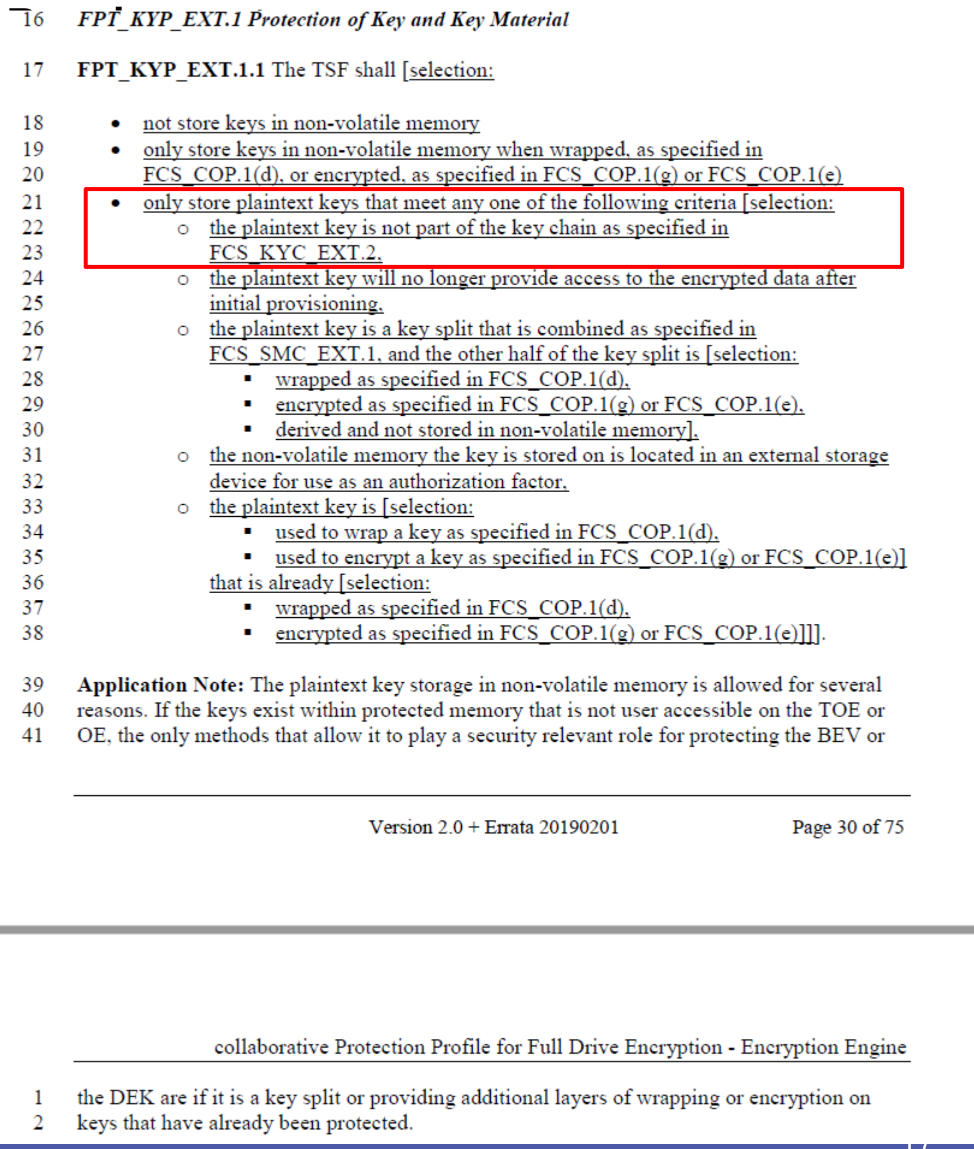
This family requires that key and key material be protected if and when written to non-volatile storage.

Component Leveling

FPT_KYP_EXT Key and Key Material Protection
1

FPT_KYP_EXT.1, Protection of Key and Key Material, requires the TSF to ensure that no plaintext key or key material are written to non-volatile storage.

5. Security Functional



FPT_KYP_EXT.1 Protection of Key and Key Material

FPT_KYP_EXT.1.1 The TSF shall [selection:

- not store keys in non-volatile memory
- only store keys in non-volatile memory when wrapped, as specified in FCS_COP.1(d), or encrypted, as specified in FCS_COP.1(g) or FCS_COP.1(e)
- only store plaintext keys that meet any one of the following criteria [selection:
  - the plaintext key is not part of the key chain as specified in FCS_KYC_EXT.2,
  - the plaintext key will no longer provide access to the encrypted data after initial provisioning,
  - the plaintext key is a key split that is combined as specified in FCS_SMC_EXT.1, and the other half of the key split is [selection:
    - wrapped as specified in FCS_COP.1(d),
    - encrypted as specified in FCS_COP.1(g) or FCS_COP.1(e),
    - derived and not stored in non-volatile memory],
  - the non-volatile memory the key is stored on is located in an external storage device for use as an authorization factor,
  - the plaintext key is [selection:
    - used to wrap a key as specified in FCS_COP.1(d),
    - used to encrypt a key as specified in FCS_COP.1(g) or FCS_COP.1(e)]

    that is already [selection:
    - wrapped as specified in FCS_COP.1(d),
    - encrypted as specified in FCS_COP.1(g) or FCS_COP.1(e)]]].

Application Note: The plaintext key storage in non-volatile memory is allowed for several reasons. If the keys exist within protected memory that is not user accessible on the TOE or OE, the only methods that allow it to play a security relevant role for protecting the BEV or

Version 2.0 + Errata 20190201 Page 30 of 75

collaborative Protection Profile for Full Drive Encryption - Encryption Engine

the DEK are if it is a key split or providing additional layers of wrapping or encryption on keys that have already been protected.

Reference: FDE cPP 2.0e

HCD iTC Status
Proposed Public Review Process for HCD cPP Documentation

Phase	Timeline	Description
Internal Draft	1st working draft release : 2020.07.21 (Tue) * Call for comment (SME) : 2020.07.21 (Wed) ~ 2020.08.17 (Mon) [4W] * Comment resolution : 2020.08.18 (Tue) ~ 2020.09.22 (Tue) [5W] * Editors works : 2020.09.23 (Wed))- 2020.10.19(Mon) [4W] 2nd working draft release : 2020.10.20 (Tue) * Call for comment : 2020.10.20 (Tue) ~ 2020.11.16 (Mon) [4W] * Comment resolution : 2020.11.17 (Tue) - 2020.12.18 (Fri) [4.5W] * Editors works : 2020.12.19 (Sat) – 2021.2.1 (Mon) [5.5W] (Editor's time off : End of 2020)	The normal, pre-release process for creating the working draft. 1st WD : Initial version - 2020.07.21 - *File name: HCD-CPP DRAFT 07-21-2020.pdf* 2nd WD : Ed, Ge, Te, New work item (at least title) – Date - *File name: HCD-CPP DRAFT 10-20-2020.pdf* Public Review Draft 1 : Ed, Ge, Te (**V0.6X**) Public Review Draft 2 : Ed, (Ge, Te) (**V0.7X**) [Optional] Public Review Draft 3 : Ed (**V0.8X**) Proposed Draft : Ed (**V0.9X**) Final Document Published (**V1.0**)
Public Review Draft 1	45 days (2021.02.02 (Tue) ~ 2021.03.19 (Fri)	HCD-iTC has voted according to Terms of Reference to release this version for public review. Public (i.e. from non-iTC participants) comments are accepted during this period
Public Review Draft 1 Update	Up to 60 days (2021.03.20 (Sat) ~ 2021.05.17 (Mon))	The HCD-iTC will review all received comments and update the documents accordingly
Public Review Draft 2	45 days (2021.05.18 (Tue) ~ 2021.07.01 (Thu))	HCD-iTC has voted according to Terms of Reference to release this version for public review. Public (i.e. from non-iTC participants) comments are accepted during this period
Public Review Draft 2 Update	Up to 60 days (2021.07.02 (Fri) ~ 2021.08.28(Sat))	The HCD-iTC will review all received comments and update the documents accordingly
Proposed Draft	30 days+ (2021.08.29 (Sun) ~ 2021.09.30(Thu))	HCD-iTC has voted according to Terms of Reference to propose this as the final document. Public (i.e. from non-iTC participants) comments are accepted during this period
Proposed Update	10 days+ (2021.10.01(Fri) ~ 2021.10.12 (Tue)	HCD-iTC reviews any further comments and prepares the document for final publishing (updating all dates, producing official versions for publication)
Final Document Published		Documents are posted to Common Criteria Portal

HCD iTC Status
Changes to the Schedule

- Release of 2nd Internal Draft HCD cPP delayed until week of 10/26/2020
  - Comments due by Nov 23rd
  - Comments resolved by Dec 15th
  - Updates to HCD cPP to be completed by Jan 6, 2021
- Release of 2nd Internal Draft HCD SD delayed until 11/09/2020
  - Comments due by Dec 7th
  - Comment resolution date now scheduled for Dec 23rd, but may be moved to early Jan
  - Updates to HCD SD now scheduled to be completed by Jan 13, 2021
- Added 3rd Internal Draft of both HCD cPP and HCD SD for sometime in Jan 2021 (date TBD)
  - Will only review changes; not full text
- Date of 1st Public Review Drafts still scheduled for 2/2/21

HCD iTC Status
Other Issues

- Need to get Security Problem Definition publicly reviewed and approved
- Inclusion of ALC_FLR is still a possibility
  - Problem will be developing Assurance Activities for ALC_FLR that will meet NIAP's requirements of being "achievable", "repeatable", "testable" & "consistent"
- When to start adding new SFRs and Assurance Activities into the HCD cPP and SD drafts
  - Could be a soon as the 3rd Internal Draft
- How much of what is in ND cPP v2.2e for the Secure Protocol SFRs/Assurance Activities will be included?
- What other current SFRs and associated assurance activities in the draft HCD cPP other than the Secure Protocol ones may need to be updated to sync with their corresponding SFRs and Assurance Activities in ND cPP v2.2e and ND SD v2.2

HCD iTC Status
Other Issues

- From the August 19th IDS F2F, it was stated that the following SFRs and Assurance Activities should be included in HCD cPP/SD v1.0:
  - Support for FIPS 140-3
  - Removal of all SHA-1 support
  - Removal of support for TLS 1.0 and TLS 1.1
  - “Hardware-anchored integrity of hardware/software”
- What else might be considered “absolutely necessary” for HCD cPP/SD v1.0:
  - Expansion of network-fax separation to “no bridging”
  - Syncing with applicable updates to ND cPP and FDE cPPs
  - Syncing with any applicable NIST SP updates
  - Inclusion of any applicable NIAP TDs to HCD PP and ND & FDE cPPs
  - Syncing with ENISA and the new proposed European cybersecurity certification scheme (EUCC) and NIST Cybersecurity Framework
  - Changes to ISO/IEC 15408 if they come out in the v1.0 time frame

HCD Security Guidelines Status

INCITS Presentation – Common Criteria and How It Could Be Applied to 3D Printing

Common Criteria Certification Security Concept

Security is concerned with **protection of assets**

The concept is that:

- You determine what assets need to be protected
- Determine what are the threats that result in risks to these assets that need to be protected
- Determine what countermeasures are needed to either counteract or minimize the risks caused by the threats

The basic security triad is CIA:

- **Confidentiality –** Prevent unauthorized access
- **Integrity –** Prevent unauthorized change/destruction
- **Availability –** Have access when requested

WHAT IS COMMON CRITERIA CERTIFICATION?

What is Common Criteria Certification?

- Common Criteria Certification is the international computer security certification process defined by ISO/IEC Standard 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security.
- It consists of three parts:

1. Part 1: Introduction and general model
2. Part 2: Security functional requirements (SFRs)
3. Part 3: Security assurance requirements (SARs)

There also is an accompanying Common Methodology for Information Technology Security Evaluation (CEM) document that describes how the SFRs and SARs in Parts 2 and 3, respectively, are to be evaluated.

Common Criteria Certification Key Terminology

- **Target of Evaluation (TOE):** A set of software, firmware and/or hardware possibly accompanied by guidance.

  The TOE is what gets certified. It can be anything from a piece of hardware, a software application, part of a product, an operation system to a complete software/hardware/system product
- **Protection Profile:** Implementation-independent statement of security needs for a TOE type (in this case the TOE type will be "3D printers")
- **Security Target:** Implementation-dependent statement of security needs for a specific identified TOE
- **Evaluation Scheme:** Administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community

Common Criteria Certification TOE Specifications

The two main specifications that will define the requirements for a product to be certified are the Protection Profile and the Security Target.

- **Protection Profile (PP):** Implementation-independent statement of security needs for a TOE type (i.e. generic class of products like HCDs)
- **Security Target (ST):** Implementation-dependent statement of security needs for a specific identified TOE (i.e., a specific product)

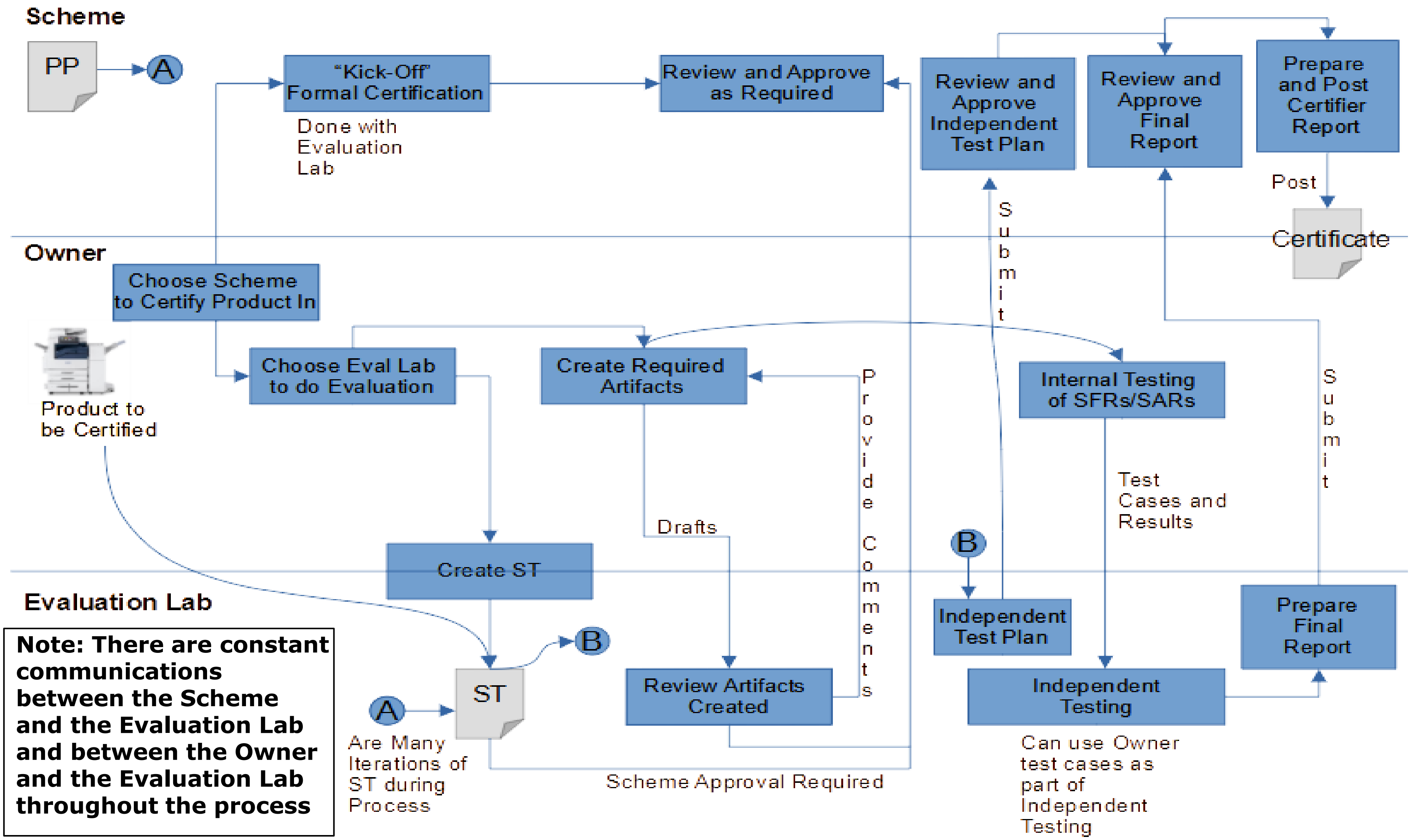
The process is that most Evaluation Schemes will require that any product to be certified by that Scheme must be certified against a PP approved by that Scheme

- The PP contains the minimum set of SFRs and Assurance Activities that every product of the type the PP covers must meet.
- When a product of the type covered by a PP is certified, an ST based on that PP that claims that PP will be created that uses the applicable SFRs and corresponding Assurance Activities from the PP tailored to the specific implementation details for the product being certified.
- It is this resultant ST that the product will be evaluated against

Common Criteria Certification PP and ST Content

Protection Profile	Security Target
For the generic class of products, the PP includes:	For a specific product in the generic class covered by the PP, the ST includes for the product being certified:
• Overview of the class of products • Conformance claim (i.e., what EAL is being claimed if any) • Security Problem Definition for the general class of products covered by the PP • Security Objectives for the class of products • Definition of any components modified from CC Part 2 • Security Requirements ○ Security Functional Requirements (SFRs) ○ Assurance Activities for each SFR plus additional Security Assurance Requirements taken from CC Part 3 ○ Rationale for both sets of Security Requirements Note: The Security Requirements listed in this PP must be applied as appropriate to any products that are certified against this Protection Profile	• Overview of the product • Conformance Claim – Usually this will be Exact Conformance to the applicable PP (i.e., per the PP with no deviations) • Security Problem Definition (usually same as what is in the PP) • Security Objectives (usually same as what is in the PP but can differ if necessary) • Definition of any components modified from CC Part 2 • Security Requirements ○ Security Functional Requirements (SFRs) included from the PP ○ Assurance Activities for the SFRs included from the PP and the SARs from the PP • Rationale for the Security Requirements included in the ST • TOE Summary Specification – Provides a technical description how the SFRs included in the ST are satisfied

Common Criteria Certification Process



Scheme

PP

A

"Kick-Off" Formal Certification

Done with Evaluation Lab

Review and Approve as Required

Review and Approve Independent Test Plan

Review and Approve Final Report

Prepare and Post Certifier Report

Post

Certificate

Submit

Owner

Choose Scheme to Certify Product In

Product to be Certified

Choose Eval Lab to do Evaluation

Create Required Artifacts

Provide Comments

Internal Testing of SFRs/SARs

Test Cases and Results

Submit

Drafts

B

Create ST

Evaluation Lab

Note: There are constant communications between the Scheme and the Evaluation Lab and between the Owner and the Evaluation Lab throughout the process

ST

B

A

Are Many Iterations of ST during Process

Review Artifacts Created

Scheme Approval Required

Independent Test Plan

Independent Testing

Can use Owner test cases as part of Independent Testing

Prepare Final Report

Common Criteria Certification

End result of a Common Criteria Certification is NEVER that the product being evaluated is secure

It is that the product being evaluated meets or does not meet its specification (either the PP or the ST as appropriate)

HCD SECURITY PROBLEM DEFINITION

What is a Hardcopy Device?

A Hardcopy Device is defined as “A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, MFPs (multifunction peripherals), MFDs (multifunction devices), “all-in-ones,” and other similar product”

Although the definition “technically” could embrace 3D printers, all the security work to date has been around 2D printers and has focused on two main areas:

- Single Function Printers that can only print
- Multi-Function Devices (devices that can do two or more of print, scan, copy, PSTN fax and many other functions)

Typical 2D Hardcopy Device Use Cases

Principally performing one or more of the following functions:

- Printing
- Copying
- Scanning

Other important security-related functions that Hardcopy devices perform are:

- Configuration of security settings by authorized administrators
- Monitoring security-related events in audit logs by authorized personnel
- Verifying the integrity and authenticity of software updates
- Checking for malfunctions via self-tests during power-up sequences

Typical 2D Hardcopy Device Use Cases

Hardcopy Devices may also perform the following optional functions:

- Send and receive fax over PSTN
- Store electronic documents temporarily or permanently in volatile or non-volatile memory on the device
- Overwrite temporary user image data stored on the device
- Store audit log data on the device
- Purge customer data on the device to aid redeployment or decommissioning of a device

2D Hardcopy Devices Key Security Threats

- Unauthorized Access to user document data stored in the HCD (primarily in non-volatile storage)
- Unauthorized Access to TSF data stored in the HCD
- Unauthorized Access to User and TSF data transmitted to/from the HCD over a network
- Unauthorized Software Update
- Failure of the TSF

2D Hardcopy Devices
Key Security Assumptions

Title	Assumption
Physical Security	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment
Network Security	The Operational Environment is assumed to protect the HCD from direct, public access to its LAN interface
Administrator Trust	The HCD Owner shall establish trust that Administrators will not use their privileges for malicious purposes
Trained Users	Authorized Users are trained to use the HCD according to site security policies

2D Hardcopy Devices
Key Organizational Security Policies

Title	Policy
User Authorization	Users must be authorized before performing Document Processing and administrative functions
Auditing	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity
Protected Communications	The HCD must be able to identify itself to other devices on the LAN
PSTN Fax-Network Separation	If the HCD includes a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN
Storage Encryption	If the HCD stores User Document Data or Confidential TSF Data on Nonvolatile Storage Devices, it will encrypt such data on those devices

2D Hardcopy Devices Key Organizational Security Policies

Title	Policy
Key Material	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device
Image Overwrite	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Nonvolatile Storage Devices
Purge Data	The HCD shall provide a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices

2D Hardcopy Devices
Key Security Objectives of the HCD

Title	Objective
User Identification and Authentication	Perform identification and authentication of Users for operations that require access control, User authorization, or Administrator roles
User Authorization	Perform authorization of Users in accordance with security policies
Access Control	The HCD shall enforce access controls to protect User Data and TSF Data in accordance with security policies
Administrator Roles	The HCD shall ensure that only authorized Administrators are permitted to perform administrator functions
Software Update Verification	The HCD shall provide mechanisms to verify the authenticity of software updates
Self-Test	The HCD shall test some subset of its security functionality to help ensure that subset is operating properly
Auditing	The 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 TOE

2D Hardcopy Devices
Key Security Objectives of the HCD

Title	Objective
Communications Protection	The HCD shall have the capability to protect LAN communications of User Data and TSF Data from Unauthorized Access, replay, and source/destination spoofing
Storage Encryption	If the HCD stores User Document Data or Confidential TSF Data in Nonvolatile Storage devices, then the HCD shall encrypt such data on those devices
Image Overwrite	Upon completion or cancellation of a Document Processing job, the HCD shall overwrite residual image data in its Nonvolatile Storage Devices
Protection of Key Material	The HCD 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 Nonvolatile Storage Devices; The HCD shall ensure that such key material is not stored in cleartext on the storage device that uses that material
Purge Data	The HCD provides a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices
PSTN Fax-Network Separation	If the HCD provides a PSTN fax function, then the HCD shall ensure separation of the PSTN fax telephone line and the LAN, by system design or active security function

2D Hardcopy Devices
Key Security Objectives of the Operating Environment

Title	Objective
Physical Protection	The Operational Environment shall provide physical security, commensurate with the value of the HCD and the data it stores or processes
Network Protection	The Operational Environment shall provide network security to protect the HCD from direct, public access to its LAN interface
Trusted Administrators	The HCD Owner shall establish trust that Administrators will not use their privileges for malicious purposes
Trained Users	The HCD Owner shall ensure that Users are aware of site security policies and have the competence to follow them
Trained Administrators	The HCD Owner shall ensure that Administrators are aware of site security policies and have the competence to use manufacturer’s guidance to correctly configure the HCD and protect passwords and keys accordingly

WHAT ABOUT 3D PRINTERS?

2D Printing vs 3D Printing

At the 10,000 foot Level, 2D Printing and 3D Printing are not that dissimilar.

Essentially 2D Printing is converting a document from an electronic representation of the document stored on an IT device or some other type of media to a physical representation of the document on some type of paper

Similarly, 3D printing is essentially converting an object that is desired to be printed from an electronic representation of the object in terms of a CAD file and later an STL/3MF file to a physical representation of the object in terms of the final 3D printed object

Digital Thread for Additive Manufacturing Process Steps

1. Product Inception
   - Requirements Definition
   - Concept generation/evaluation
   - Design intent
2. Design/Scan and Analyze
   - **CAD file created** (asset that needs to be protected?)
   - Traditional analysis
   - **Advanced multi-physics modeling and simulation** (asset that might need to be protected?)
3. Build and Monitor
   - **Simulation of build** (asset that needs to be protected?)
   - Detailed Build Plan and Machine Data
   - Part Fabrication (includes **Slicer software** which may be an asset that needs to be protected)
   - Per part post processing and finishing

Digital Thread for Additive Manufacturing
Other Assets That Might Need to Be Protected

- Software on the computer storing the CAD File
- Software of the 3D Printer that controls the 3D printer
- STL or 3MF file the CAD file is transformed into

Digital Thread for Additive Manufacturing
Some Data and IT Security Concerns

- Cybersecurity Threats
  - Espionage
  - Tampering / Hacking / Mischief / Extortion / Terrorism
  - Privacy
  - Intellectual Property / Trade Secrets
- Data Integrity along the entire Digital Thread
- Protect Data Confidentiality
- Ensure/Protect Data Integrity
- Verify Data Integrity
- Protect Intellectual Property

3D Printers and Common Criteria Certification

Could the Common Criteria Certification process that was used to certify 2D Hardcopy Devices be used to perform a similar security certification for the Digital Thread for Additive Manufacturing?

Remember – The high-level goal of a Common Criteria Certification is to provide confidence to the owner for the product in question that the mitigations they have put in place to protect the assets that need to be protected from the identified security threats are correct and sufficient.

It does that by determining that the product meets its specification of the security requirements as stated in the Security Target by evaluating that the product passes the assurance requirements stated in the Security Target.

3D Printers and Common Criteria Certification

Could the Common Criteria Certification process that was used to certify 2D Hardcopy Devices be used to perform a similar security certification for the Digital Thread for Additive Manufacturing?

Paul and I think the answer is '**YES IT CAN BE**'

Fundamentally what would be needed is to define:

1. What are the assets that need to be protected in the Digital Thread for Additive Manufacturing
    - CAD and STL/3MF files
    - Software
    - Simulations
    - Slicer software
    - etc.

3D Printers
Security Problem Definition

Need to determine what the Security Problem Definition (SPD) for the Digital Thread is:

- What are the key security threats to those assets?
- What key assumptions need to be made around protection of these key assets
- What key organizational security policies need to be in place to assure that the key assets are protected
- What security objectives does the 3D printer and its operating environment have to meet to ensure that the key threats identified above are either mitigated or eliminated?

3D Printers
Some Thoughts on Threats to the Digital Thread

- Recall the 5 Threats to 2D Printers
  - Unauthorized Access to user document data stored in the HCD (primarily in non-volatile storage)
  - Unauthorized Access to TSF data stored in the HCD
  - Unauthorized Access to User and TSF data transmitted to/from the HCD over a network
  - Unauthorized Software Update
  - Failure of the TSF

We think some of same threats might apply to the Digital Thread:

- Unauthorized access to the CAD file and model/simulations while stored on the computer hosting the CAD file/models/simulations (even if it is the 3D printer)
- Unauthorized access to the STL/3MF file created from the CAD file while stored in either on the computer hosting the CAD file or on the 3D printer itself
- Unauthorized access to the STL/3MF file while in transit between the computer hosting the CAD filer and the 3D printer if stored on separate computers
- Unauthorized access to the build simulation and slicer software stored on the 3D printer
- Unauthorized software upgrade of either the computer hosting the CAD file or the 3D printer

3D Printers
Answers to the key security questions (in our view)

- As far as Assumptions and Security Policies that is something that would have to be determined
- Regarding Security Objectives, we think the following 2D Security Objectives might also apply in total or in part to the Digital Thread:
  - User Identification and Authentication
  - Access Control
  - Software Update Verification
  - Self-Test
  - Communications Protection
  - Storage Encryption
  - Protection of Key Material

Once you have an SPD then you can start determining what Security Requirements from CC Part 2 and what associated Security Assurance Requirements will be necessary to meet the security objectives of the Digital Thread for Additive Manufacturing

3D Printers
Common Criteria Certification Next Steps

- If the SPD for 3D Printers is similar enough to the SPD for 2D Printers, and we think it is based on the previous slides, then the Common Criteria Certification approach could work for providing a level of security assurance to the Digital Thread for Additive Manufacturing
- Next Steps would be to:
  - Create of a 3D Printing Technical Community (TC) to work this problem in coordination with the HCD international TC
  - Determine who the customers/audience for this TC would be
  - Generate an approved 3D Printing Protection Profile. Our initial thought is that it could be a PP-Module based off of the HCD collaborative PP that is currently being developed for publication sometime in 4Q 2021
  - Recognize this will take time; realistically we are probably talking end of 2022 at the earliest before we would have a PP
  - Once we have a 3D Printing PP we can start certifying 3D Printers against that PP

Next Steps – IDS WG

- Next IDS Conference Call – Nov 12, 2020
- Next IDS Face-to-Face Meeting Feb 9-11, 2021 (probably Feb 10) at next PWG Virtual F2F
- Start looking at involvement in some of these other standards activities individually and maybe as a WG