The Printer Working Group

Imaging Device Security

November 17, 2022

PWG November 2022 Virtual Face-to-Face

Agenda

When	What
10:00 – 10:05	Introductions, Agenda review
10:05 – 11:00	Discuss results of latest HCD iTC Meetings and HCD cPP/SD v1.0 status
11:00 – 11:25	ASTM ICAM 2022 Presentation Summary
11:25 – 11:30	HCD Security Guidelines v1.0 Status
11:30 – 11:55	TCG/IETF Liaison Reports
11:55 – 12:00	Wrap Up / Next Steps

Antitrust and Intellectual Property Policies

"This meeting is conducted under the rules of the Antitrust and PWG IP policies".

- Refer to the Antitrust and 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)

- Since last IDS F2F on August 18, 2022 HCD iTC meetings have been held on:
  - August 22nd, 29th
  - September 12th, 19th, 21st, 26th, 28th
  - October 3rd, 10th, 17th, 24th, 26th, 31st
  - November 7th, 10th

HCD cPP/SD Status

- HCD cPP V1.0 published on October 31, 2022

	Internal Drafts	1st Public Draft	2nd Public Draft	Final Draft	Total
Comments against Security Problem Definition - 19 All were accepted					19
Accepted	161	70	56	52	339
Accepted in Principle	3	0	0	1	4
Deferred	16	1	10	2	29
Not Accepted	11	14	17	3	45
Not Adjudicated	0	0	0	0	0
Total	191	85	83	58	436

HCD cPP/SD Status

- HCD SD V1.0 published on October 31, 2022

	Internal Drafts	1st Public Draft	2nd Public Draft	Final Draft	Total
Accepted	57	24	25	34	140
Accepted in Principle	1	0	1	1	3
Deferred	15	2	0	1	18
Not Accepted	1	2	3	2	8
Not Adjudicated	0	0	0	0	0
Total	74	28	29	38	169

HCD cPP/SD Status
Key Issues Resolved in HCD cPP V1.0 from Final Draft

- Added missing Auditable Events for the Selection-Based SFRs
- Corrected the Auditable Events table for SFR FAU_GEN.1 Audit data generation to indicated there is no additional information needed for SFR FMT_SMF.1 Specification of Management Functions
- Corrected the description of Required Use Cases of HCDs to indicate that, for auditing purposes, the HCD has the capability to protect audit logs for unauthorized disclosure or alteration" while in transit to an external IT product and, if stored in the HCD, while stored
- Corrected the description of the Optional Use Cases of HCDs to clarify that (1) this section is about wiping data and (2) that the capability to make all customer data that may be present in the HCD unavailable for recovery if it is removed from the Operational Environment is not dependent on fata being encrypted and its cryptographic keys destroyed
- Clarified that for the Storage Encryption Organizational Security Policy, destroying keys is mandatory
- Corrected the Security Objectives Tables to add the missing threats for security objective O.AUTH_FAILURES and the missing mapping between T.UNAUTHORIZED_ACCESS and O.AUTH_FAILURES

HCD cPP/SD Status
Key Issues Resolved in HCD cPP V1.0 from Final Draft

- Moved **SFR FCS_CKM.1/AKG Cryptographic Key Generation (Asymmetric Keys)** from an Optional to a Mandatory SFR
- Made 'remote audit server' a mandatory selection in SFR **FTP_ITC.1 Inter-TSF trusted channel,** elements **FTP_ITC.1.1** and **FTP_ITC.1.3**
- Removed 'AES GCM-192' as a selection option in SFR **FCS_IPSEC_EXT.1.6** to comply with NIAP Technical Decision TD0657
- Modified SFR **FPT_KYP_EXT.1 Extended: Protection of Key and Key Material** to clarify what the requirements and Application Note should be for an initial key and clarify what some of the conditions where keys can be stored are
- Removed references to "Distributed TOEs" in the document because the HCD cPP does not include any requirements for Distributed TOEs
- Included the SFR Dependencies Analysis requested by the Japanese Scheme JISEC
- Corrected multiple uses of improper SFR nomenclature throughout the document
- Implemented a consistent convention for bolding of SFRs, a consistent use of the term "Extended" for the Extended Components throughout the document and a consistent convention for listing and linking references

HCD cPP/SD Status
Key Issues Resolved in HCD SD V1.0 from Final Draft

- Provided necessary clarifications to the KMD, Guidance and Test Assurance Activities, as applicable, for the following SFRs:
  - **FCS_CKM.4 Cryptographic key destruction** regarding selections mentioned in the text
  - **FCS_COP.1/CMAC Cryptographic Operation (for cipher-based message authentication)** regarding no KMD and Guidance assurance activities required for this SFR
  - **FPT_WIPE_EXT.1 Data Wiping** regarding cryptographic erasing of data and in Test 6 to add clarification that searches for test strings are being performed on storage in unlocked state (i.e., on plaintext data being decrypted on access) and not in ciphertext data
  - **FCS_COP.1/DataEncryption Cryptographic Operation (Data Encryption/Decryption)** regarding the content of the **AES-CTR Monte-Carlo Test** tests
  - **FCS_TLSS_EXT.2.1** and **FCS_TLSS_EXT.2.2** regarding the contents of Test 1b
  - **FCS_CKM.4 Cryptographic key destruction** regarding the contents of Test 1
  - **FDP_DSK_EXT.1 Extended: Protection of Data on Disk** to provide a better description of what is meant by "special tools which allow inspection of the encrypted drive either in-band or out-of-band" in the Tests

HCD cPP/SD Status
Key Issues Resolved in HCD SD V1.0 from Final Draft

- Provided necessary clarifications to the KMD, Guidance and Test Assurance Activities, as applicable, for the following SFRs:
  - **FPT_TST_EXT.1 Extended: TSF testing** to provide additional clarification of how to induce self-test errors to the TOE as part of the tests so an evaluator can use debug version or modified firmware to achieve a failing verdict.
  - **FPT_SBT_EXT.1 Extended: Secure Boot** to clarify that the tests are modifying each stage in the boot process, not each link in the Chain of Trust.
  - **FPT_KYP_EXT.1 Extended: Protection of Key and Key Material** to clarify (1) what is required of the evaluator (and how it can be done) for determining that the key is not in the key chain and (2) what is required of the evaluator for determining that the key is stored in the protected storage device
- Moved assurance activities that were improperly placed into their proper Assurance Activity category (TSS, KMD, Guidance or Test as appropriate) for the following SFRs:
  - **FDP_DSK_EXT.1 Extended: Protection of Data on Disk**
  - **FCS_CKM.1/SKG Cryptographic key generation (Symmetric Keys)**

HCD cPP/SD Status
Key Issues Resolved in HCD SD V1.0 from Final Draft

- For SFR **FCS_CKM.1/SKG Cryptographic key generation (Symmetric Keys)**, modified the Test assurance activities so that they are consistent with the SFR and require that the evaluator follows the operational guidance to ensure that a communication channel can be initiated from authorized IT entities as well as from the TOE
- Modified SFR names for the extended components to be consistent with the nomenclature used in the HCD cPP
- Added a note to the SFR **FPT_SBT_EXT.1 Extended: Secure Boot** Test assurance activities saying that the algorithm verification for Root of Trust should be avoided, because authenticity check in Root of Trust should be performed by some kind of immutable code, so the algorithm verification tests should be difficult to perform
- Added the following note to the Test assurance activities section for all the cryptographic SFRs that are dependencies to the **FPT_SBT_EXT.1 Extended: Secure Boot** SFR - "NOTE: The tests detailed below are not required to be performed for cryptographic functions implemented in the Root of Trust for Secure Boot (FPT_SBT_EXT.1)."

HCD iTC Status
Original Proposed HCD cPP/SD Schedule – 2/9/21

Phase	Timeframe	Description
Resolve ESR Issue and Approve SPD	• Resolve ESR issue: 2/26 • Update ESR: 3/1 – 3/12 • Update SPD: 3/1 – 3/12 • Submit ESR changes to HCD WG (if needed): 3/15 • HCD WG Review and comment: 3/15 – 4/9 • Submit SPD for public review: 3/15 • SPD Public review: 3/15 – 4/16 • Update SPD and update cPP/SD: 3/29 – 4/16	Assume get response back from HCD WG in no more that 30 days
Internal Draft	• Submit 3rd internal draft: 4/19 • Review 3rd internal draft: 4/19 – 5/14 • Review comments & update documents: 5/17 – 6/11	Assume approval of ESR changes
Public Review Draft 1	• Submit 1st Public Draft: 6/14 • Review 1st Public Draft: 6/14 – 7/23 • Review comments and update documents: 7/26-9/17	Must include all new SFRs that want to include in v1.0
Public Review Draft 2	• Submit 2nd Public Draft: 9/20 • Review 2nd Public Draft: 9/20 – 10/29 • Review comments and update documents: 11/1 – 12/3	
Final Draft	• Submit Final Draft: 12/6 • Review 2nd Public Draft: 12/6/21 – 1/14/22 • Review comments and update documents: 1/17/22 – 2/11/22	
Final Document Published	• Publish Version 1.0: 2/14/22	

HCD iTC Status
HCD cPP/SD Schedule Status Update

Phase	Timeframe	Status Updates
Resolve ESR Issue and Approve SPD	• Resolve ESR issue: 2/26 **DONE** • Update ESR: 3/1 – 3/12 **NOT NEEDED** • Update SPD: 3/1 – 3/12 **DONE** • Submit ESR changes to HCD WG (if needed): 3/15 **NOT NEEDED** • HCD WG Review and comment: 3/15 – 4/9 **NOT NEEDED** • Submit SPD for public review: 5/10 **DONE** • SPD Public review: 5/10 – 6/4 **DONE** • Update SPD: 6/7 – 6/25 **DONE**	
Internal Draft	**New Proposed Schedule** • Submit 3rd internal draft: 6/1 **DONE** • Review 3rd internal draft: 6/1 – 6/18 **DONE** • Review comments & update documents: 6/21 – 7/16 **DONE**	
Public Review Draft 1	**New Proposed Schedule** • Submit 1st Public Draft: 8/18 (cPP); 8/30 (SD) • Review 1st Public Draft: 8/18 – 10/12 (45d) • Review comments and update documents: 10/13-12/10 (60d)	Was 7/19 on original schedule Note: 1st Public Draft of HCD cPP released on 8/30 – Comment end date 10/8 **DONE** 1st Public Draft of HCD SD released on 10/13 – Comment end date 11/15 **DONE**

HCD iTC Status
Updated Proposed HCD cPP/SD Schedule

Phase	Timeframe	Status Updates
Public Review Draft 2	**New Proposed Schedule (3/29/2022)** • Submit 2nd Public Draft: 12/14 DONE • Review 2nd Public Draft: 12/15 – 1/31/22 (49d) DONE • Review comments and update documents: 1/31/1/22 – 5/13/22(60d) DONE	HCD cPP 2nd Public Draft released 12/14 - DONE Comments Received by 1/31/22 - DONE HCD SD 2nd Public Draft Planned Release 12/13 – Released 2/24/22 DONE Comments due by 3/18/22 (~one month)
Final Draft	**New Proposed Schedule (as of 7/14/22)** • Submit Final Draft: 6/13/22 -> 7/18/22 DONE • Review Final Public Draft: 7/19/ – 8/22 (28d) DONE • Review comments and update documents: 8/23/22 – 9/6/22 (10d) DONE	Final Drafts of HCD cPP and HCD SD submitted for Public Review on 8/1/22; Comments received by 9/15/22 All comments received were addressed and several updated drafts of each document were created up through 10/28/22
Final Document Published	**New Proposed Schedule (as of 7/14/22)** • Publish Version 1.0: 8/2/22 -> 9/7/22 DONE	Was 3/25/22 on original schedule Because of the technical nature of some of the Final Draft comments it took 1-1/2 months to address all the issues raised. "Final" version of each document was created dated 10/31/22 and published on 10/31/22

HCD cPP/SD
Current Parking Lot Issues – HCD cPP

- Addressing hardware-based Roots of Trust stored in mutable memory as well as immutable memory
- Clarification that the Secure Boot SFR only requires verification of firmware/software that is stored in mutable memory at boot time and does not require verification of firmware/software stored in immutable memory
- Comments that require implementation of TLS 1.3 to resolve
- Support for NTP
- Addition of 3 TLS cipher suites required per NIAP Technical Decision TD422
- Add a selection in FCS_COP.1/SigGen for IKEv1 RSA schemes
- Removal of support for:
  - TLS 1.1
  - SHA-1 support
  - Cipher suites with RSA Key Generation with keys < 2048 bits
  - All RSA and DHE Key Exchanges

HCD cPP/SD
Current Parking Lot Issues – HCD SD

- Correcting TSS Assurance Activities for SFR FCS_CKM.4 Key Destruction
- Correcting Test 2 for SFR FCS_CKM.4 Key Destruction to provide a valid test for where the data read operation would fail
- Clarification of TSS Assurance Activities for SFR FIA_X509_EXT.2 X.509 Certificate Authentication

HCD cPP/SD Issues Post-Version 1.0

Implementing the HCD Interpretation Team (HIT)

- Agree on the HIT process and the HIT procedures which will describe how the HIT will operate
  - Draft procedures under review by the full HCD iTC
  - Need to create any necessary artifacts such as the Request for Interpretation (RfI) form and how to track RfI status
- Agree on who will initially be on the HIT
- Agree on the various roles needed for the HIT and who will fill those roles, especially who will be the Chair and Deputy Chair
- Based on the agreed HIT process and procedures and the HIT members begin actual HIT activities
  - Looking to have HIT implemented by end of February 2023

HCD cPP/SD Issues Post-Version 1.0

- Developing release plan for future updates of the HCD cPP and HCD SD
  - We will have major and minor releases
  - What is the time frame between minor releases – every 9 -12 months, as needed, etc.
  - What is the time frame between major releases – is it based on time (e.g., every 2 or 3 years), number of minor releases (e.g., a major release every 4 minor releases), volume of changes, number of new requirements/features added, a combination of these factors or something else
  - What goes into a major or minor release – could be any or all of:
    - Technical Decisions (TDs) approved by the HIT or Technical Recommendations (TRs) from the Interpretation Team that are approved by the full HCD iTC
    - Applicable NIAP TDs
    - Changes resulting from syncing with ND and FDE cPPs/SDs
    - Requests from Schemes, especially JISEC, ITSCC and NIAP
    - Response to new technologies, new crypto algorithms, new or updated standards or NIST SPs
    - New or updated requirements/features

HCD cPP/SD Content Post-Version 1.0

Will very likely be in next version

- Inclusion of support for TLS 1.3 and deprecation of TLS 1.1
- Inclusion of NTP
- Inclusion of AVA_VAN and ALC_FLR
- Sync with key changes in ND cPP/SD v3.0 to be published in Oct 2022
  - Incorporate NIAP SSH Package
- Changes to comply with Commercial National Security Algorithm (CNSA) Suite 2.0 to address cryptanalytically relevant quantum computers (CRQCs)
- Changes due to HCD Integration Team (HIT) responses to comments/questions to HCD cPP/SD v1.0
- Changes due to requests from JISEC, ITSCC or NIAP
- Updates to ISO/IEC 15408/18045 to be published by EOY 2022
  - Adds new SFRs in Part 2 and pre-packaged PP and ST Assurance Activities in new Part 4
- Incorporate NIAP IPsec and X.509 packages if they are available in time
- Any implications of potential mutual recognition between CC and EUCC

HCD cPP/SD Content Post-Version 1.0

Potential for inclusion in next or later versions

- Support for Wi-Fi and maybe Bluetooth
- Support for Security Information and Event Monitoring (SIEM) and related systems
- Updates due to changes from other ISO, FIPS or NIST Standards/Guidelines, NIAP TDs
- CCDB Crypto WG, other CCUF Crypto WG Packages or NIAP TLS Package
- Support for SNMPv3
- Support for NFC
- Support for new crypto algorithms
- Indirect updates based on new technologies or customer requests
- Expand to address 3D printing

HCD iTC Status
Key Next Steps

- Implement the HIT for maintaining HCD cPP/SD v1.0
- Agree on the HCD cPP/HCD SD release plan
- Determine the content for and then create the next HCD cPP/SD release (v1.1)
- Ensure that the HCD iTC continues to be fully engaged now that HCD cPP v1.0 and HCD SD v1.0 have been published

HCD iTC Status
More Lessons Learned to Date (My Take)

- I have said this before, but developing v1.0 of the HCD cPP and HCD SD in 2 years, 8 months is an accomplishment worth celebrating
- Input from Stakeholders is critical for success
- Feedback and buy-in from all vendor communities is also critical for success
- Setting an initial aggressive schedule is not advisable because it will never be met. Better to set a realistic schedule, and even that one will likely not be met

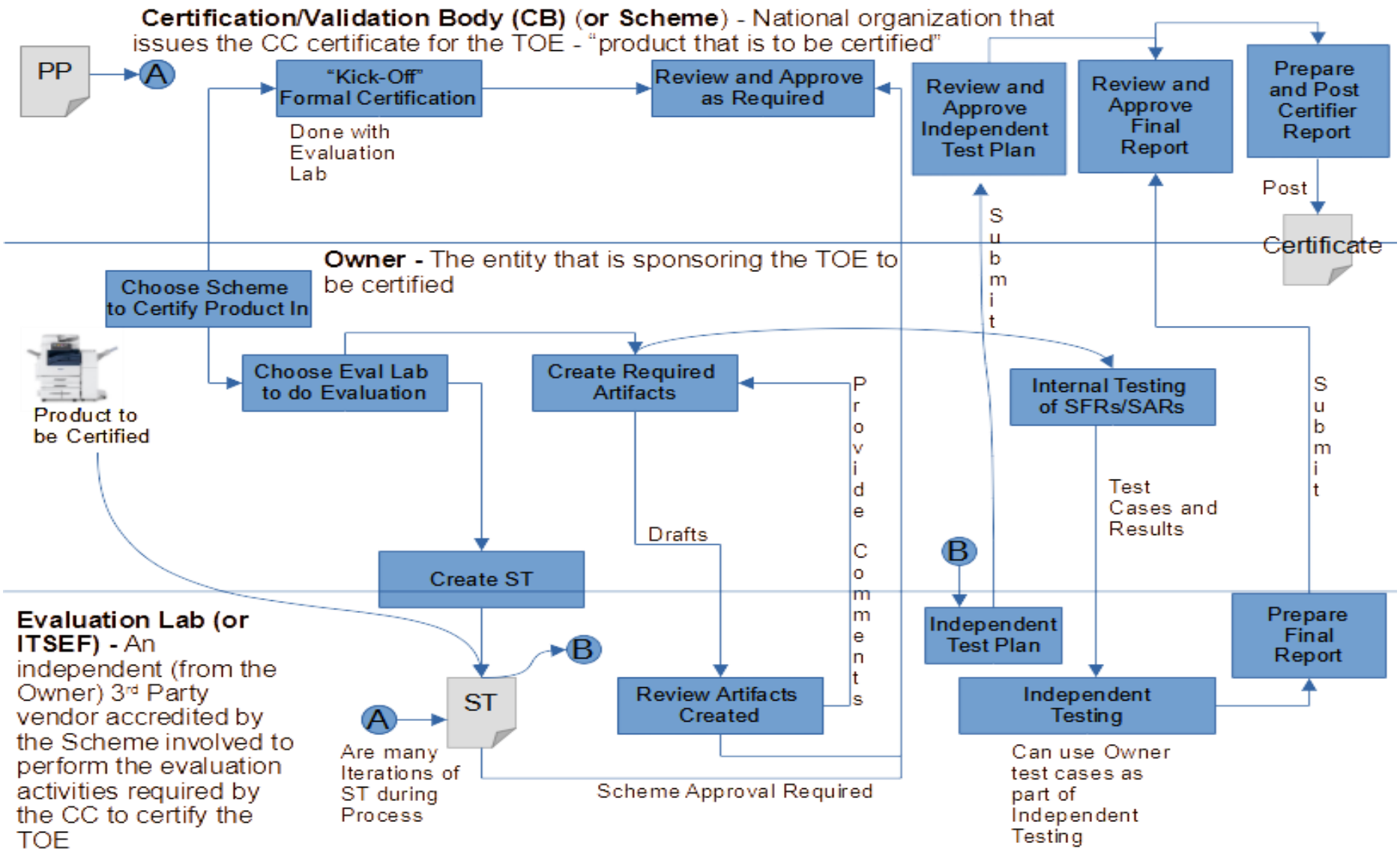
ASTM International Conference on Additive Manufacturing (ICAM) 2022 Presentation

Developing Common Criteria Based 3D Printing Equipment Cybersecurity Certification

What is Common Criteria?

- The Common Criteria for Information Technology Security Evaluation (generally shortened to just Common Criteria (CC)) is an international standard (ISO/IEC Standard 15408-1:2009) for security certification of information security products.
- Common Criteria standard is broken into 3 Parts:
  - General Process Model (Part 1)
  - Security Functional Requirements (SFRs) (Part 2)
  - Security Assurance Requirements (SARs) (Part 3)
- Is a Common Evaluation Methodology (CEM) document that defines how to apply CC to evaluate a product
- CC is governed by a Common Criteria Recognition Arrangement (CCRA) signed by 31 countries

Common Criteria Certification Process



Results of the Common Criteria Process

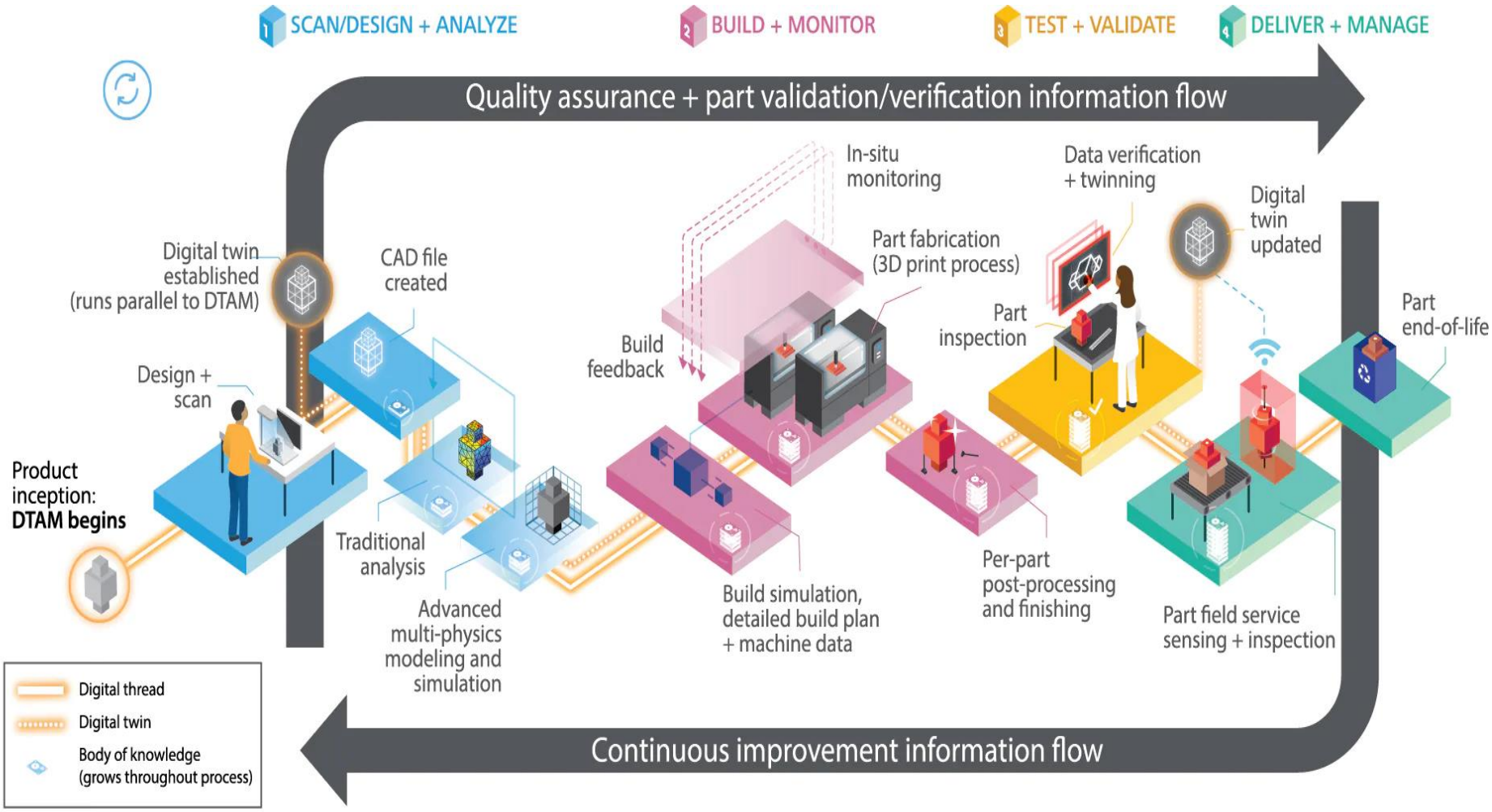
- Common Process is based on protection of assets. The concept is that:
  - You determine what assets need to be protected
  - Determine what are the threats that result in risks to these assets that need to be protected
  - Determine what countermeasures in terms or security requirements and associated assurance activities are needed to either counteract or minimize the risks caused by the threats
- The Common Criteria process is driven by three major components:
  - Protection Profile (PP): Defines security a standard set of security functional requirements for a general type of product
  - Security Target (ST): Defines a set of security functional requirements for a specific product to be certified
  - Supporting Document (SD): Defines how the product is to be inspected and evaluated to determine it meets the security functional requirements defined in the PP or ST as applicable
- End result of a CC Certification is assuring that the product being evaluated meets its requirements specification

HOW CAN COMMON CRITERIA BE APPLIED TO THE ADDITIVE MANUFACTURING PROCESS AND 3D PRINTING?

Common Criteria Certification of 2D Printers

- The industry has spent the last 17+ years developing the necessary infrastructure to perform Common Criteria Certifications on 2D printers – mostly Hardcopy Devices (HCDs) - that perform some combination of print/scan/copy/fax
- As part of this process we have identified the:
  - Key Security Threats to HCDs (and 2D printers in general)
  - Key Assumptions about the Operational Environment necessary so Key Threats can be mitigated
  - Key Organizational Security Policies (OSPs) that have to be in place in an organization to support the security of HCDs
  - Key security functions that the HCD has to perform to support the security of HCDs

Digital Thread for Additive Manufacturing



Digital Thread for Additive Manufacturing and Common Criteria Certification

Could the Common Criteria Certification process that was used to certify 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**'

Digital Thread vs. HCDs

From a security certification perspective, at the 10,000 foot Level, the Digital Thread and HCDs are not that dissimilar

- Both have major assets that must be protected from unauthorized disclosure or modification. In the case of the Digital Thread, assets can include things like:
  - CAD model
  - Build Simulations
  - STL file the CAD model is transformed into
- Both have similar security threats that these assets must be protected from such as:
  - Unauthorized access to the CAD model and build simulations
  - Unauthorized access to the STL file created from the CAD file
  - Unauthorized access to the STL file while in transit between the computer hosting the CAD model 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 model or the 3D printer

Digital Thread and Common Criteria Certification

- Similarly, the following HCD Security Objectives might also apply in total or in part to the Digital Thread for Additive Manufacturing:
  - User Authorization
  - User Identification and Authentication
  - Access Control
  - Communications Protection
  - Auditing
  - Storage Encryption
  - Firmware/Software Update Verification
  - Protection of Key Material
  - Authentication Failures
  - Strong Cryptography

Digital Thread and Common Criteria Certification Next Steps

- Identify one or more National Bodies to sponsor and then create a 3D Printing Technical Community (TC) to develop a Protection Profile (PP) for the Digital Thread (or separately for 3D Printers)
- Determine who the customers/audience for this TC would be
- Determine what are the following for the Digital Thread (or for 3D printers alone):
  - Threats
  - Key assumptions that must be upheld
  - Organizational Security Policies that must be upheld
  - Security Objectives
- Generate an approved Digital Thread/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 in 4Q 2022
- Recognize this will take a minimum of two – four years to complete
- Once we have a Digital Thread/3D Printing PP we can start certifying 3D Printers or the entire Digital Thread against that PP

HCD Security Guidelines

Liaison Status

Trusted Computing Group (TCG)

- **Next TCG Members Meetings**
  - **TCG Hybrid F2F (Vancouver, BC) – 21-23 February 2022 – Ira to call in**
- **Trusted Mobility Solutions (TMS) – Ira is co-chair and co-editor**
  - **Formal – GP (TEE, SE), ETSI (NFV/MEC/SAI)**
  - **Informal – 3GPP, GSMA, IETF, ISO, ITU-T, SAE, US NIST**
  - ***TCG TMS Use Cases v2 – published September 2018***
- **Mobile Platform (MPWG) – Ira is co-editor**
  - **Formal – GP (TEE, SE), ETSI (NFV/MEC/SAI)**
  - **Informal – 3GPP, GSMA, IETF, ISO, ITU-T, SAE, US NIST**
  - ***TCG Mobile Reference Architecture v2 – work-in-progress for review Q4 2022***
  - ***TCG TPM 2.0 Mobile Common Profile – work-in-progress for review Q4 2022***
  - ***TCG MARS 1.0 Mobile Profile – new work-in-progress Q4 2021***
  - ***TCG Runtime Integrity Preservation for Mobile Devices – Nov 2019***
  - ***GP TPS Client API / Entity Attestation Protocol / COSE Keystore – joint work***
- **Recent Specifications**
  - **http://www.trustedcomputinggroup.org/resources**
  - ***TCG Measurement and Attestation RootS Library – publication Q4 2022***
  - ***TCG Component Class Registry – review October 2022***
  - ***TCG Storage Component Class Registry – review October 2022***
  - ***TCG PC Client Platform Physical Presence Interface – review July 2022***
  - ***DICE Endorsement Architecture for Devices – review May 2022***

Internet Engineering Task Force (IETF) (1 of 4)

- **Next IETF Members Meetings**
  - **IETF 116 Hybrid F2F (Yokohama, Japan) – 27-31 March 2023 – Ira to call in**
  - **IETF 117 Hybrid F2F (San Francisco, CA) – 24-28 July 2023 – Ira to call in**
- **Transport Layer Security (TLS)**
  - **IETF Exported Authenticators in TLS – RFC 9261 – July 2022 https://datatracker.ietf.org/doc/rfc9261/**
  - **IETF Importing External Pre-Shared Keys (PSKs) for TLS 1.3 – RFC 9258 – July 2022 https://datatracker.ietf.org/doc/rfc9258/**
  - **IETF Guidance for External Pre-Shared Key (PSK) Usage in TLS – RFC 9257 – July 2022 https://datatracker.ietf.org/doc/rfc9257/**
  - **IETF TLS Ticket Requests – RFC 9149 – April 2022 https://datatracker.ietf.org/doc/rfc9149/**
  - **IETF DTLS Protocol Version 1.3 – RFC 9147 – April 2022 https://datatracker.ietf.org/doc/rfc9147/**
  - **IETF TLS 1.3 (errata update) – draft-05 – October 2022 https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8446bis/**
  - **IETF IANA Registry Updates for TLS/DTLS – draft-02 – October 2022 https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8447bis/**
  - **IETF IETF Using Attestation in TLS and DTLS - draft-02 – October 2022 https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/**
  - **IETF Well-known URI for Publishing ECHConfigList Values – draft-01 – October 2022 https://datatracker.ietf.org/doc/draft-ietf-tls-wkech/**
  - **IETF Quantum Relief with TLS and Kerberos - draft-08 - October 2022 https://datatracker.ietf.org/doc/draft-vanrein-tls-kdh/**
  - **IETF TLS Encrypted Client Hello - draft-15 – October 2022 https://datatracker.ietf.org/doc/draft-ietf-tls-esni/**
  - **IETF Secure Element for TLS Version 1.3 - draft-05 - September 2022 https://datatracker.ietf.org/doc/draft-urien-tls-se/**

Internet Engineering Task Force (IETF) (2 of 4)

- **Security Automation and Continuous Monitoring (SACM)**
  - **IETF SACM WG – closed July 2022 – IETF Security ADs https://mailarchive.ietf.org/arch/msg/sacm/3UYKoLiQWA2h6CbIxBbCXGG6Qi4/**
  - **IETF Concise Software Identifiers – draft-22 – Sept 2022 – RFC Editor https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/**
- **Concise Binary Object Representation (CBOR)**
  - **IETF Additional Control Ops for CDDL – RFC 9165 – December 2021 https://datatracker.ietf.org/doc/rfc9165/**
  - **IETF CBOR tags for IPv4/v6 Adresses – RFC 9164 – December 2021 https://datatracker.ietf.org/doc/rfc9164/**
  - **IETF CBOR Tags for OIDs – RFC 9090 – July 2021 https://datatracker.ietf.org/doc/rfc9090/**
  - **IETF Feature Freezer for CDDL – draft-10 – October 2022 https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-freezer/**
  - **IETF CDDL 2.0 -- a draft plan - draft-00 - October 2022 https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-2-draft/**
  - **IETF CBOR Tags for Time, Duration, and Period – draft-02 – October 2022 https://datatracker.ietf.org/doc/draft-ietf-cbor-time-tag/**
  - **IETF Using CDDL for CSVs – draft-01 – August 2022 https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-csv/**
  - **IETF Packed CBOR – draft-07 – July 2022 https://datatracker.ietf.org/doc/draft-ietf-cbor-packed/**
  - **IETF Notable CBOR Tags – draft-07 – July 2022 https://datatracker.ietf.org/doc/draft-bormann-cbor-notable-tags/**
  - **IETF Storing CBOR on Stable Storage – draft-12 – May 2022 – RFC Editor https://datatracker.ietf.org/doc/draft-ietf-cbor-file-magic/**

Internet Engineering Task Force (IETF) (3 of 4)

- **Remote ATtestation ProcedureS (RATS)**
  - **IETF Entity Attestation Token (EAT) – draft-17 – October 2022 – WG LC**
    https://datatracker.ietf.org/doc/draft-ietf-rats-eat/
  - **IETF EAT-based Key Attestation Token - draft-00 - October 2022**
    https://datatracker.ietf.org/doc/draft-bft-rats-kat/
  - **IETF RATS Conceptual Messages Wrapper – October 2022**
    https://datatracker.ietf.org/doc/draft-ftbs-rats-msg-wrap/
  - **IETF EAT Media Types – draft-01 – October 2022**
    https://datatracker.ietf.org/doc/draft-ietf-rats-eat-media-type/
  - **IETF Concise TA Stores (CoTS) – draft-01 – October 2022**
    https://datatracker.ietf.org/doc/draft-wallace-rats-concise-ta-stores/
  - **IETF RATS Architecture – draft-22 – September 2022 – RFC Editor**
    https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/
  - **IETF Direct Anonymous Attestation for RATS – draft-02 – September 2022**
    https://datatracker.ietf.org/doc/draft-ietf-rats-daa/
  - **IETF Attestation Event Stream Subscription - draft-02 - September 2022**
    https://datatracker.ietf.org/doc/draft-ietf-rats-network-device-subscription/
  - **IETF Reference Interaction Models for RATS - draft-06 - September 2022**
    https://datatracker.ietf.org/doc/draft-ietf-rats-reference-interaction-models/
  - **IETF Attestation Results for Secure Interactions - draft-03 - September 2022**
  - **https://datatracker.ietf.org/doc/draft-ietf-rats-ar4si/**
  - **IETF CBOR Tag for Unprotected CWT Claims Sets – draft-03 – July 2022**
    https://datatracker.ietf.org/doc/draft-ietf-rats-uccs/
  - **IETF Concise Reference Integrity Manifest – draft-00 – September 2022 – WG adopted**
    https://datatracker.ietf.org/doc/draft-ietf-rats-corim/
  - **IETF ARM's PSA Attestation Token - draft-10 – September 2022**
    https://datatracker.ietf.org/doc/draft-tschofenig-rats-psa-token/
  - **IETF Trusted Path Routing - draft-06 - September 2022**
    https://datatracker.ietf.org/doc/draft-voit-rats-trustworthy-path-routing/

Internet Engineering Task Force (IETF) (4 of 4)

- **IRTF Crypto Forum Research Group (CFRG) – future algorithms**
  - **IRTF Hybrid Public Key Encryption – RFC 9180 – February 2022**
    https://datatracker.ietf.org/doc/rfc9180/
  - **IRTF Argon2 password hash and proof-of-work – RFC 9106 – September 2021**
    https://datatracker.ietf.org/doc/rfc9106/
  - **IRTF BBS Signature Scheme – draft-01 – October 2022 – WG adopted**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/
  - **IRTF NTRU Key Encapsulation - draft-00 - October 2022**
    https://datatracker.ietf.org/doc/draft-fluhrer-cfrg-ntru/
  - **IRTF Ristretto255 and Decaf448 Groups - draft-04 - October 2022**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-ristretto255-decaf448/
  - **IRTF Properties of AEAD algorithms - draft-01 - October 2022**
    https://datatracker.ietf.org/doc/draft-bozhko-cfrg-aead-properties/
  - **IRTF Two-Round Threshold Schnorr Signatures with FROST – draft-11 – October 2022**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-frost/
  - **IRTF Oblivious PRFs w/ Prime-Order Groups – draft-14 – October 2022**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-voprf/
  - **IRTF RSA Blind Signatures - draft-05 - October 2022**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-rsa-blind-signatures/
  - **IRTF Verifiable Distributed Aggregation Functions – draft-03 – August 2022**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-vdaf/
  - **IRTF Additional Parameter sets for LMS Hash-Based Signatures - draft-08 - August 2022**
    https://datatracker.ietf.org/doc/draft-fluhrer-lms-more-parm-sets/
  - **IRTF KangarooTwelve - draft-08 - to CFRG Last Call - August 2022**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-kangarootwelve/
  - **IRTF Verifiable Random Functions (VRFs) – draft-15 – August 2022**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-vrf/

Next Steps – IDS WG

- Next IDS WG Meeting– December 1, 2022
- Next IDS Face-to-Face Meeting February TBD, 2023 at next PWG F2F
- Start looking at involvement in some of these other standards activities individually and maybe as a WG

Backup

HCD Implementation Team Process