The Printer Working Group

Common Criteria Certification and How It May Be Applied to 3D Printing

October 20, 2020

IT Security Evaluations

Can you guarantee that any product is totally secure -- **NO**

There are many things you can do to increase your confidence in the security of a product such as following the security best practices that apply to the industry the product belongs to

But how can you determine in a quantitative way that the measures you have implemented to maximize the security of a product have done that?

It has been demonstrated that a security certification process involving independent third party inspections and security evaluations of a product can provide this quantitative measure

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

Common Criteria Certification Evaluation Concept

An Evaluation is “a detailed examination of the security aspects of a product performed in parallel with the necessary tests to assure that the product works correctly (from a security perspective), it is effective and it does not show any logical vulnerabilities”

Evaluations are conducted to provide product owners with an independent (typically third party) assessment that the countermeasures put in place to minimize the risks to assets that need to be protected are sufficient and correct

WHAT IS COMMON CRITERIA CERTIFICATION?

What is Common Criteria Certification?

Is an internationally recognized security architecture paradigm to which a catalog of coherent software functional requirements is applied using a common language for the expression of IT products and systems security

Useful to:

- Specify security features in a product
- Assist in building of security features in a product
- Evaluating security features of products
- Supporting procurement of products with security features

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.

What is Common Criteria Certification?

The Common Criteria (CC), and the companion CEM are the technical basis for an international agreement, the Common Criteria Recognition Agreement (CCRA), which is signed by 31 countries and which ensures that:

- Products can be evaluated by competent and independent licenses laboratories so as to determine the fulfilment of particular security properties, to a certain extent or assurance;
- Supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies;
- The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes (there are currently 17 such country schemes), with this certification being based on the result of their evaluation;

•These certificates are recognized by all the signatories of the CCRA.

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 Key Terminology

- **Evaluation:** Assessment of a PP, an ST or a TOE, against defined criteria
- **Assurance:** Grounds for confidence that a TOE meets the SFRs
- **Security Functional Requirement (SFR):** A functional requirement which is taken from Part 2 of the Common Criteria
- **Security Assurance Requirement (SAR):** An assurance requirement which is taken from Part 3 of the Common Criteria
- **Evaluation Assurance Level:** A set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package
- **TOE Security Functionality (TSF)**: Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

Common Criteria Certification Key Terminology

- **Evaluation:** Assessment of a PP, an ST or a TOE, against defined criteria
- **Assurance:** Grounds for confidence that a TOE meets the SFRs
- **Security Functional Requirement (SFR):** A functional requirement which is taken from Part 2 of the Common Criteria
- **Security Assurance Requirement (SAR):** An assurance requirement which is taken from Part 3 of the Common Criteria
- **Evaluation Assurance Level:** A set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package
- **TOE Security Functionality (TSF)**: Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

Common Criteria Certification Key Terminology

- **Security Problem Definition (SPD):** Defines the security problem that is to be addressed for either the general TOE type in a PP or the specific TOE in an ST.
- **Organizational Security Policy (OSP):** set of security rules, procedures, or guidelines for an organization. Note that "organization" in this context is ultimate customer for the TOE or product being certified
- **TOE Summary Specification (TSS)**: Provides a description within the ST of how the TOE satisfies all the SFRs included in the ST
- **Operational Environment (OE)**: Environment in which the TOE is operated

Common Criteria Certification Security Functional Requirements

- ISO/IEC Standard 15408 Part 2 defines a set of Security Functional Components that are the basis for Security Functional Requirements (SFRs) that are expressed in a Protection Profile (PP) or a Security Target (ST)
  - Meet the security objectives as stated in a PP or an ST.
  - Describe security properties that users can detect by direct interaction (i.e. inputs, outputs) with the IT or by the IT response to stimulus
  - Express security requirements intended to counter threats in the assumed operating environment of the TOE and/or
    cover any identified organizational security policies and assumptions
- 11 Functional Classes that each address a specific security problem area like cryptographic support or user data protection
- Each class has a set of families with components within each family; you select the component(s) within each family and class that are appropriate for the product class (PP) or specific product (ST) of interest

Common Criteria Certification Security Assurance Requirements

- ISO/IEC Standard 15408 Part 3 defines SARs in terms of Evaluation Assurance Levels (EALs) 1-7. Each EAL has a predefined set of assurance components from several Assurance Families
- Typically PPs and STs claim EALs 2-4 and most certifications were done against PPs claiming EALs 2-4; EALs 5-7 are reserved for components meant for very secure operational uses.
- However, in 2012 the paradigm for SARs changed significantly. Instead of using predefined EALs in PPs and STs, PPs and STs now have Assurance Activities that are unique to each SFR with no EAL claims. In fact, many Schemes will now only accept PPs that have Assurance Activities that are unique to each SFR and that have no EAL claims

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

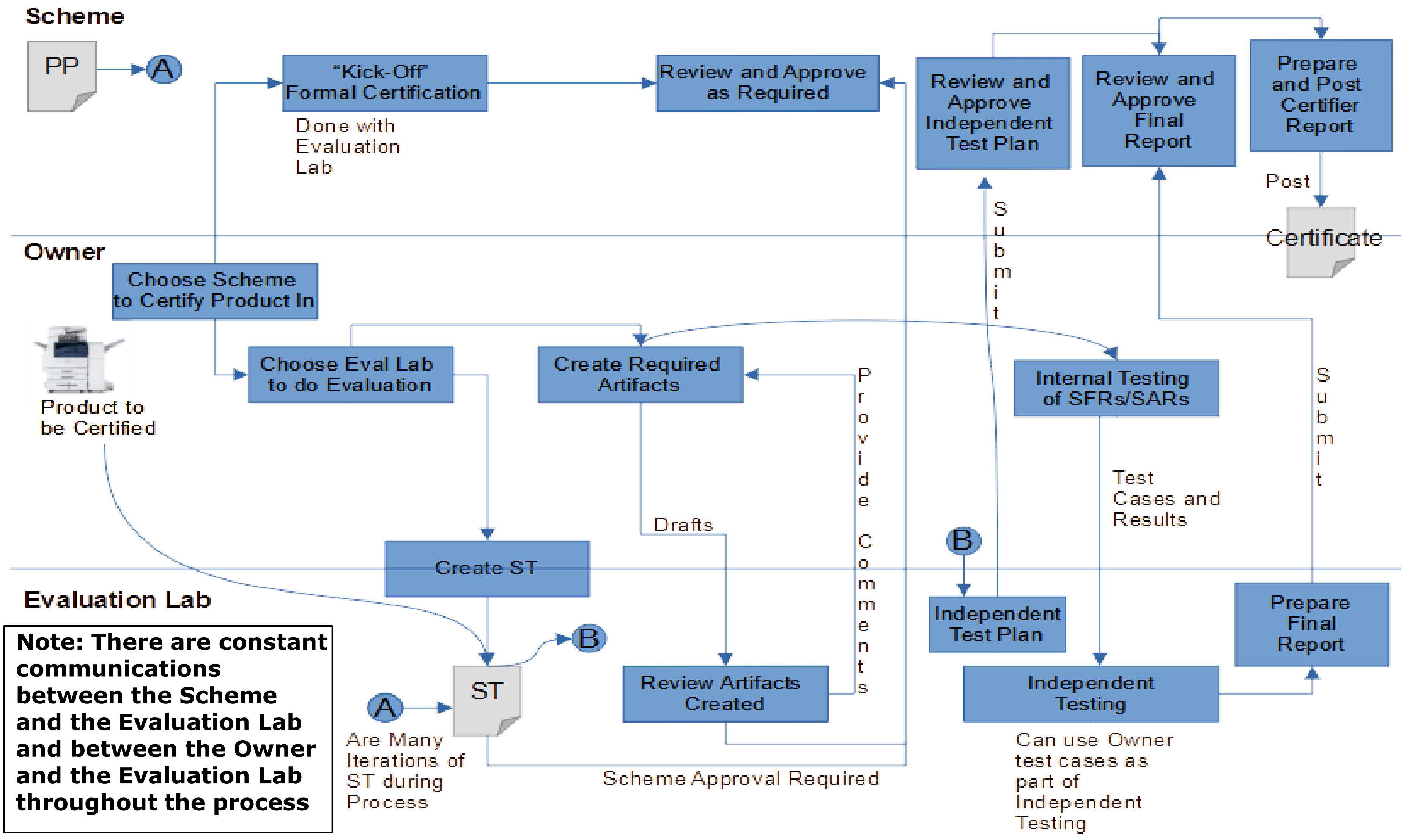
Protection Profile	Security Target
For the generic class of products, the PP includes:	For a specific product in the generic class covered by the PP, the ST includes for the product being certified:
• Overview of the class of products • Conformance claim (i.e., what EAL is being claimed if any) • Security 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

KEY PLAYERS:

- **SCHEME** – Certificate Authorizing Scheme that the TOE (i.e., the "product that is to be certified") will be certified in. The Scheme is responsible for final approval of the certification activity and issuance of the certificate
- **OWNER** or **SPONSOR**– The entity that is sponsoring the TOE to be certified. In 95%+ of the time this is the company or vendor that developed the "product that is to be certified"
- **EVALUATION LAB** – An independent (from the **Owner**) vendor accredited by the **Scheme** involved to perform the evaluation activities required by the Common Criteria Standard to certify the TOE

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)

Is there a CC Protection Profile for Hardcopy Devices?

Protection Profile for Hardcopy Devices, Version 1.0

- Developed by the MFP Technical Committee
- Approved by US and Japanese Schemes Sep 15, 2015
- Became effective immediately in the US; became effectiveness in Japan in 2017
  - Have been multiple 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
- An international Technical Committee has been formed and approved to create a Hardcopy Device collaborative PP to replace this PP by 1Q 2022.

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 Security Assumptions

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

- HCD Administrators are trusted to administer the HCD according to site security policies.

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

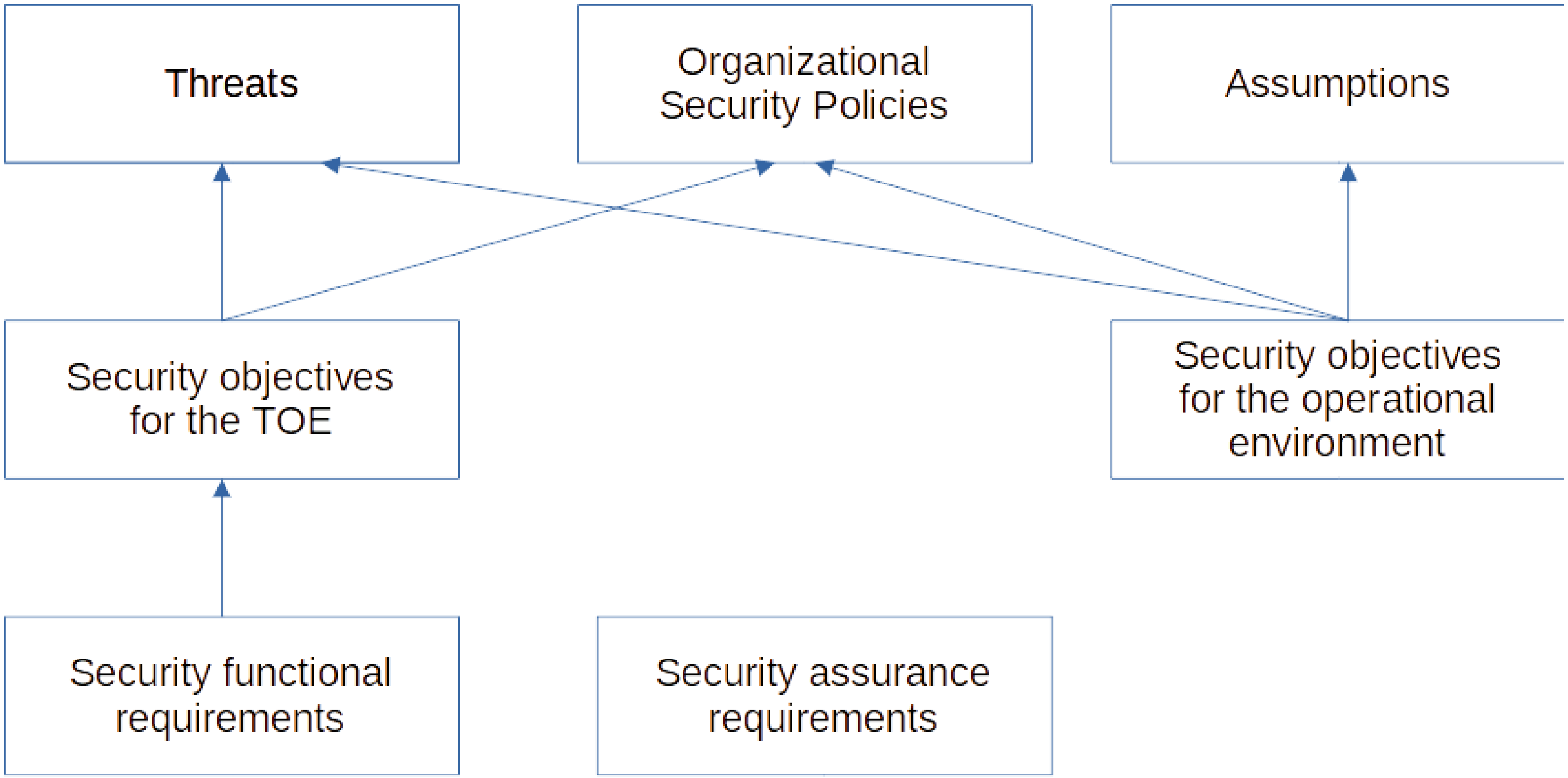
2D Hardcopy Devices
Key Security Objectives of the HCD

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

Hardcopy Devices Security Problem Definition How It All Fits Together


Threats
Organizational Security Policies
Assumptions
Security objectives for the TOE
Security objectives for the operational environment
Security functional requirements
Security assurance requirements

If all the SFRs and SARs are satisfied and all the Security Objectives for the operational environment are achieved, then the Security Problem defined in the Security Problem Definition is solved

Hardcopy Device Protection Profile Sample of Security Functional Requirements related to Security Objectives

User Identification and Authentication

- Authentication failure handling
- Password management
- Protected authentication feedback
- Timing of authentication

User Authorization and Access Control

- Subset access control
- Security attribute access control

Administrator Roles

- Management of security functions behavior
- Management of TSF data
- Specification of Management functions
- Security roles

Hardcopy Device Protection Profile Sample of Security Functional Requirements related to Security Objectives

Software Update Verification

- Trusted update

Self-Test

- TSF testing

Auditing

- Audit data generation
- User identity association
- Reliable time stamps
- Audit Review
- Prevention of audit data loss

Hardcopy Device Protection Profile Sample of Security Functional Requirements related to Security Objectives

Communications Protection

- Inter-TSF Trusted Channel
- Trusted path (for Administrators)
- Trusted path (for non-administrators)

Storage Encryption

- Cryptographic key derivation
- Cryptographic key generation (Symmetric keys)
- Cryptographic Operation (Symmetric encryption/decryption)
- Protection of Data on Disk
- Cryptographic Key Generation (for asymmetric keys)
- Cryptographic operation (AES Data Encryption/Decryption)
- Cryptographic key destruction

Hardcopy Device Protection Profile Sample of Security Functional Requirements related to Security Objectives

Image Overwrite

- Subset residual information protection

Protection of Key Material

- Protection of Key and Key Material

Purge Data

- Subset residual information protection

PSTN Fax-Network Separation

- Fax Separation

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