The Printer Working Group

Imaging Device Security

November 13, 2024

PWG August 2024 Virtual Face-to-Face

Agenda

Please Note: This PWG IDS Meeting is Being Recorded

When	What
10:00 – 10:05	Introductions, Agenda review
10:05 – 10:55	Discuss status of HCD iTC, HIT and plans for future HCD cPP/HCD SD releases
10:55 – 11:25	Al Sukert's ICAM 2024 Paper
11:25 – 11:30	Wrap Up / Next Steps

Antitrust and Intellectual Property Policies

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

- Refer to the Antitrust, IP and Patent 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 ITC / HCD Interpretation Team (HIT) Status

HCD international Technical Community (iTC) Status

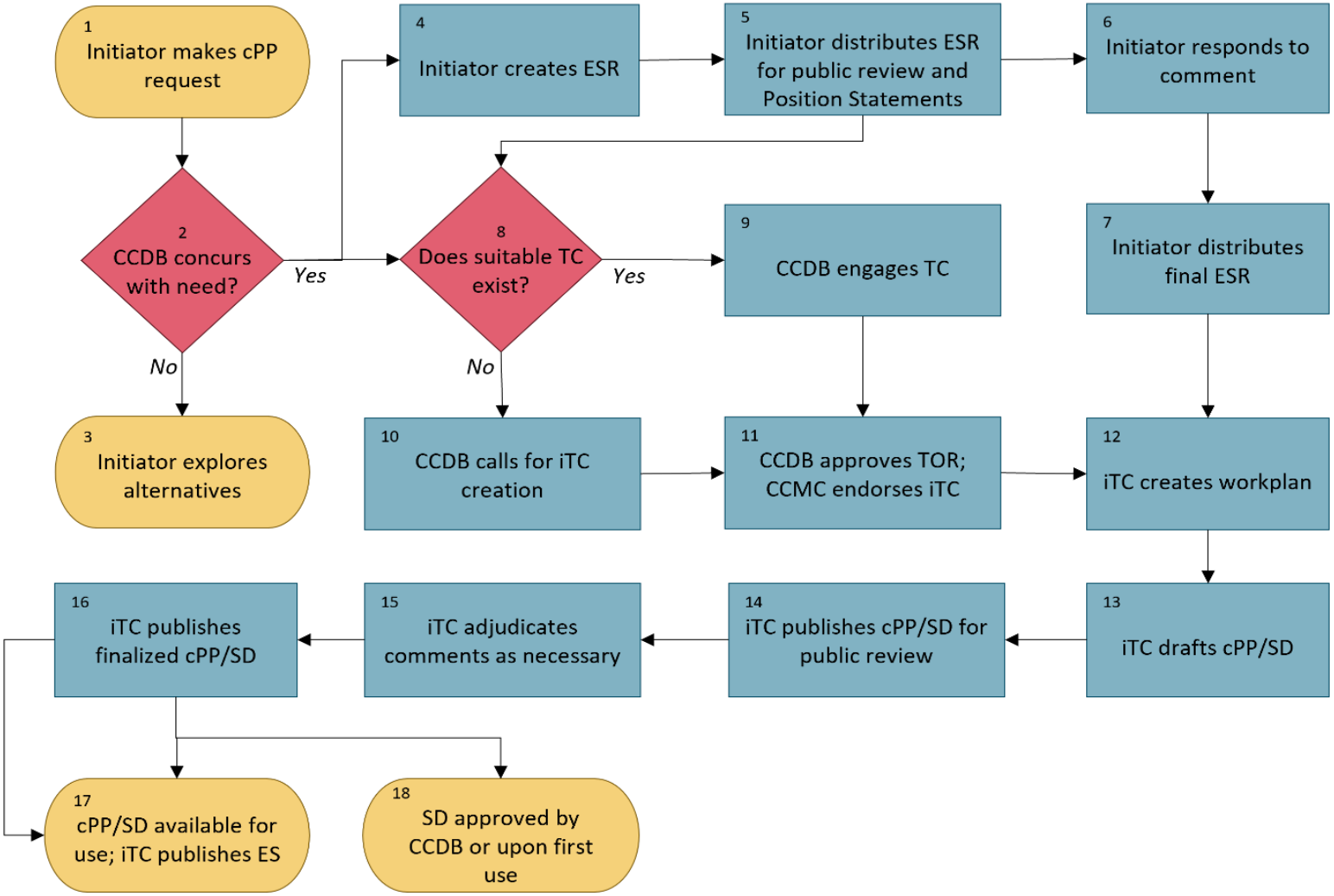
- Since last IDS F2F on August 7, 2024 HCD iTC meetings have been held on:
  - Sep 9th, Oct 14th

  NOTE: Since publishing the HCD cPP v1.0 and HCD SD v1.0 in Oct 2022 the HCD iTC has gone to monthly meetings
- Current focus has been and is now on:
  - Creating and issuing the Errata to HCD cPP v1.0 and HCD SD v1.0 (see next slide)
  - Developing a release plan for future versions of the HCD cPP and HCD SD
  - Determining content of and then implementing the next HCD cPP / HCD SD release (v2.0)
  - Addressing issues against HCD cPP / SD v1.0e

Errata to HCD cPP v1.0 and HCD SD v1.0 (v1.0e)

- The Errata – HCD cPP v1.0e and HCD SD v1.0e – were published on Mar 4th, 2024
- Endorsements have been obtained from the Canadian and Korean Schemes, NIAP and JISEC (the Japanese Scheme); JISEC's endorsement was posted as part of an updated Position Statement
- NIAP's endorsement is a formal statement that products successfully evaluated against the HCD cPP V1.0e that demonstrate exact conformance to the cPP, meeting the below identified conditions, and in compliance with all NIAP policies, will be placed on the NIAP Product Compliant List:
  - Each applicable cryptographic support security functional requirement (FCS_) must include at least one selection conforming to Commercial National Security Algorithm (CNSA) Suite V1.0 or V2.0
  - SHA-256 may be selected in FCS_PCC_EXT.1 and may be included in FCS_COP.1/Hash and FCS_COP.1/KeyedHash for that function; and
  - **SHA-1 may not be selected**
- **HCD cPP v1.0e and HCD SD v1.0e have both now been officially certified by the Canadian Scheme via the completion of the first HCD certification against the HCD cPP/SD v1.0e**

Process Flow Diagram for cPP Development



Commercial National Security Algorithm (CNSA) Suite 1.0 Algorithms

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS Pub 197	Use 256 bit keys to protect up to TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384 to protect up to TOP SECRET.
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS Pub 180-4	Use SHA-384 to protect up to TOP SECRET.
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for key establishment	NIST SP 800-56B rev 1	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4	Minimum 3072 bit-modulus to protect up to TOP SECRET.

Commercial National Security Algorithm (CNSA) Suite 2.0 Algorithms

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels
CRYSTALS-Kyber	Asymmetric algorithm for key establishment	TBD	Use Level V parameters for all classification levels
CRYSTALS-Dilithium	Asymmetric algorithm for digital signatures	TBD	Use Level V parameters for all classification levels
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels SHA256/192 recommended
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels

HIT Issues Resolved by the Errata

Issue #	Issue Summary
HCD-IT #2	In HCD SD Section 2.6.1 FPT_SBT_EXT.1 Extended: Secure Boot, 2.6.1.3 Tests, need clarification that the algorithm verification for Root of Trust should be avoided
HCD-IT #4- HCD-IT #7	These four issues were a set of four comments from NIAP stating areas such as improperly defined Extended Component Definitions and bolding of the selection prompt where the HCD cPP did not follow the conventions stated in Section 5.1
HCD-IT #9	This issue is about the test cases for SFR FDP_DSK_EXT.1 in the HCD SD requiring an "operational TSFI" (i.e., an external human interface such as a web interface) when user and confidential data stored on nonvolatile data on the HCD is only accessed by the OS and required no human interface
HCD-IT #12	This issue is from the Canadian Scheme and was for the fact that three threats - T.TSF_FAILURE. T.UNAUTHORIZED_UPDATE, and T.WEAK_CRYPTO did not have the required asset information in their definition
HCD-IT #16	This issue documents three comments – two editorial and one technical – from the required CCMB review of the HCD SD v1.0

HIT Issues Resolved by the Errata

Issue #	Issue Summary
HCD-IT #18	The issue is that the TSS Assurance Activity for SFR FCS_CKM.1/SKG Cryptographic key generation (Symmetric Keys) has to clarify a disconnect how the TOE obtains a symmetric key through direct generation from a random bit generator between the two standards referenced in the SFR.
HCD-IT #19	This issue is whether Tests 1 and 2 for SFR FCS_CKM.4 Cryptographic key destruction apply to only volatile memory
HCD-IT #21	This issue is to clarify when Tests 3 and 4 for SFR FDP_DSK_EXT.1 are required to be run
HCD-IT #22	cPP Section 5.8.4. "FPT_TST_EXT.1 Extended: TSF testing" has the following two paragraphs under Application Note, which has minor consistency among each other: **Application Note:** Power-on self-tests may take place before the TSF is operational, in which case this SFR can be satisfied by verifying the TSF image by digital signature as specified in FCS_COP.1/SigGen, or by hash specified in FCS_COP.1/Hash. Self-test is intended to detect malfunctions which may compromise the TSF. Since the integrity of the firmware/software is guaranteed by FPT_SBT_EXT, the function for FPT_TST_EXT should address the malfunction detection like DRBG self-test defined in ISO/IEC 18031:2011. Is it sufficient to only run an integrity test (no other tests) on start-up/power on?

Other HIT Issues Resolved

Issue #	Issue Summary	Reason For Closure
HCD-IT #3	Section 5.3.5, FCS_CKM.4 Cryptographic key destruction on page 33: in FCS_CKM.4.1 the last line of the SFR states "] that meets the following: [selection: no standard]." Since the selection has already been made in the cPP, the "selection:" should be deleted.	Issue is a duplicate of a NIAP assessment comment
HCD-IT #17	Numerous comments against the HCD SD v1.0	This issue was a duplicate of HCD-IT #16
HCD-IT #20	Test 2 of FDP_DSK_EXT.1 described in “3.1.3.4” of HCD SD requires the evaluator to verify that the data can be decrypted by proper key and key material. When the data is a key and encrypted by “another key that is not part of key chain” specified in FPT_KYP_EXT.1, the evaluator cannot decrypt the data, because “another key” cannot be retrieved from “protected storage device”.	Issue was withdrawn by submitter

Other HIT Issues Resolved

Issue #	Issue Summary	Reason For Closure
HCD-iTC-Template #355	Comments by the Canadian Scheme as part of the certification of HCD cPP v1.0e	Comments were addressed and the Issue was closed
HCD-iTC-Template #356	Comments by the Canadian Scheme as part of the evaluation of HCD SD v1.0e	Comments were addressed and the Issue was closed
HCD-iTC-Template #357	Comments by the Korean Scheme from its review of the draft of the HCD SD v1.0e	Comments were addressed and the Issue was closed

HIT Issue Summaries – Remaining Open Priority 1s

Issue #	Issue Summary	Status
HCD-IT #1	CFB is the only AES mode allowed by the TPM 2.0 specification but it is not included as n allowable mode in SFR FCS_COP.1/KeyEnc	Potential solutions being reviewed by HIT
HCD-IT #8	Requested that the Application Notes in SFR FPT_KYP_EXT.1 be modified to more clearly explain what each of the conditions for key storage in that SFR mean	This issue is linked to Issue HCD-IT #11 and will be fixed jointly with that issue
HCD-IT #10	This issue is for the Security Objective an O.KEY_MATERIAL being mapped to a Conditionally Mandatory SFR FPT_KYP_EXT.1 when it should be mapped to a Mandatory SFR, because protection of keys and key material should be a mandatory security objective	The solution for this issue is known and is being worked by the HIT
HCD-IT #11	This issue deals with FCS_CKM.4 and whether encrypted keys are within the scope of key destruction. The real issue, though, is the fact that FCS_CKM_EXT.1 states that only plaintext keys and key material must be destroyed, whereas other cPPs require all keys and key material must be destroyed	Resolution of this issue is on hold while we determine why the HCD cPP only required plaintext keys to be destroyed; HiT divided on this issue

HIT Issue Summaries – Remaining Open Priority 1s

Issue #	Issue Summary	Status
HCD-IT #23	In HCD cPP SFR FIA_X509_EXT.2.2 - Usage of an offline CRL (CRL may be imported to TOE by USB memory) is not considered as an option. In this case, TOE doesn't need to establish a connection. A potential solution is to add the option "allow the Administrator to import CRL file and perform OFFLINE-validation of a certificate" in the selection in this SFR.	Potential Solution under reviewed by HIT

HIT Issue Summaries – Remaining Open Priority 2s

Issue #	Issue Summary	Status
HCD-IT #13	This issue stated that the title of SFR FDP_DSK_EXT.1 - Protection of Data on Disk – was misleading as it might lead someone to assume it only applied to HCDs that had a hard disk drive.	Solution is to change title so it is clear this SFR applies to any HCD that stores data in Nonvolatile Storage
HCD-IT #15	This issue is a case where the title of the SFR FCS_COP.1/CMAC is correct where it is defined in Section A,,3, but is incorrect when FCS_COP.1/CMAC is included in a dependency list for another SFR	Issue has been assigned to a HIT member to resolve
HCD-IT #24	This issue is that in the HCD cPP the name of the SFR in the HCD cPP is "FCS_X509_EXT.2", but it should be "FIA_X509_EXT.2	This issue is awaiting review by a HIT member
HCD-IT #25 **NOTE: IS TOP PRIORITY FOR HIT**	This issue deals with two issues associated with SFR FPT_SBT_EXT.1 – (1) definitions of immutable code or HW-based write-protection and (2) guidance on the level of assurance the evaluator shall take into consideration to confirm a compliant Root of Trust protection mechanism	Agreed on definition of immutability from NIST SP 800-193; TR created for solution and approved by the HIT Issue of HW-based write-protection is still under discussion

HIT Issue Summaries – Open Issues Awaiting a Priority

HCD-IT #14	This issue is a simple issue where the sections where the SFRs FIA_AFL.1 and FCS_CKM.1/AKG reside are different between the HCD cPP and the HCD SD	Issue has been assigned to a HIT member to resolve
HCD-IT-Template #360	This issue involves Tests 1 and 2 of the test assurance activities for SFR FCS_IPSEC_EXT.1.10. These tests appear to be TSS requirements rather than testing activities.	This issue was against the Lexmark certification which Hs been competed, so the issue should be closed
HCD-IT-Template #361	The issue is whether it would be acceptable to have multiple immutable roots of trust, any one of which could be used to verify firmware integrity?	No priority has been assigned, but the issue has been discussed at multiple HIT meetings with no consensus as to a resolution at this time
HCD-IT-#26	The following notes on FCS_COP.1/xxx were added at the request of JISEC -- "Note: Testing of cryptographic functions implemented in the Root of Trust for Secure Boot (FPT_SBT_EXT.1) may not be feasible and independent testing may not be available. In this situation, contact the CC Scheme.“ This requires manufacturers to describe the information to identify the Root of Trust product or implementation in TSS. JBMIA now feels this information should go in the KMD rather that the TSS	The HIT determined that this issue needs to be resolved by the full HCD iTC and approved a Technical Recommendation (TR) for this issue that has been forwarded to the full iTC for consideration

HIT Issue Summaries – Open Issues Awaiting a Priority

HCD-IT-#27	For FCS_COP.1/CMAC, it's difficult to remove the dependency on key generation for CMAC even if CMAC is used in Secure Boot.	Issue affects an ongoing JISEC certification, so it needs to be resolved by EOY. The originator of this issue provided multiple solutions for this issue which are being reviewed by the HIT

HIT Status

- Priorities now, in order, are:
  - Address open issues that impact ongoing HCD certifications
  - Resolve remaining unaddressed Priority 1 Issues
  - Resolving any remaining Priority 2 Issues
  - Assigning priorities to issues with no priority assigned
  - Addressing any new issues that are raised against the Errata
- Focus right now is on Issues #26 and #27. Once those are resolved the focus will turn to the unresolved remaining unaddressed Priority 1 issues
- Because of the use of GitHub and changes made to the documented HIT process because we did much of the infrastructure and actual implementations “on the fly”, a Technical Decision (D) is being created by the HIT to update the HIT Procedures to reflet what we are actually doing

HCD iTC
Issues Post-Version 1.0e – 2024 Priorities

The Roadmap for the issues that the HCD iTC will address in 2024, in priority order:

#1 Issue is CC:2022 Transition Policy – Ensuring the HCD cPP and HCD SD are compliant with CC:2022 by Dec 31, 2025 (CCDB deadline for certifications against prior CC version)

- Subgroup was formed and is actively working this issue
- Developed following list of items to review:
  - Determine which items in the CC:2022 Errata should be included in the HCD cPP and SD (either v1.0e or v2.0)
  - Determine which new SFRs included in CC:2022 Part 2 should be included in the HCD cPP and create the appropriate Assurance Activities in the HCD SD for these SFRs
  - Determine what changes to SFRs in CC:2022 Part 2 that have counterparts in the HCD cPP should be made in the HCD cPP counterparts
  - Review CC:2022 Parts 3 -5 to determine if any content in these parts should be included in either the HCD cPP or HCD SD
  - Assuring that the HCD SD's requirements for AVA_VAN are consistent with EUCC for AVA_VAN.1 – AVA_Van.3, which are the levels for "Substantial" assurance in the EUCC, is important
- Goal is to determine minimum changes needed

HCD iTC
CC:2022 Subgroup

The Roadmap for the issues that the HCD iTC will address in 2024, in priority order:

#1 Issue is CC:2022 Transition Policy – Ensuring the HCD cPP and HCD SD are compliant with CC:2022 by Dec 31, 2025 (CCDB deadline for certifications against prior CC version)

- Subgroup was formed and is actively working this issue
- Developed following list of items to review:
  - Determine which items in the CC:2022 Errata should be included in the HCD cPP and SD (either v1.0e or v2.0)
  - Determine which new SFRs included in CC:2022 Part 2 should be included in the HCD cPP and create the appropriate Assurance Activities in the HCD SD for these SFRs
  - Determine what changes to SFRs in CC:2022 Part 2 that have counterparts in the HCD cPP should be made in the HCD cPP counterparts
  - Review CC:2022 Parts 3 -5 to determine if any content in these parts should be included in either the HCD cPP or HCD SD
  - Assuring that the HCD SD's requirements for AVA_VAN are consistent with EUCC for AVA_VAN.1 – AVA_Van.3, which are the levels for "Substantial" assurance in the EUCC, is important
- Goal is to determine minimum changes needed

HCD iTC
CC:2022 Subgroup Status

- Looked at differences between SFRs on CC:2022 and corresponding SFRs in HCD cPP v1.0e
  - Considering recommending replacing several SFRs currently in HCD cPP with corresponding SFRs from CC:2022. Examples include:

    FAU_STG_EXT.1 External Audit Trail Storage (HCD cPP) → FAU_STG.1 Audit Storage Data Location (CC:2022)

    FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation) (HCD cPP) → FCS_RBG.1 Random Bit Generation (CC:2022)

    FCS_CKM.4 Cryptographic key destruction (HCD cPP) → FCS_CKM.6 Timing and event of cryptographic key destruction (CC:2022)

    FDP_DSK_EXT.1 Protection of data on disk (HCD cPP) → FDP_SDC.1Stored data confidentiality (CC:2022)

HCD iTC
CC:2022 Subgroup Status

- Did a comparison of dependencies between SFRs on CC:2022 and corresponding SFRs in HCD cPP v1.0e. Found differences between the following SFRs:

  FAU_STG.1 Audit Storage Data Location

  FTA_SSL.3 TSF-initiated termination

  FTP_TRP.1 Trusted Path

- Canadian Scheme developed list of SFRs changed between CC v3.1R5 and CC:2022
  - Subgroup will review list at its next meeting

HCD iTC
Issues Post-Version 1.0e – 2024 Priorities

The Roadmap for the remaining issues that the HCD iTC will address in 2024, in priority order from top to bottom are:

1. Syncing with Network Device cPP/SD v3.0
2. Syncing with the output from the CCDB Crypto Working Group – SFR Catalog planned for release by end of 2024
3. Implementing HIT Technical Decisions
4. Implementing AVA_VAN requirements to sync with EUCC
5. NIAP PQC Requirements (CNSA 2.0) – currently on hold by NIAP
6. Parking Lot Issues
7. Any New Issues

HCD iTC
Post-Version 1.0e Release Plan

Based on current information, as of now the HCD iTC is still planning two Post-Version 1.0e Releases:

- V2.0 – 2026:
  - Will contain everything in v1.0e, syncing with ND cPP/SD 3.0, results from the CCDB Crypto WG's SFR Catalog as they pertain to what is currently in the HCD cPP, results from the CC:2022 subgroup and any other subgroups as applicable, and TDs from resolved HIT issues
  - May include initial CNSA 2.0 components such as elimination of SHA-1 and CNSA 2.0 algorithms for digital signatures if NISP provides necessary direction in time
- V3.0 - 2027 – 2028:
  - Will likely contain applicable CNSA 2.0 components and content from the other priorities

HCD cPP/SD Content Post-Version 1.0e Likely Specific V2.0 Content

- Incorporate TDs for resolved HIT Issues
- Recommended changes from the CC:2022 Subgroup and, as applicable, other HCD iTC subgroups
- Incorporate applicable SFRs from the CCDB Specification of Functional Requirements for Cryptography once it is published and a transition plan for these SFRs is released by the CCDB
- Update for the relevant changes in ND cPP v3.0e
  - Inclusion of support for TLS/DTLS 1.3 and deprecation of TLS 1.1
  - Standardizing on the ND cPP/SD 3.0 Implementation
  - Incorporate the NIAP Functional Package for SSH so can claim conformance to it
- Inclusion of appropriate AVA_VAN assurance requirements to sync with EUCC
- Changes due to requests from JISEC, ITSCC, NIAP, Canada and possible other Schemes due to on-going certifications against HCD cPP/SD v1.0e

HCD cPP/SD Content Post-Version 1.0e Potential for Inclusion in V3.0 and Later Versions

- **NTP**
- **Full implementation of CNSA 2.0**
- **Support for Cloud Printing**
- **Support for post quantum and other new crypto algorithms**
- **Support for Artificial Intelligence**
- **Support for 3D printing and the Digital Thread to Additive Manufacturing**
- Incorporate NIAP Functional Package for X.509 when it becomes available
- Any other new NIAP Packages
- Updates due to changes from other ISO, FIPS or NIST Standards/Guidelines, and NIAP TDs
- Support for Wi-Fi
- Any new CCDB Crypto WG or CCUF Crypto WG Packages or Specifications

HCD cPP/SD Content Post-Version 1.0 Potential for Inclusion in V3.0 and Later Versions

- Support for Security Information and Event Monitoring (SIEM) and related systems
- Support for SNMPv3
- Support for NFC
- Updates based on new technologies, customer requests or government mandates
- Syncing with Other iTCs such as DSC iTC and FDE iTC
- Syncing with newer versions of ND cPP/SD

HCD iTC Status
Key Next Steps

- Continue HIT activities for maintaining HCD cPP/SD v1.0e and issue the necessary TDs/TRs and possibly Errata to address all documented RfIs
- Determine the content from the results of the CC:2022 Subgroup, any TDs/TRs created by the HIT, other HCD iTC subgroups, the CCDB Crypto Working Group Crypto SFR List, and other applicable inputs and then implement that content into HCD cPP v2.0 and HCD SD v2.0
- Start planning for HCD cPP/SD v3.0 and later versions

The Printer Working Group

Implementing a Cyber Security Certification for the Additive Manufacturing Process

October 29, 2024

APPLYING COMMON CRITERIA TO THE DIGITAL THREAD AND 3D PRINTING?

What is Common Criteria?

- The Common Criteria for Information Technology Security Evaluation (or Common Criteria (CC)) is an international standard (ISO/IEC Standard 15408-1:2009) for security certification of information security products.
- Common Evaluation Methodology (CEM) is the 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 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 (PP):** Implementation-independent statement of security needs (both functional and assurance) for a TOE type (in our case the TOE type will be “3D printers”)
- **Security Target (ST):** Implementation-dependent statement of security needs for a specific identified TOE

Common Criteria Certification of Hardcopy Devices (2D Printers)

- Developed and published a collaborative Protection Profile for Hardcopy Devices (HCD cPP v1.0e)
- In the HCD cPP the following were identified as part of the Security Problem Definition:
  - 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 and Common Criteria Certification

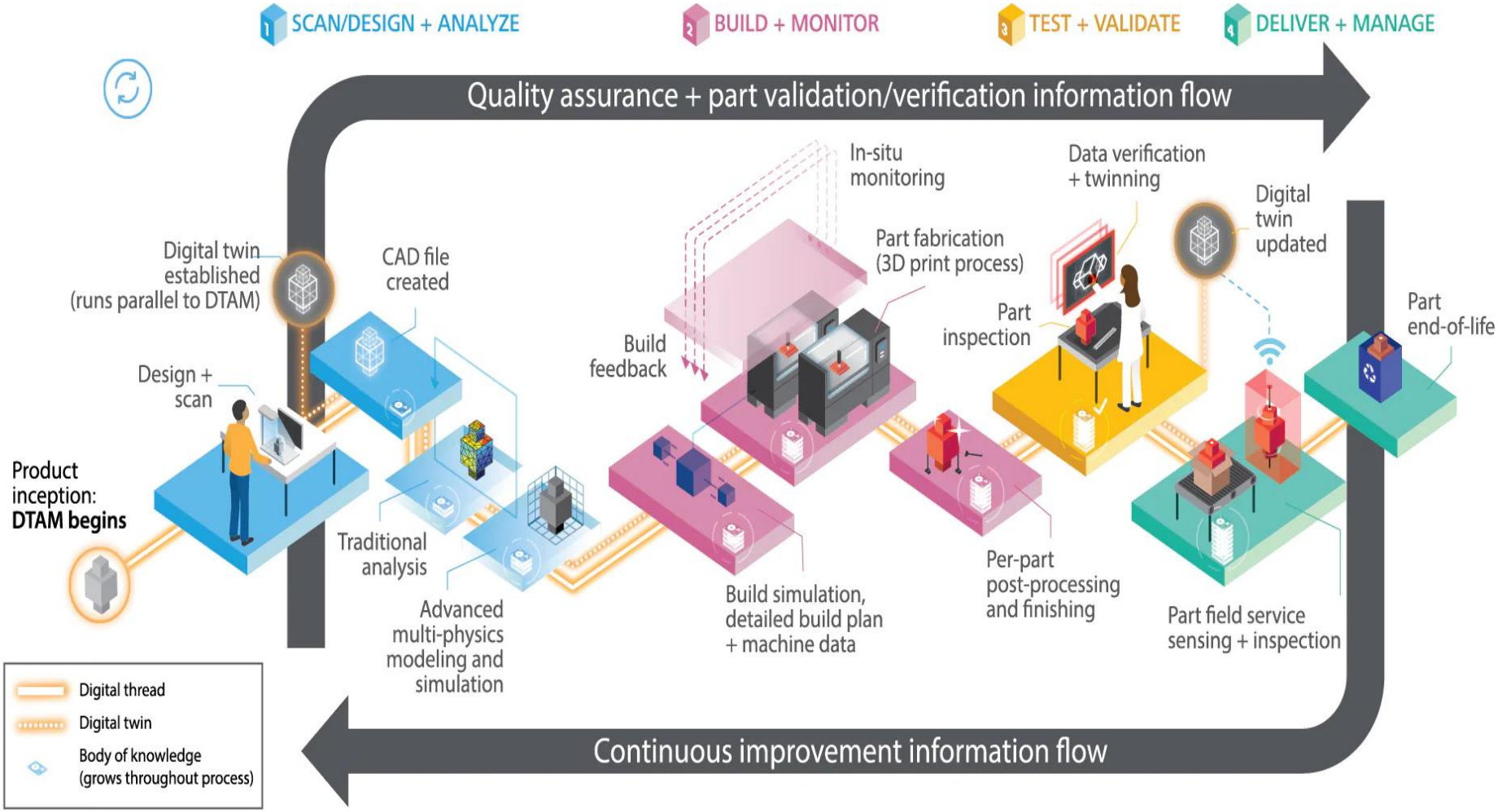
Could the Common Criteria Certification process that was used to certify Hardcopy Devices be used to perform a similar security certification for the Digital Thread for Additive Manufacturing?

We have established in our talks the past two years that we believe the answer is '**YES IT CAN BE**' because 2D and 3D printers have:

- Major assets that must be protected from unauthorized disclosure or modification (e.g., in the case of 3D printers - CAD files and models/simulations)
- Similar security threats that these assets must be protected from (e.g. Unauthorized Access to Confidential Data)
- Similar security objectives that have to be performed to support the security of the HCDs or Digital Thread (e.g. User Authorization, Access Control, Firmware/software Verification, Administrator Roles and Communications Protection)
- Similar security objectives of the operational environment (e.g., trusted administrators and physical protection)

APPLYING THE CHANGES IN COMMON CRITERIA Version 2022 (CC:2022)TO POTENTIALLY CERTIFY THE DIGITAL THREAD FOR THE ADDITIVE MANUFACTURING PROCESS

Digital Thread for Additive Manufacturing



Why the CC:2022 Changes Are Significant For the Digital Thread

- CC:2022 defines the concept of PP-Configurations and PP-Modules
- **How could the use of PP-Configurations and PP-Modules be applied to allow for Common Criteria Certifications of the entire Digital Thread for Additive Manufacturing?**

Common Criteria Certification
Some Additional Key Terminology

- **Protection Profile Configuration (PP-Configuration):** Implementation-independent statement of security needs for a *target of evaluation (TOE)* type containing at least one *protection profile (PP)* and an additional non-empty set of PPs and *PP-Modules* (with the associated PP-Modules Bases)
- **Protection Profile Module (PP-Module):** Implementation-independent statement of security needs (both functional and assurance) and for a *target of evaluation (TOE)* type complementary to one or more base *Protection Profiles* and possibly some *base PP-Modules*

  •PP-Modules address those security features of a given TOE type that cannot be required uniformly for all products of this TOE type. Unlike PPs, PP-Modules shall be used only in PP-Configurations
- **Base Protection Profile (Base PP):** *Protection Profile* specified in a *PP-Module*, as part of that PP-Module's *PP-Module Base*, used as a basis to build a *PP-Configuration*
- **Base PP-Module (Base PP-Module):** *PP-Module* specified in a different PP-Module, as part of that PP-Module's *PP-Module Base*, used as a basis to build a *PP-Configuration*

Actual Example of a Common Criteria Certification Using the Concept of PP-Configuration

- Product being certified in this case is an Aruba Mobility Controller (MC) with ArubaOS 8.10. The TOE is a multi-purpose network device that includes a **WLAN access system,** a **stateful traffic filter firewall and VPN gateway capabilities**
- The Aruba Mobility Controller platform serves as a gateway between wired and wireless networks and provides command and control over Aruba Access Points (APs) within an Aruba dependent wireless network
- The Aruba Mobility Controllers (MCs) and Aruba Virtual Mobility Controllers (VMCs) are wireless switch hardware and virtual appliances that provide a wide range of security services and features including wireless and wired network mobility, security, centralized management, auditing, authentication, secure remote access, self-verification of integrity and operation, stateful traffic filtering and VPN gateway functionality
- The ArubaOS is a suite of mobility applications that runs on all Aruba controllers and allows administrators to configure and manage the wireless and mobile user environment. The TOE is generally deployed in a configuration consisting of one or more Aruba mobility controllers (MC and/or VMC) and multiple Aruba wireless APs

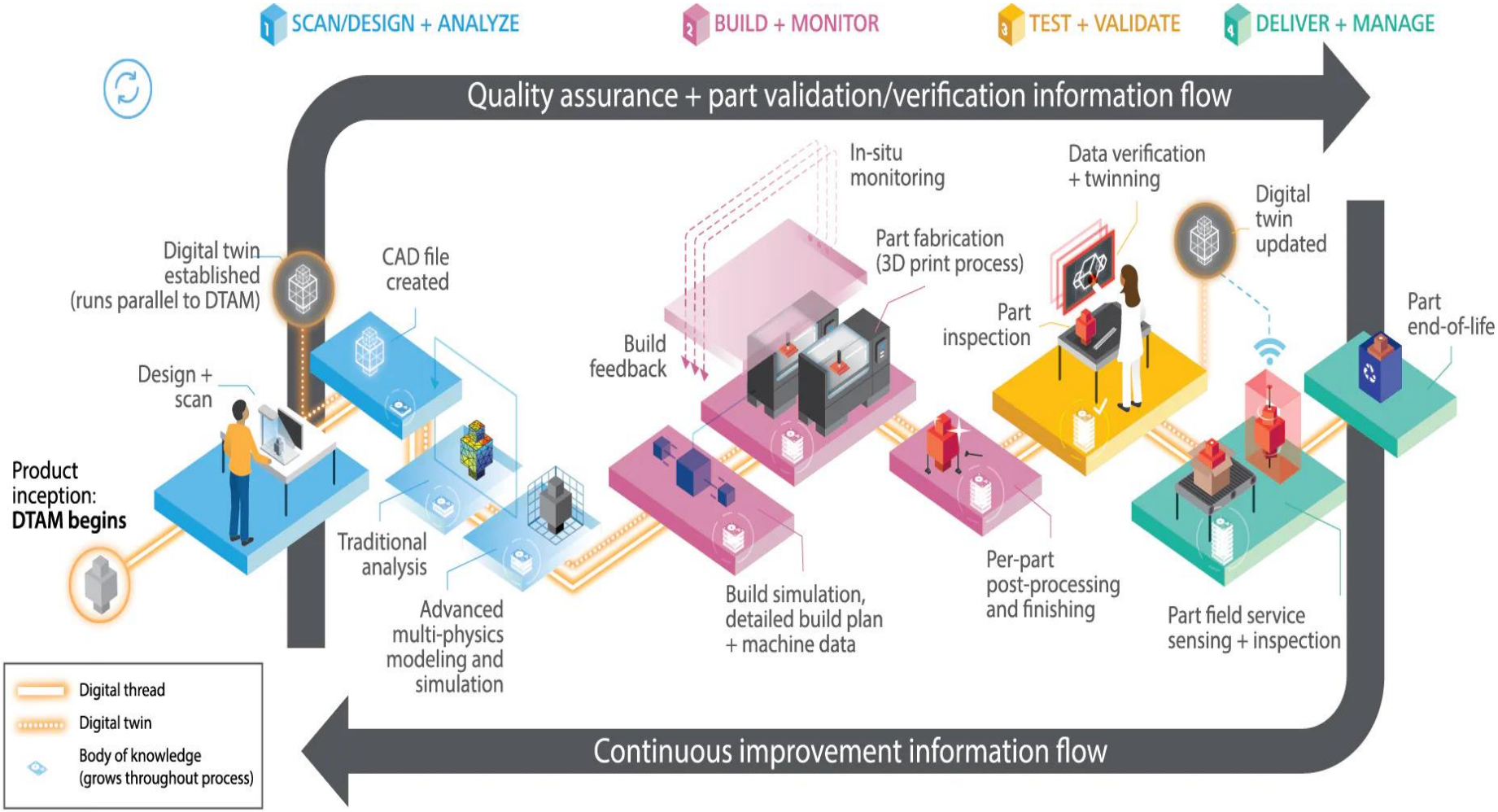
Actual Example of a Common Criteria Certification Using the Concept of PP-Configuration

- **COMPLIANCE CLAIMS**
- This TOE is conformant to the following CC specifications:
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017
  - Part 3 Conformant
- Package Claims:
  - **PP-Configuration** for Network Devices, Wireless Local Area Network (WLAN) Access Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, 2022-06-16.(CFG_NDcPP-WLANAS-FW-VPNGW_V1.0)
  - **Base-PP**: collaborative Protection Profile for Network Devices, Version 2.2e(CPP_ND_V2.2E)
  - **PP-Module**: PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0)
  - **PP-Module**: PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata20200625 (MOD_CPP_FW_V1.4E)▪
  - **PP-Module**: PP-Module for VPN Gateways, Version 1.2 (MOD_VPNGW_V1.2)

Actual Example of A Common Criteria Certification Using the Concept of PP-Configuration

- The PP-Configuration in this case consists of the following:
  - **Base-PP**: collaborative Protection Profile for Network Devices, Version 2.2e
  - **PP-Modules**:
    - **PP-Module**: PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0)
    - **PP-Module**: PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata20200625 (MOD_CPP_FW_V1.4E)
    - **PP-Module**: PP-Module for VPN Gateways, Version 1.2 (MOD_VPNGW_V1.2

Digital Thread for Additive Manufacturing



How Could PP-Configurations Be Applied to Digital Thread for Additive Manufacturing for Additive Manufacturing?

Here is a possible scenario for certifying the Digital Thread:

1. Create a Protection Profile based on the Hardcopy Device collaborative PP (HCD cPP) for a 3-D Printer, since a 3-D Printer is essentially an HCD that prints 3-D objects rather than paper.
2. Create a **PP-Module** for the following:
   - IT System containing the CAD files, modeling and simulations

- Then you can create the following **PP-Configuration**:
  - **Base-PP**: 3D Printer Protection Profile
  - **PP-Module**: PP-Module for the IT System containing the CAD files, modeling and simulations

Once the **PP-Configuration** is created you can do a Common Criteria certification on either:

- A 3D printer alone using just the **Base-PP** or
- The entire digital thread using the full **PP-Configuration**

What Are The Next Steps?

- Create a 3-D Printing Technical Community (TC) to develop the applicable Base-PP and PP-Modules for the Digital Thread
  - Determine what are the following for a 3-D printer and for the IT System
    - Threats
    - Key assumptions that must be upheld
    - Organizational Security Policies that must be upheld
    - Security Objectives
    - Required Security Functional and Assurance Requirements
  - Generate and obtain approval for these Protection Profiles.
  - Recognize this will likely take a minimum of two – four years to complete
- Once we have the necessary PPs we can start certifying 3D Printers, or the entire Digital Thread against the PP-Configuration shown in the previous slide

BACKUP

Content of a Protection Profile (PP)

- PP Introduction
- Conformance claims and conformance statements
  - Shall state the edition of the relevant parts of the CC to which the PP claims conformance
  - Shall describe the conformance to CC Part 3
  - May also include a conformance claim with respect to other PPs
  - May include a package conformance claim
- Software Problem Definition (SPD)
  - Contains Assumptions; Security Objectives of the TOE and of the Operational Environment; threats against the TOE and Organizational Security Policies
- Security Functional Requirements
- Security Assurance Requirements

Content of a PP-Module

- Must specify one or more PP-Module Base(s) consisting of a set of PPs and possibly other PP-Modules
- Conformance claims and conformance statements
  - Shall state the edition of relevant parts of the CC to which the PP-Module claims conformance
  - May include a conformance claim made with respect to functional packages. More than one functional package may be claimed by a PP-Module
  - Shall include a conformance claim in respect to CC Part 3
  - Shall provide a conformance statement which describes the manner in which STs shall conform to this PP-Module as part of a PP-Configuration
- Assurance requirements
  - Shall define the set of SARs that applies to the TSF defined in the PP-Module, which can be either inherited from the PP-Module Base(s) or explicitly declared by the PP-Module author
  - Shall provide an assurance rationale that justifies the internal consistency of its set of SARs

Next Steps – IDS WG

- Next IDS WG Meeting– No other meetings scheduled in 2024
- Next IDS Face-to-Face Meeting during PWG February 2025 F2F – Feb 4-6, 2025
- Start looking at involvement in some of these other standard's activities individually and maybe as a WG

Backup

HCD iTC
Issues Post-Version 1.0 – CNSA 2.0

- Commercial National Security Algorithm (CNSA) 2.0 released by NSA Sep 2022
- Addresses problem that future deployment of a cryptanalytically relevant quantum computer (CRQC) would break public-key systems still used today
- Need to plan, prepare, and budget for an effective transition to quantum-resistant (QR) algorithms, to assure continued protection of National Security Systems (NSS) and related assets
- Is an update to CNSA 1.0 Algorithms
- Applies to all NSS use of public cryptographic algorithms (as opposed to algorithms NSA developed), including those on all unclassified and classified NSS
- Using any cryptographic algorithms the National Manager did not approve is generally not allowed, and requires a waiver specific to the algorithm, implementation, and use case
- Per CNSSP 11, software and hardware providing cryptographic services require NIAP or NSA validation in addition to meeting the requirements of the appropriate version of CNSA

Transitioning to CNSA Suite 2.0

- The timing of the transition depends on the proliferation of standards-based implementations
- NSA expects the transition to QR algorithms for NSS to be complete by 2035 in line with NSM-10.
- NSA urges vendors and NSS owners and operators to make every effort to meet this deadline.
- Where feasible, NSS owners and operators will be required to prefer CNSA 2.0 algorithms when configuring systems during the transition period.
- When appropriate, use of CNSA 2.0 algorithms will be mandatory in classes of commercial products within NSS, while reserving the option to allow other algorithms in specialized use cases