The Printer Working Group

Imaging Device Security

August 7, 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 – 10:30	Discuss status of HCD iTC, HIT and plans for future HCD cPP/HCD SD releases
10:30 – 10:35	Connectivity Standards Alliance
10:55 – 11:00	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 May 8, 2024 HCD iTC meetings have been held on:
  - May 13th, Jun 3rd, Jul 8th, Aug 5th

  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 was and is 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 for and then implementing the next HCD cPP / HCD SD release
  - Addressing issues against HCD cPP / SD v1.0

Errata to HCD cPP v1.0 and HCD SD v1.0

- 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 and from NIAP. JISEC (the Japanese Scheme) has finally posted its endorsement as part of an updated Position Statement
- Note that 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**

  The Errata version will succeed the HCD PP V1.0 **which will be sunset by NIAP effective 23 October 2024**

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?

HIT Status

- Priorities now, in order are:
  - Resolving the remaining 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
- The key question the HIT will need to address is whether the HIT will issue any more standalone HCD cPP or HCD SD v1.0.x releases after the Errata release to address the Priority 1 issues at least (or do we pass them on the HCD iTC to include in the next full release of the documents)
- If the HIT does decide to do standalone releases, how many of these releases will occur likely depends on the comments we get from:
  - The review of the HCD cPP from the other Schemes and
  - Future certifications against HCD cPP v1.0 or HCD SD v1.0 from the applicable Evaluation Lab or applicable Scheme

  Note: The nature and severity of the comments will probably determine whether comments against HCD cPP or HCD SD v1.0 get fixed in a v1.0.x release or get fixed in a later version of the HCD cPP and HCD SD

HIT Issue Summaries – Remaining 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 Solution 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 jointly by the HIT at a HIT meeting
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
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 to be circulated to full iTC Issue of HW-based write-protection is still under discussion

HIT Issue Summaries – Remaining 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 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

HIT Issue Summaries – Issues Not Yet Prioritized

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 #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

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
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 the results from the CCDB Crypto WG's SFR Catalog, Syncing with ND cPP/SD 3.0 and CC:2022 Compliant efforts
- V3.0 - 2027 – 2028:
  - Will likely contain some CNSA 2.0 components and content from the other priorities

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

- Updates for the relevant changes in CC:2022
- Incorporate SFRs from the CCDB Specification of Functional Requirements for Cryptography once it is published and we get a transition plan
- Update for the relevant changes in ND cPP v3.0e
- Inclusion of support for TLS 1.3 and deprecation of TLS 1.1
  - Standardizing on ND 3.0 Implementation
- Incorporate the NIAP Functional Package for SSH so can claim conformance to it
- Inclusion of AVA_VAN to sync with EUCC
- Incorporate Priority 1 and other HIT Issues into HCD cPP/SD versions
- 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 1.0 Potential for Inclusion in V3.0 and Later Versions

- NTP
- Full implementation of CNSA 2.0
- Support for Cloud Printing
- Incorporate NIAP Functional Package for X.509 when it becomes available
- Support for post quantum and other new crypto algorithms
- Any other new NIAP Packages
- Updates due to changes from other ISO, FIPS or NIST Standards/Guidelines, and NIAP TDs
- Updates to Address 3D printing and the Digital Thread to Additive Manufacturing
- Support for Artificial Intelligence
- 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 Errata to address all documented RfIs
- Complete HCD cPP/SD v1.0e certification by Canadian Scheme
  - Current plan is to be done sometime in Sep 2024
  - Will also include certification of HCD cPP v1.0e
- Fully engage the HCD iTC to work on HCD cPP v2.0 and HCD SD v2.0
- Start planning for HCD cPP/SD v3.0 and beyond

CONNECTIVITY STANDARDS ALLIANCE (CSA)

Connectivity Standards Alliance

Mission: Ignite creativity and collaboration in the Internet of Things, by developing, evolving, and promoting universal open standards that enable all objects to securely connect and interact. We believe all objects can work together to enhance the way we live, work, and play

Key Offerings:

Develop - Create, evolve and manage IoT technology standards through a well-established, collaborative process. We empower companies with practical, usable assets and tools to ease and accelerate development, freeing them to focus on new areas of IoT innovation

Certify - Our strong certification programs help Members avoid unnecessary development cycles, ensure compliance and validate interoperability. Certification and our stamp of approval tells the world they can buy and use certified products and platforms with confidence

Promote

- We are allies for a connected future. Our membership, spanning the global and the IoT value chain, actively seeks to promote the benefits of global, open standards, the value of the IoT to customers and consumers and to break down the barriers to broad access and adoption of IoT technologies and solutions.

Connectivity Standards Alliance Certification Process

1. Become a member of the CSA - Read Connectivity Standards Alliance Policies and Governing Documents and become a member
2. **Request a Manufacturer ID / Vendor ID -** Contact the Alliance Certification Team to reserve your Manufacturer ID or Vendor ID.
3. **Select a Compliant Platform or Network Transport**
4. **Choose a Testing Provider -** Select from Connectivity Standards Alliance authorized Test Providers at locations all around the world
5. **Send Product to be Tested -**After scheduling testing with an Authorized Test Provider, the facility will make arrangements for testing samples and Protocol Implementation Conformance Statement (PICS) documents to be submitted. Test Provider will issue a final report to the Connectivity Standards Alliance when testing is successfully completed
6. **Submit Certification Application -** Complete and submit an application for certification in the Connectivity Standards Alliance Certification Tool. Instructions for requesting a Certification Tool account and creating/submitting applications can be found in the Connectivity Standards Alliance Members Area

Connectivity Standards Alliance Certification Process

7. **Application Pending -** Connectivity Standards Alliance Certification Team will review your application and, if necessary, request action on specific identified items or information required to make a determination of approval or rejection. At any time during this process, you may reach out to the Connectivity Standards Alliance Certification Team with any questions
8. **Upon Approval -** After your product certification is approved, you will receive a formal certificate from the Alliance and may immediately begin using the Certified Product logo. Certified Product logos have usage guidelines that govern how they are used. Please review the applicable sections before affixing. Logos are provided to the applicant's contact for the certification. For more information about Alliance logos and their usage, please contact us

CSA IoT Device Security Specification Version 1.0

CSA IoT Device Security Specification Version 1.0

Created March 18, 2024

Purpose: Define the requirements that must be met by devices within the initial scope of this Specification to be certified under the Alliance Product Security certification and define the baseline security threshold requirements for an Alliance-based device security certification program defined by the Alliance that can be used to certify the security of IoT Devices

Scope: Certifying the security of consumer IoT Devices, contemplating the use of each such IoT Device in an IoT System for consumer use in the smart home, to meet the level current as of June 2023 required by:

- international standards (specifically European Telecommunications Standards Institute (ETSI) EN 303 645 [3] and National Institute of Standards and Technology (NIST) IR 8425 [4]); and
- regulations (specifically Singapore Cybersecurity Labeling Scheme (CLS) [5]); and
- the markets

Does not cover home healthcare products

CSA IoT Device Security Specification Version 1.0 Key Definitions

- **Best Practice Cryptography -** Cryptographic Algorithms, modes and protocols, key generation and handling, and random number generation required by any government or regulatory body in the applicable market, or markets, in which the IoT Device is intended to be deployed. The choices may be determined by the need for interoperability as required by established specifications as described in section on Best Practices for Cryptography of the PSWG Assessment Guidance
- **Critical Security Parameters -** Security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs), the disclosure or modification of which can compromise the security of an IoT Device.
- **Cryptographic Algorithms -** Cryptographic primitives and higher-level algorithms that perform functions essential to maintaining cryptographic security.

CSA IoT Device Security Specification Version 1.0 Key Definitions

- **IoT Associated Service -** Software that complements an IoT Device, providing an external service that is not executed within the IoT Device.
- **IoT Device -** A tangible product, composed of IoT Sub-Components, that comprises at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth) for interfacing with the digital world. PSWG 1.0 is limited to devices intended principally for consumer use in the home (excluding home healthcare devices).
- **IoT Device Manufacturer -** An organization that designs, develops, manufactures or markets an IoT Device.
- **IoT Sub-Component -** The underlying hardware/firmware/software from which an IoT System Component is built
- **IoT System -** A collection of related IoT System Components, including IoT Devices and IoT Associated Services. There is no assumption in this Specification that all of the IoT System Components in an IoT System come from the same vendor.
- **IoT System Component -** An IoT Device, an IoT Associated Service, or other equipment used to create an IoT System instance. An example of other equipment would include a router.

CSA IoT Device Security Specification Version 1.0 Key Definitions

- **Security-Related Configuration -** The configuration for security countermeasures for an IoT System or IoT System Component that facilitates the management of risk.
- **Security-Relevant Information -** Information that could identify the combination of the IoT Device and the version of that IoT Device's software and/or hardware.
- **Security Best Practices -** These are the best practices for IoT Device security:
  1. Perform a risk analysis and threat model for the IoT Device in light of the expected usage and target deployment context
  2. Identify and classify data storage points and data flow assets, and safeguard assets classified as Sensitive Data in a manner that satisfies some or all of the following: availability, integrity, and confidentiality, as applicable to each asset
  3. Select appropriate countermeasures to reduce residual risk to acceptable levels
  4. Implement the selected countermeasures.
- **Sensitive Data -**Data that is of particular concern from a security perspective, including, by way of example and without limitation: safety- and/or control-related commands/functions or parameters; data strings; data attributes; personal identifiable information; data in memory being used for calculations; credentials; keys; protocol header fields; and intellectual property

CSA IoT Device Security Specification Version 1.0 Key Technical Requirements

Unique Identity

- The IoT Device SHALL be uniquely identifiable for cybersecurity purposes. This MAY require a set of identities depending upon the specific use.

IoT System Inventory

- If the IoT Device is able to collate or store an inventory of connected IoT System Components, the IoT Device SHALL uniquely identify each such IoT System Component and maintain an up-to-date inventory.

Authentication for Configuration Changes

- If the IoT Device makes or allows Security-Related Configuration changes, including Critical Security Parameters and passwords, via a network or other interface, the related configuration changes SHALL only be accepted after authentication and authorization. Best Practice Cryptography SHALL be used.

Configuring IoT System Components

- If the IoT Device is able to configure other IoT System Components within an IoT System instance, it SHALL be demonstrated that any changes are applied to the other IoT System Component(s). If the IoT Device is able to be configured by other IoT System Components within an IoT System instance, it SHALL be demonstrated that any changes are actually applied in the IoT Device and reflected in the other IoT System Component(s). This requirement only applies to Security-Related Configuration changes.

CSA IoT Device Security Specification Version 1.0 Key Technical Requirements

Uniqueness

- If the IoT Device makes use of Critical Security Parameters, including passwords and identities, they SHALL be unique per IoT Device at the time it is manufactured and SHALL NOT be resettable to any universal factory default. It follows that Critical Security Parameters SHALL NOT be embedded in source code.

  Critical Security Parameters provided by the IoT Device Manufacturer SHALL NOT be easily determined by automated means or obtained from publicly available information or derivatives from fixed parameters associated with the IoT Device.

Security Best Practices

- If the IoT Device makes use of Critical Security Parameters, including passwords, they SHALL conform with Security Best Practices, including, length, complexity, generation of keys from passwords, secure management processes, and secure storage. Best Practice Cryptography SHALL be used.

Preventing Brute Force Attacks

- The IoT Device SHALL implement a mechanism that protects against brute force authentication attacks.

Changing Authentication Values

- If the user can authenticate against the IoT Device, at least the IoT Device or some other IoT System Component SHALL include a mechanism for simply changing user authentication values.

CSA IoT Device Security Specification Version 1.0 Key Technical Requirements

Cryptographic Agility

- The IoT Device SHOULD support updating Cryptographic Algorithms and primitives.

Secure Storage of Persistent Data

- All Sensitive Data stored persistently on the IoT Device SHALL be stored in a secure manner consistent with Security Best Practices.

Erasure from Device

- The IoT Device SHALL support the erasure of local data that is from or about the user which may include personal data about the user, their home or family, user configuration, and cryptographic material.

  Any such erasure, including through a Factory Reset, SHALL be authorized, and SHALL leave the IoT Device in a secure state.

  Note: Requirements related to deleting data outside the IoT Device are not in the scope of this Specification

Restricting Access to Security-Relevant Information

- The IoT Device SHALL require authentication and authorization when exposing Security-Relevant Information via the network interfaces of the device.

Confidentiality Protection

- The IoT Device SHALL, by default, ensure the confidentiality of Security-Relevant Information and Sensitive Data exchanged with IoT Devices and IoT Associated Services. Best Practice Cryptography SHALL be used

CSA IoT Device Security Specification Version 1.0 Key Technical Requirements

Remote Trust Relationships

- For two-way communication, the IoT Device SHALL establish a trust relationship ensuring that both parties at each end of a network connection are authenticated. Best Practice Cryptography SHALL be used.

Disabling Unused Interfaces

- The IoT Device SHALL disable all interfaces not necessary for the intended use of the IoT Device.

Input Data Validation

- Data input into the IoT Device via network and any other interfaces SHALL be validated against malformed input.

Restrict Unused Functionality

- Functionality not needed for the intended use of the IoT Device SHALL NOT be installed, or SHALL be disabled where non-installation is not practical

Least Privilege

- All IoT Device software SHOULD be executed with the lowest possible level of privilege necessary for the intended function.

Secure Boot

- The IoT Device SHOULD perform a secure boot process, using Security Best Practices

CSA IoT Device Security Specification Version 1.0 Key Technical Requirements

Verification of Software Updates

- The IoT Device SHALL support a software update process and SHALL ensure the authenticity and integrity of software updates. Best Practice Cryptography SHALL be used.

Automatic Software Updates

- Automatic software update installation methods SHOULD be employed for updating the IoT Device. The IoT Device SHOULD check for available updates at least once after initialization and then periodically.

Ease of Software Update Installation

- Software updates for the IoT Device SHALL be easy for users to install.

Enablement of Software Updates

- If the IoT Device supports automatic updates and/or update notifications, these SHOULD be enabled by default but an authorized entity SHOULD be able to enable, disable, or postpone installation of security updates and/or update notifications.

Audit Logging

- The IoT Device SHOULD support audit logging of security-relevant events and errors. The log SHOULD include enough details to determine what happened.

CSA IoT Device Security Specification Version 1.0 Key Technical Requirements

Reporting Security State

- The IoT Device SHOULD be able to report the current security-related state

Reporting Unauthorized Software Changes

- If the IoT Device detects an unauthorized change to the software, it SHOULD limit connectivity to the minimum required to report the error to authorized recipients. Detection mechanisms include secure boot, or regular monitoring.

Protected Access to Logs

- If the IoT Device supports an audit log as described in Section 5.5.6.1, Audit Logging and that audit log is stored on the IoT Device, it SHOULD restrict access to the log files to authorized personnel only for defined purposes.

Recovery from Power Failure and Network Outage

- The IoT Device SHOULD be resilient to power and network outages. There SHOULD be no impact on the IoT Device security. The effects of an internet connection outage SHOULD be minimized as much as possible to establish continued local functional operation. After the outage is ended, the IoT Device SHOULD gracefully recover to its normal operational state

Isolation of Processing

- The IoT Device SHOULD make use of isolated processing approaches employing both software-based and hardware-based mechanisms, using best practices and in support of the principle of least privilege.

CSA IoT Device Security Specification Version 1.0 Key Non-Technical Requirements

Design Considerations

- The IoT Device Manufacturer SHALL document the expected usage and target deployment context relating to the IoT Device, including at least:
  - Expected customers and use cases, including known potential misuses
  - Laws and regulations that must be complied with
  - Expected device lifespan
  - Expected cybersecurity costs for the end users
  - Intended security context, including assumed cybersecurity requirements and physical
  - environment
  - Threat model
  - Risk analysis

Development Processes, Platforms, and Tools

- The IoT Device Manufacturer SHALL document the processes, platforms, and tools used to develop the IoT Device, including at least:
  - Platforms and tools
  - Accreditation, certification, and/or evaluation results for these processes, if any
  - Other aspects of development processes related to IoT Device Security, including, by way of example, activities taken under the Development Process Related to IoT Device Security section

CSA IoT Device Security Specification Version 1.0 Key Non-Technical Requirements

Secure development processes are fundamental to IoT Device security. Thus, these requirements for secure development processes are included.

Threat Modeling

- The IoT Device Manufacturer SHALL conduct threat modeling to identify, analyze, and mitigate relevant threats.

Secure Engineering Approach

- The IoT Device Manufacturer SHALL employ a secure engineering approach.

IoT Sub-Components

- The IoT Device Manufacturer SHALL maintain an inventory of IoT Sub-Components used in the IoT Device, including version as well as applied patches and updates.

Hardware/Software Supply Chain

- The IoT Device Manufacturer SHALL implement and maintain the IoT Device using IoT Sub-Components from a secure supply chain, with a risk-appropriate process for addressing vulnerabilities

CSA IoT Device Security Specification Version 1.0 Key Non-Technical Requirements

History has shown that diligent vulnerability management and response is critical for cybersecurity. Thus, these requirements and recommendations are included.

Vulnerability Disclosure

- The IoT Device Manufacturer SHALL establish, publicize, and implement a vulnerability disclosure process for the IoT Device.

  This process SHALL include at least a documented method for reporting issues as well as a timeline for acknowledging receipt of a report and for providing status updates on the resolution of the reported issues.

Vulnerability Response

- The IoT Device Manufacturer SHOULD continually monitor, identify, and respond in a timely manner to security vulnerabilities throughout the defined support period.

Vulnerability Assessment

- The IoT Device Manufacturer SHALL conduct penetration testing or vulnerability testing or both periodically, including at least before every major release.

Security Updates

- Security updates are changes that mitigate or fix security vulnerabilities and follow Security Best Practices

CSA IoT Device Security Specification Version 1.0 Key Non-Technical Requirements

Timely Updates

- The IoT Device Manufacturer SHALL provide timely security updates during the defined support period for the IoT Device.

User Notification of Updates

- The IoT Device Manufacturer SHOULD ensure that the user is notified when a security update is needed, including information about the risks mitigated by the update. If the update will disrupt the IoT Device's functionality, this SHOULD be disclosed.

When Updates Cannot Be Provided

- When updates cannot be provided, the IoT Device Manufacturer SHOULD clearly explain to users why no updates are available, how affected hardware can be isolated and replaced, and the defined support period

Consumer Disclosure

- The IoT Device Manufacturer SHALL provide information to consumers about what personal data (and telemetry data, if any) is being processed, how it is being used, by whom, and for what purposes.

Consent

- When consumer consent is obtained for personal data processing, this consent SHALL be obtained in a valid manner. Consumers SHALL have the power to withdraw this consent at any time.

CSA IoT Device Security Specification Version 1.0 Key Non-Technical Requirements

Minimization

When data is collected from IoT Devices, that data SHALL be kept to the minimum necessary for the intended functionality.

Non-compliance with Requirements or Recommendations

If any provision (requirement or recommendation) in this Specification is not met, the IoT Device Manufacturer SHALL document why this is an appropriate decision based on design assumptions such as the expected use cases, intended security context, and the threat model. Justifications SHALL be based on risk and Security Best Practices not just on cost or previous design decisions.

Compliance with an established specification for the ecosystem in which the IoT Device is intended to be deployed, e.g., for interoperability, may be required. In these circumstances, it is possible that certain requirements cannot be met in order to comply with that specification. In these circumstances, justification for non-compliance SHALL be provided.

Next Steps – IDS WG

- Next IDS WG Meeting– August 22, 2024
- Next IDS Face-to-Face Meeting during PWG November 2024 F2F Nov 12-14, 2024
- Start looking at involvement in some of these other standards 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