The Printer Working Group

Imaging Device Security

May 8, 2024

PWG May 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 – 10:50	Discuss status of HCD iTC, HIT and plans for future HCD cPP/HCD SD releases
10:40 – 11:25	EUCC Implementing Regulation
11:25 – 11:55	TCG/IETF Liaison Reports
11:55 – 12:00	Wrap Up / Next Steps

Antitrust and Intellectual Property Policies

"This meeting is conducted under the rules of the 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 10, 2023 HCD iTC meetings have been held on:
  - In 2023: Aug 21st, Oct 10th, Nov 27th
  - In 2024: Jan 22nd, Feb 12th, Mar 18th, Apr 29th

  NOTE: Since publishing the HCD cPP v1.0 and HCD SD v1.0 in Oct 2022 the HCD iTC has gone to meeting once a month

- 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

HCD international Technical Community (iTC) Status

- Since last IDS F2F on August 10, 2023 HCD iTC meetings have been held on:
  - In 2023: Aug 21st, Oct 10th, Nov 27th
  - In 2024: Jan 22nd, Feb 12th, Mar 18th, Apr 29th

  NOTE: Since publishing the HCD cPP v1.0 and HCD SD v1.0 in Oct 2022 the HCD iTC has gone to meeting once a month

- 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
- 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**

This version succeeds the HCD PP V1.0 **which will sunset 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

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

- The Errata was required to address comments against HCD cPP v1.0 and HCD SD v1.0 that were received by the HCD Interpretation Team (HIT) from the following sources:
  - NIAP and the Canadian and Korean Schemes as part of their review of these documents
  - Evaluation labs performing certifications of HCDs against these two documents
  - Issues raised by Individual Contributors
- The criteria for issues included in the Errata was:
  - Any issue that was raised by one of the Schemes
  - Any issue that was required to be fixed for a certification against an HCD to be completed

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 initial 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

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 #25	This issue is that SFR FPT_SBT_EXT.1 in the HCD cPP states that Root of Trust is implemented in immutable code or a HW-based write-protection mechanism but provides no further description or additional detail on the definition for the Root of Trust in terms of its protection. The HCD SD includes a requirement that the TSS shall describe how the Root of Trust is immutable. However, HCD cPP is not clear on how the immutable code or HW-based write-protection is defined. The SD does not provide clear guidance on the level of assurance the evaluator shall take into consideration to confirm a compliant Root of Trust protection mechanism.	Issue is awaiting a priority assignment.

HCD iTC
Post-Version 1.0e Release Plan

Based on current information, as of now the HCD iTC is 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

- Incorporate SFRs from the CCDB Specification of Functional Requirements for Cryptography once it is published and we get a transition plan
- Updates for the relevant changes in CC:2022
- 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 for now
- Incorporate the NIAP Functional Package for SSH so can claim conformance to it
- Inclusion of AVA_VAN to sync with EUCC
- Priority 1 Issues) to HCD cPP/SD v1.0
- 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 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 on down) are:

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

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
- 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

HCD iTC Status
One Last Set of Lessons Learned from 19 Years of Developing PPs and cPPs (My Take)

EUCC Implementing Regulation

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA) CYBERSECURITY CERTIFICATION (EUCC)

Replaces candidate Version: v1.1.1 dated May 2021

Will go into force 27 Feb 2025

Key Goals

(1) Specifies the roles, rules and obligations, as well as the structure of the European Common Criteria- based cybersecurity certification scheme (EUCC) in accordance with the European cybersecurity certification framework set out in Regulation (EU) 2019/881

(2) The scheme should be based on established international standards such as the Common Criteria. The Common Criteria is accompanied by the Common Evaluation Methodology.

- The EUCC uses the Common Criteria's vulnerability assessment family (AVA_VAN), components 1 to 5. The applicant for an EUCC certificate should provide the documentation related to the intended use of the ICT product and the analysis of the levels of risks associated with such usage in order to enable the conformity assessment body to evaluate the suitability of the assurance level selected. Where the evaluation and certification activities are performed by the same conformity assessment body, the applicant should submit the requested information only once

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA) CYBERSECURITY CERTIFICATION (EUCC)

SCOPE

- This Regulation sets out the European Common Criteria-based cybersecurity certification scheme (EUCC)
- This Regulation applies to all information and communication technologies ('ICT') products, including their documentation, which are submitted for certification under the EUCC, and to all protection profiles which are submitted for certification as part of the ICT process leading to the certification of ICT products.

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA) CYBERSECURITY CERTIFICATION (EUCC)

Evaluation Standards EUCC Evaluations Shall Be Based On:

- ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation
- ISO/IEC 18045, Common Methodology for Information Technology Security Evaluation

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA) CYBERSECURITY CERTIFICATION (EUCC)

Methods for Certifying ICT Products

- Certification of an ICT product shall be carried out against its security target:
  - as defined by the applicant; or
  - incorporating a certified protection profile as part of the ICT process, where the ICT product falls in the ICT product category covered by that protection profile.
- Protection profiles shall be certified for the sole purpose of the certification of ICT products falling in the specific category of ICT products covered by the protection profile.

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA) CYBERSECURITY CERTIFICATION (EUCC)

Assurance Levels

- Certification bodies shall issue EUCC certificates at assurance level 'substantial' or 'high'.
- EUCC certificates at assurance level 'substantial' shall correspond to certificates that cover AVA_VAN level 1 or 2.
- EUCC certificates at assurance level 'high' shall correspond to certificates that cover AVA_VAN level 3, 4 or 5.
- The assurance level confirmed in a EUCC certificate shall distinguish between the conformant and augmented use of the assurance components as specified in the Common Criteria in accordance with Annex VIII.
- Conformity assessment bodies shall apply those assurance components on which the selected AVA_VAN level depends in accordance with the standards referred to in Article 3.

EUCC
CERTIFICATION OF ICT PRODUCTS

Evaluation criteria and methods for ICT products

An ICT product submitted for certification shall, as a minimum, be evaluated in accordance with the following:

- The applicable elements of the standards referred to in Article 3 (Evaluation Stan dards)
- The security assurance requirements classes for vulnerability assessment and independent functional testing, as set out in the evaluation standards referred to in Article 3 (Evaluation Standards)
- The level of risk associated with the intended use of the ICT products concerned and their security functions that support the security objectives
- The applicable state-of-the-art documents listed in Annex I; and the applicable certified protection profiles listed in Annex II
- In the case of an ICT product undergoing a composite product evaluation in accordance with the relevant state-of- the-art documents, the ITSEF that carried out the evaluation of the underlying ICT product shall share the relevant information with the ITSEF performing the evaluation of the composite ICT product.

EUCC
CONDITIONS FOR ISSUANCE OF AN EUCC CERTIFICATE

The certification bodies shall issue an EUCC certificate where all of the following conditions are met:

- The category of ICT product falls within the scope of the accreditation, and where applicable of the authorisation, of the certification body and the ITSEF involved in the certification;
- The applicant for certification has signed a statement undertaking all commitments listed in paragraph 2;
- The ITSEF has concluded the evaluation without objection in accordance with the evaluation standards, criteria and methods referred to in Articles 3 and 7;
- The certification body has concluded the review of the evaluation results without objection;
- The certification body has verified that the evaluation technical reports provided by the ITSEF are consistent with the provided evidence and that the evaluation standards, criteria and methods referred to in Articles 3 and 7 have been correctly applied.

EUCC
PERIOD OF VALIDITY FOR A EUCC CERTIFICATE

- The certification body shall set a period of validity for each EUCC certificate issued taking into account the characteristics of the certified ICT product.
- The period of validity of the EUCC certificate shall not exceed 5 years.
- By derogation from paragraph 2 that period may exceed 5 years, subject to the prior approval of the national cybersecurity certification authority. The national cybersecurity certification authority shall notify the European Cybersecurity Certification Group of the granted approval without undue delay.

EUCC
CERTIFICATION OF PROTECTION PROFILES

Evaluation criteria and methods for Protection Profiles

A protection profile shall be evaluated, as a minimum, in accordance with the following:

- The applicable elements of the standards referred to in Article 3;
- The level of risk associated with the intended use of the ICT products concerned pursuant to Article 52 of Regulation (EU) 2019/881 and their security functions that support the security objectives set out in Article 51 of that; and
- The applicable state-of-the-art documents listed in Annex I. A protection profile covered by a technical domain shall be certified against the requirements set out in that technical domain.

EUCC
CONDITIONS FOR ISSUANCE OF AN EUCC CERTIFICATE FOR A PROTECTION PROFILE

- The applicant for certification shall provide the certification body and the ITSEF with all the necessary complete and correct information.
- Articles 9 and 10 shall apply mutatis mutandis.
- The ITSEF shall evaluate whether a protection profile is complete, consistent, technically sound and effective for the intended use and the security objectives of the ICT product's category covered by that protection profile.
- A protection profile shall be certified solely by:
- a national cybersecurity certification authority or another public body accredited as certification body; or
- a certification body, upon prior approval by the national cybersecurity certification authority for each individual protection profile.

EUCC
PERIOD OF VALIDITY FOR A EUCC CERTIFICATE FOR A PROTECTION PROFILE

- The certification body shall set a period of validity for each EUCC certificate.
- The period of validity may be up to the lifetime of the protection profile concerned.

EUCC VULNERABILITY MANAGEMENT PROCEDURES

- The holder of an EUCC certificate shall establish and maintain all necessary vulnerability management procedures in accordance with the rules laid down in this Section and, where necessary, supplemented by the procedures set out in EN ISO/IEC 30111
- The holder of an EUCC certificate shall maintain and publish appropriate methods for receiving information on vulnerabilities related to their products from external sources, including users, certification bodies and security researchers
- Where a holder of an EUCC certificate detects or receives information about a potential vulnerability affecting a certified ICT product, it shall record it and carry out a vulnerability impact analysis
- When a potential vulnerability impacts a composite product, the holder of the EUCC certificate shall inform the holder of dependent EUCC certificates about potential vulnerability
- In response to a reasonable request by the certification body that issued the certificate, the holder of an EUCC certificate shall transmit all relevant information about potential vulnerabilities to that certification body

EUCC
VULNERABILITY MANAGEMENT
VULNERABILITY IMPACT ANALYSIS

- Vulnerability impact analysis shall refer to the target of evaluation and the assurance statements contained in the certificate. Vulnerability impact analysis shall be carried out in a timeframe appropriate for the exploitability and criticality of the potential vulnerability of the certified ICT product
- Where applicable, an attack potential calculation shall be performed in accordance with the relevant methodology included in the standards referred to in Article 3 and the relevant state-of-the-art documents listed in Annex I, in order to determine the exploitability of the vulnerability. The AVA_VAN level of the EUCC certificate shall be taken into account

EUCC
VULNERABILITY MANAGEMENT
VULNERABILITY IMPACT ANALYSIS REPORT

- Where the vulnerability impact analysis report determines that the vulnerability is not residual within the meaning of standards referred to in Article 3, and that it can be remedied, Article 36 shall apply
- Where the vulnerability impact analysis report determines that the vulnerability is not residual and that it cannot be remedied, the EUCC certificate shall be withdrawn in accordance with Article 14
- The holder of the EUCC certificate shall monitor any residual vulnerabilities to ensure that it cannot be exploited in case of the changes in the operational environment

EUCC
VULNERABILITY MANAGEMENT
VULNERABILITY REMEDIATION

The holder of an EUCC certificate shall submit a proposal for an appropriate remedial action to the certification body. Certification body shall review the certificate in accordance with Article 13. The scope of the review shall be determined by the proposed remediation of the vulnerability

EUCC
VULNERABILITY MANAGEMENT
VULNERABILITY DISCLOSURE

- The information provided by the certification body to the national cybersecurity certification authority shall include all elements necessary for the national cybersecurity certification authority to understand the impact of the vulnerability, the changes to be made to the ICT product and, where available, any information from the certification body on the broader implications of the vulnerability for other certified ICT products
- The information provided in accordance with paragraph 1 shall not contain details of the means of exploitation of the vulnerability
- The national cybersecurity certification authority shall share the relevant information received with other national cybersecurity certification authorities and ENISA.
- Other national cybersecurity certification authorities may decide to further analyse the vulnerability or, after informing the holder of the EUCC certificate, request the relevant certification bodies to assess whether the vulnerability may affect other certified ICT products.
- Upon withdrawal of a certificate, the holder of the EUCC certificate shall disclose and register any publicly known and remediated vulnerability in the ICT product on the European vulnerability database

EUCC
MUTUAL RECOGNITION AGREEMENTS WITH THIRD COUNTRIES

Third countries willing to certify their products in accordance with this Regulation, and who wish to have such certification recognised within the Union, shall conclude a mutual recognition agreement with the Union.

The mutual recognition agreement shall cover the applicable assurance levels for certified ICT products and, where applicable, protection profiles.

Mutual recognition agreements referred to in paragraph 1, may only be concluded with third countries that meet the following conditions:

- Have an authority that:
  - Is a public body, independent of the entities it supervises and monitors in terms of organisational and legal structure, financial funding and decision making;
  - Has appropriate monitoring and supervising powers to carry out investigations and is empowered to take appropriate corrective measures to ensure compliance;
  - Has an effective, proportionate and dissuasive penalty system to ensure compliance;

EUCC
MUTUAL RECOGNITION AGREEMENTS WITH THIRD COUNTRIES

Mutual recognition agreements referred to in paragraph 1, may only be concluded with third countries that meet the following conditions:

- Have an authority that:
  - Agrees to collaborate with the European Cybersecurity Certification Group and ENISA to exchange best practice and relevant developments in the field of cybersecurity certification and to work towards a uniform interpretation of the currently applicable evaluation criteria and methods, amongst others, by applying harmonised documentation that is equivalent to the state-of-the-art documents listed in Annex I
  - Have an independent accreditation body performing accreditations using equivalent standards to those referred to in Regulation (EC) No 765/2008;
  - Commit that the evaluation and certification processes and procedures will be carried out in a duly professional manner, taking into account compliance with the international standards referred to in this Regulation, in particular in Article 3;
  - Have the capacity to report previously undetected vulnerabilities and an established, adequate vulnerability management and disclosure procedure in place;

EUCC
MUTUAL RECOGNITION AGREEMENTS WITH THIRD COUNTRIES

Mutual recognition agreements referred to in paragraph 1, may only be concluded with third countries that meet the following conditions:

- Have an authority that:
  - Have established procedures that enable it to effectively lodge and handle complaints and provide effective legal remedy for the complainant;
  - Establishing a mechanism for cooperation with other Union and Member States' bodies relevant to the cybersecurity certification under this Regulation

In addition to the conditions set out in paragraph 3, a mutual recognition agreement referred to in paragraph 1 covering assurance level "high" may only be concluded with third countries where also the following conditions are met:

- The third country has an independent and public cybersecurity certification authority performing or delegating evaluation activities necessary to allow certification under assurance level 'high' that are equivalent to the requirements and procedures laid down for national cybersecurity authorities in this Regulation and in Regulation (EU) 2019/881;
- The mutual recognition agreement establishes a joint mechanism equivalent to the peer assessment for EUCC certification to enhance the exchange of practices and jointly solve issues in the area of evaluation and certification.

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA) CYBERSECURITY CERTIFICATION (EUCC)

Assorted Other Requirements

- Conformity of Self Assessments – Are not permitted
- Requirements for Marking and Labels
- Withdrawal of Certificates – Can be done by the Certifying Body or by request of the holder of the certificate
- Monitoring Activities by the Certifying Body and by the Holder of the Certificate
  - Certifying Bodies shall monitor the compliance of the ICT products it has certified with their respective security requirements and the assurance expressed in the certified protection profile
  - The holder of the certificate shall monitor vulnerability information regarding the certified ICT product and the assurance expressed in the EUCC certificate

.

EUCC
ANNEX I – TECHNICAL DOMAINS AND STATE-OF-THE-ART DOCUMENTS

Technical domains at AVA_VAN level 4 or 5:

(a) documents related to the harmonised evaluation of technical domain 'smart cards and similar devices' and in particular the following documents in their respective version in force on [date of entry into force]:

(1) 'Minimum ITSEF requirements for security evaluations of smart cards and similar devices', initially approved by ECCG on 20 October 2023;

(2) 'Minimum Site Security Requirements', initially approved by ECCG on 20 October 2023;

(3) 'Application of Common Criteria to integrated circuits', initially approved by ECCG on 20 October 2023;

(4) 'Security Architecture requirements (ADV_ARC) for smart cards and similar devices', initially approved by ECCG on 20 October 2023;

(5) 'Certification of "open" smart card products', initially approved by ECCG on 20 October 2023;

(6) 'Composite product evaluation for smart cards and similar devices', initially approved by ECCG on 20 October 2023;

(7) 'Application of Attack Potential to Smartcards', initially approved by ECCG on 20 October 2023;

EUCC
ANNEX I – TECHNICAL DOMAINS AND STATE-OF-THE-ART DOCUMENTS

Technical domains at AVA_VAN level 4 or 5:

(a) documents related to the harmonised evaluation of technical domain 'hardware devices with security boxes' and in particular the following documents in their respective version in force on [date of entry into force]:

(1) 'Minimum ITSEF requirements for security evaluations of hardware devices with security boxes', initially approved by ECCG on 20 October 2023;

(2) 'Minimum Site Security Requirements', initially approved by ECCG on 20 October 2023;

(3) 'Application of Attack Potential to hardware devices with security boxes', initially approved by ECCG on 20 October 2023.

State-of-the-art documents in their respective version in force on [date of entry into force]:

(a) document related to the harmonised accreditation of conformity assessment bodies: 'Accreditation of ITSEFs for the EUCC', initially approved by ECCG on 20 October 2023.

EUCC
ANNEX IV – ASSURANCE CONTINUITY AND CERTIFICATE REVIEW

Scope of Assurance Continuity

The following requirements for assurance continuity apply to the maintenance activities related to the following:

- a re-assessment if an unchanged certified ICT product still meets its security requirements;
- an evaluation of the impacts of changes to a certified ICT product on its certification;
- if included in the certification, the application of patches in accordance with an assessed patch management process;
- if included, the review of the certificate holder's lifecycle management or production processes.

The holder of an EUCC certificate may request the review of the certificate in the following cases:

- the EUCC certificate is due to expire within nine months;
- there has been a change either in the certified ICT product or in another factor which could impact its security functionality;
- the holder of the certificate demands that the vulnerability assessment is carried out again in order to reconfirm the EUCC certificate's assurance associated with the ICT product's resistance against present cyberattacks.

EUCC
ANNEX IV – ASSURANCE CONTINUITY AND CERTIFICATE REVIEW

Reassessment

- Where there is a need to assess the impact of changes in the threat environment of an unchanged certified ICT product, a re-assessment request shall be submitted to the certification body.
- The re-assessment shall be carried out by the same ITSEF that was involved in the previous evaluation by reusing all its results that still apply. The evaluation shall focus on assurance activities which are potentially impacted by the changed threat environment of the certified ICT product, in particular the relevant AVA_VAN family and in addition the assurance lifecycle (ALC) family where sufficient evidence about the maintenance of the development environment shall be collected again.
- The ITSEF shall describe the changes and detail the results of the re-assessment with an update of the previous evaluation technical report.
- The certification body shall review the updated evaluation technical report and establish a re-assessment report. The status of the initial certificate shall then be modified in accordance with Article 13.
- The re-assessment report and updated certificate shall be provided to the national cybersecurity certification authority and ENISA for publication on its cybersecurity certification website

EUCC
ANNEX IV – ASSURANCE CONTINUITY AND CERTIFICATE REVIEW

Changes To A Certified ICT Product

- Where a certified ICT product has been subject to changes, the holder of the certificate wishing to maintain the certificate shall provide to the certification body an impact analysis report.
- The impact analysis report shall provide the following elements:
  - an introduction containing necessary information to identify the impact analysis report and the target of evaluation subject to changes;
  - a description of the changes to the product;
  - the identification of affected developer evidence;
  - a description of the developer evidence modifications;
  - the findings and the conclusions on the impact on assurance for each change.
- The certification body shall examine the changes described in the impact analysis report in order to validate their impact upon the assurance of the certified target of evaluation, as proposed in the conclusions of the impact analysis report.
- Following the examination, the certification body determines the scale of a change as minor or major in correspondence to its impact.

EUCC
ANNEX IV – ASSURANCE CONTINUITY AND CERTIFICATE REVIEW

Changes To A Certified ICT Product

- Where the changes have been confirmed by the certification body to be minor, a new certificate shall be issued for the modified ICT product and a maintenance report to the initial certification report shall be established, under following conditions:
  - The maintenance report shall be included as a subset of the impact analysis report, containing following sections:
    - introduction;
    - description of changes;
    - affected developer evidence;
  - The validity date of the new certificate shall not exceed the date of the initial certificate.
- The new certificate including the maintenance report shall be provided to ENISA for publication on its cybersecurity certification website.
- Where the changes have been confirmed to be major, a re-evaluation shall be carried out in the context of the previous evaluation and by reusing any results from the previous evaluation that still apply.

EUCC
ANNEX IV – ASSURANCE CONTINUITY AND CERTIFICATE REVIEW

Changes To A Certified ICT Product

- After completion of the evaluation of the changed target of evaluation, the ITSEF shall establish a new evaluation technical report. The certification body shall review the updated evaluation technical report and, where applicable, establish a new certificate with a new certification report.
- The new certificate and certification report shall be provided to ENISA for publication.

EUCC
ANNEX IV – ASSURANCE CONTINUITY AND CERTIFICATE REVIEW

Patch Management

- A patch management procedure provides for a structured process of updating a certified ICT product. The patch management procedure including the mechanism as implemented into the ICT product by the applicant for certification can be used after the certification of the ICT product under the responsibility of the conformity assessment body.
- The applicant for certification may include into the certification of the ICT product a patch mechanism as part of a certified management procedure implemented into the ICT product under one of the following conditions:
  - the functionalities affected by the patch reside outside the target of evaluation of the certified ICT product;
  - the patch relates to a predetermined minor change to the certified ICT product;
  - the patch relates to a confirmed vulnerability with critical effects on the security of the certified ICT product.
- If the patch relates to a major change to the target of evaluation of the certified ICT product in relation to a previously undetected vulnerability having no critical effects to the security of the ICT product, the provisions of Article 13 apply.

Patch Management

- The patch management procedure for an ICT product will be composed of the following elements:
  - the process for the development and release of the patch for the ICT product;
  - the technical mechanism and functions for the adoption of the patch into the ICT product;
  - a set of evaluation activities related to the effectiveness and performance of the technical mechanism.
- During the certification of the ICT product:
  - the applicant for certification of the ICT product shall provide the description of the patch management procedure;
  - the ITSEF shall verify the following elements:
    - the developer implemented the patch mechanisms into the ICT product in accordance to the patch management procedure that was submitted to certification;
    - the target of evaluation boundaries are separated in a way that the changes made to the separated processes do not affect the security of the target of evaluation;
    - the technical patch mechanism performs in accordance with the provisions of this section and the applicant's claims;
  - the certification body shall include in the certification report the outcome of the assessed patch management procedure.

EUCC
ANNEX IV – ASSURANCE CONTINUITY AND CERTIFICATE REVIEW

Patch Management

- The holder of the certificate may proceed to apply the patch produced in compliance of the certified patch management procedure to the concerned certified ICT product and shall take the following steps within 5 working days in the following cases:
  - in the case referred to in point 2(a), report the patch concerned to the certification body that shall not change the corresponding EUCC certificate;
  - in the case referred to in point 2(b), submit the patch concerned to the ITSEF for review. The ITSEF shall inform the certification body after the reception of the patch upon which the certification body takes the appropriate action on the issuance of a new version of the corresponding EUCC certificate and the update of the certification report;
  - in the case referred to in point 2(c), submit the patch concerned to the ITSEF for the necessary re-evaluation but may deploy the patch in parallel. The ITSEF shall inform the certification body after which the certification body starts the related certification activities.

HCD Security Guidelines

Liaison Status

Trusted Computing Group (TCG)

- **Recent and Next TCG Members Meetings**
  - **TCG Hybrid F2F (Tokyo, Japan) – 27-29 February 2024 – Ira called in**
  - **TCG Hybrid F2F (Athens, Greece) – 4-6 June 2024 – Ira to call in**
  - **TCG Hybrid F2F (Boston, MA) – 29-31 October 2024 – Ira to call in**
- **Trusted Mobility Solutions (TMS) – Ira is co-chair and co-editor**
  - **Formal Liaisons – GP (TEE, SE, TPS), ETSI (NFV/SAI Security and Privacy)**
  - **Informal Liaisons – 3GPP, GSMA, IETF, ISO, ITU-T, SAE, US NIST**
  - ***TCG TMS Use Cases v2 – published September 2018***
- **Mobile Platform (MPWG) – Ira is co-editor**
  - **Formal and Informal Liaisons – jointly with TMS WG above**
  - ***GP TPS Client API / Entity Attestation API / Keystore API – to be published Q2/Q3 2024 – joint work w/ TCG***
  - ***TCG TPM 2.0 Mobile Common Profile v2 – work-in-progress since Q1 2024***
  - ***TCG MARS 1.0 Mobile Profile – work-in-progress since Q4 2023***
  - ***TCG Mobile Reference Architecture v2 – published August 2023***
- **Recent Specifications**
  - **http://www.trustedcomputinggroup.org/resources**
  - ***TCG Technologies for Device ID and Attestation v1.0 – TCG approved April 2024***
  - ***TCG PC Client Platform TPM Profile v1.06 – public review April 2024***
  - ***TCG Trusted Platform Module Library v1.81 – published March 2024***
  - ***TCG MARS Serialization Interface v1 – published January 2024***
  - ***TCG PC Client Platform Firmware Profile v1.06 – published December 2023***

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

- **Recent and Next IETF Members Meetings**
  - **IETF 119 Hybrid F2F (Brisbane, Australia) – 18-22 March 2024 – Ira called in**
  - **IETF 120 Hybrid F2F (Vancouver, Canada) – 22-26 July 2024 – Ira to call in**
  - **IETF 121 Hybrid F2F (Dublin, Ireland) – 4-8 November 2024 – Ira to call in**
- **Transport Layer Security (TLS)**
  - **IETF Delegated Credentials for TLS and DTLS – RFC 9345 – July 2023**
    https://datatracker.ietf.org/doc/rfc9345/
  - **IETF Exported Authenticators in TLS – RFC 9261 – July 2022**
    https://datatracker.ietf.org/doc/rfc9261/
  - **IETF SSLKEYLOGFILE Format for TLS – draft-02 – April 2024 – IETF Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-tls-keylogfile/
  - **IETF Compact TLS 1.3 – draft-10 – April 2024**
    https://datatracker.ietf.org/doc/draft-ietf-tls-ctls/
  - **IETF Hybrid key exchange in TLS 1.3 – draft-10 – April 2024**
    https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/
  - **IETF TLS 1.2 is in Feature Freeze – draft-00 – April 2024 – WG adopted**
    https://datatracker.ietf.org/doc/draft-ietf-tls-tls12-frozen/
  - **IETF Return Routability Check for DTLS 1.2/1.3 – draft-11 – April 2024 – Waiting for WG Chair**
    https://datatracker.ietf.org/doc/draft-ietf-tls-dtls-rrc/
  - **IETF Bootstrapping TLS Encrypted ClientHello with DNS Service Bindings – draft-01 – March 2024**
    https://datatracker.ietf.org/doc/draft-ietf-tls-svcb-ech/
  - **IETF Flags Extension for TLS 1.3 – draft-13 – March 2024**
    https://datatracker.ietf.org/doc/draft-ietf-tls-tlsflags/
  - **IETF TLS Encrypted Client Hello – draft-18 – March 2024 – Waiting for Writeup**
    https://datatracker.ietf.org/doc/draft-ietf-tls-esni/
  - **IETF Transport Layer Security (TLS) Protocol 1.3 – draft-10 – Waiting for WG Chair**
    https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8446bis/

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

- **Concise Binary Object Representation (CBOR)**
  - **IETF More Control Operators for CDDL – draft-04 – March 2024 – WG Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-cddl-more-control/
  - **IETF CDDL Module Structure – draft-02 – March 2024**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-cddl-modules/

  IETF CBOR Common Deterministic Encoding (CDE) – draft-02 – March 2024
  https://datatracker.ietf.org/doc/draft-ietf-cbor-cde/

  IETF Packed CBOR – draft-12 – March 2024 – Waiting for WG Chair
  https://datatracker.ietf.org/doc/draft-ietf-cbor-packed/

  IETF Updates to the CDDL grammar of RFC 8610 – draft-04 – March 2024 – Waiting for Writeup
  https://datatracker.ietf.org/doc/draft-ietf-cbor-update-8610-grammar/

  - **IETF CBOR Ext Diagnostic Notation – draft-08 – February 2024 – Waiting for Writeup**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-edn-literals/
  - **IETF CBOR Time, Duration, Period – draft-12 – January 2024 – RFC Editor**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-time-tag/
- **Network Time Protocols (NTP)**
  - **IETF Secure Selection and Filtering for NTP with Khronos – RFC 9523 – February 2024**
    https://datatracker.ietf.org/doc/rfc9523/
  - **IETF Roughtime – draft-09 – March 2024**
    https://datatracker.ietf.org/doc/draft-ietf-ntp-roughtime/
  - **IETF NTPv5 Use Cases and Requirements – draft-04 – January 2024 – WG Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-ntp-ntpv5-requirements/
  - **IETF NTP Over PTP – draft-02 – January 2024 – WG Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-ntp-over-ptp/
  - **IETF Updating the NTP Registries – draft-13 – December 2023 – IETF Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-ntp-update-registries/
  - **IETF Network Time Protocol v5 – draft-01 – October 2023**
    https://datatracker.ietf.org/doc/draft-ietf-ntp-ntpv5/

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

- **Remote ATtestation ProcedureS (RATS)**
  - **IETF RATS Architecture – RFC 9334 – January 2023**
    https://datatracker.ietf.org/doc/rfc9334/
  - **IETF YANG Data Model for Challenge-Response-based RATS – draft-22 – April 2024 – RFC Editor**
    https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/
  - **IETF EAT Media Types – draft-07 – April 2024 – WG Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-rats-eat-media-type/
  - **IETF Attestation Results for Secure Interactions – draft-06 – March 2024**
    https://datatracker.ietf.org/doc/draft-ietf-rats-ar4si/
  - **IETF Concise Reference Integrity Manifest – draft-04 – March 2024**
    https://datatracker.ietf.org/doc/draft-ietf-rats-corim/
  - **IETF Direct Anonymous Attestation (DAA) for RATS – draft-05 – March 2024**
    https://datatracker.ietf.org/doc/draft-ietf-rats-daa/
  - **IETF Reference Interaction Models for RATS – draft-09 – March 2024**
    https://datatracker.ietf.org/doc/draft-ietf-rats-reference-interaction-models/
  - **IETF CBOR Tag for Unprotected CWT Claims Sets – draft-09 – March 2024 – IETF Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-rats-uccs/
  - **IETF RATS Conceptual Messages Wrapper (CMW) – draft-04 – February 2024**
    https://datatracker.ietf.org/doc/draft-ietf-rats-msg-wrap/
  - **IETF Entity Attestation Token (EAT) – draft-25 – January 2024 – RFC Editor**
    https://datatracker.ietf.org/doc/draft-ietf-rats-eat/
  - **IETF ARM PSA Attestation Token – draft-20 – December 2023**
    https://datatracker.ietf.org/doc/draft-tschofenig-rats-psa-token/
  - **IETF Concise TA Stores (CoTS) – draft-02 – December 2023**
    https://datatracker.ietf.org/doc/draft-ietf-rats-concise-ta-stores/ – WG Adopted
  - **IETF RATS Endorsements – draft-00 – December 2023**
    https://datatracker.ietf.org/doc/draft-ietf-rats-endorsements/– WG Adopted

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

- **IRTF Crypto Forum Research Group (CFRG) – future algorithms**
  - **IRTF Oblivious Pseudorandom Functions (OPRFs) Using Prime-Order Groups – RFC 9497 – December 2024**
    https://datatracker.ietf.org/doc/rfc9497/
  - **IRTF Ristretto255 and Decaf448 Groups – RFC 9496 – December 2024**
    https://datatracker.ietf.org/doc/rfc9496/
  - **IRTF RSA Blind Signatures – RFC 9474– October 2023**
    https://datatracker.ietf.org/doc/rfc9474/
  - **IRTF SPAKE2, a Password-Authenticated Key Exchange – RFC 9382 – September 2023**
    https://datatracker.ietf.org/doc/rfc9382/
  - **IRTF Verifiable Random Functions (VRFs) – RFC 9381 – August 2023**
    https://datatracker.ietf.org/doc/rfc9381/
  - **IRTF Hashing to Elliptic Curves – RFC 9380 – August 2023**
    https://datatracker.ietf.org/doc/rfc9380/
  - **IRTF Additional Parameter sets for HSS/LMS Hash-Based Signatures – draft-13 – April 2024 – Waiting for Shepherd**
    https://datatracker.ietf.org/doc/draft-fluhrer-lms-more-parm-sets/
  - **IRTF Guidelines for Writing Cryptography Specifications – draft-01 – April 2024 – WG Adopted**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-cryptography-specification/
  - **IRTF Usage Limits on AEAD Algorithms – draft-08 – April 2024**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-aead-limits/
  - **IRTF Properties of AEAD algorithms – draft-06 – April 2024**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-aead-properties/
  - **IRTF Key Blinding for Signature Schemes – draft-06 – April 2024**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-signature-key-blinding/
  - **IRTF CPace, a balanced composable PAKE – draft-11 – March 2024**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-cpace/
  - **IRTF OPAQUE Augmented PAKE Protocol – draft-14 – March 2024**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-opaque/
  - **IRTF Hedged ECDSA and EdDSA Signatures – draft-03 – March 2024**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-det-sigs-with-noise/
  - **IRTF KangarooTwelve and TurboSHAKE – draft-13 – February 2024**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-kangarootwelve/

Next Steps – IDS WG

- Next IDS WG Meeting– May 30, 2024
- Next IDS Face-to-Face Meeting likely August 14, 2024 at PWG August 2024 F2F
- 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

Detailed NIAP Transition Plan for CNSA Suite 2.0

- Currently all NIAP PPs must have CNSA 1.0 algorithms
- Will add SHA-512 to all NIAP PPs
- Will require either CNSA 1.0 or CNSA 2.0 be mandatory on all NIAP PPs
- Will implement CNSA asymmetric algorithms for software/firmware signing per following
  - LMS – 1H 2023
  - XMSS – 2H 2023
- Will implement following Key Establishment CNSA 2.0 algorithms in all NIAP PPs when they are standardized and all relevant Assurance Activities have been defined and agreed upon:
  - CRYSTALS - Kyber
  - CRYSTALS – Dilithium (used for Digital Signatures)
- Will deprecate CNSA 1.0 in 2030 – 2033 timeframe
- No current timeline established to make CNSA 2.0 mandatory
  - Will make use of CNSA 2.0 mandatory to be listed on PCL at some point
- Will work with vendors to help try to meet NSA schedule
- Will discuss with CCRA and engage with iTCs how best to integrate CNSA 2.0 into cPPs