The Printer Working Group

Imaging Device Security

November 4, 2021

PWG November 2021 Virtual Face-to-Face

Agenda

When	What
10:00 – 10:10	Introductions, Agenda review
10:10 – 11:10	Discuss results of latest HCD iTC Meetings and HCD cPP/SD v1.0 status
11:10 – 11:55	EUCC / ISO Update
11:55 – 12:00	Wrap Up / Next Steps

Antitrust and Intellectual Property Policies

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

- Refer to the Antitrust and IP statements in the plenary slides

Officers

- Chair:
  - Alan Sukert
- Vice-Chair:
  - TBD
- Secretary:
  - Alan Sukert
- Document Editor:
  - Ira McDonald (High North) – HCD Security Guidelines

HCD international Technical Community (iTC) Status

HCD international Technical Community (iTC)

- Since last IDS F2F on August 19, 2021 HCD iTC meetings have been held on:
  - August 23rd, 30th
  - September 13th, 27th
  - October 4th, 11th, 18th, 25th
  - November 1st

HCD cPP/SD Status

- Released 1st Public Review draft of the HCD cPP (v0.10 dated 8/30/2021) on 8/30/21
  - To date, have received 85 comments against the 1st Public Draft of the HCD cPP
  - 64 of the 85 comments have been adjudicated by the HCD iTC
  - Tally for the comments adjudicated to date:
    - 58 Comments Accepted
    - 0 Comments Accepted in Principle but will be addressed in a later v1.0 draft
    - 4 Comments Deferred to be addressed by the HCD iTC at a later point in time
    - 2 Comment Not Accepted or Rejected

HCD cPP/SD Status

- Released 1st Public Review draft of the HCD SD (v0.91 dated 10/08/2021) on 10/13/21
  - To date, have received 4 comments against the 1st Public Draft of the HCD SD
  - So far none of the 4 comments have been adjudicated by the HCD iTC

HCD cPP/SD Status
Key Closed Issues

- FPT_KYP_EXT.1 Protection of Key and Key Material SFR
  - JBMIA wanted to change SFR, based on the corresponding SFR from the FDE EE cPP, to state requirements for how key and key material are to be protected to meet requirement in the ESR that "*To support encryption, the HCD shall maintain key chains in such a way that keys and key materials are protected*"
  - HCD iTC members and JBMIA agreed on reworking the proposal for wording and clarity
  - Ended up with a new:
    - SFR with completely revised text in line with the FPT_KYP_EXT SFR from the Full Drive Encryption Encryption Engine (FDE EE) cPP and a revise Application Note
    - Revised Assurance Activities that are also in line with the Assurance Activities for the FPT_KYP_EXT SFR in the FDE EE SD

Current HCD cPP/SD Issues

- Resolving all open and deferred comments to prepare and release of 2nd Public Drafts of both the HCD cPP and HCD SD
  - This draft should have "full content" for both documents
- Inclusion of NTP
  - Concern ND cPP requirements for NTP constitute requirement for "secure NTP"
  - Not sure all vendors support "secure NTP"
- Does the Secure Boot SFR FPT_SBT_EXT as currently stated properly address both software and hardware-based Roots of Trust
  - Does the requirement that the Root of Trust is "implemented in immutable memory" cover both software and hardware Roots of Trust?

Other Current HCD cPP/SD Issues

Inclusion of Cryptographic Erase in HCD cPP

- HCD cPP needs to address how user, job and confidential data stored on the device is made irretrievable
- HCDs generally use the "Image Overwrite" mechanism for this since most HCDs have standard nonvolatile drives
- However, for HCDs self-encrypting nonvolatile storage devices or Self-Encrypting Drives (SEDs) "Image Overwrite" mechanism will not work – have to use Cryptographic Erase where the encryption keys are destroyed
- JISEC wants the Image Overwrite discussions in the Security Problem Definition and in the FDP_RIP.1/Overwrite SFR to only include the "Image Overwrite" mechanism
  - JISEC feels Cryptographic Erase is covered by the two Key Destruction SFRs (FCS_CKM.4 & FCS_CKM_EXT.4) already in the HCD cPP
  - Some HCD iTC members disagree and feel Cryptographic Erase is not adequately covered by the two Key Destruction SFRs
  - ITSCC feels Image Overwrite and Cryptographic Erase are two different things and agrees with JISEC; suggested HCD iTC create optional requirements for Cryptographic Erase
- HCD iTC creating a subgroup to address the Cryptographic Erase requirements

Other HCD cPP/SD Issues

Issues HCD iTC still needs to resolve (in order of priority):

- Internationalization of SFRs
- Closure of "deferred" comments
- Update of spec/standard versions – when and if it should be done
  - Need to be concerned about implications of updating versions
- Support for Solid State Devices
- Agreement on removal of support for:
  - TLS 1.1
  - SHA-1 support
  - Cipher suites with RSA Key Generation with keys < 2048 bits
  - All RSA and DHE Key Exchanges

Other Current HCD cPP/SD Issues

Additional New Content (SFRs)

- Goal for HCD cPP/SD at the point is still to "keep it simple" and build on it for later versions
- TLS 1.3 will not be in HCD cPP/SD v1.0
- Anticipate not picking up any additional new requirements for the HCD cPP/SD beyond what already has been proposed at this time unless either:
  - They are requested by JISEC or ITSCC or NIAP
  - They are suggested by JBMIA
  - They are required by changes to ISO, FIPS or NIST Standards/Guidelines
  - Necessitated by comments to 1st (and possibly 2nd) Public Drafts
  - Necessitated by any new NIAP TDs to either the HCD PP or any applicable ND & FDE cPPs/SDs
  - Syncing with applicable updates to ND cPP/SD and FDE cPPs/SDs or applicable NIST SP updates
  - **Advent of EUCC (ENISA Cryptographic Certification)**

HCD iTC Status
HCD cPP/SD Schedule Status Update

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

HCD iTC Status
Updated Proposed HCD cPP/SD Schedule

Phase	Timeframe	Status Updates
Public Review Draft 2	**New Proposed Schedule** • Submit 2nd Public Draft: 12/13 • Review 2nd Public Draft: 12/13 – 1/31/22 (49d) • Review comments and update documents: 2/1/22 – 4/1/22(60d)	Was 10/25 on original schedule Current planned dates: 12/1 12/1 – 1/15/22 1/16/22 – 3/13/22
Final Draft	**New Proposed Schedule** • Submit Final Draft: 4/4/22 • Review Final Public Draft: 4/4/22 – 5/2/22 (28d) • Review comments and update documents: 5/2/22 - 5/12/22 (10d)	Was 1/17/22 on original schedule Current planned dates: 3/14/22 3/14/22 – 4/15/22 4/16/22 – 4/25/22
Final Document Published	**New Proposed Schedule** • Publish Version 1.0: 5/13/22	Was 3/25/22 on original schedule Current planned publish date is 4/25/22

Potential HCD cPP Content Post-Version 1.0

- Inclusion of support for TLS 1.3 and deprecation of TLS 1.1
- Inclusion of NTP if it doesn't make v1.0
- Inclusion of ALC_FLR.* if it doesn't make v1.0
- Incorporate, as applicable, the changes to ISO 15408, particularly any relevant new SFRs in the updated Part 2
- Support for SNMPv3
- Support for Wi-Fi and maybe Bluetooth
- Support for NFC
- Support for Security Information and Event Monitoring (SIEM) and related systems
- Expand to address 3D printing
- Support for new crypto algorithms
- Updates due to changes from ISO, FIPS or NIST Standards/Guidelines, NIAP TDs, or CCDB Crypto WG
- Indirect updates based on new technologies or customer requests

HCD iTC Status
Key Next Steps

- Address all the comments against the 1st Public Drafts
- Finalize all new content for v1.0
- Determine "parking lot" issues for later versions of the HCD cPP/SD (e.g., TLS 1.3 support)
- Add all agreed-upon SFRs and Assurance Activities into the HCD cPP and SD
  - Goal is to complete this by the 2nd Public Draft
- Submit 2nd Public Draft and Final Draft HCD cPP and HCD SD per the updated schedule
- Review and resolve all comments and update the HCD cPP and HCD SD drafts per the agreed schedule
- Publish HCD cPP/SD v1.0 per the agreed schedule
- After Jan 1, start thinking about creating an Interpretation Team for maintaining HCD cPP/SD v1.0 and start planning for next HCD cPP/SD update (whether it is v1.x or v2.0)

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

- Even after the third attempt at creating a PP for the same class of products, it still amazes me how bad we are at estimating how long it takes to develop a PP
- Along the same lines, it's always the topics that you think will be the easy ones to resolve that most often turn out to be the biggest stumbling blocks, so never assume any comment or topic will be an "easy" one to resolve
- Minutes of meetings are crucial when developing something like a cPP or SD, because you often need to know what was decided or discussed at a previous meeting
- All iTC documentation including minutes should be available on-line to everyone
- iTCs have to be flexible because sometimes unexpected requirements come from both the expected sources and sometimes surprise sources
- Use of a good document management/version control tool from the start is essential

ENISA
CYBERSECURITY CERTIFICATION (EUCC)

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

ENISA (The European Union Agency for Cybersecurity)

- Established in 2004 by the EU Cybersecurity Act
- Mission is to achieve a high common level of cybersecurity across the European Union in cooperation with the wider community
- Key Goals:
  - Contribute to EU cyber policy
  - Enhance the trustworthiness of ICT products, services and processes with cybersecurity certification schemes - EUCC
  - Cooperate with Member States and EU bodies
  - Help Europe prepare for the cyber challenges of tomorrow

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

Candidate Version: v1.1.1 dated May 2021

EUCC GOALS

- Serve as a candidate EU cybersecurity certification scheme
- Successor to existing schemes operating under the SOG-IS MRA (Senior Officials Group Information Systems Security Mutual Recognition Agreement)
- Base it on the Common Methodology for Information Technology Security Evaluation, and corresponding standards, respectively, ISO/IEC 15408 and ISO/IEC 18045
- Cover the certification of any type of Information and Communications Technology (ICT) Product, Service or Process

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

Key Terminology

- ICT product: an element or a group of elements of a network or information system
- ICT service: a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems
- ICT process: a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service
- CAB: Conformity Assessment Body – Plays a role similar to the CCDB and CCMC
- CB: Certification Body - National Authority in charge of the activities of certification
- ITSEF: Third-party conformity assessment body or national authority, or the subcontractor of a CAB or national authority, that is in charge of the activities of evaluation (i.e., the Testing Lab)

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

SCOPE

- Cybersecurity Certification of ICT products according to ISO/IEC 15408 and the Common Criteria (CC)
- Covers any type of ICT product addressing the European Union Internal Market, with the conditions that the ICT product:
  - Embeds a meaningful set of security functional requirements as described by the CC Part 2
  - Aims at reaching the assurance levels 'substantial' or 'high' of the CSA covered by this scheme
- Covers the assessment of vulnerabilities of cryptographic implementations into the security functionalities of an ICT product in accordance with the requirements of the evaluation criteria and methodology defined in the CC

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

Key Security Objectives the EUCC is to achieve:

- Protect stored, transmitted or otherwise processed data against accidental or unauthorized storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process
- Protect stored, transmitted or otherwise processed data against accidental or unauthorized destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process
- Authorized persons, programs or machines are able only to access the data, services or functions to which their access rights refer
- Identify and document known dependencies and vulnerabilities
- Record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom

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

Key Security Objectives the EUCC is to achieve (cont'd):

- Make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom
- Verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities
- Restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident
- ICT products, ICT services and ICT processes are secure by default and by design
- ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates

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

SFR and SAR Requirements

- SFR and SAR Classes are mapped to EUCC Security Objectives
- Allows the use of Extended Components
- User of certified products or applicant to certification:
  - Decides which security objectives to evaluate the ICT product(s)
  - Selects applicable requirements, either in a Protection Profile or a Security Target of the individual ICT product
- By default, any evaluation shall be based on the use of the SAR Class AVA: Vulnerability assessment and the SAR Family ALC_FLR: Flaw remediation

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

Assurance Activities

- Requires use of the 7 Evaluation Assurance Levels from Common Criteria Part 3 of ISO/IEC 15408
- Requires that European cybersecurity certificate that refer to assurance level 'substantial' shall provide assurance that:
  - ICT products, services and processes meet corresponding security requirements, including security functionalities
  - Have been evaluated at a level intended to minimize known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources
  - Evaluation activities to be undertaken include:
    - At least a review to demonstrate the absence of publicly known vulnerabilities
    - Testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities

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

Assurance Activities

- Requires that European cybersecurity certificate that refer to assurance level 'high' shall provide assurance that:
  - ICT products, services and processes for which that certificate is issued meet the corresponding security requirements, including security functionalities
  - Have been evaluated at a level intended to minimize the risk of state-of- the-art cyberattacks carried out by actors with significant skills and resources
  - Evaluation activities to be undertaken shall include at least the following:
    - Review to demonstrate the absence of publicly known vulnerabilities
    - Testing to demonstrate that the ICT products, services or processes correctly implement the necessary security functionalities at the state of the art
    - Assessment of their resistance to skilled attackers, using penetration testing

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

Some Key Additional Requirements

- Handling of Vulnerabilities
  - Manufacturer or provider reports within a business day to the CB that issued the certificate the possibility of a related vulnerability and provides within five business days a date for when a vulnerability analysis will be established
  - The CB agrees on the proposed date, which is not to exceed 90 days
  - If a vulnerability is found in a certified ICT product and is confirmed to apply to ICT product:
    - If it cannot be circumvented the certificate is withdrawn
    - If it can be patched, the certificate is suspended until the patch is implemented per the Patch Management process defined in the EUCC

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

Some Key Additional Requirements

- Non-Compliance Processing
  - Holder of a certificate has to inform the CB of any subsequently detected vulnerabilities or irregularities concerning the security of the certified ICT product that may have an impact on its compliance with the requirements related to the certification
  - For confirmed deviations or irregularities associated to a non-compliance:
    - Manufacturer or provider has to provide assertions and amendments within the time frame of 14 days/30 days for certificates at the assurance level ‘high’/‘substantial’, to restore compliance
    - Continued infringements of such obligations triggers certificate suspension of the certificate
    - When the handling is refused, or the suspension reaches a 90 day period the certificate is withdrawn

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

Certificate Maintenance/Assurance Continuity

- **Certificate Maintenance**: Process undertaken by a developer to have a TOE listed in the maintenance addendum for that TOE.
  - Must demonstrate that the changes to the TOE, the IT environment and/or the development environment do not adversely affect the assurance baseline
- **Re-evaluation**: Evaluation of a changed TOE, such that the developer could not (or chooses not to) demonstrate that changes to the certified TOE do not adversely affect the assurance baseline
- **Re-assessment**: Evaluation of a previously certified TOE against a changed threat environment

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

Certificate Maintenance Process

- Can be initiated by either the manufacturer or provider of the ICT product or any other party (e.g., a CB)
- Based on the Impact Analysis report (IAR) or maintenance rationale, the CB validates whether some evaluation tasks are deemed necessary before its review and decision, and validates accordingly
- The CB validates the result of the necessary evaluation tasks once completed by the ITSEF
- Based on CB review, the results of the continuous maintenance process can be:
  - Continuing the certificate without change
  - Renewing the certificate with a new validity period
  - Issuing a certificate with either an extended scope, a reduced assurance level, or a reduced scope of the certificate to still meet the current assurance level, potentially with a new validity period
  - Suspending the certificate pending remedial action by the manufacturer or provider of the ICT product
  - Withdrawing the certificate

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

Assurance Continuity Process

- Developer ensures following inputs are available to the CB:
  - Certificate for the TOE (including existing maintenance addendum)
  - Certification Report
  - Evaluation Technical Report
  - Security Target for the certified TOE
  - Impact Analysis Report (IAR)
- CB reviews IAR and other relevant inputs to determine what impact the changes described in the IAR have on the assurance baseline
  - Key focus of this review is to determine whether the changes (to the TOE, the ICT environment and/or the development environment) can be considered major or minor, based on their apparent impact on the assurance baseline
- If changes are considered minor, a certificate maintenance addendum is added to the certificate and posted
- If the changes are considered major, a Re-Evaluation has to be done

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

Re-Evaluation

- Performed when a change to a certified TOE has been determined to be of major impact
- Reuses any results from that earlier evaluation that still apply
- If an IAR has been provided, is used as the basis for identifying those parts of the changed TOE remaining unchanged from the previously-evaluated TOE.
- New ETR is derived from the ETR of the original TOE
- At the completion of the evaluation of the changed TOE, a new ETR is produced, along with a certification report that constitutes the maintenance report, and certificate for the changed TOE.
- Changed TOE becomes the updated basis for any future changes that might be made

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

Re-Assessment

- When the threat environment has changed since the initial certification of a TOE, the certificate holder may want the TOE's to be re-assessed
- Re-assessment is performed by the same evaluator who performed the initial evaluation, reusing all results from that earlier evaluation that still apply
- Only tasks pertaining to the AVA_VAN (Vulnerability Assessment) family are reopened, as well as, when relevant, those of the ALC (Fault Remediation) class for which sufficient evidence that they are still fulfilled cannot be provided
- When updating the vulnerability analysis of the product, the evaluation lab may consider the following:
  - List of potential vulnerabilities established during the initial evaluation
  - New potential vulnerabilities which were not addressed during the initial certification, and associated attack methods
- No change to the security problem can be made and only new or evolved attack techniques are covered
- At the completion of the re-assessment of the TOE, a new ETR is produced, along with a re-assessment report for the reassessed TOE

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

Some Unique Aspects of the EUCC

- Requires annual Monitoring of Compliance to detect non-compliances in certified ICT products/services/processes
  - Uses a minimum of 5% of the products and at least one product per annum which received certificates in the previous year
  - If non-compliances are found, can result in a certificate being withdrawn depending on its assurance level
- Includes a defined Patch Management Process
  - 4 Patch Levels:
    - Patch Level 1: where the TOE is part of a bigger ICT product, and product parts not affecting the TOE may be patched whenever required
    - Patch Level 2: for minor changes
    - Patch Level 3: application of Assurance Continuity for a major change
    - Critical Process Flow: for changes where an attack is already possible to be exploited or update is critical and needs to be released urgently

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

Patch Management – Applicable Actions for Each Level

Actions/Patch Levels	Action 1	Action 2	Action 3	Comment
Patch Level 1	Changes to the product under Patch Level 1 shall be made the decision of the Manufacturer (No time limit set)	The Manufacturer shall inform the CAB within five business days of any such applied changes	The CAB may decide to apply the maintenance or other relevant CB decision	
Patch Level 2	Manufacturer develops and tests the corrective patch according to the applied accepted approach	ITSEF shall proceed to an evaluation before the product can be patched, This is documented by the ITSEF. A time limit for the evaluation may be agreed between the stakeholders of the process	If the evaluation result allows it, the Manufacturer can patch the product	Based on the provided documentation the CB shall decide where applicable to update the version of the certificate, or make a decision based on the certification process
Patch Level 3	Assurance Continuity for a major change			
Critical Update Flow	Manufacturer/Provider develops corrective patch (No time limit set)	ITSEF and the CB shall be informed of the changes within 5 business days, and shall perform the necessary evaluation and certification activities.	ITSEF shall evaluate the already deployed patch with the highest priority, to evaluate the changes and create the relevant documentation in previously agreed time.	Based on the provided documentation the CB shall decide where applicable to update the version on the certificate

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

Assorted Other Requirements

- Each manufacturer or provider of ICT products maintains a publication system for the information to be made available to the public
- Each CB that issues a certificate must be peer reviewed at least once every 5 years
- All information is to be available for a period of at least five (5) years after the expiration date of the certificate
- The maximum period of validity of the certificates is five (5) years
- The certificates are to be disclosed by ENISA, with the related certification report and any relevant information as requested by other chapters of this document, in a dedicated website on European cybersecurity certification schemes
  - The certificates shall be disclosed with their applicable status

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

CURRENT STATUS

- A text describing the proposed EUCC scheme has been published by ENISA (v1.1.1)
- EU commission will transpose proposal into a legal act
- Adoption of legal act will establish the EUCC scheme
- Entry into force expected 1st Half 2022, with a transition period from existing national schemes
- Currently work is done by ENISA on guidance documents
  - Accreditation guidance for CABs accrediting CBs and ITSEFs (ISO 17065+17025)
  - Manufacturer commitments: application form, etc.
  - Security of information

ISO 15408 / ISO 18045 UPDATE

ISO 15408 / ISO 18045 Update Current Standards (3rd Edition)

- A framework (ISO/IEC 15408 Part 1) that explains how to generate specifications that can be evaluated by Labs under scheme policies
  - Protection Profiles (PP) (product-type specification of requirements)
  - Security Targets (ST) (product-level specification of requirements)
- Catalogues of security requirements
  - Functional security requirements (Part 2)
  - Assurance security requirements (Part 3)
- How to evaluate a Security Target or PP
  - Core methodology for evaluation (ISO/IEC 18045)
  - Specifying methodologies for specific product-type evaluations

ISO 15408 / ISO 18045 Update
Proposed Updated Standards (4th Edition)

Input from stakeholders for the 21st Century

- Security evaluation approaches allowing both:
  - Specification-based : Exact Conformance added
  - Attack-based : “Traditional EAL approach”
- Addition of modularity and composition techniques to the model
- Enhanced specification for packages
- Updated Security Policy definition
- Updated to include state-of-the art for the highest levels of evaluation (EAL 6 and EAL 7)

ISO 15408 / ISO 18045 Update
Specification-Based vs. Attacked-Based

Specification-Based Approach	Attack-Based Approach
Keywords: exact conformance, direct rationale PPs, TOE and SFR-specific evaluation methods	Keywords: strict/demonstrable conformance. EALs, TOE type-specific evaluation methods
All evaluated TOEs are compliant to a given list of functional and assurance requirements: nothing more and nothing less	All evaluated TOEs are protected against a given set of threats Allows for additions to assurance activities beyond what is in EALs
All tests are set and known beforehand	The attacker strength is set and known beforehand; the tests themselves may be fine-tunes (penetration testing)

ISO 15408 / ISO 18045 Update
Proposed Updated Standards (4th Edition)

- The general model has been significantly revised (Part 1)
- New & changed security functional requirements (Part 2)
- Updated security assurance requirements (Part 3)
- Adds support in developing evaluation methodologies for specific technologies/product types (New part 4)
- All pre-defined packages of assurance packages moved to a (new) part 5
  - For example this is where the evaluation assurance level (EALs) are now found
  - (To facilitate use by scheme/MRA policies)
- Updated the common evaluation methodology (ISO/IEC 18045 aka “CEM”)

ISO 15408 / ISO 18045 Update Progress With The 4th Edition

- Draft International Standard (DIS) ballots completed
- 27 nations approved. 5 nations had mostly editorial comments
- The Final Draft International Standard (FDIS) stage where nations indicate their Final Approval before publishing was initiated and approved by SC 27.
- The standards are expected be published before the end of 2021(?)
  - Key issue holding up publishing is ISO wants to copyright both ISO standards

Next Steps – IDS WG

- Next IDS WG Meeting– Nov 11, 2021
- Next IDS Face-to-Face Meeting February 8-10, 2022 (probably February 10th) at next PWG Virtual F2F
- Start looking at involvement in some of these other standards activities individually and maybe as a WG