IDS WG Meeting Minutes
November 30, 2023

This IDS WG Meeting was started at approximately 3:00 pm ET on November 30, 2023.

Attendees

Graydon Dodson	Lexmark
Smith Kennedy	HP
Jeremy Leber	Lexmark
Alan Sukert	
Bill Wagner	TIC

Agenda Items

1. The topics to be covered during this meeting were:
   - Latest updates on the HCD iTC
   - Special Topic on the EUCC Implementing Regulation
2. Meeting began by stating the PWG Anti-Trust Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-antitrust-policy.pdf and the PWG Intellectual Property Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-ip-policy.pdf.
3. Al began by discussing the results of the November 27th HCD international Technical Committee (iTC) Meeting:
   - Kwangwoo LeAe, HCD iTC Chair, plans to update the Key Persons document, so he asked everyone to let him know of any changes.
   - Some upcoming events:
     - The next CCUF Workshop will be in Apr/May 2024
     - ICCC 2024 will be in Qatar
     - ICCC 2025 will be in Korea
   - The HCD cPP/SD v1.0 Errata (v1.0e) is planned to contain only the fixes for the issues/comments submitted by NIAP, the Canadian Scheme and the CC Management Board (CCMB). It was determined that the comments submitted by the Japanese lab were also relate to an ongoing certification against HCD cPP?SD v1.0, so the fixes for those comments will also be included in the Errata. The NIAP representative at the meeting indicated that as of now NIAP has no additional comments from its HCD cPP v1,0 evaluation.
     - The key is that the iTC has to align the fixes for all the above comments
   - Next we went through the various HCD iTC Subgroup reports:
     - For the HIT report Al indicated that the HIT is working on refining the HIT process to documenting the Technical Decisions for these fixes, generating the files containing the fixes and then merging the fixes into a single HCD cPP and single HCD SD documents.
     - For the CC:2022 Subgroup report Al indicated that the next step is to develop a roadmap of what the HCD iTC needs to do to comply with CC:2022 and a timeline of when the HCD iTC can achieve that compliance
   - The next HCD iTC Meeting will be 12/18; the next HIT Meetings will be 12/1 and 12/8
4. Al then presented his special topic for the day, which is a closer look at the EUCC Implementing Regulation (IR) that Al discussed at the IDS Session of the November 2023 PWG. Virtual Face-to-Face Meeting. Since Al did not have time to prepare slides, he went through a PDF version of the EUCC IR for the meeting. The final draft version of the EUCC IR that was review at the meeting can be downloaded from the following EU web site: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13382-Cybersecurity-security-requirements-for-ICT-product-certification_en.

Al did not go through every Article in the EUCC IR, but picked out key ones that created comments and issues from both the CCUF and members of the CC Development Board when the IR came2 out in late October 2023 during the time of ICCC 2023. The key points from the review of the EUCC IR were:

- Concerning the Scope of EUCC (Article 1), it is the same as before – it "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 those ICT products".
- Article 3 states that evaluations conducted under EUCC will follow the CC and the Common Evaluation Methodology. That will be important given what is stated in later articles.
- Article 4 talks about "Substantial" and "High" Assurance Levels and relates then to AVA_VAN levels – "Substantial" Assurance Level is AVA_VAN Levels 1 & 2, and "High" Assurance Level is AVA_VAN Levels 3, 4 & 5. Al indicated the the AVA_VAN levels mentioned in Article 4 were pointing to AVA_VAN (Vulnerability Analysis) Security Assurance Requirements (SARs) AVA_VAN.1 – AVA_VAN.6 (see Section 17.1 in CC3.1v5 Part 3 or Section 14.3 in CC:2022 Part 3)
- In Article 5, Al pointed out the requirement that "Protection profiles shall be certified for the sole purpose of the certification of ICT products falling into the specific category of ICT products covered by the protection profile". That is slightly different than in the CC case, where PP/cPPs are certified by a Scheme as part of the first certification of a new PP/cPP.
- Article 7 lists the evaluation criteria for product certification. One of them is "the applicable state-of-the-art documents listed in Annex I (2)". When we looked at the list in Annex 1, we found that most of the documents listed were older documents – many at least 10 years old or older. We wondered why the IR didn't reference newer documents.
- Chapter III discusses certification of PPs. Most of it repeats the requirements for issuing, renewing or withdrawing certificates that were stated in earlier articles for general certifications. What is interesting are the evaluation requirements for PPs:
    - the applicable elements of the standards referred to in Article 3
    - the security assurance requirements classes for vulnerability assessment, independent functional testing and flaw remediation, as set out in the evaluation 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 Regulation (EU) 2019/881
    - the relevant evaluation methodologies, listed as state-of-the-art documents in Annex I. Note: There are no evaluation methodologies listed in Annex 1)

  They are different and much less detailed than the evaluation requirements for PP certification listed in Part 1 of either CC3.1R5 or Part 1 of CC:2022.
- Chapter VI was about Vulnerability Management. Al noted that vulnerability assessment and vulnerability management is very important to the EU. Thus, you have requirements like "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" in Article 33 and "Within 90 days after having become aware of a possible vulnerability relating to its certified ICT product, the holder of an EUCC certificate shall carry out a vulnerability analysis with reference to the target of evaluation and the assurance statements contained in the certificate" in Article 34 or the detailed requirements for vulnerability remediation in Article 36.
- Chapter VIII, Mutual recognition agreements with third countries – this is the chapter that caused most of the comments and consternation, especially by the CCDB.

Condition 1 states “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”. At the meeting we spent much time debating what this condition actual meant, and agreed that what is was saying was that once this IR gets implemented each CCRA nation will have to make a separate mutual recognition agreement with the EU that will (we think) apply to all EU member nations. Note: This would be similar to the CCRA in that respect).

The problem is that the CCMC does not want separate mutual recognition agreements with each CCRA member; they want one mutual recognition agreement that covers all CCRA members.

- Another issue that was brought up at the IDS Session of the November 2023 PWG was in Item 33 in the preamble to the IR - This Regulation shall apply **12 months** after its entry into force. Many Schemes, especially NIAP, have complained that 12 months is way too short a time for a transition to EUCC.
- Finally, the issue that blinded eve EU Nation Members in the CCDB and created the most comments. Item 32 in the preamble to the IR states that “In a number of Member States Common Criteria certificates are issued under national schemes using mutual recognition rules established in SOG-IS MRA and CCRA. This Regulation should provide an indicative list of existing national schemes which will cease to produce effects. **Member States should end their participation in the CCRA in the areas covered by this Regulation**.” Not even the EU Member State reps want this – they want to continue partnership with the CCRA.

5. To follow up the EUCC IR discussion AL went briefly through the list of comments to the EUCC IR developed by the CC Users Forum at their Fall 2023 CCUF Workshop. The list can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/EUCC comments.pdf.

   A sample of some of the comments are:

   - Article #2 “state-of-the-art”:
     - What specifically is meant by “Start of the Art”? The way this term is used does not make much sense as many of the documents that are considered state of the art of around 10 years old, which is old in tech (and security).
     - Can a better term, or an updated description replace this term?
   - Article 4: Multi-level Assurance Product:
     - CC:2022 (or the equivalent ISO), provides for multi-assurance evaluations where sub-components are evaluated at higher assurance than the product as a whole. How would the whole product be evaluated: at the Highest Assurance or individual components of the resulting TOE?
     - Would this be considered High or Substantial?
   - Article 4: General:
     - How are protection profiles (PPs) certified with respect to Substantial? Is it required to have a certified PP?
   - Article #9 1e combined with Article #8 2:
     - These imply that source code must be shared by Vendor with CB. While some level of sharing with the ITSEF is “common”, sharing with the CB is likely to be very limited.
     - When is source code “Necessary”?
     - Is this required for Substantial or only for High?
   - Article 17
     - A mechanism needs to be defined certifying EUCC approved PPs
     - Today most PPs are certified on first use, though others may be certified independently. What are the allowed methods for this?

- Article #18:
  - Clarification on the validity period for PPs. These statements seem somewhat contradictory to each other. Lifetimes are normally explicit time periods, not “lifetime” which is undefined
- Article 45:
  - What is the transition plan for Mutual Recognition between SOG-IS, CCRA, ISO, etc. preventing members from having to pull out of their existing organization?
  - What is the plan to ensure that vendors currently utilizing mutual recognition agreements that become void with EUCC that they will not need to perform multiple, separate evaluations in different countries (or regions) to have evaluated products accepted?

6. **Actions:** None

Next Steps

The next IDS WG Meeting will December 14, 2023 at 3:00P ET / 12:00N PT. Main topics will be HIT Status and a special topic TBD.