

IDS WG Meeting Minutes

January 20, 2022

This IDS WG Meeting was started at approximately 3:00 pm ET on January 20, 2022.

Attendees

Graydon Dodson	Lexmark
Erin Huber	Xerox
Smith Kennedy	HP
Ira McDonald	High North
Alan Sukert	
Bill Wagner	TIC

Agenda Items

1. The topics to be covered during this meeting were:
 - Review of the discussions at the Hardcopy Device international Technical Community (HCD iTC) Meetings since the last IDS Workgroup Meeting on 12/16/21.
 - Latest status on the HCD Security Guidelines
 - Thoughts on IDS Workgroup looking forward
 - Round Table
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. AI began with a summary of what was covered at the HCD iTC Meetings since the last IDS Workgroup meeting on 12/16/21.
 - For the most part the main items covered at these meetings was addressing comments against the 1st Public Draft of the HCD collaborative Supporting Document (SD) since the 2nd Public Draft of the HCD cPP – Version 0.11 dated 12/14/21 – was released for public review on 12/15/21 and the review period for this 2nd Public Draft of the HCD cPP will last until January 31, 2022. The HCD iTC is trying to get the 2nd Public Draft of the HCD SD released for review
 - The main comment holding up the release of the 2nd Public Draft of the HCD SD is a set of comments from ITSCC (the Korean Scheme) dealing with requested additions to the Assurance Activities for several of the cryptographic SFRs. This set of comments was first submitted in Mar 2021 but “fell thru the cracks” and is now finally being reviewed by the full iTC.

ITSCC’s comments involved two main issues – requesting additional detail be added to the TSS and guidance documentation (AGD) for the selected SFRs and adding additional testing (in many cases extensive additional testing) to sync up with the testing recommended by the CCUF Crypto Working Group. When the HCD iTC did its initial review of the ITSCC comments it has two main concerns:

 1. The comments on TSS and AGD are too detailed and are appropriate to relatively high assurance evaluation and not for the level of assurance (EAL1) that a PP-compliant cPP like the HCD cPP would be evaluated against.
 2. There were references to non-existent or incorrect SFRs in the ITSCC comments.

ITSCC submitted a revised version of its comments that corrected the SFR naming issues. The revised version also shortened or removed the TSS and AGD requirements because ITSCC felt the testing comments were much more important.

IDS WG Meeting Minutes January 20, 2022

We went through the proposed ITSCC tests for each SFR at the meeting and the general consensus was that in most cases the requested testing was extensive and would be difficult to do. Ira brought up the point that it was a lot to ask at this point in the timeline of the documents, but Al said that since the iTC was partly to blame for not addressing the comments in Mar 2021 when they were first submitted, we may have to live with them.

Al indicated that the HCD iTC will be reviewing the updated proposal at the next iTC meeting on 1/24/22.

- Al then reviewed a comment that the HCD iTC's Hardware-anchored Integrity Verification Subgroup reviewed concerning Roots of Trust (RoTs) implemented in mutable code. The current requirement in the Secure Boot SFR states that "The TSF shall contain one or more chains of trust with each chain of trust anchored in a Root of Trust that is implemented in immutable code". A comment against the 1st Public Draft of the HCD cPP was made that the HCD cPP needed to consider RoTs that are implemented in mutable code also because some vendors might implement such RoTs.

The Subgroup did a quick polling of members and found that the vendors represented all implemented their RoTs in immutable code. The subgroup looked at a couple of options – leave the requirement as is (i.e., do nothing); try to address the case of RoTs implemented in both mutable and immutable code in the Final Draft of the HCD cPP or essentially "punt" this comment into a Parking Lot to be looked at for implementation in a later version of the HCD cPP after Version 1.0.

After looking at what would have to be done to try to revise the Secure Boot SFR to address RoTs implemented in both mutable and immutable code, the Subgroup agreed that the changes would be too large to be made at this point in the process since we are going into a Final Draft. However, since there might be some validity to the comment the Subgroup agreed to the third option – defer the comment and put it in the Parking Lot to be implemented post-Version 1.0.

- Al then reviewed the latest status of the "Cryptographic Erase" issue that had been discussed at the 10/28/21 IDS Workgroup meeting (see the minutes from the 12/16/21 IDS WG Meeting for the background of this issue).

The Cryptographic Erase Subgroup put together the final version of the FPT_WIPE_EXT SFR and corresponding Assurance Activities that is to be proposed to the full HCD iTC and sent it to the Japanese and Korean Schemes for their buy-in. So far, neither Scheme has indicated any issues with the new SFR/Assurance Activities that will replace FDP_RIP.1/PURGE. The plan is to present the new SFR to the HCD iTC as soon as possible. However, before that will occur the final version is undergoing one last review by the Subgroup which is to be completed via email by Friday 1/21/22.

- Finally, Al did a quick review of the HCD iTC schedule. The HCD cPP is essential on schedule but the likelihood is that the 2nd Public Draft of the HCD SD will go out the end of January so it will be about 6 weeks behind the HCD cPP. Based on that, Al's best guess is that the HCD cPP and HCD SD will likely get published some time in June 2022.

Given that the HCD iTC was formed in Feb 2020, that would put the publishing on Version 1.0 some 28 months after the iTC was formed. Considering the 2600 PPs took 5+ years to be developed and the HCD PP 3+ (almost 4) years to be developed, getting the HCD cPP/SD in 28 months would not be bad at all.

4. Ira then gave a quick status of the HCD Security Guidelines. He is working on a "working draft" but does not have a date when it will be ready for review. Ira did have a couple of important items regarding TLS that he thought would be of interest:
 - A "best practices" document for TLS 1.3 is being sent to IETF for final processing
 - Use of OCSP is being "discouraged" but not deprecated because browsers and servers are not using it. Al indicated that could have negative implications to the HCD cPP because the X.509 Certificate Verification SFR requires the use of either OCSP or CRL and a lot of vendors are

IDS WG Meeting Minutes January 20, 2022

choosing OCSP; if OCSP gets deprecated that could really cause havoc. Ira said he will be watching this issue closely.

5. AI wanted to end the meeting looking forward to what IDS should be doing in the future besides developing the HCD Security Guidelines and following the progress of the HCD cPP/SD. In soliciting the members present, some of the suggestions put forward were:
 - Provide follow-up to the special topics from 2021 such as EUCC and the Cybersecurity Executive Order.
 - Look into the evolution of security as it effects printing. This could lead to areas including 3D printing and even production printing and the whole area of cybersecurity beyond just what NIST and EUCC are doing.
 - Ira suggested that we become involved in IETF Working Groups of interest, especially ones related to print protocols and things like syslog and SIEM that interface with HCDs.
 - AI mentioned that he'd like to see the IDS WG more closely tied to IPP WG so they don't become just "stovepipes" but rather integrated pieces under the PWG umbrella
 - Ira suggested that IDS go back to what it was originally – a developer of applicable specs related to device security in addition to the current standard support role. There may be some specs that may apply in the new environment.
 - AI repeated that there was a need for a Vice-Chair for the IDS WG so AI had a back-up.
6. **Actions:** None

Next Steps

- The next IDS WG Meeting will be February 3, 2022 at 3:00P ET / 12:00N PT. Main topics will be review of the 1/24/22 and 1/31/22 HCD iTC Meetings and preparation for the February PWG IDS Face-to-Face Meeting on February 9, 2022.
- February PWG IDS Face-to-Face Meeting will be on February 9, 2022 at 10:00 AM ET.