IDS WG Meeting Minutes
June 16, 2022

This IDS WG Meeting was started at approximately 3:00 pm ET on June 16, 2022.

Attendees

Smith Kennedy	HP
Alan Sukert	
Mike Trent	Xerox
Bill Wagner	TIC
Steve Young	Canon

Agenda Items

1. The topics to be covered during this meeting were:
   - Review of the HCD iTC Meetings since our last IDS WG Meeting on 5/26/22
   - Presentation by Smith Kennedy on IPP Authentication
   - 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. Smith Kennedy began the meeting with a summary of Best Practice 5199.10-2019, IPP Authentication Methods (IPPAUTH) which can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/IPP%20Authentication%20Methods%20Overview%20220220616.pdf. Smith's slides can be found at https://ftp.pwg.org/pub/pwg/informational/bp-ippauth10-20190816-5199.10.pdf.

   Smith outlined the seven HTTP client authentication methods that are used with IPP:

   - 'none' - iindicates that the receiving Printer provides no method to accept an asserted identity for the User operating the Client
   - 'requesting-user-name' - indicates that the Client will provide the "requesting-user-name" operation attribute in its IPP operation request (essentially same as 'none'
   - Basic - uses the HTTP Basic authentication scheme [RFC7617]
   - Digest - uses the HTTP Digest authentication scheme [RFC7616]
   - Negotiate - uses the HTTP Negotiate authentication scheme [RFC4559], which is used to support Kerberos and NTLM authentication methods with HTTP. Smith indicated this is not used very often; Al commented that for HCDs Kerberos is the widely used protocol for network user authentication.
   - OAUTH - pertains to OAuth 2.0, which uses:
     - The OAuth 2.0 authentication scheme [RFC6749], which defines the OAuth 2.0 system, authentication protocol framework, and OAuth 2.0 access tokens, which represents the scope, duration, and other attributes of an authorization grant;
     - The OAuth 2.0 Bearer Token [RFC6750] which specifies the ways that an OAuth 2.0 access token can be encoded into general purpose HTTP requests and responses as an HTTP Bearer Token;
     - The OAuth 2.0 Authentication Server Metadata [RFC8414] which provides the necessary metadata for interoperability;

- The OAuth 2.0 Dynamic Client Registration Protocol [RFC7591] which allows an IPP Client to register its local redirection URI with the Authorization Server; and
- OAuth 2.0 Token Introspection [RFC7662] which allows an IPP Printer to query information about a Bearer token provided by the IPP Client, including the list of granted scopes.

- Certificate (TLS Client certification) - uses X.509 certificate authentication via TLS [RFC8446]

Smith then provided some more detail about OAUTH. It was developed with the help of Microsoft. However, Google Chromium OS has developed an updated method for doing OAUTH authentication for IPP that differs from what is in 5199.10. The IPP WG is having a meeting with Google on July 7th to discuss these updated and see if they can resolve the misalignment between the two OAUTH authentication methods.

Smith then gave a brief run-through of the actual 5199.10 Best Practice document, highlighting the discussions of the seven authentication methods in the document. Smith stated that 5199.10 is an important document because there are 3rd Party and OpenSource implementations of IPP being used now. Mike Trent also mentioned that OAUTH will be used in the future for SMTP authentication.

4. Al then provided a summary of what was covered at the HCD iTC Meetings since the last IDS Workgroup meeting on 5/26/22.

- The time spent at the HCD iTC meetings since the last IDS WG Meeting was spent continuing work on finalizing the new FPT_WIPE_EXT SFR and its associated Assurance Activities (AAs). The main issue that was discussed the past two meetings was a request from the Japanese Scheme JISEC to make the FPT_WIPE_EXT SFR a mandatory SFR instead of an optional SFR which it currently is. JBMIA, the Japanese vendor association, asked to discuss this issue and the 6/13 HCD iTC meeting came back with the following concerns about making FPT_WIPE_EXT mandatory:

  - In the future MFPs, the vendor will be required to change the design spec in order to obtain CC certification if FPT_WIPE_EXT.1 would be mandatory. Specifically, JBMIA is concerned that the Security Objective O.PURGE_DATA requires that all customer-supplied User Data and TSF Data to be made permanently irretrievable, but the FDP_DSK_EXT SFR requires encryption of only User Document and TSF Confidential Data. As a result, JBMIA feels Cryptographic Erase (CE) by virtue of how it works will not make all customer-supplied User Data and TSF Data permanently irretrievable; this will require some other possibly new method to make this data permanently irretrievable and thus require redesign.

    Bill Wagner then brought up that the 6/13 meeting at this point seemed to veer off to a discussion around what appeared to be JBMIA's real concern – they were developing some new method for making data permanently irretrievable on a nonvolatile storage media and they were concerned they wouldn't be able to add that new method to the selection in the FPT_WIPE_EXT SFR via the current processes. JBMIA mentioned possibly using the Integration Team to do that once Version 1.0 is published.

  - The second JBMIA concern was that it seems inappropriate that CE is a mandatory requirement in FPT_WIPE_EXT.1. From the discussion at the 6/13 HCD iTC meeting it was clear that most of the attendees shared the same concern. Al indicated that the reason CE was moved out of the selection and was made mandatory in the SFR was that the iTC misunderstood JISEC's concern about what it wanted to be mandatory – the iTC thought it wanted CE to be mandatory but as it turned out JISEC wanted the entire SFR to be mandatory. Bill also mentioned that we made CE mandatory because we thought it might be a solution JISEC would accept.

  - In response to the two concerns JBMIA offered the following recommendations:

    - For the first concern, JBMIA would prefer to leave WIPE optional as it is. After some discussion it was clear that the HCD iTC did not have a consensus on this particular

issue. The HCD iTC decided that we needed someone from JISEC to give the iTC the rationale for why they wanted the WIPE SFR to be mandatory before it could make a final decision. JBMIA said that it would contact JISEC but that it would take two weeks before a JISEC rep could provide a response to the HCD iTC.

- Regarding the second issue, JBMI had two recommendations – either (1) make CE a selection of methods as the other media-specific method (i.e., move CE back into the selection) or (2) change the target of O.PURGE_DATA and FPT_WIPE_EXT.1 so that it includes only D.USER.DOC and D.TSF.CONF. Al indicated he was against the second option because there may be protected TSF data that customers might want "purged" also such as configuration settings. There seemed to be a consensus of the HCD iTC members present at the 6/13 meeting that moving CE back inside the selection was the preferred option.

- Al then indicated there were other comments against the "WIPE" proposal from Jerry Colunga and himself that the HCD iTC still had to review that would affect both the SFR and the Assurance Activities. So, as a result it will be at least two more weeks at best before the "WIPE" proposal can be finalized.

- With that Al showed the HCD iTC schedule he had presented at the Feb 19th IDS Face to Face Meeting. The current plan called for the Final Drafts of the HCD cPP and HCD SD to be released for public review of 6/13 leading to a final publishing date of Version 1.0 for both documents around 8/2/22.

  Clearly, that date was missed. Al indicated that in the best case the HCD iTC can probably have the Final Drafts of both documents ready for public review around July 11th, a slip of about 4 weeks. If the schedule holds from there, the best case for publishing Version 1.0 of the HCD cPP and HCD SD would be around August 30th, which is what Al predicted at the Feb 19th IDS Face to Face Meeting. Since the HCD iTC has not seen anything close to "best case" yet, it's more likely we are looking at sometime in Sep 2022 for publishing Version 1.0.

5. For one last thing Al showed a slide presented by Kristy Knowles, the ND iTC Chair at the CCUF Workshop held in May 2022. The slide showed some of the items that are planned for the next version of the ND cPP (Version 3.0) that is planned to be released in Oct 2022. This list is important because some of these items will likely find their way into the next version of the HCD cPP. The key items on the NC cPP Version 3.0 list were:

   - Adding TLS 1.3 (and removal of TLS 1.1)
   - Adding ALC_FLR as optional additional assurance component. Al has mentioned this at the Face to Faces because EUCC is including ALC_FLR as a mandatory assurance component so the CCDB is palling to incorporate into CC anyway.
   - SSH SFR Updates - SSH package defined by the CCUF Crypto Group. One of the HCD iTC subgroups had looked at the SSH Package before and it is very different in terms of requirements and setup from what is currently in ND cPP and thus in the HCD cPP. If ND iTC does add this SSH Package, the HCD iTC will probably have to include it also and that will have impacts on vendors because of the differences.
   - Lastly, it wasn't on the ND list but the HCD iTC voted not to include NTP in Version 1.0. NTP will definitely be one of the top items to be include in the next update to the HCD cPP.

6. **Actions:** None

Next Steps

- The next IDS WG Meeting will be June 30, 2022 at 3:00P ET / 12:00N PT. Main topics will be review of the HCD iTC Meetings since this meeting and possibly a special topic.