IDS Face-to-Face Minutes
November 16, 2017

Meeting was called to order at approximately 9:00 am local November 16, 2017.

Attendees –

Gyaneshwar Gupta	Oki Data
Smith Kennedy	HP Inc.
Ira McDonald	High North
Alan Sukert	Xerox
Michael Sweet	Apple
Bill Wagner	TIC
Rick Yardumian	Canon

Note: This was a virtual meeting

Agenda Items

Note: Meeting slides are available at http://ftp.pwg.org/pub/pwg/ids/Presentation/2017-11-16-IDS-F2F.pdf.

1. Minute Taker
   - Alan Sukert taking the minutes
2. Agenda:
   - Introductions, Agenda Review, Status
   - Review October 2076 MFP Technical Committee Meeting
   - Wrap-Up / Next Steps
3. Went through the PWG Intellectual Property policy.
4. Reviewed the outcomes from the latest MFP Technical Committee (TC) Meeting held on October 25, 2017. The meeting slides provide a summary of the results from this meeting.

   The following points were also made as part of the discussion:

   - There was a lot of discussion on the NIAP direction implementing the changes to NIST SP 800-131A and NIST SP 800-56B. The net result of the NIAP actions was basically “no action” – NIAP is waiting for NIST to determine based on industry feedback what the final changes to these two SPs will be and whether NIST will enforce disallowance of any TLS cipher suites that utilize RSA key exchange.
   - There was also a lot of discussion on password requirements in the HCD Protection Profile (PP) and in NIST SP 800-171 that becomes effective on Jan 1, 2018. The requirements in NIST SP 800-171 are more extensive than in the HCD PP, so one of the issues that the MFD TC (by the way has been renamed to the HCD TC) will have to deal with in the next update to the HCD PP is what password requirements need to be included under the FIA_PMG_EXT Security Functional Requirement (SFR).
   - There is a Version 1.1 update planned by the HCD TC for the HCD PP in the next 6-9 months and a major Version 2.0 update planned in the next 12-18 months. The main areas that will be covered in the Version 1.1 update are a subset of the following:
     - Incorporating existing Technical Decisions against HCD PP Version 1.0

- Current Errata created by JISEC (the Japanese Scheme) as part of its evaluation of the HCD PP
- RSA Key Agreement implementation when NIST determines what it will do with NIST SP 800-131A and SP 800-56B
- New Audit Log Server Requirements
- Applicable requirements updates implemented in the latest versions of Network Device collaborative PP (NDcPP) and the Full Disk Encryption cPP (FDEcPP)
- Updated requirements from Technical Decisions on applicable PPs other than the HCD PP
- Assurance Activities (AAs) for the Key Transport SFR (FCS_COP.1(i))
- Additional implicit requirements that show up in Assurance Activities
- Inconsistencies between Key Management Description (KMD) appendix and KMD Assurance activities in the HCD PP
- How to properly address 3rd Party Entropy Sources
- More user friendly testing of the Key Destruction SFR
- Trusted Platform Modules (TPMs) used in the TOE
- Including an EAL Claim for HCD PP

The Version 2.0 update will include what is not in Version 1.1 plus possibly the following additional topics:

- Password Policies discussed above
- Password Policy Applicability (normal vs. admin users)
- Wi-Fi Support
- SNMPv3 Support
- Kerberos Support
- S/MIME Support
- SMBv3 Support
- Internationally-friendly crypto requirements that don't rely on FIPS

Wrap Up

- We will schedule a future IDS Conference Call early in 2018.

The meeting was adjourned at approximately 10:30 pm local on November 16, 2016.