The Printer Working Group

Imaging Device Security

May 19, 2022

PWG May 2022 Virtual Face-to-Face

Agenda

When	What
12:45 – 12:55	Introductions, Agenda review
12:55 – 1:50	Discuss results of latest HCD iTC Meetings and HCD cPP/SD v1.0 status
1:50 – 2:10	IPP Encrypted Jobs and Documents
2:10 – 2:15	HCD Security Guidelines v1.0 Status
2:15 – 2:40	TCG/IETF Liaison Reports
2:40 – 2:45	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 February 17, 2022 HCD iTC meetings have been held on:
  - February 21st, 28th
  - March 7th, 14th, 21st, 28th
  - April 4th, 11th, 18th, 25th
  - May 2nd, 9th, 16th

HCD cPP/SD Status

- Released 2nd Public Review draft of the HCD cPP (v0.11 dated 12/14/2021) on 12/14/2021

	Internal Drafts	1st Public Draft	2nd Public Draft
Accepted	156	70	56
Accepted in Principle	5	0	0
Deferred	33	1	10
Not Accepted	10	14	17
Not Adjudicated	0	0	1

HCD cPP/SD Status

- Released 2nd Public Draft of the HCD SD (v0.98 dated 2/24/2022) released on 2/24/2022

	Internal Drafts	1st Public Draft	2nd Public Draft
Accepted	57	24	25
Accepted in Principle	1	0	1
Deferred	15	2	0
Not Accepted	1	2	3
Not Adjudicated	0	0	0

HCD cPP/SD Status
Key Issues Resolved in 2nd Public Draft of HCD SD

- Added a Test Assurance Activity for SFR **FPT_TST_EXT: TSF testing** where one was not present in previous drafts
- Moved the Assurance Activities for the following:
  - All of the Audit Log related SFRs to under "Security Audit (FAU)" rather than because they are all mandatory SFRs
  - SFR **FCS_CKM.1/AKG Cryptographic Key Generation (for asymmetric keys)** to **Chapter 3. Evaluation Activities for Conditionally Mandatory Requirements** as required by NIAP Technical Decision TD 0074
  - SFR **FCS_CKM.2 Cryptographic Key Establishment** to **Chapter 3. Evaluation Activities for Conditionally Mandatory Requirements** because it refers to the conditional requirement SFR **FCS_CKM.1.1/AKG Cryptographic Key Generation (for asymmetric keys)**
- Added ISO/IEC 11770-6:2016 to the list of references an evaluator shall verify the approved derivation mode and key expansion algorithm for in the TSS Assurance Activity for SFR **FCS_KDF_EXT.1: Cryptographic Key Derivation**
- Corrected an incorrect CEM paragraph reference in **Section 6.2.1. Basic Functional Specification (ADV_FSP.1)** *Table 2. Mapping of ADV_FSP.1 CEM Work Units to Evaluation Activities*

HCD cPP/SD Status
Key Issues Resolved in 2nd Public Draft of HCD SD

- Corrected several unreachable URLs in Appendix C: Public Vulnerability Sources.
- Removed redundant Operator User Guidance Evaluation Activities related to the evaluator ensuring that the Operational guidance contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE and providing a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE
- Corrected two incorrect paragraph references in **Section 6.6.1. Vulnerability Survey (AVA_VAN.1)** *Table 3. Mapping of AVA_VAN.1 CEM Work Units to Evaluation Activities*
- Added the missing content of the Evaluation Activity (Documentation) and Evaluation Activity sections under **Section 6.6.1. Vulnerability Survey (AVA_VAN.1)**

HCD cPP/SD Status
Key Issues Resolved in 2nd Public Draft of HCD SD

- Implemented the significant updates to the Assurance Activities (mostly in the Test Assurance Activities) requested by ITSCC (the Korean Common Criteria Scheme) for the following SFRs:
  - FCS_CKM.1/SKG Cryptographic key generation (Symmetric Keys)
  - FCS_COP.1/DataEncryption Cryptographic Operation (Data Encryption/Decryption)
  - FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)
  - FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)
  - FCS_COP.1/StorageEncryption Cryptographic operation (Data Encryption/Decryption)
  - FCS_COP.1/KeyWrap Cryptographic operation (Key Wrapping)
  - FCS_CKM.1/AKG Cryptographic Key Generation (for asymmetric keys)
  - FCS_KDF_EXT.1 Extended: Cryptographic Key Derivation

Current HCD cPP/SD Issues Affecting Final Drafts of HCD cPP/SD

Inclusion of Cryptographic Erase in HCD cPP

- Initial Comments that raised the issue:
  - JISEC felt Cryptographic Erase covered by the two Key Destruction SFRs (FCS_CKM.4 & FCS_CKM_EXT.4) already in the HCD cPP
  - ITSCC felt Image Overwrite and Cryptographic Erase are two different things and agreed with JISEC; suggested HCD iTC create optional requirements for Cryptographic Erase
- HCD iTC created a subgroup to address the Cryptographic Erase requirement
- Result was creation of a new Data Wiping SFR FPT_WIPE_EXT and associated Assurance Activities (AAs) to replace the current FDP_RIP.1/PURGE SFR that is still undergoing HCD iTC review
  - FPT_WIPE_EXT originally required D.USER and D.TSF data stored on non-volatile storage to be made unavailable upon the request of an Administrator using one or more of the following methods: (1) *overwrite, (2) block erase,* (3) *Cryptographic Erase,* (4) *[**assignment:** media-specific method(s)]*

Note: In this context, "Cryptographic Erase" encompasses any method that destroys the decryption key while leaving encrypted D.USER and/or D.TSF on the storage media. This would include, for example, some ATA commands that only destroy the key

Current HCD cPP/SD Issues Affecting Final Drafts of HCD cPP/SD

Inclusion of Cryptographic Erase in HCD cPP

- Received key comments against FPT_WIPE_EXT SFR and associated AAs from NIAP, ITSCC and JISEC:

  NIAP

  - Not clear whether the concern for this is related to cryptographic erase, overwrite in general on SSDs, or both
  - Inclusion "[assignment: media-specific method(s)]" seems overly broad
  - Wanted some wording changes in the Application Notes to the FPT_WIPE_EXT SFR

  ITSSC

  - Unclear whether the FDP_RIP.1/Overwrite SFR applies to cryptographic erase or not
  - In SFR FDP_RIP.1.1/Overwrite, the option "by destroying its cryptographic key" seems to be for "wear-leveled storage device", while the other option "by overwriting data" seems to be for "non-wear-leveled storage device". Is it possible to select "by overwriting data" for "wear-leveled storage device"? It is possible to overwrite data on a wear-leveled storage device such as SSDs?

Current HCD cPP/SD Issues Affecting Final Drafts of HCD cPP/SD

Inclusion of Cryptographic Erase in HCD cPP

JISEC

- The proposal of FDP_RIP.1.1/Overwrite does not meet the requirements of original FDP_RIP.1 defined in the CC part2, nor the allowed refinement operation defined in the CC part1
- We are not sure why NIAP and HCD iTC want to include a mandatory requirement, cryptographic erase (destroying cryptographic key), as an optional requirement (i.e., cryptographic erase should be a mandatory requirement)

- To address comments from the three Schemes, the HCD iTC Secure Erase Subgroup agreed on the following:
  - Replace FDP_RIP.1/Overwrite with a new Extended User.Doc Unavailability SFR FDP_UDU_EXT that contains what was in FDP_RIP.1/Overwrite with some modifications to address Scheme (especially JISEC) comments
  - Update FPT_WIPE_EXT to make cryptographic erase a mandatory method for making data unavailable and to delineate specific allowable media-methods to select from
  - Added additional TSS and Guidance elements to ensure types of overwrite and medium being overwritten are identified
  - Make the requested changes to the FPT_WIPE_EXT Application Notes

Current HCD cPP/SD Issues Affecting Final Drafts of HCD cPP/SD

- Addressing changes to ND SFRs and Assurance Activities documented in NIAP Technical Decisions (TDs) by the ND Integration Team (NIT) that affect corresponding SFRs and Assurance Activities in the HCD cPP and HCD SD
  - These may end up as “Parking Lot” issues
- Update of spec/standard versions
  - Addressed version update comments from Korean Scheme
- Resolving all open comments to prepare and release of Final Drafts of both the HCD cPP and HCD SD
  - Final Drafts will have “full content” for both documents

Other HCD cPP/SD Issues Affecting Final Drafts of the HCD cPP/SD

Issues HCD iTC still need to be resolved (in order of priority):

- Closure of "deferred" comments
  - Need to be concerned about implications of updating versions
  - Update of spec/standard versions
    - Did we miss anything?
  - 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 HCD cPP/SD Issues Affecting Final Drafts of the HCD cPP/SD

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

- What" issues will be moved to the "parking lot" for inclusion in later versions of the HCD cPP/SD.

  Current Parking Lot Issues

  - Addressing hardware-based Roots of Trust stored in mutable memory as well as immutable memory
  - Clarification that the Secure Boot SFR only requires verification of firmware/software that is stored in mutable memory at boot time and does not require verification of firmware/software stored in immutable memory
  - Comments that require implementation of TLS 1.3 to resolve

Other HCD cPP/SD Issues

Additional New Content (SFRs)

- At this point do not expect any additional new requirements for the HCD cPP/SD beyond what already been discussed unless either:
  - They are requested by JISEC or ITSCC or NIAP
  - They are suggested by JBMIA
  - Necessitated by comments to 2nd Public Drafts or Final Drafts
  - Necessitated by any new NIAP TDs to either the HCD PP or any applicable SFRs in the ND & FDE cPPs/SDs
- Given the current known schedules, syncing with applicable updates to ND cPP/SD and FDE cPPs/SDs is not likely to happen within the time frame for HCD cPP/SD v1.0.
- Don’t expect any applicable ISO, FIPS or NIST Standards/Guidelines updates within this time frame either

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 **DONE**

HCD iTC Status
Updated Proposed HCD cPP/SD Schedule

Phase	Timeframe	Status Updates
Public Review Draft 2	**New Proposed Schedule (3/29/2022)** • Submit 2nd Public Draft: 12/14 • Review 2nd Public Draft: 12/15 – 1/31/22 (49d) • Review comments and update documents: 1/31/1/22 – 5/13/22(60d)	HCD cPP 2nd Public Draft released 12/14 - DONE Comments Received by 1/31/22 - DONE HCD SD 2nd Public Draft Planned Release 12/13 – Released 2/24/22 DONE Comments due by 3/18/22 (~one month)
Final Draft	**New Proposed Schedule (as of 5/16/22)** • Submit Final Draft: 6/13/22 • Review Final Public Draft: 6/14/ – 7/17 (28d) • Review comments and update documents: 7/18/22 – 8/1/22 (10d)	Was 1/17/22 on original schedule As of 7/9 HCD iTC Meeting was on track to meet 5/16 date. However, at 7/16 meeting agreed on new schedule to get full iTC and Scheme buy-in on final WIPE proposal
Final Document Published	**New Proposed Schedule (as of 5/16/22)** • Publish Version 1.0: 8/2/22	Was 3/25/22 on original schedule If past history is a guide, Publish date will likely be closer to end of August 2022

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
- Coordination with EUCC
- Inclusion of AVA_VAN and ALC_FLR.*
  - May require a PP Module to avoid duplicate certifications in EU
- Changes due to HCD Integration Team responses to comments/questions
- Support for Wi-Fi and maybe Bluetooth
- Support for Security Information and Event Monitoring (SIEM) and related systems
- Expand to address 3D printing
- Update to ISO/IEC 15408/18045
  - Will be published in Oct 2022
  - Adds new SFRs and pre-packaged PP and ST Assurance Activities in new Part 4

Potential HCD cPP Content Post-Version 1.0

- Incorporation of CCDB Crypto WG Packages
- Syncing with upcoming ND CPP Version 2.0 planned for Oct 2022
- Updates due to requests from JISEC, ITSCC or NIAP
- Updates due to changes from other ISO, FIPS or NIST Standards/Guidelines, NIAP TDs, or CCDB Crypto WG
- Incorporate, as applicable, the changes to ISO 15408, particularly any relevant new SFRs in the updated Part 2
- Support for SNMPv3
- Support for NFC
- Support for new crypto algorithms
- Indirect updates based on new technologies or customer requests

HCD iTC Status
Key Next Steps

- Finalize all new content for v1.0
- Address all the comments against the 2nd Public Drafts and Final Drafts
- Determine “parking lot” issues for later versions of the HCD cPP/SD
- Add all agreed-upon SFRs and Assurance Activities into the HCD cPP and SD
- Submit 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
- Start planning for and creating an Interpretation Team for maintaining HCD cPP/SD v1.0 and start planning for the next HCD cPP/SD update (whether it is v1.x or v2.0)

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

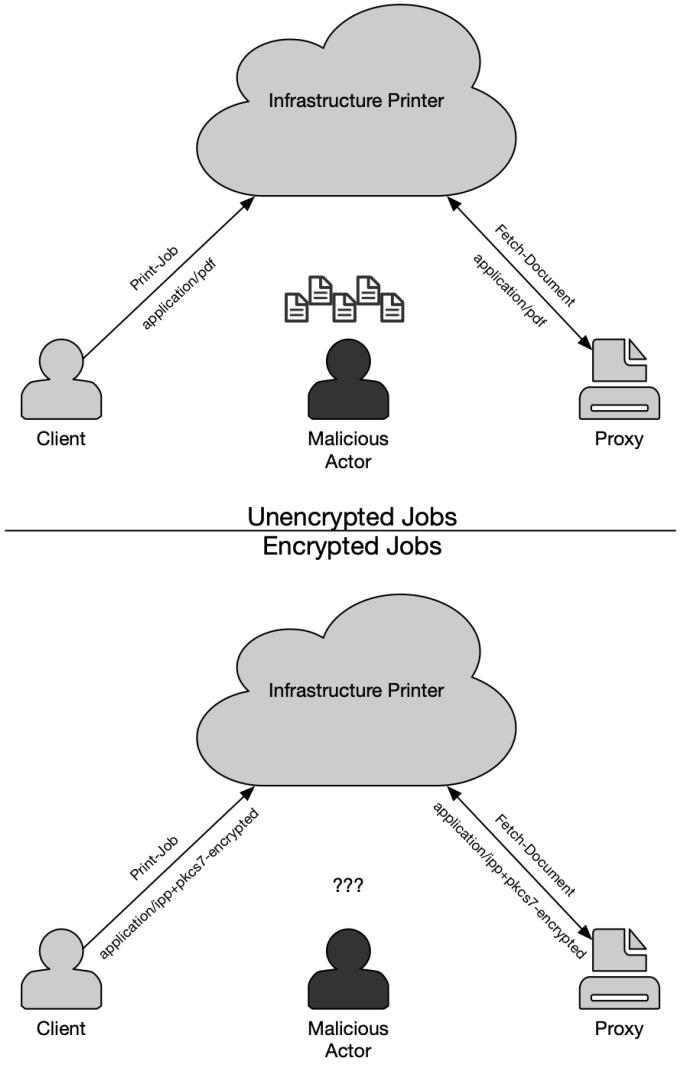
- The end game is always the hardest part, because every time you think you're close to the end your not
- It's never too early to start planning for what comes after initial release because you always think you have more time to plan for what comes next than you actually do
- It is critical that you avoid "reinventing the wheel" whenever possible – or in other words leverage what others have done before you whenever you can
- Considering we started in February 2020, getting a new iTC established and creating/publishing a major cPP and SD within 2-1/2 years is still quite a feat

IPP Encrypted Jobs and Documents

IPP Encrypted Jobs and Documents

- Current prototype draft (needs prototyping):
  - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ipptrustnoone10-20210519.pdf
- Implements an S/MIME container for Print Jobs and Job Receipts (attributes containing accounting info)
  - PGP container was also proposed but ultimately was shelved due to lack of interest
- Works for both direct and cloud/local server printing solutions
- One new Client operation to query encrypted Job attributes/receipts
- Two new Proxy operations to return encrypted Job attributes/receipts

Architecture



Encrypted Print-Job

- Printer/Proxy advertises an X.509 certificate and public key to use for encrypted printing
- Client encrypts an IPP Print-Job request with document data in an S/MIME container using the Printer's X.509 certificate, signed using the Client's X.509 certificate
  - Job ticket and document data are both protected and signed to prevent modification
  - An additional password/passcode can be set for release at the printer's console
- Printer/Proxy decrypts the S/MIME message, validates the Client signature, and processes the Print-Job request and document data

Encrypted Print-Job

Typical Print-Job Request

POST /ipp/print
Host: printer.example.com:631
Transfer-Encoding: chunked

IPP Message

version-number='2.0'
operation-code='Print-Job'
request-id='42'

operation-attributes-tag
  attributes-charset='utf-8'
  attributes-natural-language='en-us'
  printer-uri='ipps://printer.example.com/ipp/print'
  document-format='application/pdf'
  job-name='Employee Review - John Doe'

job-attributes-tag
  copies='2'
  media='iso_a4_210x297mm'
  other job template attributes

end-of-attributes-tag

Document Data

...

Encrypted Print-Job Request

POST /ipp/print
Host: printer.example.com:631
Transfer-Encoding: chunked

IPP Message

version-number='2.0'
operation-code='Print-Job'
request-id='42'

operation-attributes-tag
  attributes-charset='utf-8'
  attributes-natural-language='en-us'
  printer-uri='ipps://printer.example.com/ipp/print'
  document-format='application/ipp+pkcs7-encrypted'
  job-name='8675309'
  requesting-user-name='...'

end-of-attributes-tag

Encrypted Message Header

Algorithms/cipher suite (e.g. 'aes256gcm')
Symmetric key packet(s)

IPP Message (Encrypted)

version-number='2.0'
operation-code='Print-Job'
request-id='42'

operation-attributes-tag
  attributes-charset='utf-8'
  attributes-natural-language='en-us'
  document-format='application/pdf'

job-attributes-tag
  copies='2'
  media='iso_a4_210x297mm'
  other job template attributes

end-of-attributes-tag

Document Data (Encrypted)

...

Encrypted Message Trailer

Digital signature of encrypted IPP message and document data using Client's X.509 certificate

Get-Encrypted-Job-Attributes

- Client send a Get-Encrypted-Job-Attributes request with its own X.509 certificate and public key
  - Client certificate must match Print-Job request's signature
  - An ordinary Get-Job-Attributes request will only return basic state information
- Printer/Proxy encrypts a Get-Encrypted-Job-Attributes response in an S/MIME container using the Client's X.509 certificate, signed using the Printer's X.509 certificate
- Client decrypts the S/MIME message, verifies the Printer's signature, and processes the response attributes as needed

Get-Encrypted-Job-Attributes

G-E-J-A Request

POST /ipp/print
Host: printer.example.com:631
Transfer-Encoding: chunked

IPP Message

version-number='2.0'
operation-code='Get-Encrypted-Job-Attributes'
request-id='43'

operation-attributes-tag
  attributes-charset='utf-8'
  attributes-natural-language='en-us'
  printer-uri='ipps://printer.example.com/ipp/print'
  job-id='123'
  requested-attributes='…'
  requesting-user-name='…'
  requesting-user-pkcs7-public-key='…'

end-of-attributes-tag

G-E-J-A Response

HTTP/1.1 200 OK
Content-Type: application/ipp
Transfer-Encoding: chunked

IPP Message

version-number='2.0'
status-code='successful-ok'
request-id='43'

operation-attributes-tag
  attributes-charset='utf-8'
  attributes-natural-language='en-us'
  encrypted-job-request-format='application/ipp+pkcs7-encrypted'
  requesting-user-pkcs7-public-key='…'

end-of-attributes-tag

Encrypted Message Header

Algorithms/cipher suite (e.g. 'aes256gcm')
Symmetric key packet

IPP Message (Encrypted)

version-number='2.0'
status-code='successful-ok'
request-id='43'

operation-attributes-tag
  attributes-charset='utf-8'
  attributes-natural-language='en-us'

job-attributes-tag
  copies-actual='2'
  impressions-completed='8'
  impressions-completed-col={…}
  media-actual='iso_a4_210x297mm'
  media-sheets-completed='8'
  media-sheets-completed-col={…}
  other job status attributes

end-of-attributes-tag

Encrypted Message Trailer

Digital signature of encrypted IPP message using Printer's X.509 certificate

Discussion

- Should we talk about using separate certificates and keys for signing and encryption?
  - Separate certificates sometimes used in email, where any validation seems to be limited to matching the common names of the certificates and "are the CAs that issued the certificates trusted?"
- What should the common name be for Printer certificates?
  - Should be something the Client can use for validation
  - "printer-uuid" value?

HCD Security Guidelines

Trusted Computing Group (TCG)

- **Next TCG Members Meetings**
  - **TCG Hybrid F2F (Chevy Chase, MD) – 18-22 July 2022 – Ira to call in**
  - **TCG Hybrid F2F (New Orleans, LA) – 24-28 October 2022 – Ira to call in**
- **Trusted Mobility Solutions (TMS) – Ira is co-chair and co-editor**
  - **Formal – GP (TEE, SE), ETSI (NFV/MEC/SAI)**
  - **Informal – 3GPP, GSMA, IETF, ISO, ITU-T, SAE, US NIST**
  - ***TCG TMS Use Cases v2 – published September 2018***
- **Mobile Platform (MPWG) – Ira is co-editor**
  - **Formal – GP (TEE, SE), ETSI (NFV/MEC/SAI)**
  - ***TCG Mobile Reference Architecture v2 – work-in-progress for review Q3 2022***
  - ***TCG TPM 2.0 Mobile Common Profile – work-in-progress for review Q3 2022***
  - ***TCG MARS 1.0 Mobile Profile – new work-in-progress Q4 2021***
  - ***TCG Runtime Integrity Preservation for Mobile Devices – Nov 2019***
  - ***GP TPS Client API / Entity Attestation Protocol / COSE Keystore – joint work***
- **Recent Specifications**
  - **http://www.trustedcomputinggroup.org/resources**
  - ***TCG DICE Endorsement Architecture for Devices – review May 2022***
  - ***TCG EK Credential Profile for TPM 2.0 – review March 2022***
  - ***TCG Cyber Resilient Module and Building Block Requirements – March 2022***
  - ***TCG Canonical Event Log Format – published February 2022***

Liaison Status

Trusted Computing Group (TCG)

- **Next TCG Members Meetings**
  - **TCG Hybrid F2F (Chevy Chase, MD) – 18-22 July 2022 – Ira to call in**
  - **TCG Hybrid F2F (New Orleans, LA) – 24-28 October 2022 – Ira to call in**
- **Trusted Mobility Solutions (TMS) – Ira is co-chair and co-editor**
  - **Formal – GP (TEE, SE), ETSI (NFV/MEC/SAI)**
  - **Informal – 3GPP, GSMA, IETF, ISO, ITU-T, SAE, US NIST**
  - ***TCG TMS Use Cases v2 – published September 2018***
- **Mobile Platform (MPWG) – Ira is co-editor**
  - **Formal – GP (TEE, SE), ETSI (NFV/MEC/SAI)**
  - ***TCG Mobile Reference Architecture v2 – work-in-progress for review Q3 2022***
  - ***TCG TPM 2.0 Mobile Common Profile – work-in-progress for review Q3 2022***
  - ***TCG MARS 1.0 Mobile Profile – new work-in-progress Q4 2021***
  - ***TCG Runtime Integrity Preservation for Mobile Devices – Nov 2019***
  - ***GP TPS Client API / Entity Attestation Protocol / COSE Keystore – joint work***
- **Recent Specifications**
  - **http://www.trustedcomputinggroup.org/resources**
  - ***TCG DICE Endorsement Architecture for Devices – review May 2022***
  - ***TCG EK Credential Profile for TPM 2.0 – review March 2022***
  - ***TCG Cyber Resilient Module and Building Block Requirements – March 2022***
  - ***TCG Canonical Event Log Format – published February 2022***

Internet Engineering Task Force (IETF) (1 of 4)

- **Next IETF Members Meetings**
  - **IETF 114 Hybrid F2F (Philadelphia, US) – 25-29 July 2022 – Ira to call in**
  - **IETF 115 Hybrid F2F (London, UK) 7-11 November 2022 – Ira to call in**
- **Transport Layer Security (TLS)**
  - **IETF TLS Ticket Requests – RFC 9149 – April 2022**
    https://datatracker.ietf.org/doc/rfc9149/
  - **IETF DTLS Protocol Version 1.3 – RFC 9147 – April 2022**
    https://datatracker.ietf.org/doc/rfc9147/
  - **IETF Connection Identifier for DTLS 1.2 – RFC 9146 – March 2022**
    https://datatracker.ietf.org/doc/rfc9146/
  - **IETF Delegated Credentials for (D)TLS – draft-13 – May 2022 – IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-tls-subcerts/
  - **IETF Importing External PSKs for TLS – draft-08 – April 2022 – RFC Editor**
    https://datatracker.ietf.org/doc/draft-ietf-tls-external-psk-importer/
  - **IETF IANA Registry Updates for TLS/DTLS – draft-00 – March 2022**
    https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8447bis/
  - **IETF Secure Element for TLS 1.3 – draft-04 – March 2022**
    https://datatracker.ietf.org/doc/draft-urien-tls-se/
  - **IETF Compact TLS 1.3 – draft-05 – March 2022**
    https://datatracker.ietf.org/doc/draft-ietf-tls-ctls/
  - **IETF Return Routability Check for DTLS 1.2/1.3 – draft-05 – March 2022**
    https://datatracker.ietf.org/doc/draft-ietf-tls-dtls-rrc/
  - **IETF TLS 1.3 – draft-04 – March 2022**
    https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8446bis/
  - **IETF Flags Extension for TLS 1.3 – draft-09 – March 2022**
    https://datatracker.ietf.org/doc/draft-ietf-tls-tlsflags/
  - **IETF Exported Authenticators in TLS – draft-15 – March 2022 – RFC Editor**
    https://datatracker.ietf.org/doc/draft-ietf-tls-exported-authenticator/
  - **IETF Suppressing CA Certificates in TLS 1.3 – draft-01 – March 2022**
    Suppressing CA Certificates in TLS 1.3

Internet Engineering Task Force (IETF) (2 of 4)

- **Security Automation and Continuous Monitoring (SACM)**
  - **IETF Concise Software Identifiers – draft-21 – March 2022 – IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/
- **Concise Binary Object Representation (CBOR)**
  - **IETF Additional Control Ops for CDDL – RFC 9165 – December 2021**
    https://datatracker.ietf.org/doc/rfc9165/
  - **IETF CBOR tags for IPv4/v6 Adresses – RFC 9164 – December 2021**
    https://datatracker.ietf.org/doc/rfc9164/
  - **IETF CBOR Tags for OIDs – RFC 9090 – July 2021**
    https://datatracker.ietf.org/doc/rfc9090/
  - **IETF Storing CBOR Items on Stable Storage – draft-12 – May 2022**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-file-magic/
  - **IETF Packed CBOR – draft-05 – April 2022**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-packed/
  - **IETF Using CDDL for CSVs – draft-00 – February 2022**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-csv/
  - **IETF Notable CBOR Tags – draft-06 – February 2022**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-notable-tags/
  - **IETF Feature Freezer for CDDL – draft-09 – December 2021**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-freezer/

Internet Engineering Task Force (IETF) (3 of 4)

- **Remote ATtestation ProcedureS (RATS)**
  - **IETF ARM PSA Attestation Verifier Endorsements – draft-01 – May 2022**
    https://datatracker.ietf.org/doc/draft-fdb-rats-psa-endorsements/
  - **IETF Epoch Markers – draft-01 – May 2022**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-epoch-markers/
  - **IETF Automatic Integration of Secure Silicon Attestation Token – draft-01 – April 2022**
    https://datatracker.ietf.org/doc/draft-tschofenig-rats-aiss-token/
  - **IETF YANG Data Model for CHARRA using TPMs – draft-19 – April 2022 – IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/
  - **IETF TPM-based Network Device RIV – draft-14 – March 2022 – RFC Editor**
    https://datatracker.ietf.org/doc/draft-ietf-rats-tpm-based-network-device-attest/
  - **IETF Attestation Results for Secure Interactions – draft-02 – March 2022**
    https://datatracker.ietf.org/doc/draft-ietf-rats-ar4si/
  - **IETF Attestation Event Stream Subscription – draft-01 – March 2022**
    https://datatracker.ietf.org/doc/draft-ietf-rats-network-device-subscription/
  - **IETF ARM PSA Attestation Token – draft-09 – March 2022**
    https://datatracker.ietf.org/doc/draft-tschofenig-rats-psa-token/
  - **IETF Trusted Path Routing – draft-05 – March 2022**
    https://datatracker.ietf.org/doc/draft-voit-rats-trustworthy-path-routing/
  - **IETF Entity Attestation Token (EAT) – draft-12 – February 2022**
    https://datatracker.ietf.org/doc/draft-ietf-rats-eat/
  - **IETF RATS Architecture – draft-15 – February 2022 – IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/
  - **IETF Reference Interaction Models for RATS – draft-05 – January 2022**
    https://datatracker.ietf.org/doc/draft-ietf-rats-reference-interaction-models/
  - **IETF Concise Reference Integrity Manifest – draft-02 – January 2022**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-corim/

Internet Engineering Task Force (IETF) (4 of 4)

- **IRTF Crypto Forum Research Group (CFRG) – future algorithms**
  - **IRTF Hybrid Public Key Encryption – RFC 9180 – February 2022**
    https://datatracker.ietf.org/doc/rfc9180/
  - **IRTF Argon2 password hash and proof-of-work – RFC 9106 – September 2021**
    https://datatracker.ietf.org/doc/rfc9106/
  - **IRTF SPAKE2+, an Augmented PAKE – draft-08 – May 2022**
    https://datatracker.ietf.org/doc/draft-bar-cfrg-spake2plus/
  - **IRTF Key Blinding for Signature Schemes – draft-02 – May 2022**
    https://datatracker.ietf.org/doc/draft-dew-cfrg-signature-key-blinding/
  - **IRTF Verifiable Distributed Aggregation Functions – draft-00 – April 2022**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-vdaf/
  - **IRTF Two-Round Threshold Schnorr Signatures with FROST – draft-04 – March 2022**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-frost/
  - **IRTF Usage Limits on AEAD Algorithms – draft-04 – March 2022**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-aead-limits/
  - **IRTF OPAQUE Asymmetric PAKE Protocol – draft-08 – March 2022**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-opaque/
  - **IRTF Ristretto255 and Decaf448 Groups – draft-03 – February 2022**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-ristretto255-decaf448/
  - **IRTF Deterministic Nonce-less Hybrid PKE – draft-01 – February 2022**
    https://datatracker.ietf.org/doc/draft-harkins-cfrg-dnhpke/
  - **IRTF KangarooTwelve – draft-07 – February 2022 – RG LC**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-kangarootwelve/
  - **IRTF Hashing to Elliptic Curves – draft-14 – February 2022 – IRSG Poll**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve/
  - **IRTF Deterministic ECDSA and EdDSA Signatures with Additional Randomness – draft-04 – February 2022**
    https://datatracker.ietf.org/doc/draft-mattsson-cfrg-det-sigs-with-noise/
  - **IRTF SPAKE2, a PAKE – draft-26 – February 2022 – RFC Editor**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-spake2/

Next Steps – IDS WG

- Next IDS WG Meeting– May 26, 2022
- Next IDS Face-to-Face Meeting August 16-18, 2022 (probably August 18th) at next PWG F2F
- Start looking at involvement in some of these other standards activities individually and maybe as a WG

Backup