
# The Printer Working Group

## Imaging Device Security

August 18, 2022

PWG August 2022 Virtual Face-to-Face

# Agenda

| When | What |
|---|---|
| 10:00 – 10:05 | Introductions, Agenda review |
| 10:05 – 11:00 | Discuss results of latest HCD iTC Meetings and HCD cPP/SD v1.0 status |
| 11:00 – 11:25 | Cybersecurity Executive Order Status Update |
| 11:25 – 11:30 | HCD Security Guidelines v1.0 Status |
| 11:30 – 11:55 | TCG/IETF Liaison Reports |
| 11:55 – 12:00 | 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 May 19, 2022 HCD iTC meetings have been held on:
  - May 23rd
  - June 6th, 13th, 20th, 27th
  - July 6th, 11th, 18th, 25th
  - August 1st, 8th, 15th

# HCD cPP/SD Status

- Released Final Review draft of the HCD cPP (v0.13 dated 7/25/2022) for Public Review on 8/1/2022

| | Internal Drafts | 1st Public Draft | 2nd Public Draft |
|---|---|---|---|
| **Comments against Security Problem Definition - 19 All were accepted** | | | |
| **Accepted** | 161 | 70 | 56 |
| **Accepted in Principle** | 3 | 0 | 0 |
| **Deferred** | 16 | 1 | 10 |
| **Not Accepted** | 11 | 14 | 17 |
| **Not Adjudicated** | 0 | 0 | 0 |

# HCD cPP/SD Status

- Released Final Draft of the HCD SD (v0.99 dated 7/29/2022) for Public Review on 8/1/2022

| | 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 Final Public Draft of HCD cPP

- To include Cryptographic Erase into the HCD cPP the following was done:
  - Replaced SFR FDP_RIP.1/Overwrite Subset residual information protection with a new SFR FDP_UDU_EXT.1 User.DOC Unavailable that (1) provides the option for Overwrite for the SFR to apply to both wear-levelling and non-wear-levelling storage devices and (2) to include destruction of cryptographic keys as well as overwrite to make USER.DOC unavailable
  - Replaced SFR FDP_RIP.1/Purge Subset residual information protection with a new SFR FPT_WIPE_EXT.1 Data Wiping that requires that customer-supplied D.USER and D.TSF data stored in non-volatile storage be made unavailable using Cryptographic Erase as a mandatory method and optionally using none or one or more of five other methods – overwrite, block erase, media specific eMMC method, media specific ATA erase method, or media specific NVMe method
  - Added or modified wording addressing Cryptographic Erase or destruction of cryptographic keys in the following Sections:
    a. Section 1.4.2 USE CASE 2: Conditionally Mandatory Use Cases, Item 4. Nonvolatile Storage Devices
    b. Section 1.4.3 USE CASE 3: Optional Use Cases, Item 2. Redeploying or Decommissioning the HCD

# HCD cPP/SD Status
# Key Issues Resolved in Final Public Draft of HCD cPP

- To include Cryptographic Erase into the HCD cPP the following was done:
  - Added the following statement to the definition of O.STORAGE_ENCRYPTION in Section 3.5.4 Storage Encryption: "…and the TOE shall provide a function that an authorized administrator may destroy encryption keys or keying material if the TOE supports a function for removing the TOE from its Operational Environment"
  - Added the following note to Section 3.5.7 Wipe Data (optional): Note: Cryptographic erase which is covered in the mandatory requirement of FCS_CKM_EXT.4 and FCS_CKM.4 can be used as a method to remove some parts of User Data and TSF Data, but it cannot be a single method to remove User Data and TSF Data unless all the data are encrypted
  - Because of the new FDP_UDU_EXT.1 SFR, modified Section 3.5.6 Image Overwrite (optional) to remove the statement "or by destroying its cryptographic key" in the last sentence since it was no longer necessary
  - Changed the title of Section 3.5.7 from Purge Data (optional) to Wipe Data (optional) reflect the new FPT_WIPE_EXT.12 Data Wiping SFR
  - Changed the title of Section 4.1.13 from Purge Data (optional) to Wipe Data (optional) reflect the new FPT_WIPE_EXT.12 Data Wiping SFR
  - Changed the Organizational Security Policy (OSP) O.PURGE_DATE to O.WIPE_DATA to reflect the new FPT_WIPE_EXT.12 Data Wiping SFR

# HCD cPP/SD Status
# Key Issues Resolved in Final Public Draft of HCD cPP

- To include Cryptographic Erase into the HCD cPP the following was done:
  - Modified the Application Note for the SFR FDP_DSK_EXT.1 Protection of Data on Disk to state that if additional data other than D.USER.DOC and D.TSF.CONF are encrypted, it will be purged by the cryptographic erase process
- Modified SFRs FPT_SBT_EXT.1.5 and FPT_SBT_EXT.1.6 for Secure Boot to clarify that they apply only to Hardware Roots of Trust
- Removed the previous Software Functional Requirements table that was in Appendix H: SFR List, as well as the entire appendix, that mapped SFRs to OSPs. Replaced this table with a new table in Section 5.12 TOE Security Functional Requirements Rationale that maps OSPs to SFRs and provides the rationale for that mapping
- Moved SFR FCS_CKM.1/AKG Cryptographic Key Generation (for asymmetric keys) from a Conditionally Mandatory to an Optional requirement
- Added missing or incorrect SFR Mapping Information for several SFRs
- Removed the Consistency Rationale Appendix as being repetitive and no longer needed

# HCD cPP/SD Status
# Key Issues Resolved in Final Public Draft of HCD cPP

- The term File Encryption Key (FEK) was incorrectly used in several places in the document; it was replaced by “BEV or DEK”. Also, is some instances “DEK” was missing when it should have been included, so in those instances “BEV” was changed to “BEV or DEK” also
- Corrected a typo in Section 5.4.2. FDP_ACF.1 Security attribute based access control, Table 5. D.USER.JOB Access Control SFP, where “log’ should have been “job”
- Addressed the following NIAP Technical Decisions:
  - TD0642: FCS_CKM.1(a) Requirement; P-384 keysize moved to selection
  - TD0636: NIT Technical Decision for Clarification of Public Key User Authentication for SSH
  - TD0631: NIT Technical Decision for Clarification of public key authentication for SSH Server

# HCD cPP/SD Status
# Key Issues Resolved in Final Public Draft of HCD SD

- Added the Assurance Activities for the new SFRs FDP_UDU_EXT.1 User.Doc Unavailable and FPT_WIPE_EXT.1 Data Wiping that replaced the previous SFRs FDP_RIP.1/Overwrite and FDP_RIP.1/Purge, respectively
- Because of the inclusion of Cryptographic Erase due to the new SFRs FDP_UDU_EXT.1 User.Doc Unavailable and FPT_WIPE_EXT.1 Data Wiping, made the following changes to the Assurance Activities for SFR FDP_DSK_EXT.1 Extended: Protection of Data on Disk:
  - Added the following paragraph to the TSS Assurance Activities:
    - If data (e.g., D.USER.JOB, D.TSF.PROT) other than D.USER.DOC and D.TSF.CONF are encrypted, the evaluator shall verify that TSS identifies all such data and states that no other customer-supplied data are encrypted
  - Added the following new tests to the Test Assurance Activities:
    - Test 3. (If data other than D.USER.DOC and D.TSF.CONF are encrypted,) write the data to the storage device with operating TSFI which enforce write process of the data
    - Test 4. (If data other than D.USER.DOC and D.TSF.CONF are encrypted,) verify that the data written in Test 3 is not in plaintext form; and verify that the data can be decrypted by proper key and key material

# HCD cPP/SD Status
# Key Issues Resolved in Final Public Draft of HCD SD

- Updated the discussion in Section 1.1. Technology Area and Scope of Supporting Document to indicate that certifiers/certification bodies are users of this document
- Removed wording in Section 1.2 Structure of the Document that implied that Certifying Bodies (CB) could modify Evaluation Activities in the SD
- Removed wording in the preliminary paragraph in Chapter 2. Evaluation Activities for SFRs that suggested witnessing developer-generated tests vs. independently performing tests, because that would require CB approval.
- Revised the Test Assurance Activities for both SFR FCS_COP.1/DataEncryption and SFR FCS_COP.1/StorageEncryption to add testing of the key size of 192 bits
- Broke up the Test Assurance Activities for SFR FIA_PMG_EXT.1 Extended: Password Management into two separate test cases to avoid confusion
- Revised Section A.1.1. Type 1 Hypotheses - Public-Vulnerability-based to add the missing information and to clarify the text from the previous versions of this document

# HCD cPP/SD Status
# Key Issues Resolved in Final Public Draft of HCD SD

- Revised Section A.1.2. Type 2 Hypotheses - iTC-sourced to indicate that there are currently are no iTC-sourced flaw hypotheses, but that a future revision of the HCD cPP may update this section for relevant findings made by evaluation laboratories.
- Corrected and/or updated the Evaluation Activities for the following areas in Chapter 6 Evaluation Activities for SARs:
  - ADV_FSP.1-5 Evaluation Activity
  - Operational User Guidance (AGD_OPE.1)
  - Vulnerability Survey (AVA_VAN.1)

# Outstanding Issues After Final Drafts of the HCD cPP/SD

- Addressing comments to Final Drafts of the HCD CPP and HCD SD
- Will 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

  be in HCD cPP v1.0 or in a later version?
- Publishing HCD cPP and HCD SD v1.0

# Other HCD cPP/SD Issues Affecting Final Drafts 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
- Support for NTP
- Support for the CCUF Crypto Working Group SSH Package
- Correcting TSS Assurance Activities for SFR FCS_CKM.4 Key Destruction
- Clarification of TSS Assurance Activities for SFR FIA_X509_EXT.2 X.509 Certificate Authentication

# Other HCD cPP/SD Issues

Additional New Content (SFRs)

- At this point the HCD cPP and HCD SD are "locked down" for v1.0 content. The only changes at this point that would necessitate new content and significant changes to existing content would be:
  - Request from JISEC or ITSCC or NIAP (or any other Scheme)
  - Necessitated by any new NIAP TDs to either the HCD PP or any applicable SFRs in the ND & FDE cPPs/SDs
- Unlikely HCD iTC would accept Final Draft comments against either the HCD cPP or HCD SD from any other source other than the two above that would require substantive technical changes to the content of either document

# 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**<br>• Update ESR: 3/1 – 3/12 **NOT NEEDED**<br>• Update SPD: 3/1 – 3/12 **DONE**<br>• Submit ESR changes to HCD WG (if needed): 3/15 **NOT NEEDED**<br>• HCD WG Review and comment: 3/15 – 4/9 **NOT NEEDED**<br>• Submit SPD for public review: 5/10 **DONE**<br>• SPD Public review: 5/10 – 6/4 **DONE**<br>• Update SPD: 6/7 – 6/25 **DONE** | |
| Internal Draft | **New Proposed Schedule**<br>• Submit 3rd internal draft: 6/1 **DONE**<br>• Review 3rd internal draft: 6/1 – 6/18 **DONE**<br>• Review comments & update documents: 6/21 – 7/16 **DONE** | |
| Public Review Draft 1 | **New Proposed Schedule**<br>• Submit 1st Public Draft: 8/18 (cPP); 8/30 (SD)<br>• Review 1st Public Draft: 8/18 – 10/12 (45d)<br>• Review comments and update documents: 10/13-12/10 (60d) | Was 7/19 on original schedule<br>Note: 1st Public Draft of HCD cPP released on 8/30 – Comment end date 10/8 **DONE**<br>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)**<br>• Submit 2nd Public Draft: 12/14<br>• Review 2nd Public Draft: 12/15 – 1/31/22 (49d)<br>• Review comments and update documents: 1/31/1/22 – 5/13/22(60d) | HCD cPP 2nd Public Draft released 12/14 - DONE<br>Comments Received by 1/31/22 - DONE<br>HCD SD 2nd Public Draft Planned Release 12/13 – Released 2/24/22 DONE<br>Comments due by 3/18/22 (~one month) |
| Final Draft | **New Proposed Schedule (as of 7/14/22)**<br>• Submit Final Draft: 6/13/22 -> 7/18/22<br>• Review Final Public Draft: 7/19/ – 8/22 (28d)<br>• Review comments and update documents: 8/23/22 – 9/6/22 (10d) | Final Drafts of HCD cPP and HCD SD submitted for Public Review on 8/1/22; Comments are due by 9/15/22 |
| Final Document Published | **New Proposed Schedule (as of 7/14/22)**<br>• Publish Version 1.0: 8/2/22 -> 9/7/22 | Was 3/25/22 on original schedule<br>Are currently 2 weeks behind new schedule; best estimate is that documents will be published towards the end of Sep 2022 if we don't get any significant technical comments |

# HCD cPP/SD Content Post-Version 1.0

<u>Will almost certainly be in next version</u>

- Inclusion of support for TLS 1.3 and deprecation of TLS 1.1
- Inclusion of NTP
- Inclusion of AVA_VAN and ALC_FLR.*
  - May require a PP Module to avoid duplicate certifications in EU
- Sync with key changes in ND cPP/SD v3.0 to be published in Oct 2022
  - Incorporate CCDB Crypto WG SSH Package
- Changes due to HCD Integration Team (HIT) responses to comments/questions to HCD cPP/SD v1.0
- Expand to address 3D printing
- Changes due to requests from JISEC, ITSCC or NIAP
- Update to ISO/IEC 15408/18045 to 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

Potential for next or later versions

- Support for Wi-Fi and maybe Bluetooth
- Support for Security Information and Event Monitoring (SIEM) and related systems
- Updates due to changes from other ISO, FIPS or NIST Standards/Guidelines, NIAP TDs
- CCDB Crypto WG, other CCUF Crypto WG Packages or NIAP TLS Package
- Support for SNMPv3
- Support for NFC
- Support for new crypto algorithms
- Indirect updates based on new technologies or customer requests

# HCD iTC Interpretation Team (HIT)

- Goal is to provide timely responses to requests for interpretation (RFIs) from the CC community
- Has its own set of procedures based on the HCD iTC's Terms of Reference including rules for:
  - Determining what RFIs to review and how to process them
  - Voting and decision making
  - Membership and participation
  - What RFIs to pass on to the full iTC
- General HIT process is:
  1. HIT gets an RFI from a Scheme or vendor doing a certification using HCD cPP/SD or another source
  2. HIT analyzes RFI to determine whether to accept RFI for some type of action
     a. If rejects, indicates rationale for rejection
     b. If accepts:
        - Prioritizes RFI
        - Determines Response
        - Generates either Technical Recommendation (TR), which goes to full iTC for approval, or a Technical Decision (TD) which does not need full iTC approval
        - Publishes TR or TD

# HCD iTC Status
# Key Next Steps

- Address all the comments against the Final Drafts
- Finalize “parking lot” issues for next and future versions of the HCD cPP/SD
- 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 implement the HCD iTC Interpretation Team (HIT) 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)

- Being an Document Editor is hard work but they are the unsung heroes of any iTC and don't get the credit they deserve
- In 20-20 hindsight, the one thing the HCD iTC needs to do a better job of is:
  - Handling major issues more efficiently – it took us way too long to reach agreement on the key areas of disagreement
- Having templates for the key documents an iTC must produce like the cPP and the SD was a big help in getting started
- A personal one – this being my third attempt at developing an HCD Protection Profile, you'd think it would get easier the third time around. But it doesn't because each time there are a different set of challenges and timelines.
- However, in the three tries we've done it faster – from 5 years to 3 years to 2 years, 7 months (assuming the cPP/SD are published in Sep 2022)

# Cybersecurity Executive Order Status Update

# Executive Order on Improving the Nation's Cybersecurity

Issued May 12, 2021 by President Biden

Key Areas Covered by this Executive Order:

1. Policy – Federal Government must
   - Bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid.
   - Must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).
2. Sharing Threat Information
3. Cyber Incident Reporting
4. Enhancing Software Supply Chain Security
5. Standardizing the federal government's playbook for responding to cybersecurity vulnerabilities and incident
6. Improving detection of cybersecurity vulnerabilities and incidents on federal government networks
7. Improving the federal government's investigative and remediation capabilities

# Executive Order on Improving the Nation's Cybersecurity - Update

## Current Status

- On February 04, 2022 NIST released the following documents supporting the execution of this Executive Order:

**Software Security Practices**

- Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e (https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-cybersecurity-producers-and)
- NIST Special Publication 800-218, Secure Software Development Framework (SSDF) Version 1.1:Recommendations for Mitigating the Risk of Software Vulnerabilities (https://csrc.nist.gov/publications/detail/sp/800-218/final)

# Executive Order on Improving the Nation's Cybersecurity -Update

## Current Status (cont'd)

- On February 04, 2022 NIST released the following documents supporting the execution of this Executive Order:

**Software Security Labeling**

- Recommended Criteria for Cybersecurity Labeling of Consumer Internet of Things (IoT) Products (https://doi.org/10.6028/NIST.CSWP.02042022-2)
- Recommended Criteria for Cybersecurity Labeling of Consumer Software (https://doi.org/10.6028/NIST.CSWP.02042022-1)
- Consumer Cybersecurity Labeling Pilots: The Approach and Feedback (https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/consumer-cybersecurity-labeling-pilots)

# Executive Order on Improving the Nation's Cybersecurity - Update

Current Status (cont'd)

- On Jul 9, 2021 NIST published Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028 - (https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eocritical-software-use-2)
- In Oct 2021 NIST published NISTIR 8397 Guidelines on Minimum Standards for Developer Verification of Software (https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/recommendedminimum-standards-vendor-or)
- In Oct 2021 NIST released 2nd Draft of NIST Special Publication 800-161 Revision 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (https://doi.org/10.6028/NIST.SP.800-161r1-draft2)

# NISTIR 8397
# Guidelines on Minimum Standards for Developer Verification of Software

- Recommends **minimum standards** (not "best practices") of software verification by software producers
- Based on assumption no single software security verification standard can encompass all types of software and be both specific and prescriptive while supporting efficient and effective verification
- Recommends guidelines for software producers to use in creating their own processes
- Provides for the process to be very specific and tailored to the software products, technology (e.g., language and platform), toolchain, and development lifecycle model

# NISTIR 8397
# Guidelines on Minimum Standards for Developer Verification of Software

SCOPE

- Includes "software source code" and software in general including binaries, bytecode, and executables, such as libraries and packages
- Does not include specialized testing regimes such as real-time software, firmware (microcode), embedded/cyberphysical software, machine learning (ML) or neural net code
- Excludes ancillary yet vital material such as configuration files, file or execution permissions, operational procedures, and hardware

# NISTIR 8397
# Guidelines on Minimum Standards for Developer Verification of Software


Minimum Standards for Developer Testing

- #1. Do Threat Modeling
- #2. Do Automated Testing
- #3. Code-Based, or Static, Analysis
- #4. Review for Hardcoded Secrets
- #5. Run with Language-Provided Checks and Protection
- #6. Black Box Test Cases
- #7. Code-Based Test Cases
- #8. Historical Test Cases
- #9. Fuzzing
- #10. Web Application Scanning
- #11. Check Included Software Components

# HCD Security Guidelines

# Liaison Status

# Trusted Computing Group (TCG)

- **Next TCG Members Meetings**
  - **TCG Hybrid F2F (New Orleans, LA) – 25-27 October 2022 – Ira to call in**
  - **TCG Hybrid F2F (TBD location) – February 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)**
  - **Informal – 3GPP, GSMA, IETF, ISO, ITU-T, SAE, US NIST**
  - ***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 PC Client Platform Physical Presence Interface – review July 2022***
  - ***TCG Measurement and Attestation Roots (MARS) Library – review July 2022***
  - ***TCG DICE Endorsement Architecture for Devices – review May 2022***
  - ***TCG Endorsement Key (EK) Credential Profile to TPM 2.0 – review March 2022***

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

- **Next IETF Members Meetings**
  - **IETF 115 Hybrid F2F (London, UK) 7-11 November 2022 – Ira to call in**
  - **IETF 116 Hybrid F2F (Yokohama, Japan) – 27-31 March 2023 – Ira to call in**
- **Transport Layer Security (TLS)**
  - **IETF Exported Authenticators in TLS – RFC 9261 – July 2022**
    **https://datatracker.ietf.org/doc/rfc9261/**
  - **IETF Importing External Pre-Shared Keys (PSKs) for TLS 1.3 – RFC 9258 – July 2022**
    **https://datatracker.ietf.org/doc/rfc9258/**
  - **IETF Guidance for External Pre-Shared Key (PSK) Usage in TLS – RFC 9257 – July 2022**
    **https://datatracker.ietf.org/doc/rfc9257/**
  - **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 Flags Extension for TLS 1.3 – draft-10 – July 2022**
    **https://datatracker.ietf.org/doc/draft-ietf-tls-tlsflags/**
  - **IETF Well-known URI for Publishing ECHConfigList Values – draft-00 – July 2022**
    **https://datatracker.ietf.org/doc/draft-ietf-tls-wkech/**
  - **IETF Compact TLS 1.3 – draft-06 – July 2022**
    **https://datatracker.ietf.org/doc/draft-ietf-tls-ctls/**
  - **IETF IANA Registry Updates for TLS/DTLS – draft-01 – July 2022**
    **https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8447bis/**
  - **IETF Return Routability Check for DTLS 1.2/1.3 – draft-06 – July 2022**
    **https://datatracker.ietf.org/doc/draft-ietf-tls-dtls-rrc/**
  - **IETF Secure Negotiation of Incompatible Protocols in TLS - draft-02 – June 2022**
    **https://datatracker.ietf.org/doc/draft-ietf-tls-snip/**
  - **IETF Delegated Credentials for (D)TLS – draft-15 – June 2022 – IETF LC**
    **https://datatracker.ietf.org/doc/draft-ietf-tls-subcerts/**

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

- **Security Automation and Continuous Monitoring (SACM)**
  - **IETF SACM WG – closed July 2022 – IETF Security ADs https://mailarchive.ietf.org/arch/msg/sacm/3UYKoLiQWA2h6CbIxBbCXGG6Qi4/**
  - **IETF Concise Software Identifiers – draft-22 – July 2022 – RFC Editor 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 CBOR Tags for Time, Duration, and Period – draft-01 – July 2022 https://datatracker.ietf.org/doc/draft-ietf-cbor-time-tag/**
  - **IETF Packed CBOR – draft-07 – July 2022 https://datatracker.ietf.org/doc/draft-ietf-cbor-packed/**
  - **IETF Notable CBOR Tags – draft-07 – July 2022 https://datatracker.ietf.org/doc/draft-bormann-cbor-notable-tags/**
  - **IETF Storing CBOR on Stable Storage – draft-12 – May 2022 – RFC Editor https://datatracker.ietf.org/doc/draft-ietf-cbor-file-magic/**
  - **IETF Using CDDL for CSVs – draft-00 – February 2022 https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-csv/**
  - **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 RATS Architecture – draft-20 – July 2022 – IETF LC**
    **https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/**
  - **IETF CBOR Tag for Unprotected CWT Claims Sets – draft-03 – July 2022**
    **https://datatracker.ietf.org/doc/draft-ietf-rats-uccs/**
  - **IETF Concise Reference Integrity Manifest – draft-03 – July 2022**
    **https://datatracker.ietf.org/doc/draft-birkholz-rats-corim/**
  - **IETF Direct Anonymous Attestation for RATS – draft-01 – July 2022**
    **https://datatracker.ietf.org/doc/draft-ietf-rats-daa/**
  - **IETF Entity Attestation Token (EAT) – draft-14 – July 2022 – WG LC**
    **https://datatracker.ietf.org/doc/draft-ietf-rats-eat/**
  - **IETF Time-Based Uni-Directional Attestation – draft-07 – July 2022**
    **https://datatracker.ietf.org/doc/draft-birkholz-rats-tuda/**
  - **IETF Entity Attestation Token (EAT) Collection Type – draft-01 – June 2022**
    **https://datatracker.ietf.org/doc/draft-frost-rats-eat-collection/**
  - **IETF Concise TA Stores (CoTS) – draft-00 – June 2022**
    **https://datatracker.ietf.org/doc/draft-wallace-rats-concise-ta-stores/**
  - **IETF EAT Media Types – draft-00 – May 2022**
    **https://datatracker.ietf.org/doc/draft-lundblade-rats-eat-media-type/**
  - **IETF YANG Data Model for CHARRA using TPMs – draft-21 – May 2022 – RFC Editor**
    **https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/**
  - **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 – draft-01 – April 2022**
    **https://datatracker.ietf.org/doc/draft-tschofenig-rats-aiss-token/**
  - **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/**

# 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 Key Blinding for Signature Schemes – draft-02 – August 2022**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-signature-key-blinding/**
  - **IRTF Oblivious PRFs w/ Prime-Order Groups – draft-12 – August 2022**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-voprf/**
  - **IRTF Verifiable Random Functions (VRFs) – draft-14 – July 2022**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-vrf/**
  - **IRTF CPace, a balanced composable PAKE – draft-06 – July 2022**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-cpace/**
  - **IRTF Usage Limits on AEAD Algorithms – draft-05 – July 2022**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-aead-limits/**
  - **IRTF Two-Round Threshold Schnorr Signatures with FROST – draft-07 – July 2022**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-frost/**
  - **IRTF Verifiable Distributed Aggregation Functions – draft-02 – July 2022**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-vdaf/**
  - **IRTF BBS Signature Scheme – draft-01 – July 2022**
    **https://datatracker.ietf.org/doc/draft-looker-cfrg-bbs-signatures/**
  - **IRTF OPAQUE Asymmetric PAKE Protocol – draft-09 – July 2022**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-opaque/**
  - **IRTF BLS Signatures – draft -05 – June 2022**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-bls-signature/**
  - **IRTF Hashing to Elliptic Curves – draft-16 – June 2022**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve/**
  - **IRTF SPAKE2+, an Augmented PAKE – draft-08 – May 2022**
    **https://datatracker.ietf.org/doc/draft-bar-cfrg-spake2plus/**

# Next Steps – IDS WG

- Next IDS WG Meeting– September 8, 2022
- Next IDS Face-to-Face Meeting November 15-17, 2022 at next PWG F2F
- Start looking at involvement in some of these other standards activities individually and maybe as a WG

# Backup