The Printer Working Group

Imaging Device Security

February 9, 2022

PWG February 2022 Virtual Face-to-Face

Agenda

When	What
10:00 – 10:10	Introductions, Agenda review
10:10 – 11:05	Discuss results of latest HCD iTC Meetings and HCD cPP/SD v1.0 status
11:05 – 11:20	Cybersecurity Executive Order Follow-up
11:20 – 11:35	HCD Security Guidelines v1.0 Status
11:35 – 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 November 4, 2021 HCD iTC meetings have been held on:
  - November 8th, 15th, 22nd, 29th
  - December 6th, 13th
  - January 10th, 17th, 24th
  - February 6th

HCD cPP/SD Status

- Released 2nd Public Review draft of the HCD cPP (v0.11 dated 12/14/2021) on 12/14/2021
  - To date, have received 76 comments against the 2nd Public Draft of the HCD cPP
    - Not all are editorial; many are technical comments
  - 31 of the 76 comments have been adjudicated by the HCD iTC
  - Tally for the comments against the 2nd Public Draft of the HCD cPP that have been adjudicated:
    - 28 Comments Accepted
    - 0 Comments Accepted in Principle but will be addressed in the Final Draft
    - 1 Comment Deferred to be addressed by the HCD iTC a future version
    - 2 Comments Not Accepted or Rejected

HCD cPP/SD Status

- 2nd Public Draft of the HCD SD still in development
- Addressing comments against 1st Public Review draft of the HCD SD (v0.91 dated 10/08/2021) released on 10/13/21
  - Received 29 comments against the 1st Public Draft of the HCD SD
  - All 29 comments have been adjudicated by the HCD iTC
  - Tally for the comments against the 1st Public Draft of the HCD cPP that have been adjudicated:
    - 25 Comments Accepted
    - 0 Comments Accepted in Principle but will be addressed in the Final Draft
    - 0 Comments Deferred to be addressed by the HCD iTC in a future version
    - 3 Comments Not Accepted or Rejected
    - 1 Comment on hold pending discussion with ITSCC

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

- Added a note for the optional Organizational Security Policy Purge in Section 3.5.7 indicating that Cryptographic Erase is not included in this optional requirement because it is covered in the mandatory requirement of FCS_CKM_EXT.4 and FCS_CKM.4.
- Replaced the text of the Application Note for SFR **FPT_KYP_EXT.1 Extended: Protection of Key and Key Material** in the 1st Public Draft to add clarity to what the Application Note was trying to convey.
- Removed the part of the sentence in the application note in SFR **FCS_KYC_EXT.1.1** (**Key Chaining**) that talks about "keys in areas of protected storage" because keys in areas of protected storage are already discussed in SFR **FPT_KYP_EXT.1 Protection of Key and Key Material** in a superior way.
- Clarified via an addition to the Application Note that the scope of TST Testing for SFR **FPT_TST_EXT.1 TSF testing** is focused on correct operation of the cryptographic function and detection of malfunctions, since the integrity of the executable code can be guaranteed by SFR **FPT_SBT_EXT Secure Boot**

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

- Clarified that the requirement in SFR **FPT_SBT_EXT Secure Boot** to use the chain(s) of trust to confirm integrity of its firmware/software using one or more of the selected methods applies only at boot time.
- Clarified that support for TLS Mutual Authentication and DTLS Mutual Authentication, whether as a client or as a server, are optional in all cases.
- Corrected numerous incorrect references, External Component Definitions and header information for several SFRs.
- Clarified that SFRs **FIA_X509_EXT.1 X.509 Certificate Validation and FIA_X509_EXT.2 X.509 Certificate Authentication** must be selected (they are both Selection-Based Requirements) if 'X.509 Certificate' is selected in **FPT_TUD_EXT.1.3 (Trusted Update).**
- Added AES bit selection option to SFR **FCS_COP.1.1/StorageEncryption.**

Current HCD cPP/SD Issues

Inclusion of Cryptographic Erase in HCD cPP

- JISEC felt Cryptographic Erase is 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 agrees 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 to replace the current FDP_RIP.1/PURGE SFR that is still undergoing HCD iTC review
  - This new SFR requires 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

- Resolving all open comments to prepare and release of 2nd Public Draft of HCD SD and Final Drafts of both the HCD cPP and HCD SD
  - Key holdup to 2nd Public Draft of HCD SD was addressing ITSCC (Korean Scheme) request to add substantive additional testing to Assurance Activities for several cryptographic SFRs
    - Was resolved at 2/6 HCD iTC Meeting
  - Final Drafts have to have "full content" for both documents
- Inclusion of NTP
  - Concern ND cPP requirements for NTP constitute requirement for "secure NTP"
  - Not sure all vendors support "secure NTP"
  - Still strongly feel it should be included in Version 1.0
- Should the Secure Boot SFR FPT_SBT_EXT properly address hardware-based Roots of Trust stored in mutable memory as well as immutable memory as currently stated
  - HCD iTC decided to address this issue in future versions of HCD cPP

Other HCD cPP/SD Issues

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

- Internationalization of SFRs
- Closure of "deferred" comments
  - Update of spec/standard versions – when and if it should be done
  - Need to be concerned about implications of updating versions
  - 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
- What issues will be moved to later versions of the HCD cPP/SD
  - Example - TLS 1.3 will not be in HCD cPP/SD v1.0

Other Current 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 has "in the pipeline" at this time unless either:
  - They are requested by JISEC or ITSCC or NIAP
  - They are suggested by JBMIA
  - Necessitated by comments to 2nd Public Drafts
  - Necessitated by any new NIAP TDs to either the HCD PP or any applicable ND & FDE cPPs/SDs
- Given the current known schedules, syncing with applicable updates to ND cPP/SD and FDE cPPs/SDs is probably not going to be needed 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** • Submit 2nd Public Draft: 12/13 • Review 2nd Public Draft: 12/13 – 1/31/22 (49d) • Review comments and update documents: 2/1/22 – 4/1/22(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 – Now Expected around 2/18/22 Comments due by 3/18/22 (~one month)
Final Draft	**New Proposed Schedule** • Submit Final Draft: 4/4/22 • Review Final Public Draft: 4/4/22 – 5/2/22 (28d) • Review comments and update documents: 5/2/22 - 5/12/22 (10d)	Was 1/17/22 on original schedule Expect HCD cPP to meet proposed schedule within a week or two Expect HCD SD to be up to two months behind proposed schedule
Final Document Published	**New Proposed Schedule** • Publish Version 1.0: 5/13/22	Was 3/25/22 on original schedule Current planned publish date is 4/25/22 Current expected publish date is likely in July 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
- Inclusion of ALC_FLR.*
- Incorporate, as applicable, the changes to ISO 15408, particularly any relevant new SFRs in the updated Part 2
- Impacts from EUCC and Cybersecurity Executive Order
- Support for SNMPv3
- Support for Wi-Fi and maybe Bluetooth
- Support for NFC
- Support for Security Information and Event Monitoring (SIEM) and related systems
- Expand to address 3D printing
- Support for new crypto algorithms
- Updates due to changes from ISO, FIPS or NIST Standards/Guidelines, NIAP TDs, or CCDB Crypto WG
- Indirect updates based on new technologies or customer requests

HCD iTC Status
Key Next Steps

- Address all the comments against the 2nd Public Drafts and Final Drafts
- Finalize all new content for v1.0
- Determine "parking lot" issues for later versions of the HCD cPP/SD (e.g., TLS 1.3 support and support for RoTs stored in mutable code)
- Add all agreed-upon SFRs and Assurance Activities into the HCD cPP and SD
  - Will be completed by the Final Draft
- Submit 2nd Public Draft and 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
- **After Jan 1, start thinking about creating an Interpretation Team for maintaining HCD cPP/SD v1.0 and start planning for next HCD cPP/SD update (whether it is v1.x or v2.0)**

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

- You have to be aggressive in the way you attack a problem or you will never get done
- No matter when you think you've finished solving a problem, you'll find that you're not finished at all
- Standards work takes a lot of patience
- You have to rely on a same core group of dedicated volunteers or you'll never get it done

Executive Order on Improving the Nation's Cybersecurity – Follow-up

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
   - Make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life.
   - 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)).

Actions Taken Since Cybersecurity Executive Order Was Issued

- NIST defined "critical software" as:

  any software that has or has direct software dependencies upon, one or more components with at least one of these attributes:

  - *Software that is designed to run with elevated privilege or manage privileges;*
  - *Software that has direct or privileged access to networking or computing resources;*
  - *Software that is designed to control access to data or operational technology;*
  - *Software that performs a function critical to trust; or operates outside of normal trust boundaries with privileged access.*

- National Telecommunications and Information Administration (NTIA) defined the minimum elements of a Software Bill of Materials (SBOM) to be:
  - Required data fields (e.g., "supplier name," "component name," and "cryptograph hash of the component,")
  - Operational considerations - a set of operational and business decisions and actions that establish the practice of requesting, generating, sharing, and consuming SBOMs
  - Support for automation - support relates to whether the SBOM can be automatically generated and is machine-readable.

Actions Taken Since Cybersecurity Executive Order Was Issued

- NIST Publishes Guidelines Recommending Minimum Standards for Vendor Verification of Their Software Source Codes
  - Consists of Technique Classes - (1) Threat Modeling; (2) Automated Testing; (3) Code-Based (Static) Analysis; (4) Dynamic Analysis; (5) Check Included Software; and (6) Fix Bugs
  - Each of these Technique Classes includes one or more specific techniques.
- NIST released the final version of NISTIR 8259B, "IOT Non-Technical Supporting Capability Core Baseline".
  - Complements NISTIR 8259A, "Core Device Cybersecurity Capability Baseline (May 2020), which is NIST's guide to the technical aspects of manufacturing secure Internet of Things ("IOT") devices and products.
  - Describes four recommended non-technical supporting capabilities related to the lifecycle of cybersecurity management that manufacturers should implement, including (1) documentation, (2) information and query reception, (3) information dissemination, and (4) education and awareness
  - NISTIR 8259A and NISTIR 8259B are intended to define a baseline set of activities that manufacturers should undertake during the planning, development, and operational life of IOT devices to address the cybersecurity needs and goals of their customers.

Actions Taken Since Cybersecurity Executive Order Was Issued

- NIST Publishes Preliminary Guidelines for Enhancing Software Supply Chain Security - NIST Special Publication 800-161 Revision 1

  Three targeted initiatives:

  - Critical Software Definition and Security Measures;
  - Recommended Minimum Standard for Vendor or Developer Verification of Code; and
  - Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software
- NIST Issues Three Guidance Documents on Cloud Security
  - The Second Draft NIST Internal Report (IR) 8320, "Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases"
  - Draft NIST IR 8320B, "Hardware-Enabled Security: Policy-Based Governance in Trusted Container Platforms"
  - Draft NIST Publication (SP) 1800-19, "Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments."
  - These documents provide guidance on practices, techniques, and technologies for securing data in connection with various cloud services

Actions Taken Since Cybersecurity Executive Order Was Issued

- NIST released a draft Secure Software Development Framework (Draft SSDF) at the end of September 2021 - Draft NIST Special Publication 800-218, Version 1.1
  - Consists of a core set of high-level secure software development practices that can be integrated into software development life cycles
- Cybersecurity and Infrastructure Security Agency (CISA) Published Cybersecurity Incident Response and Vulnerability Response Playbooks – one for incidence response and one for vulnerability response
  - Incident Response Playbook covers incidents that involve confirmed malicious cyber activity and for which a "major incident" (as defined by the Office of Management and Budget) has been declared or not yet reasonably ruled out.
    - Provides Federal Civilian Executive Branch (FCEB) agencies with a standard set of procedures to identify, coordinate, remediate, recover, and track mitigations from incidents affecting FCEB systems, data, and networks
  - Vulnerability Response Playbook applies to any vulnerability "that is observed to be used by adversaries to gain unauthorized entry into computing resources."
    - Sets forth standard, high-level processes and practices that FCEBs should follow when responding to vulnerabilities that pose significant risk

Actions Taken Since Cybersecurity Executive Order Was Issued

- NIST Issues Draft Criteria for Consumer Software Cybersecurity Labeling
  - Describes the baseline technical criteria as a series of attestations, i.e., claims made about the software associated with the label. I
  - Organizes these attestations into the following categories: (1) Descriptive Attestations, such as who is making the claims in the label, what the label applies to, and how consumers can obtain other supporting information; (2) Secure Software Development Attestations, such as how the software provider adheres to accepted secure software development practices throughout the software development cycle; (3) Critical Cybersecurity Attributes and Capability Attestations, and (4) Data Inventory and Protection Attestations, including declarations concerning the data that is processed, stored, or transmitted by the software.
- NIST Publishes Security Guidance for Internet of Things Devices
  - Establishing IoT Device Cybersecurity Requirements (NIST Special Publication (SP) 800-213) - overviews areas of consideration for organizations when determining the applicable cybersecurity requirements for an IoT device
  - Revised IOT Device Cybersecurity Requirements Catalog (NIST SP 800-213A) - contains controls similar to those in NIST SP 800-53 that can be selected in categories such as Data Protection, Software Update, Cybersecurity State Awareness and Device Security

HCD Security Guidelines Status

Liaison Status

Trusted Computing Group (TCG)

- **Next TCG Members Meetings**
  - **TCG Virtual F2F – 21-25 February 2022 – Ira to call in**
- **Trusted Mobility Solutions (TMS) – Ira is co-chair and co-editor**
  - **Formal – GP (TEE, SE), ETSI (NFV/MEC), ATIS (5G Security)**
  - **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), ATIS (5G Security)**
  - ***TCG Mobile Reference Architecture v2 – work-in-progress for review Q1 2022***
  - ***TCG TPM 2.0 Mobile Common Profile – work-in-progress for review Q1 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 Guidance on Integrity Measurements & Event Log – review January 2022***
  - ***TCG Guidance on Secure Industrial Control Systems – published January 2022***
  - ***TCG SNMP MIB for TPM-Based Attestation – published January 2022***
  - ***TCG Measurement and Attestation RootS (MARS) – review January 2022***
  - ***TCG TSS 2.0 Enhanced System API (ESAPI) – published October 2021***

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

- **Next IETF Members Meetings**
  - **IETF 113 Hybrid F2F (Vienna, Austria) – 21-25 March 2022 – Ira to call in**
  - **IETF 114 Hybrid F2F (Philadelphia, USA) – 25-29 July 2022 – Ira to call in**
- **Transport Layer Security (TLS)**
  - **IETF Deprecating MD5 and SHA-1 in TLS 1.2 and DTLS 1.2 – December 2022 https://datatracker.ietf.org/doc/rfc9155/**
  - **IETF Deprecating TLS 1.0 and TLS 1.1 – RFC 8996 – March 2021 https://datatracker.ietf.org/doc/rfc8996/**
  - **IETF Hybrid key exchange in TLS 1.3 – draft-04 – January 2022 https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/**
  - **IETF Guidance for External PSK Usage in TLS – draft-05 – January 2022 Guidance for External PSK Usage in TLS**
  - **IETF Flags Extension for TLS 1.3 - draft-08 – January 2022 – WG LC https://datatracker.ietf.org/doc/draft-ietf-tls-tlsflags/**
  - **IETF Return Routability Check for DTLS – draft-04 – December 2021 https://datatracker.ietf.org/doc/draft-ietf-tls-dtls-rrc/**
  - **IETF TLS Resumption across Server Names – draft-02 – December 2021 https://datatracker.ietf.org/doc/draft-ietf-tls-cross-sni-resumption/**
  - **IETF TLS 1.3 (errata update) – draft-03 – October 2021 https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8446bis/**
  - **IETF Compact TLS 1.3 – draft-04 – October 2021 https://datatracker.ietf.org/doc/draft-ietf-tls-ctls/**
  - **IETF Guidance for Ext PSK in TLS - draft-03 – October 2021 – IETF LC https://datatracker.ietf.org/doc/draft-ietf-tls-external-psk-guidance/**

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

- **Security Automation and Continuous Monitoring (SACM)**
  - **IETF Concise Software Identifiers – draft-20 – January 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-07 – December 2021**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-file-magic/
  - **IETF Feature Freezer for CDDL – draft-09 – December 2021**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-freezer/
  - **IETF App Literals in CBOR Ext Diagnostic – draft-00 – October 2021**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-edn-literals/
  - **IETF Notable CBOR Tags – draft-04 – August 2021**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-notable-tags/
  - **IETF Packed CBOR – draft-03 – August 2021**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-packed/

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

- **Remote ATtestation ProcedureS (RATS)**
  - **IETF TPM-based Network Device RIV – draft-11 – January 2022 – IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-rats-tpm-based-network-device-attest/
  - **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/
  - **IETF YANG Data Model for CHARRA using TPMs – draft-12 – January 2022 – IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/
  - **IETF CBOR Tag for Unprotected CWT Claims Sets – draft-02 – January 2022**
    https://datatracker.ietf.org/doc/draft-ietf-rats-uccs/
  - **IETF Time-Based Uni-Directional Attestation – draft-06 – January 2022**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-tuda/
  - **IETF Trustworthiness Vectors for SUIT – draft-03 – January 2022**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-suit-claims/
  - **IETF RATS Architecture – draft-14 – December 2022 – WG LC**
    https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/
  - **IETF Attestation Results for Secure Interactions – draft-01 – December 2021 – WG adopted**
    https://datatracker.ietf.org/doc/draft-ietf-rats-ar4si/
  - **IETF Direct Anonymous Attestation for RATS – draft-00 – December 2021 – WG adopted**
    https://datatracker.ietf.org/doc/draft-ietf-rats-daa/
  - **IETF ARM PSA Attestation Verifier Endorsements – draft 00 – November 2021**
    https://datatracker.ietf.org/doc/draft-fdb-rats-psa-endorsements/
  - **IETF Entity Attestation Token (EAT) – draft-11 – October 2021**
    https://datatracker.ietf.org/doc/draft-ietf-rats-eat/
  - **IETF Use TEE Identification in EAP-TLS – draft-03 – October 2021**
    https://datatracker.ietf.org/doc/draft-chen-rats-tee-identification/
  - **IETF Attestation Event Stream Subscription – draft-00 – October 2021**
    https://datatracker.ietf.org/doc/draft-ietf-rats-network-device-subscription/
  - **IETF Trusted Path Routing – draft-04 – September 2021**
    https://datatracker.ietf.org/doc/draft-voit-rats-trustworthy-path-routing/

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

- **IRTF Crypto Forum Research Group (CFRG) – future algorithms**
  - **IRTF Argon2 password hash and proof-of-work – RFC 9106 – September 2021**
    https://datatracker.ietf.org/doc/rfc9106/
  - **IRTF CPace, a balanced composable PAKE – draft-05 – January 2022**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-cpace/
  - **IRTF SPAKE2+, an Augmented PAKE – draft-04 – January 2022**
    https://datatracker.ietf.org/doc/draft-bar-cfrg-spake2plus/
  - **IRTF SPAKE2, a PAKE – draft-25 – December 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-spake2/
  - **IRTF OPAQUE Asymmetric PAKE Protocol – draft-07 – October 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-opaque/
  - **IRTF OPRFs using Prime-Order Groups – draft-08 – October 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-voprf/
  - **IRTF Verifiable Distributed Aggregation Functions – draft-00 – October 2021**
    https://datatracker.ietf.org/doc/draft-patton-cfrg-vdaf/
  - **IRTF Hashing to Elliptic Curves – draft-12 – September 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve/
  - **IRTF Hybrid Public Key Encryption – draft-12 – September 2021 – to IRSG review**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-hpke/
  - **IRTF KangarooTwelve - draft-06 – to CFRG Last Call – August 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-kangarootwelve/
  - **IRTF Two-Round Threshold Signatures with FROST – draft-01 – August 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-frost/
  - **IRTF Ristretto255 and Decaf448 Groups – draft-01 – August 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-ristretto255-decaf448/
  - **IRTF RSA Blind Signatures – draft-02 – August 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-rsa-blind-signatures/
  - **IRTF Pairing-Friendly Curves – draft-10 – July 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-pairing-friendly-curves/

Next Steps – IDS WG

- Next IDS WG Meeting– Feb 17, 2022
- Next IDS Face-to-Face Meeting May 10-13, 2022 (probably May 12th) at next PWG F2F
- Start looking at involvement in some of these other standards activities individually and maybe as a WG