
# The Printer Working Group

## Imaging Device Security

February 10, 2021

PWG February 2021 Virtual Face-to-Face

# Agenda

| When | What |
|---|---|
| 9:45 – 9:50 | Introductions, Agenda review |
| 9:50 – 11:05 | Discuss results of latest HCD iTC Meetings and HCD cPP/SD v1.0 status |
| 11:05 – 11:20 | HCD Security Guidelines v1.0 Status |
| 11:20 – 11:40 | TCG/IETF/Linux Foundation Liaison Reports |
| 11:40 – 11:45 | 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)

- HCD iTC formally approved by Common Criteria Management Committee in Feb 2020

- Key HCD iTC Officers:
  - Chairperson – Kwangwoo Lee, HP
  - Deputy Chairperson – Alan Sukert
  - CCDB Liaison - Eunkyoung Yi, Korean Scheme
  - Editors – Alan Sukert; Brian Volkoff, Ricoh; Geraldo Colunga, HP
  - Record Manager – TBD (Kwangwoo Lee acting for now)

# HCD international Technical Community (iTC)

- Agreed to hold bi-weekly meetings. However, to resolve comments against the draft HCD collaborative PP (cPP) and Supporting Document (SD), went to weekly meeting.
- Since last IDS F2F on November 4, 2020 meetings have been held on:
  - November 9, 16, 23 & 30, 2020
  - December 7 & 14, 2020
  - January 4. 11. 18 & 25, 2021
  - February 1 & 8, 2021

# HCD cPP/SD Status

- Released 2nd internal draft of the HCD cPP v1.0 on 11/17/2020
  - Received 15 comments against 2nd draft HCD cPP version
  - All comments have been adjudicated by the HCD iTC
  - Final tally:
    - 13 Comments Accepted
    - 1 Comment Accepted in Principle but will be addressed in a later v1.0 draft
    - 1 Comment Deferred to be addressed by the HCD iTC at a later point in time

# HCD cPP/SD Status

- Released 2nd internal draft of the HCD SD v1.0 on 11/19/2020
  - Received 30 comments against that draft HCD SD version
  - All comments have been adjudicated by the HCD iTC
  - Final tally:
    - 24 Comments Accepted
    - 0 Comments Accepted in Principle to be addressed in a later v1.0 draft
    - 5 Comments Deferred to be addressed by the HCD iTC at a later point in time
    - 1 Comment Not Accepted

# HCD cPP/SD Status
# HCD iTC Network Subgroup

- Is a Network Subgroup of the HCD iTC looking at what to do with the functional and assurance requirements for the four Secure Protocols – IPsec, TLS, SSH and HTTPS – in HCD cPP/SD v1.0 and the SFRs that are the dependencies to the four secure protocols

Key recommendations from the HCD iTC Network Subgroup:

- Use the IPsec, TLS, SSH and HTTPS requirements taken from ND cPP v2.2e / ND SD v2.2 **as the basis** for the SFRs/assurance activities in HCD cPP/SD v1.0 – That includes DTLS requirements
  - Splits both TLS and SSH requirements into separate server and client requirements
- Include TLS 1.3 in HCD cPP/SD v1.0 if ND does incorporate TLS 1.3 into the next published ND cPP/SD updates within the next year as the ND TLS Subgroup indicates it plans to do
  - However, latest ND iTC status is that TLS WG is stalled, so likelihood is it will not be ready in time to make v1.0

# HCD cPP/SD Status
# HCD iTC Network Subgroup

More Key recommendations from the HCD iTC Network Subgroup:

- IETF Transport Layer Security Working Group's is mandating deprecation of TLS 1.0 and TLS 1.1
  - Recommendation in v1.0 is to modify the ND TLSC/TLSS SFRs to make TLS v1.2 mandatory and TLS v1.1 optional
- Comparing the recently published CCUF Crypto Working Group's SSH Package against the ND cPP/SD, recommendation is to stay with the ND SSHS/SSHC SFRs/Assurance Activities, but pull in selected options and tests from some of the SSH Package SFRs/Assurance Activities
- Need to include the FIA_X509_EXT.* SFRs/Assurance Activities related to certificate evaluation
  - Are referenced in several of the ND SFRs and Assurance Activities such as DTLS

# HCD cPP/SD Status
# HCD iTC Network Subgroup

More key recommendations from the HCD iTC Network Subgroup:

- Are some cases where some SFRs or options in some SFRs and portions of Assurance Activities that are in the current draft HCD cPP/SD should be retained and incorporated into the corresponding ND cPP SFRs or ND SD Assurance Activities that become part of HCD cPP/SD v1.0
- Are some cases where options in some current HCD cPP SFRs will be lost when we switch to corresponding ND SFRs that are incorporated into HCD cPP v1.0
  - Need to make sure vendors are not negatively affected

# HCD cPP/SD Status
# HCD iTC Network Subgroup

More key recommendations from the HCD iTC Network Subgroup:

- Recommend that the following HCD cPP SFRs use the corresponding SFR and Assurance Activities taken from the ND cPP and SD rather than the current versions in the HCD cPP/SD:

| HCD cPP SFR | ND SFR |
|---|---|
| FCS_COP.1(a), Cryptographic Operation (Symmetric encryption/decryption | FCS_COP.1/Data Encryption (Cryptographic Operation (AES Data Encryption/ Decryption |
| FCS_CKM.1(a), Cryptographic Key Generation (for asymmetric keys) | FCS_CKM.1 Cryptographic Key Generation (for Asymmetric Keys) |
| FCS_COP.1(b), Cryptographic Operation (for signature generation/verification) | FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification) |
| FCS_COP.1(c) Cryptographic Operation (Hash Algorithm) | FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm) |
| FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication) | FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm/Keyed Hash Message Authentication) |
| FCS_RBG_EXT.1 Random Bit Generation | FCS_RBG_EXT.1 Random Bit Generation |

# HCD iTC Status
# Encryption of Non-Volatile Storage Devices

- Has been critical issue since October 2020
- Ricoh proposed that non-field replaceable non-volatile storage be allowed to store key material in clear text rather than be encrypted as long as the HCD had some type of "purge" function that would allow the key material to be deleted when the HCD was ready to be decommissioned or moved to another location
- Central to the issue is the Essential Security Requirements (ESR) document approved by the Common Criteria Development Board (CCDB) that contains the following requirement:

  "The HCD shall encrypt user document data and/or the HCD critical data (for confidentiality protection) stored on the nonvolatile storage device if it uses nonvolatile storage device for the purpose of storing those data. To support encryption, the HCD shall maintain key chains in such a way that keys and key materials are protected. Note that the initial data of the key chain stored on the nonvolatile storage device without protection do not meet the requirement"

# HCD iTC Status
## Encryption of Non-Volatile Storage Devices

- HCD iTC can change the ESR without requiring Common Criteria Development Board (CCDB) approval to allow the Ricoh proposal
  - However, might need approval of the Korean and Japanese Schemes
- HCD iTC concern is that it can't really address the issue properly until it can understand what the two Scheme's rationale was for this requirement and what this requirement really meant
- Sent request to the Korean Scheme for additional information – the following two slides provide the Korean Scheme's response

# HCD iTC Status
# Encryption of Non-Volatile Storage Devices

## Background

- We consider the a nonvolatile storage device contains sensitive data such as user document data and/or the HCD critical data.
- We consider both of use cases i) a Field-replaceable nonvolatile storage device can be taken out of operational environment, and ii) the HCD itself (includes either non-Field-replaceable or Field-replaceable nonvolatile storage device) can be taken out of operational environment.
- When a Field-replaceable nonvolatile storage device or the HCD itself is taken out of operational environment, sensitive data need to be protected from disclosure.
  - Note that our intention regarding Assumption "the physical security of the HCD" is strongly related to the operational environment.
  - When a Field-replaceable nonvolatile storage device or the HCD is taken out of operational environment, they are physically accessible.
- Thus, both of a Field-replaceable and non-Field-replaceable nonvolatile storage device are subject to protection.

## Interim outcomes

- For the reasons above, if 'purge' is appropriate measure to protection of a non-Field-replaceable nonvolatile storage device contained in the HCD which is taken out of operational environment, then we can consider the same level of security protection could be levied to a Field-replaceable nonvolatile storage device.
- But we do require more security protection requirements such as encryption.
- According to the Reference noted in the email, we assumed that the issue was raised due to the Essential Security Requirements "To support encryption, the HCD shall maintain key chains in such a way that keys and key materials are protected. Note that the initial data of the key chain stored on the nonvolatile storage device without protection do not meet the requirement".
- >> We heard that the iTC was discussing this issue from last year, and we would like to understand "how to protect" keys and key materials. Note that we do understand that "initial" key materials are the most difficult ones, and we do not require any specific mechanism for the protection of "initial" key materials.
- **We do expect that vendors suggest the "proper" level of the protection for "initial" key materials.**

# HCD iTC Status
## Encryption of Non-Volatile Storage Devices

- HCD iTC vendors submitted proposed ESR changes to address this issue which the full iTC have reviewed
- HCD iTC vendors tasked to determine what is the “proper" level of the protection for "initial" key material”

What Needs to Be Done to Resolve This Issue

- Update Security Problem Definition (SPD) and ESR to include the Use Case where the device is removed from the Operational Environment and user and critical data need to be protected
- Make a final decision on whether the ESR needs to change to address the non-field replaceable non-volatile storage issue

# HCD iTC Status
# Encryption of Non-Volatile Storage Devices

What Needs to Be Done to Resolve This Issue

- If the ESR does need to change:
  - Make a final decision on what is ESR changes (if any) are to be made
  - Make the appropriate ESR changes
  - Submit the changes to the Korean and Japanese Schemes for approval
  - Update the Security Problem Definition (SPD) to be consistent with the updated ESR

# HCD iTC Status
# Original Proposed Schedule for Publishing HCD cPP/SD Documentation

| Phase | Timeline | Description |
|---|---|---|
| Internal Draft | 1st working draft release : 2020.07.21 (Tue)<br>* Call for comment (SME) : 2020.07.21 (Wed) ~ 2020.08.17 (Mon) [4W]<br>* Comment resolution : 2020.08.18 (Tue) ~ 2020.09.22 (Tue) [5W]<br>* Editors works : 2020.09.23 (Wed))- 2020.10.19(Mon) [4W]<br>2nd working draft release : 2020.10.20 (Tue)<br>* Call for comment : 2020.10.20 (Tue) ~ 2020.11.16 (Mon) [4W]<br>* Comment resolution : 2020.11.17 (Tue) - 2020.12.18 (Fri) [4.5W]<br>* Editors works : 2020.12.19 (Sat) – 2021.2.1 (Mon) [5.5W]<br>(Editor's time off : End of 2020) | The normal, pre-release process for creating the working draft.<br><br>1st WD : Initial version - 2020.07.21<br>*- File name: HCD-CPP DRAFT 07-21-2020.pdf*<br>2nd WD : Ed, Ge, Te, New work item (at least title) – Date<br>*- File name: HCD-CPP DRAFT 10-20-2020.pdf*<br>Public Review Draft 1 : Ed, Ge, Te (**V0.6X**)<br>Public Review Draft 2 : Ed, (Ge, Te) (**V0.7X**)<br>[Optional] Public Review Draft 3 : Ed (**V0.8X**)<br>Proposed Draft : Ed (**V0.9X**)<br>Final Document Published (**V1.0**) |
| Public Review Draft 1 | 45 days<br>(2021.02.02 (Tue) ~ 2021.03.19 (Fri) | HCD-iTC has voted according to Terms of Reference to release this version for public review. Public (i.e. from non-iTC participants) comments are accepted during this period |
| Public Review Draft 1 Update | Up to 60 days<br>(2021.03.20 (Sat) ~ 2021.05.17 (Mon)) | The HCD-iTC will review all received comments and update the documents accordingly |
| Public Review Draft 2 | 45 days<br>(2021.05.18 (Tue) ~ 2021.07.01 (Thu)) | HCD-iTC has voted according to Terms of Reference to release this version for public review. Public (i.e. from non-iTC participants) comments are accepted during this period |
| Public Review Draft 2 Update | Up to 60 days<br>(2021.07.02 (Fri) ~ 2021.08.28(Sat)) | The HCD-iTC will review all received comments and update the documents accordingly |
| Proposed Draft | 30 days+<br>(2021.08.29 (Sun) ~ 2021.09.30(Thu)) | HCD-iTC has voted according to Terms of Reference to propose this as the final document. Public (i.e. from non-iTC participants) comments are accepted during this period |
| Proposed Update | 10 days+<br>(2021.10.01(Fri) ~ 2021.10.12 (Tue) | HCD-iTC reviews any further comments and prepares the document for final publishing (updating all dates, producing official versions for publication) |
| Final Document Published | | Documents are posted to Common Criteria Portal |

# HCD iTC Status
# Proposed New HCD cPP/SD Schedule

| Phase | Timeframe | Description |
|---|---|---|
| Resolve ESR Issue and Approve SPD | • Resolve ESR issue: 2/26<br>• Update ESR: 3/1 – 3/12<br>• Update SPD: 3/1 – 3/12<br>• Submit ESR changes to HCD WG (if needed): 3/15<br>• HCD WG Review and comment: 3/15 – 4/9<br>• Submit SPD for public review: 3/1<br>• SPD Public review: 3/1 – 3/26<br>• Update SPD and update cPP/SD: 3/29 – 4/16 | Assume get response back from HCD WG in no more that 30 days |
| Internal Draft | • Submit 3rd internal draft: 4/19<br>• Review 3rd internal draft: 4/19 – 5/14<br>• Review comments & update documents: 5/17 – 6/11 | Assume approval of ESR changes |
| Public Review Draft 1 | • Submit 1st Public Draft: 6/14<br>• Review 1st Public Draft: 6/14 – 7/23<br>• Review comments and update documents: 7/26- 9/17 | Must include all new SFRs that want to include in v1.0 |

# HCD iTC Status
# Proposed New HCD cPP/SD Schedule

| Phase | Timeframe | Description |
|---|---|---|
| Public Review Draft 2 | • Submit 2nd Public Draft: 9/20<br>• Review 2nd Public Draft: 9/20 – 10/29<br>• Review comments and update documents: 11/1 – 12/3 | |
| Final Draft | • Submit Final Draft: 12/6<br>• Review 2nd Public Draft: 12/6/21 – 1/14/22<br>• Review comments and update documents: 1/17/22 – 2/11/22 | |
| Final Document Published | • Publish Version 1.0: 2/14/22 | |

# HCD iTC Status
# HCD cPP/SD v1.0 Content

Additional Content definitely to be included beyond what was in the original HCD PP:

- Secure protocol SFRs and Assurance Activities from ND cPP/SD with some minor additions from current HCD cPP/SD drafts
- The SFRs shown on Slide 13 above that are the dependencies for the four secure protocols will use the corresponding ND SFRs/Assurance Activities
- FIA_X.509.* Certificate Validation SFRs
- Support for FIPS 140-3
- SFRs and Assurance Activities to support “hardware-anchored integrity of hardware/software”
- Removal of support for TLS 1.0

# HCD iTC Status
# HCD cPP/SD v1.0 Content

Additional Content highly likely to be included beyond what was in the original HCD PP:

- NTP Protocol
- FCS_CKM.2 Cryptographic Key Establishment
  - Is a dependency of the secure protocols in the ND cPP that is not an SFR in the HCD cPP so far
  - Will likely be recommended to be included by the Network Subgroup

Additional Content that "may" be included beyond what was in the original HCD PP:

- Removal of SHA-1 support
- Removal of support for cipher suites with RSA Key Generation with keys < 2048 bits
- Removal of support for all RSA and DHE Key Exchanges

# HCD iTC Status
# HCD cPP/SD v1.0 Content

Additional Content that will probably not be included beyond what was in the original HCD PP:

- Removal of support for TLS 1.1 (will likely make it optional)
- Support for TLS 1.3
- Expansion of network-fax separation to “no bridging”
- Inclusion of ALC_FLR
- NIAP TLS Package

Additional Content that will definitely not be included beyond what was in the original HCD PP:

- Wi-Fi
- SNMPv3 Support
- Kerberos Support
- S/MIME Support
- SMBv3 Support

# HCD iTC Status
# Additional Considerations in Developing HCD cPP/SD v1.0


- Comparisons with relevant FDE AA and FDE EE SFRs
- Syncing with applicable updates to ND cPP and FDE cPPs
- Syncing with any applicable NIST SP updates
- Inclusion of any applicable NIAP TDs to HCD PP and ND & FDE cPPs
- Syncing with ENISA and the new proposed European cybersecurity certification scheme (EUCC) and NIST Cybersecurity Framework
- Internationalization of SFRs

# HCD iTC Status
# Key Next Steps

- Address the “Non-volatile Storage” issue once and for all
- Agree on a revised schedule
- Finalize all new content for v1.0
- Add all new SFRs and Assurance Activities into the HCD cPP and SD
  - Goal is to complete this by the next Internal Draft
  - Has to be completed by the 1st Public Draft at the latest
- Submit all internal, public and final draft HCD cPPs and HCD SDs per the agreed schedule
- Review all comments and update the HCD cPP and HCD SD drafts per the agreed schedule
- Publish HCD cPP/SD v1.0

# HCD iTC Status
# What's After HCD cPP/SD v1.0

- Should we be planning for an HCD cPP/SD v1.1? If so, how soon after v1.0 – 6 months, 1 year, …?
  - If so, what should we include in HCD cPP/SD v1/1?
- Should we set up a regular schedule for major and minor HCD cPP/SD releases like the ND iTC has done?
- How quickly should we be forming an HCD iTC Interpretation (HIT?) Team and who should be on it?
- Should we be forming a separate HCD iTC Maintenance Team like the ND iTC did and who should be on it?

# HCD Security Guidelines Status

# Liaison Status

# Trusted Computing Group (TCG)

- **Next TCG Members Meetings**
  - **TCG Virtual F2F – 22-26 February 2021 – 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 Runtime Integrity Preservation for Mobile Devices – Nov 2019***
  - ***TCG Mobile Reference Architecture v2 – work-in-progress***
  - ***TCG TPM 2.0 Mobile Common Profile – work-in-progress***
  - ***GP Trusted Platform Services Client API – work-in-progress w/ TCG***
- **Recent Specifications**
  - **http://www.trustedcomputinggroup.org/resources**
  - ***TCG Canonical Event Log Format – review December 2020***
  - ***TCG Endorsement Key Credential Profile – review December 2020***
  - ***TCG Reference Integrity Manifest (RIM) Info Model – published Nov 2020***
  - ***TCG PC Client Reference Integrity Manifest – published November 2020***
  - ***TCG SMBIOS-based Component Class Registry – review November 2020***
  - ***TCG MARS Use Cases and Considerations – review October 2020***

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

- **Next IETF Members Meetings**
  - **IETF 110 Virtual F2F – 8-12 March 2021 – Ira to call in**
  - **IETF 111 San Francisco ??? – 26-30 July 2021 – Ira to call in**
- **Transport Layer Security (TLS)**
  - **TLS Certificate Compression – RFC 8879 – December 2020**
    **https://tools.ietf.org/html/rfc8879**
  - **Issues and Requirements for SNI Encryption in TLS – RFC 8744 – July 2020**
    **https://tools.ietf.org/html/rfc8744**
  - **TLS 1.3 Extension Cert-Based Auth w/ Ext PSK – RFC 8773 – March 2020**
    **https://tools.ietf.org/html/rfc8773**
  - **Applying GREASE to TLS Extensibility – RFC 8701 – January 2020**
    **https://tools.ietf.org/html/rfc8701**
  - **TLS/1.3 – RFC 8446 – August 2018**
    **https://tools.ietf.org/html/rfc8446**
  - **DTLS/1.3 – draft-40 – January 2021 – IETF LC**
    **https://datatracker.ietf.org/doc/draft-ietf-tls-dtls13/**
  - **Connection Identifiers for DTLS 1.2 – draft-09 – January**
    **https://datatracker.ietf.org/doc/draft-ietf-tls-dtls-connection-id/**
  - **TLS Encrypted Client Hello – draft-09- December 2020**
    **https://datatracker.ietf.org/doc/draft-ietf-tls-esni/**
  - **Deprecating TLSv1.0 and TLSv1.1 – draft-11 – December 2020 – IETF LC**
    **https://datatracker.ietf.org/doc/draft-ietf-tls-oldversions-deprecate/**
  - **TLS Resumption across Server Names – draft-00 – December 2020**
    **https://datatracker.ietf.org/doc/draft-ietf-tls-cross-sni-resumption/**
  - **Importing External PSKs for TLS – draft-06 – December 2020 – IETF LC**
    **https://datatracker.ietf.org/doc/draft-ietf-tls-external-psk-importer/**

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

- **Security Automation and Continuous Monitoring (SACM)**
  - **Concise Software Identifiers – draft-16 – November 2020 – to IETF LC**
    **https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/**
  - **SACM Architecture – draft-07 – September 2020**
    **https://datatracker.ietf.org/doc/draft-ietf-sacm-arch/**
  - **Endpoint Posture Collection Profile – draft-01 – February 2020 – to IETF LC**
    **https://datatracker.ietf.org/doc/draft-ietf-sacm-epcp/**
- **Concise Binary Object Representation (CBOR)**
  - **Concise Binary Object Representation (CBOR) – RFC 8949 – Sept 2020**
    **https://tools.ietf.org/html/rfc8949**
  - **CBOR Tags for Date – RFC 8943 – November 2020**
    **https://tools.ietf.org/html/rfc8943**
  - **CBOR Tags for Typed Arrays – RFC 8746 – February 2020**
    **https://tools.ietf.org/html/rfc8746**
  - **CBOR Sequences – RFC 8742 – February 2020**
    **https://tools.ietf.org/html/rfc8742**
  - **Concise Data Definition Language (CDDL) – RFC 8610 – June 2019**
    **https://tools.ietf.org/html/rfc8610 - JSON/CBOR schema**
  - **CBOR Tags for OIDs – draft-03 – November 2020**
    **https://datatracker.ietf.org/doc/draft-ietf-cbor-tags-oid/**
  - **Additional Control Operators for CDDL – draft-01 – November 2020**
    **https://datatracker.ietf.org/doc/draft-ietf-cbor-cddl-control/**
  - **Packed CBOR – draft-00 – September 2020**
    **https://datatracker.ietf.org/doc/draft-ietf-cbor-packed/**

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

- **Remote ATtestation ProcedureS (RATS)**
  - **RATS Architecture – draft-07 – October 2020**
    **https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/**
  - **Reference Interaction Models for RATS – draft-01 – October 2020**
    **https://datatracker.ietf.org/doc/draft-ietf-rats-reference-interaction-models/**
  - **Attestation Event Stream Subscription – draft-01 – October 2020**
    **https://datatracker.ietf.org/doc/draft-birkholz-rats-network-device-subscription/**
  - **YANG Data Model for CHARRA using TPMs – draft-03 – September 2020**
    **https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/**
  - **TPM-based Network Device RIV – draft-04 – September 2020**
    **https://datatracker.ietf.org/doc/draft-ietf-rats-tpm-based-network-device-attest/**
  - **Entity Attestation Token (EAT) – draft-04 – August 2020**
    **https://datatracker.ietf.org/doc/draft-ietf-rats-eat/**
  - **Trustworthiness Vectors for SUIT Workflow Model – draft-00 – July 2020**
    **https://datatracker.ietf.org/doc/draft-birkholz-rats-suit-claims/**
  - **Time-Based Uni-Directional Attestation – draft-03 – July 2020**
    **https://datatracker.ietf.org/doc/draft-birkholz-rats-tuda/**
  - **CBOR Tag for Unprotected CWT Claims Sets – draft-01 – June 2020**
    **https://datatracker.ietf.org/doc/draft-birkholz-rats-uccs/**
  - **Trusted Path Routing – draft-00 – June 2020**
    **https://datatracker.ietf.org/doc/draft-voit-rats-trustworthy-path-routing/**
  - **MUD-Based RATS Resources Discovery – draft-00 – March 2020**
    **https://datatracker.ietf.org/doc/draft-birkholz-rats-mud/**

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

- **IRTF Crypto Forum Research Group (CFRG) – future algorithms**
  - **Randomness for Security Protocols – RFC 8937 – October 2020**
    **https://datatracker.ietf.org/doc/rfc8937/**
  - **SPAKE2, a PAKE – draft-18 – January 2021**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-spake2/**
  - **Hybrid Public Key Encryption – draft-07 – December 2020 – to IRTF Chair**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-hpke/**
  - **Verifiable Random Functions (VRFs) – draft-08 – November 2020**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-vrf/**
  - **Pairing-Friendly Curves – draft-09 – November 2020**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-pairing-friendly-curves/**
  - **OPAQUE Asymmetric PAKE Protocol – draft-01 – November 2020**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-opaque/**
  - **Oblivious Pseudorandom Functions (OPRFs) – draft-05 – November 2020**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-voprf/**
  - **Hashing to Elliptic Curves – draft-10 – October 2020**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve/**
  - **The ristretto255 and decaf448 Groups – draft-00 – October 2020**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-ristretto255-decaf448/**
  - **KangarooTwelve – draft-04 – September 2020 – RG LC**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-kangarootwelve/**
  - **Usage Limits on AEAD Algorithms – draft-01 – September 2020**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-aead-limits/**
  - **Memory-hard Argon2 Password Hash – draft-12 – September 2020**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-argon2/**
  - **Cpace Balanced Composable PAKE – draft-00 – July 2020**
    **https://datatracker.ietf.org/doc/draft-irtf-cfrg-cpace/**

# Linux Foundation OpenPrinting (1 of 2)

- **Linux Foundation OP Google Summer of Code 2020**
  - **GSoC 2020 coding completed on 31 August 2020**
    **https://developers.google.com/open-source/gsoc**
- **Linux Foundation OP Google Season of Docs 2020**
  - **GSoD 2020 project completed on 5 December 2020**
    **https://developers.google.com/season-of-docs**
- **Linux Foundation OP Mentorship Program 2020**
  - **LFMP 2020 IPP Scan project completed in December 2020**
    **https://communitybridge.org/**
- **Linux Foundation OP New Website**
  - **OP website**
    **https://openprinting.github.io/**
  - **OP news**
    **https://openprinting.github.io/news/**
  - **OP website issues**
    **https://github.com/OpenPrinting/openprinting.github.io/issues**
  - **OP Driverless Printing w/ PWG IPP Everywhere™ logo**
    **https://openprinting.github.io/driverless/01-standards-and-their-pdls/**

# Linux Foundation OpenPrinting (2 of 2)

- **OpenPrinting Projects**
  - **CUPS OP v2.3.3op1 released on 27 November 2020**
    https://github.com/OpenPrinting/cups/releases/tag/v2.3.3op1
  - **PAPPL v1.0.0 released on 11 December 2020**
    https://github.com/michaelrsweet/pappl/releases/tag/v1.0.0
  - **CUPS Filters v1.28.7 released on 7 January 2021**
    https://github.com/OpenPrinting/cups-filters/releases/tag/1.28.7
  - **PostScript Printer Application – work-in-progress**
    https://github.com/OpenPrinting/ps-printer-app
- **Linux Foundation OP Google Summer of Code 2021**
  - **GSoC 2021 projects are TBD**
  - **GSoC 2021 timeline**
    - **Organization applications – 29 January to 19 February**
    - **Student applications – 29 March to 13 April**
    - **Application Review Period – 13 April to 17 May**
    - **Coding – 7 June to 16 August (reduced weekly hours)**
    - **Results Announced – 31 August**
- **Linux Foundation OP Google Season of Docs 2021**
  - **GSoD 2021 projects are TBD**
- **Linux Foundation OP Mentorship Program 2021**
  - **LFMP 2021 projects are TBD**

# Next Steps – IDS WG

- Next IDS Conference Call – Feb 18, 2021
- Next IDS Face-to-Face Meeting May 4-6, 2021 (probably May 5th) at next PWG Virtual F2F
- Start looking at involvement in some of these other standards activities individually and maybe as a WG