The Printer Working Group

Imaging Device Security

August 19, 2021

PWG August 2021 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	Executive Order on Cybersecurity
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 May 6, 2021 HCD iTC meetings have been held on:
  - May 10, 17 & 24
  - June 7, 14 & 21
  - July 5, 12, 19 & 26
  - August 2, 9 & 16

HCD cPP/SD Status

- Released 3nd internal draft of the HCD cPP v1.0 on 06/09/2021
  - To date, have received 184 comments against the 1st - 3rd drafts of the HCD cPP
  - All comments have been adjudicated by the HCD iTC
  - Tally for the comments received to date:
    - 132 Comments Accepted
    - 5 Comment Accepted in Principle but will be addressed in a later v1.0 draft
    - 37 Comments Deferred to be addressed by the HCD iTC at a later point in time
    - 10 Comments Not Accepted or Rejected

HCD cPP/SD Status

- Released 3rd internal draft of the HCD SD v1.0 on 06/29/2021
  - To date, have received 79 comments against the 1st - 3rd internal drafts of the HCD SD
  - So far 75 of the 79 comments have been adjudicated by the HCD iTC
  - Tally for the adjudicated comments to date:
    - 64 Comments Accepted
    - 1 Comment Accepted in Principle to be addressed in a later v1.0 draft
    - 10 Comments Deferred to be addressed by the HCD iTC at a later point in time
    - 0 Comments Not Accepted

Current HCD cPP/SD Issues
Addressing HW-Anchored Integrity Verification

- Is a requirement the HCD iTC had included in the Essential Security Requirements (ESR) document
- Deals with Hardware Roots of Trust and how to verify the integrity of the boot process for an HCD
- Status since the last IDS F2F:
  - Incorporated concept of Chains of Trust as well as Root of Trust
  - Completed work on a proposed Secure Boot SFR (FPT_SBT_EXT.1)and accompanying Assurance Activities to address integrity verification of multiple chains of trust, each with its own hardware-anchored Root of Trust
  - Proposed additional wording in the appropriate sections of the HCD cPP to go along with this new Secure Boot SFR
  - Completed work on a proposed crypto SFR and accompanying Assurance Activities taken from the Full Drive Encryption Engine cPP to address the use of CMAC for message authentication
  - Determined which SFR currently in the HCD cPP (FPT_SKP_EXT.1, Protection of TSF Data) to use to address the issue of protection of symmetric keys

HCD cPP/SD Status
Key Closed Issues

- Audit Log
  - Korean Scheme felt that (1) it is mandatory that the audit log be stored on device and (2) that it is mandatory, and not optional, that the audit log should be readable by a device interface
  - JISEC and NIAP concurred with the Korean scheme
  - HCD iTC agree to make the following Audit SFRs mandatory rather than optional:
    - FAU_SAR.1 Audit review
    - FAU_SAR.2 Restricted audit review
    - FAU_STG.1 Protected audit trail storage
    - FAU_STG.4 Prevention of audit data loss
- Agreed on deletion of TLS 1.0

Other Current HCD cPP/SD Issues

- Resolving all open and deferred comments to prepare and release of 1st Public Drafts of both the HCD cPP and HCD SD
- Inclusion of NTP
  - Concern ND cPP requirements for NTP constitute requirement for "secure NTP"
  - Not sure all vendors support "secure NTP"
- FPT_KYP_EXT.1 Protection of Key and Key Material SFR
  - JBMIA wants to change SFR, based on the corresponding SFR from the FDE EE cPP, to state requirements for how key and key material are to be protected to meet requirement in the ESR that "*To support encryption, the HCD shall maintain key chains in such a way that keys and key materials are protected*"
  - HCD iTC members and JBMIA still reworking the proposal for wording and clarity

Other HCD cPP/SD Issues

Issues HCD iTC still need to resolve:

- Closure of “deferred” comments
- 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
- Internationalization of SFRs
- Update of spec/standard versions – when and if it should be done
  - Need to be concerned about implications of updating versions

Other Current HCD cPP/SD Issues

Additional New Content (SFRs)

- Goal for HCD cPP/SD at the point is to "keep it simple" and build on it for later versions
- Pretty much a given that TLS 1.3 will not be in HCD cPP/SD v1.0
- Not anticipating picking up any additional new requirements for the HCD cPP/SD beyond what already has been proposed at this time unless either:
  - They are requested by JISEC or ITSCC
  - They are suggested by JBMIA
  - They are required by changes to ISO, FIPS or NIST Standards/Guidelines
  - Necessitated by comments to first Public Drafts
  - Necessitated by any new NIAP TDs to either the HCD PP or the applicable ND & FDE cPPs/SDs
  - Syncing with applicable updates to ND cPP and FDE cPPs or applicable NIST SP updates

HCD iTC Status
Updated Proposed HCD cPP/SD Schedule

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 **IN PROCESS**	
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 previous schedule Note: 1st Public Draft of HCD cPP available and undergoing final HCD iTC review; expect to be released around 8/26

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)	Was 10/25 on previous schedule
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 previous schedule
Final Document Published	**New Proposed Schedule** • Publish Version 1.0: 5/13/22	Was 3/25/22 on previous schedule

HCD iTC Status
Key Next Steps

- Agree on a proposed new updated schedule
- 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)
- Add all agreed-upon SFRs and Assurance Activities into the HCD cPP and SD
  - Goal is to complete this by the 2nd Public Draft
- Submit all internal, public and final draft HCD cPP and HCD SD per the agreed 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

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

- I didn’t realize until we were this far along the importance of establishing and maintaining a Work Plan with schedules
- Make sure every work product a team produces is available publicly to every iTC member at all times
- Make sure the team’s rules of operation are written down, well understood by all team members and **followed**
- Make sure there are minutes for all team meetings; you have no idea how often you need to go back and use minutes from previous meetings to see what was discussed

Executive Order on Improving the Nation's Cybersecurity

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)).

Executive Order on Improving the Nation's Cybersecurity

Key Areas Covered by this Executive Order:

2. Sharing Threat Information

- Within 60 days of the date of the Executive Order the Office of Management and Budget, in consultation with other named federal agencies, will make recommendations for contract language changes regarding sharing of threat information

3. Cyber Incident Reporting

- A government contractor that provides software or services would be required to report cyber incidents to the relevant federal agencies based upon a sliding scale of risk assessment, with the highest risk requiring notice within 3 days of discovery.
- Within 45 days (June 28), Homeland Security, in consultation with other named federal agencies, is directed to recommend changes to the FAR including the nature of the cyber incidents that would require reporting, the government contractors and service providers that would be covered, the time periods for reporting based on "a graduated scale of severity," and "appropriate and effective protections for privacy and civil liberties."

Executive Order on Improving the Nation's Cybersecurity

Key Areas Covered by this Executive Order:

4. Enhancing Software Supply Chain Security

- Within 30 days of the Order (June 11), NIST, in consultation with other named federal agencies, is directed to solicit "input from the Federal Government, private sector, academia, and other appropriate actors to identify existing or develop new standards, tools, and best practices for complying with the standards, procedures, or criteria. **The guidelines shall include criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices**"

Executive Order on Improving the Nation's Cybersecurity

Key Areas Covered by this Executive Order:

4. Enhancing Software Supply Chain Security

NIST shall issue guidance identifying practices that enhance the security of the software supply chain. Such guidance shall include standards, procedures, or criteria regarding:

(i) secure software development environments, including such actions a

- (A) using administratively separate build environments;
- (B) auditing trust relationships;
- (C) establishing multi-factor, risk-based authentication and conditional access across the enterprise;
- (E) employing encryption for data; and
- (F) monitoring operations and alerts and responding to attempted and actual cyber incidents;

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

(viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process;

(ix) attesting to conformity with secure software development practices;

Executive Order on Improving the Nation's Cybersecurity

Key Areas Covered by this Executive Order:

5. Other Topics Covered

- Modernizing federal government cybersecurity
- Establishing a Cyber Safety Review Board
- Standardizing the federal government's playbook for responding to cybersecurity vulnerabilities and incidents
- Improving detection of cybersecurity vulnerabilities and incidents on federal government networks
- Improving the federal government's investigative and remediation capabilities

Executive Order on Improving the Nation's Cybersecurity

Some Follow-up (Thanks to Ira):

- Department of Commerce and NTIS (National Telecommunications and Information Administration) announcement of minimum requirements for Software Bills of Materials (SBOMs) on software deliveries to the government - https://www.ntia.doc.gov/blog/2021/ntia-releases-minimum-elements-software-bill-materials
- NIST announcement of two key publications to enhance software supply chain security called for by May 2021 Executive Order for Cybersecurity - https://www.nist.gov/news-events/news/2021/07/nist-delivers-two-key-publications-enhance-software-supply-chain-security
- Announcement of NIST recommended minimum standards for vendor or developer verification (testing) of software based on the May 2021 Executive Order for Cybersecurity -https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/recommended-minimum-standards-vendor-or

HCD Security Guidelines Status

HCD Security Guidelines Agenda

- HCDSEC Current Status
- HCDSEC Development Plan
- Questions/Comments?

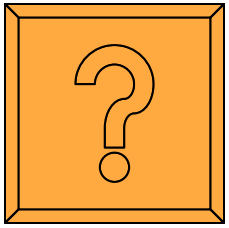
HCDSEC Current Status

- IDS Charter updated for HCDSEC project August 2019
- HCDSEC review at PWG February 2020 F2F
  - https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20200120.docx
- HCDSEC status at PWG May 2020 F2F
  - Development plan and priorities
- HCDSEC status update at PWG August 2020 F2F
  - Development plan and priorities
  - Network Security examples

HCDSEC Development Plan

- HCDSEC Interim draft in May 2021
  https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20210504.docx
  - Section 4 Network Security (additional content)
  - Section 12.2 Datalink Layer (Smith's Wi-Fi content)
- HCDSEC Interim draft in Q3 2021
  - Section 4 Network Security (additional content)
- HCDSEC Interim draft in Q4 2021
  - Section 5 Local Security (OS, Hypervisors, Peripherals, Apps)
  - Section 6 System Architecture (Firewall, AV, Process Isolation)
- HCDSEC Prototype draft in Q1/Q2 2022
  - Section 7 Conformance
  - Section 8 Internationalization Considerations
  - Section 9 Security Considerations
  - Section 10 References

IDS: HCDSEC Questions / Comments



Link to the HCD Security Guidelines Slides:
https://ftp.pwg.org/pub/pwg/ids/Presentation/ids-hcdsec-status-20210819.pptx
- PowerPoint
https://ftp.pwg.org/pub/pwg/ids/Presentation/ids-hcdsec-status-20210819.pdf
- PDF

Liaison Status

Trusted Computing Group (TCG)

- **Next TCG Members Meetings**
  - **TCG Virtual F2F – 11-15 October 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 for review Q4 2021***
  - ***TCG TPM 2.0 Mobile Common Profile – work-in-progress for review Q4 2021***
  - ***GP TPS Client API / Entity Attestation Protocol / COSE Keystore – joint work***
- **Recent Specifications**
  - **http://www.trustedcomputinggroup.org/resources**
  - ***TCG EK Credential Profile for TPM 2.0 – published July 2021***
  - ***TCG PCIe-based Component Class Registry – review July 2021***
  - ***TCG Storage SSC: Opal – review July 2021***
  - ***TCG Storage Interface Interactions Specification (SIIS) – review July 2021***
  - ***TCG SNMP MIB for TPM-based Attestation – review June 2021***
  - ***TCG TPM 2.0 Keys for Device Identity and Attestation – public May 2021***

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

- **Next IETF Members Meetings**
  - **IETF 112 Madrid, Spain ??? – 8-12 November 2021 – Ira to call in**
    – conflict w/ PWG Virtual F2F 9-11 November 2021
    – conflict w/ ESCAR Europe Frankfurt, Germany 10-11 November 2021
- **Transport Layer Security (TLS)**
  - **Deprecating TLS 1.0 and TLS 1.1 – RFC 8996 – March 2021**
    https://datatracker.ietf.org/doc/rfc8996/
  - **Deprecating FFDH Ciphersuites in TLS – draft-00 – July 2021**
    https://datatracker.ietf.org/doc/draft-bartle-tls-deprecate-ffdh/
  - **Identity Module for TLS Version 1.3 – draft-05 – July 2021**
    https://datatracker.ietf.org/doc/draft-urien-tls-im/
  - **Hybrid key exchange in TLS 1.3 – draft-03 – July 2021**
    https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/
  - **Flags Extension for TLS 1.3 – draft-06 – July 2021**
    https://datatracker.ietf.org/doc/draft-ietf-tls-tlsflags/
  - **Compact TLS 1.3 – draft-03 – July 2021**
    https://datatracker.ietf.org/doc/draft-ietf-tls-ctls/
  - **Deprecating Obsolete Key Exchange Methods in TLS – draft-00 – July 2021**
    https://datatracker.ietf.org/doc/draft-aviram-tls-deprecate-obsolete-kex/
  - **Bootstrapped TLS Authentication – draft-03 – July 2021**
    https://datatracker.ietf.org/doc/draft-friel-tls-eap-dpp/
  - **Secure Negotiation of Incompatible Protocols in TLS – draft-02 – July 2021**
    https://datatracker.ietf.org/doc/draft-thomson-tls-snip/
  - **TLS Encrypted Client Hello – draft-07 – July 2021**
    https://datatracker.ietf.org/doc/draft-ietf-tls-esni/
  - **TLS Extension for DANE Client Identity – draft-05 – July 2021**
    https://datatracker.ietf.org/doc/draft-huque-tls-dane-clientid/

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

- **Security Automation and Continuous Monitoring (SACM)**
  - **Concise Software Identifiers – draft-18 – July 2021 – to IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/
  - **SACM Architecture – draft-13 – July 2021**
    https://datatracker.ietf.org/doc/draft-ietf-sacm-arch/
- **Concise Binary Object Representation (CBOR)**
  - **CBOR Tags for OIDs – RFC 9090 – July 2021**
    https://datatracker.ietf.org/doc/rfc9090/
  - **Storing CBOR items on stable storage – draft-03 – August 2021 – to IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-file-magic/
  - **CBOR tags for IPv4 and IPv6 addresses – draft-07 – August 2021 – to IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-network-addresses/
  - **Additional Control Operators for CDDL – draft-05 – July 2021**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-cddl-control/
  - **Feature Freezer for CDDL – draft-08 – June 2021**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-freezer/
  - **Map-like data in CBOR and CDDL – draft-01 – June 2021**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-map-like-data/
  - **CBOR Tags for Time, Duration, and Period – draft-00 – May 2021**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-time-tag/
  - **Packed CBOR – draft-02 – February 2021**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-packed/

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

- **Remote ATtestation ProcedureS (RATS)**
  - **YANG Data Model for CHARRA using TPMs – draft-09 – July 2021**
    https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/
  - **TPM-based Network Device RIV – draft-08 – July 2021**
    https://datatracker.ietf.org/doc/draft-ietf-rats-tpm-based-network-device-attest/
  - **Reference Interaction Models for RATS – draft-04 – July 2021**
    https://datatracker.ietf.org/doc/draft-ietf-rats-reference-interaction-models/
  - **Concise Reference Integrity Manifest – draft-01 – July 2021**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-corim/
  - **CBOR Tag for Unprotected CWT Claims Sets – draft-01 – July 2021**
    https://datatracker.ietf.org/doc/draft-ietf-rats-uccs/
  - **Time-Based Uni-Directional Attestation – draft-05 – July 2021**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-tuda/
  - **Trustworthiness Vectors for SUIT – draft-02 – July 2021**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-suit-claims/
  - **ARM's PSA Attestation Verifier Endorsements – draft-00 – July 2021**
    https://datatracker.ietf.org/doc/draft-xyz-rats-psa-endorsements/
  - **Direct Anonymous Attestation for RATS – draft-01 – July 2021**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-daa/
  - **Attestation Results for Secure Interactions – draft-01 – June 2021**
    https://datatracker.ietf.org/doc/draft-voit-rats-attestation-results/
  - **Entity Attestation Token (EAT) – draft-10 – June 2021**
    https://datatracker.ietf.org/doc/draft-ietf-rats-eat/
  - **Trusted Path Routing – draft-03 – May 2021**
    https://datatracker.ietf.org/doc/draft-voit-rats-trustworthy-path-routing/
  - **Attestation Event Stream Subscription – draft-02 – March 2021**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-network-device-subscription/
  - **RATS Architecture – draft-11 – March 2021**
    https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/

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

- **IRTF Crypto Forum Research Group (CFRG) – future algorithms**
  - **Hashing to Elliptic Curves – draft-11 – April 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve/
  - **Argon2 password hash and proof-of-work – draft-13 – March 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-argon2/
  - **Usage Limits on AEAD Algorithms – draft-02 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-aead-limits/
  - **OPAQUE Asymmetric PAKE Protocol – draft-03 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-opaque/
  - **OPRFs using Prime-Order Groups – draft-06 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-voprf/
  - **KangarooTwelve – draft-05 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-kangarootwelve/
  - **Hybrid Public Key Encryption – draft-08 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-hpke/
  - **FROST: Flexible Round-Optimized Schnorr Threshold Signatures – draft-00 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-frost/
  - **CPace, a balanced composable PAKE – draft-01 – January 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-cpace/

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

- **IRTF Crypto Forum Research Group (CFRG) – future algorithms**
  - **Ristretto255 and Decaf448 Groups – draft-01 – August 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-ristretto255-decaf448/
  - **Hybrid Public Key Encryption – draft-11 – August 2021 – to IRSG review**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-hpke/
  - **RSA Blind Signatures – draft-02 – August 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-rsa-blind-signatures/
  - **Pairing-Friendly Curves – draft-10 – July 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-pairing-friendly-curves/
  - **CPace, a balanced composable PAKE – draft-02 – July 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-cpace/
  - **OPAQUE Asymmetric PAKE Protocol – draft-06 – July 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-opaque/
  - **Usage Limits on AEAD Algorithms – draft-03 – July 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-aead-limits/
  - **OPRFs using Prime-Order Groups – draft-07 – July 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-voprf/
  - **SPAKE2+, an Augmented PAKE – draft-03 – July 2021**
    https://datatracker.ietf.org/doc/draft-bar-cfrg-spake2plus/
  - **Deterministic Nonce-less Hybrid Public Key Encryption – draft-00 – June 2021**
    https://datatracker.ietf.org/doc/draft-harkins-cfrg-dnhpke/
  - **SPAKE2, a PAKE – draft-20 – June 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-spake2/
  - **Verifiable Random Functions (VRFs) – draft-09 – May 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-vrf/
  - **Hashing to Elliptic Curves – draft-11 – April 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve/
  - **Argon2 password hash and proof-of-work – draft-13 – March 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-argon2/

Next Steps – IDS WG

- Next IDS WG Meeting– Sep 2, 2021
- Next IDS Face-to-Face Meeting November 9-11, 2021 (probably November 11th) at next PWG Virtual F2F
- Start looking at involvement in some of these other standards activities individually and maybe as a WG