



# The Printer Working Group

IDS Liaison Status – February 2024

Ira McDonald, PWG Secretary / IDS Editor  
February 15, 2024

# Trusted Computing Group (TCG)



- **Recent and Next TCG Members Meetings**
  - TCG Hybrid F2F (Kirkland, WA) – 24-26 October 2023 – Ira called in
  - TCG Hybrid F2F (Tokyo, Japan) – 27-29 February 2024 – Ira to call in
  - TCG Hybrid F2F (Athens, Greece) – 4-6 2024 – Ira cannot attend (GP CSVF/ ESCAR USA / UPTANE same week)
- **Trusted Mobility Solutions (TMS) – Ira is co-chair and co-editor**
  - Formal Liaisons – GP (TEE, SE, TPS), ETSI (NFV/SAI Security and Privacy)
  - Informal Liaisons – 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 and Informal Liaisons – jointly with TMS WG above
  - *TCG Mobile Reference Architecture v2 – published August 2023*
  - *TCG TPM 2.0 Mobile Common Profile v2 – work-in-progress resumed in Q1 2024*
  - *TCG MARS 1.0 Mobile Profile – new work-in-progress Q4 2023*
  - *GP TPS Client API / Entity Attestation Protocol / COSE Keystore – joint work*
- **Recent Specifications**
  - <http://www.trustedcomputinggroup.org/resources>
  - *TCG Platform Certificate Profile v2 – public review February 2024*
  - *TCG MARS Serialization Interface v1 – published January 2024*
  - *TCG Hardware Requirements for a DICE v1 – public review January 2024*
  - *TCG Technologies for Device Identification and Attestation v1.0 – public review January 2024*
  - *TCG Trusted Platform Module Library v2.0 r1.81 – public review December 2023*
  - *TCG ACPI Specification v1.4 r14 – public review November 2023*
  - *TCG PC Client Reference Integrity Manifest v1.1 – public review October 2023*

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



- **Recent and Next IETF Members Meetings**

- IETF 118 Hybrid F2F (Prague, Czech Republic) – 6-10 November 2023 – Ira called in
- IETF 119 Hybrid F2F (Brisbane, Australia) – 18-22 March 2024 – Ira to call in
- IETF 120 Hybrid F2F (Vancouver, Canada) – 22-26 July 2024 – Ira to call in

- **Transport Layer Security (TLS)**

- IETF Delegated Credentials for TLS and DTLS – RFC 9345 – July 2023  
<https://datatracker.ietf.org/doc/rfc9345/>
- IETF Exported Authenticators in TLS – RFC 9261 – July 2022  
<https://datatracker.ietf.org/doc/rfc9261/>
- IETF Identity Module for TLS Version 1.3 – draft-10 – January 2024  
<https://datatracker.ietf.org/doc/draft-urien-tls-im/>
- IETF SSLKEYLOGFILE Format for TLS – draft-00 – January 2024  
<https://datatracker.ietf.org/doc/draft-ietf-tls-keylogfile/>
- IETF IANA Registry Updates for TLS and DTLS – draft-08 – January 2024  
<https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8447bis/>
- IETF TLS 1.3 Extension for Using Certificates with External PSK – draft-01 – January 2024  
<https://datatracker.ietf.org/doc/draft-ietf-tls-8773bis/>
- IETF Extended Key Update for TLS 1.3 – draft-00 – January 2024  
<https://datatracker.ietf.org/doc/draft-tschofenig-tls-extended-key-update/>
- IETF AEGIS-based Cipher Suites for TLS 1.3, DTLS 1.3 and QUIC – draft-01 – December 2023  
<https://datatracker.ietf.org/doc/draft-denis-tls-aegis/>
- IETF PEM file format for Encrypted Client Hello (ECH) – draft-06 – December 2023  
<https://datatracker.ietf.org/doc/draft-farrell-tls-pemesni/>
- IETF Legacy RSASSA-PKCS1-v1\_5 codepoints for TLS 1.3 – draft-00 – November 2023  
<https://datatracker.ietf.org/doc/draft-ietf-tls-tls13-pkcs1/>



- **Concise Binary Object Representation (CBOR)**

- IETF CBOR Ext Diagnostic Notation – draft-08 – February 2024 – Waiting for Writeup  
<https://datatracker.ietf.org/doc/draft-ietf-cbor-edn-literals/>
- IETF CBOR Time, Duration, Period – draft-12 – January 2024 – RFC Editor  
<https://datatracker.ietf.org/doc/draft-ietf-cbor-time-tag/>
- IETF Updates to the CDDL grammar of RFC 8610 – draft-03 – January 2024 – IETF Last Call  
<https://datatracker.ietf.org/doc/draft-ietf-cbor-update-8610-grammar/>
- IETF Constrained Resource Identifiers – draft-14 – January 2024 - Waiting for WG Chair  
<https://datatracker.ietf.org/doc/draft-ietf-core-href/>
- IETF Packed CBOR – draft-10 – January - Waiting for WG Chair  
<https://datatracker.ietf.org/doc/draft-ietf-cbor-packed/>
- IETF CBOR Common Deterministic Encoding (CDE) – draft-01 – January 2024  
<https://datatracker.ietf.org/doc/draft-ietf-cbor-cde/>
- IETF dCBOR: A Deterministic CBOR Application Profile – draft-07 – January 2024  
<https://datatracker.ietf.org/doc/draft-mcnally-deterministic-cbor/>

- **Network Time Protocols (NTP)**

- IETF NTPv5 Use Cases and Requirements – draft-04 – January 2024 – WG Last Call  
<https://datatracker.ietf.org/doc/draft-ietf-ntp-ntp5-requirements/>
- IETF NTP Over PTP – draft-02 – January 2024 – WG Last Call  
<https://datatracker.ietf.org/doc/draft-ietf-ntp-over-ntp/>
- IETF Secure Selection and Filtering for NTP with Khronos – draft-25 – January 2024 – RFC Editor AUTH-48  
<https://datatracker.ietf.org/doc/draft-ietf-ntp-chronos/>
- IETF Updating the NTP Registries – draft-13 – December 2023 – IETF Last Call  
<https://datatracker.ietf.org/doc/draft-ietf-ntp-update-registries/>
- IETF Network Time Protocol v5 – draft-01 – October 2023  
<https://datatracker.ietf.org/doc/draft-ietf-ntp-ntp5/>



## • Remote ATtestation ProcedureS (RATS)

- IETF RATS Architecture – RFC 9334 – January 2023  
<https://datatracker.ietf.org/doc/rfc9334/>
- IETF RATS Conceptual Messages Wrapper – draft-03 – January 2024  
<https://datatracker.ietf.org/doc/draft-ietf-rats-msg-wrap/> – WG Adopted
- IETF Proximate Location Claim – draft-01 – January 2024  
<https://datatracker.ietf.org/doc/draft-mandyam-rats-proxlocclaim/>
- IETF CBOR Tag for Unprotected CWT Claims Sets – draft-08 – January 2024 – IETF Last Call  
<https://datatracker.ietf.org/doc/draft-ietf-rats-uccs/>
- IETF Entity Attestation Token (EAT) – draft-25 – January 2024 – RFC Editor  
<https://datatracker.ietf.org/doc/draft-ietf-rats-eat/>
- IETF Intel Profile for CoRIM – draft-01 – December 2023  
<https://datatracker.ietf.org/doc/draft-cds-rats-intel-corim-profile/>
- IETF ARM PSA Attestation Token – draft-20 – December 2023  
<https://datatracker.ietf.org/doc/draft-tschofenig-rats-psa-token/>
- IETF Concise TA Stores (CoTS) – draft-02 – December 2023  
<https://datatracker.ietf.org/doc/draft-ietf-rats-concise-ta-stores/> – WG Adopted
- IETF RATS Endorsements – draft-00 – December 2023  
<https://datatracker.ietf.org/doc/draft-ietf-rats-endorsements/> – WG Adopted
- IETF EAT Media Types – draft-05 – November 2023  
<https://datatracker.ietf.org/doc/draft-ietf-rats-eat-media-type/>
- IETF Epoch Markers – draft-06 – October 2023  
<https://datatracker.ietf.org/doc/draft-birkholz-rats-epoch-markers/>
- IETF X.509-based Attestation Evidence – draft-00 – October 2023  
[X.509-based Attestation Evidence](#)



- **IRTF Crypto Forum Research Group (CFRG) – future algorithms**
  - **IRTF SPAKE2, a Password-Authenticated Key Exchange – RFC 9382 – September 2023**  
<https://datatracker.ietf.org/doc/rfc9382/>
  - **IRTF Verifiable Random Functions (VRFs) – RFC 9381 – August 2023**  
<https://datatracker.ietf.org/doc/rfc9381/>
  - **IRTF Hashing to Elliptic Curves – RFC 9380 – August 2023**  
<https://datatracker.ietf.org/doc/rfc9380/>
  - **IRTF RSA Blind Signatures – RFC 9474 – October 2023**  
<https://datatracker.ietf.org/doc/rfc9474/>
  - **IRTF KangarooTwelve and TurboSHAKE – draft-13 – February 2024**  
<https://datatracker.ietf.org/doc/draft-irtf-cfrg-kangarootwelve/>
  - **IRTF Deterministic Nonce-less Hybrid Public Key Encryption – draft-04 – February 2024**  
<https://datatracker.ietf.org/doc/draft-irtf-cfrg-dnhpke/>
  - **IRTF Properties of AEAD algorithms – draft-03 – February 2024**  
<https://datatracker.ietf.org/doc/draft-irtf-cfrg-aead-properties/>
  - **IRTF Combiner Function for Hybrid KEMs – draft-05 – January 2024**  
<https://datatracker.ietf.org/doc/draft-ounsworth-cfrg-kem-combiners/>
  - **IRTF X-Wing: General-Purpose Hybrid Post-Quantum KEM – draft-01 – January 2024**  
<https://datatracker.ietf.org/doc/draft-conolly-cfrg-xwing-kem/>
  - **IRTF Key Blinding for Signature Schemes – draft-05 – January 2024**  
<https://datatracker.ietf.org/doc/draft-irtf-cfrg-signature-key-blinding/>
  - **IRTF AEGIS Family of Authenticated Encryption Algorithms – draft-10 – January 2024**  
<https://datatracker.ietf.org/doc/draft-irtf-cfrg-aegis-aead/>
  - **IRTF Partially Blind RSA Signatures – draft-02 – January 2024**  
<https://datatracker.ietf.org/doc/draft-amjad-cfrg-partially-blind-rsa/>