CFRG
Research Group Status

IETF 119 Brisbane

Chairs:

Stanislav Smyshlyaev <smyshsv@gmail.com>

Nick Sullivan <nicholas.sullivan@gmail.com>

Alexey Melnikov <alexey.melnikov@isode.com>

Administrative

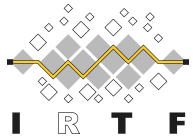
- This session is being recorded
- Minute taker in HedgeDoc
- Jabber comment relay

Participant guide: https://www.ietf.org/how/meetings/technology/meetecho-guide-participant/
Request assistance and report issues via: http://www.ietf.org/how/meetings/issues/

Bluesheets are automatically generated based on IETF Datatracker information

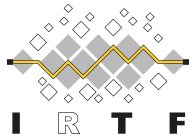
Minutes: **https://notes.ietf.org/notes-ietf-119-cfrg**

Note Well – Intellectual Property



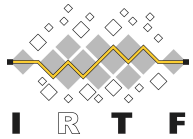
- **The IRTF follows the IETF Intellectual Property Rights (IPR) disclosure rules**
- By participating in the IRTF, you agree to follow IRTF processes and policies:
  - If you are aware that any IRTF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion
  - The IRTF expects that you file such IPR disclosures in a timely manner – in a period measured in days or weeks, not months
  - The IRTF prefers that the most liberal licensing terms possible are made available for IRTF Stream documents – see RFC 5743
  - Definitive information is in RFC 5378 (Copyright) and RFC 8179 (Patents, Participation), substituting IRTF for IETF, and at https://irtf.org/policies/ipr

Note Well – Privacy & Code of Conduct



- As a participant in, or attendee to, any IRTF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public
- Personal information that you provide to IRTF will be handled in accordance with the Privacy Policy at https://www.ietf.org/privacy-policy/
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this
- See RFC 7154 (Code of Conduct) and RFC 7776 (Anti-Harassment Procedures), which also apply to IRTF

Goals of the IRTF



- The Internet Research Task Force (IRTF) focuses on longer term research issues related to the Internet while the parallel organisation, the IETF, focuses on shorter term issues of engineering and standards making

- **The IRTF conducts research; it is not a standards development organisation**

- While the IRTF can publish informational or experimental documents in the RFC series, its primary goal is to promote development of research collaboration and teamwork in exploring research issues related to Internet protocols, applications, architecture, and technology
- See “An IRTF Primer for IETF Participants” – RFC 7418

CFRG Research Group

Online Agenda and Slides at:

https://datatracker.ietf.org/meeting/119/session/cfrg

Data tracker: https://datatracker.ietf.org/rg/cfrg/documents

Agenda

https://datatracker.ietf.org/meeting/119/session/cfrg

Chairs: Stanislav Smyshlyaev, Nick Sullivan and Alexey Melnikov

13:00 - Chairs' update (5 mins).

13:05 - John Mattson, "Hedged Signatures" (5+5 mins)

13:15 - John Mattson, "GCM-SST" (10+5 mins)

13:30 - Deirdre Connolly, "ML-KEM for HPKE" (10+5 mins)

13:45 - Chris Patton, "Next steps for draft-mouris-cfrg-mastic" (10+5 mins)

14:00 - Junye Chen, "PINE, a VDAF for federated machine learning" (5+5 mins)

14:10 - Mike Ounsworth, "Why P-256 and RSA hybrids are needed in industry" (5+5 mins)

14:20 - John Bradley, "The Asynchronous Remote Key Generation (ARKG) algorithm" (5+5 mins)

14:30 - AOB

Muhammad Usama Sardar, “Formal Analysis of RA-TLS”, (10+5 mins) - if time permits

RG Document Status

Document Status (1 of 3)

- New RFC (since November)
  - RFC 9496 (draft-irtf-cfrg-ristretto255-decaf448): The ristretto255 and decaf448 Groups
  - RFC 9497 (draft-irtf-cfrg-voprf): Oblivious Pseudorandom Functions (OPRFs) using Prime-Order Groups
- In RFC Editor's queue
  - draft-irtf-cfrg-frost-15: FROST: Flexible Round-Optimized Schnorr Threshold Signatures

- In IESG review
  - None
- In IRSG review
  - None
- Waiting for IRTF Chair
  - draft-irtf-cfrg-kangarootwelve-13: KangarooTwelve eXtendable Output Function

Document Status (2 of 3)

- Active CFRG drafts
  - draft-irtf-cfrg-aead-properties-04 (**updated, in RGLC**): Properties of AEAD algorithms
  - draft-fluhrer-lms-more-parm-sets-11 (**in RGLC**): Additional Parameter sets for LMS Hash-Based Signatures
  - draft-irtf-cfrg-dnhpke-04 (**updated, RGLC ended, needs shepherd followup**): Deterministic Nonce-less Hybrid Public Key Encryption
  - draft-irtf-cfrg-opaque-13 (**updated, in RGLC**): The OPAQUE Asymmetric PAKE Protocol

  - draft-irtf-cfrg-det-sigs-with-noise-02 **(updated)**: Deterministic ECDSA and EdDSA Signatures with Additional Randomness
  - draft-irtf-cfrg-signature-key-blinding-05 (**updated**): Key Blinding for Signature Schemes
  - draft-irtf-aegis-aead-10 (**updated**): The AEGIS family of authenticated encryption algorithms
  - draft-irtf-cfrg-bbs-signatures-05 (**updated**): The BBS Signature Scheme
  - draft-irtf-cfrg-cpace-10 (**expires soon**): CPace, a balanced composable PAKE
  - draft-irtf-cfrg-vdaf-08: Verifiable Distributed Aggregation Functions

Document Status (3 of 3)

- Recently adopted documents
  - draft-irtf-cfrg-rsa-guidance-00: Implementation Guidance for PKCS1 RSA Cryptography Specification
  - Hybrid PQ KEM: Topic adopted, design team being formed to compile requirements
- Documents in adoption call
  - None
- Expired
  - draft-irtf-cfrg-cipher-catalog-01: Ciphers in Use in the Internet
  - draft-irtf-cfrg-webcrypto-algorithms-00: Security Guidelines for Cryptographic Algorithms in the W3C Web Cryptography AP
  - draft-irtf-cfrg-augpake-09: Augmented Password-Authenticated Key Exchange (AugPAKE)
  - draft-hoffman-rfc6090bis-02: Fundamental Elliptic Curve Cryptography Algorithms
  - draft-irtf-cfrg-xchacha-03: XChaCha: eXtended-nonce ChaCha and AEAD_XChaCha20_Poly1305
  - **draft-irtf-cfrg-aead-limits-07**: Usage Limits on AEAD Algorithms
  - **draft-irtf-cfrg-bls-signature-05**: BLS Signatures
  - **draft-irtf-cfrg-pairing-friendly-curves-11**: Pairing-Friendly Curves
  - **draft-irtf-cfrg-cryptography-specification-00**: Guidelines for Writing Cryptography Specifications

Crypto Review Panel

- Formed in September 2016
  - Wiki page for the team: <https://wiki.ietf.org/group/cfrg/CryptoPanel>
- May be used to review documents coming to CFRG, Security Area or Independent Stream.
- CFRG chairs ask for reviews from Crypto Review Panel before RGLC for CFRG documents.
- **Current members (March 2024 – February 2026**):
  - **Stephen Farrell,** Scott Fluhrer, Russ Housley, Chloe Martindale, Julia Hesse, Karthikeyan Bhargavan, Thomas Pornin, Jon Callas, Virendra Kumar

AOB