CFRG
Research Group Status

IETF 116 Yokohama

Chairs:

Alexey Melnikov <alexey.melnikov@isode.com>

Nick Sullivan <nick@cloudflare.com>

Stanislav Smyshlyaev <smyshsv@gmail.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-116-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 – Audio and Video Recordings

- The IRTF routinely makes recordings of online and in-person meetings, including audio, video and photographs, and publishes those recordings online
- If you participate in-person and choose not to wear a red “do-not-photograph” lanyard, then you consent to appear in such recordings, and if you speak at a microphone, appear on a panel, or carry out an official duty as a member of IRTF leadership then you consent to appearing in recordings of you at that time
- If you participate online, and turn on your camera and/or microphone, then you consent to appear in such recordings
- **This meeting is being recorded and live streamed**

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 – whether in-person or remote, and on the mailing lists as well as during the meetings – 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

IETF 116 Meeting Tips

In-person participants

- Make sure to sign into the session using the Meetecho (usually the “Meetecho lite” client) from the Datatracker agenda
- Use Meetecho to join the mic queue
- Keep audio and video off if not using the onsite version
- **Wear masks unless actively speaking at the microphone.**

Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session
- Use of a headset is strongly recommended

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, the primary output of research groups is expected to be understanding and research results that may be disseminated by publication in scholarly journals and conferences
- See “An IRTF Primer for IETF Participants” – RFC 7418

CFRG Research Group

Online Agenda and Slides at:

https://datatracker.ietf.org/meeting/116/session/cfrg

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

Agenda

https://datatracker.ietf.org/meeting/116/session/cfrg

Chairs: Stanislav Smyshlyaev, Nick Sullivan and Alexey Melnikov

09:30 - Chairs' update (5 mins).

09:35 - Nick Sullivan, "Guidelines for writing cryptography specifications" (5+5 mins)

09:45 - Ted Eaton, "Key blinding for signature schemes" (10+5 mins)

10:00 - Phillipp Schoppmann, "VDAF" (10+5 mins)

10:15 - Tobias Looker, "The BBS Signature Scheme" (5+5 mins)

10:25 - Andrey Bozhko, "Properties of AEAD algorithms" (5+5 mins)

10:35 - Yuto Nakano, “Rocca-S” (5+5 mins)

10:45 - Ghous Amjad, “RSA Blind Signatures with Public Metadata” (10+5 mins)

11:00 - Dimitris Mouris, “PLASMA (VDAF-related protocol)” (10+5 mins)

11:15 - Mike Ounsworth, "KEM-combiners" (5+5 mins)

11:25 - AOB

RG Document Status

Document Status (1/2)

- New RFC (since November)
  - None
- In RFC Editor's queue (since November)
  - draft-irtf-cfrg-hash-to-curve-16 (**RFC-EDITOR**): Hashing to Elliptic Curves
  - draft-irtf-cfrg-spake2-26 (**RFC-EDITOR*R, Hash-to-Curve**): SPAKE2, a PAKE
  - draft-irtf-cfrg-vrf-15 (**RFC-EDITOR*R, Hash-to-Curve**): Verifiable Random Functions (VRFs)
- In IESG review
  - draft-irtf-cfrg-voprf-21 (**updated, RGLC concluded, shepherd writeup done, IRSG review concluded, IESG Review Completed, waiting for IRTF Chair**): Oblivious Pseudorandom Functions (OPRFs) using Prime-Order Groups
- In IRSG review
  - draft-irtf-cfrg-rsa-blind-signatures-11 (**updated, RGLC concluded, shepherd writeup done, revised I-D needed to address minor comments in the IRSG review**): RSA Blind Signatures
  - draft-irtf-cfrg-ristretto255-decaf448-06 (**updated, RGLC concluded, shepherd writeup done, revised I-D needed to address minor comments in the IRSG review**): The ristretto255 and decaf448 Groups
- Waiting for IRTF Chair
  - draft-irtf-cfrg-frost-12 (**updated, RGLC concluded, shepherd writeup done)** Two-Round Threshold Schnorr Signatures with FROST

Document Status (2/2)

- Active CFRG drafts
  - draft-fluhrer-lms-more-parm-sets-09 (**updated, in RGLC**): Additional Parameter sets for LMS Hash-Based Signatures
  - draft-irtf-cfrg-aead-limits-06 (**updated**): Usage Limits on AEAD Algorithms
  - draft-irtf-cfrg-aegis-aead-01 (**updated**): The AEGIS family of authenticated encryption algorithms
  - draft-irtf-cfrg-vdaf-05 (**updated**): Verifiable Distributed Aggregation Functions
  - draft-irtf-cfrg-bbs-signatures-02 (**updated**): The BBS Signature Scheme
  - draft-irtf-cfrg-cpace-07 (**updated**): CPace, a balanced composable PAKE
  - draft-irtf-cfrg-opaque-10 (**updated**): The OPAQUE Asymmetric PAKE Protocol
  - draft-irtf-cfrg-kangarootwelve-10 (**updated**, **RGLC unsuccessful**): KangarooTwelve and TurboSHAKE
  - draft-irtf-cfrg-signature-key-blinding-03 (**updated**): Key Blinding for Signature Schemes
  - draft-irtf-cfrg-pairing-friendly-curves-11 (unchanged): Pairing-Friendly Curves
  - draft-irtf-cfrg-aead-properties-01 (**adopted**): Properties of AEAD algorithms
  - draft-irtf-cfrg-dnhpke-00 (**adopted**): Deterministic Nonce-less Hybrid Public Key Encryption
- Expired (after 2020):

  draft-irtf-cfrg-det-sigs-with-noise-00: Deterministic ECDSA and EdDSA Signatures with Additional Randomness

  draft-irtf-cfrg-bls-signature-05: BLS Signature Scheme

  draft-hoffman-c2pq-07: The Transition from Classical to Post-Quantum Cryptography

  draft-irtf-cfrg-xchacha-03: XChaCha: eXtended-nonce ChaCha and AEAD_XChaCha20_Poly1305

AOB