

CFRG Research Group Status

IETF 117 San Francisco

Chairs:

Alexey Melnikov <alexey.melnikov@isode.com>

Nick Sullivan <nicholas.sullivan+ietf@gmail.com>

Stanislav Smyshlyaev <smyshsv@gmail.com>

Administrative

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

Participant guide:

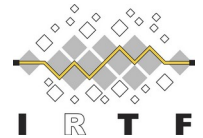
<https://www.ietf.org/how/meetings/technology/meetecho-guide-participant/>

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-117-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



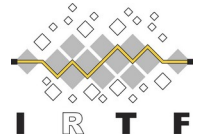
- The IRTF routinely makes recordings of online and in-person meetings, including audio, video and photographs, and publishes those recordings online
- If you participate in-person and choose not to wear a red “do-not-photograph” lanyard, then you consent to appear in such recordings, and if you speak 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 117 Meeting Tips

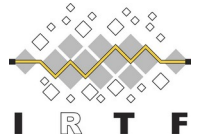


In-person participants

- 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/117/session/cfrg>

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

Agenda

<https://datatracker.ietf.org/meeting/117/session/cfrg>

Chairs: Alexey Melnikov, Stanislav Smyshlyaev and Nick Sullivan

15:00 - Chairs' update (5 mins).

15:05 - Nick Sullivan, "Guidelines for writing cryptography specifications" (5+5 mins)

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

15:30 - Frank Denis, "AEGIS" (5 mins)

15:35 - Scott Fluhrer, "LMS parameter sets" (5 mins)

15:40 - Andrey Bozhko, "Properties of AEAD algorithms" (5 mins)

15:45 - Dan Harkins, "Deterministic Nonce-less Hybrid Public Key Encryption" (5+5 mins)

15:55 - Bjoern Haase, "CPace" (5 mins)

16:00 - Kevin Lewi, "OPAQUE" (5+5 mins)

16:10 - Joe Harvey, "Merkle Tree Ladder Mode" (10+5 mins)

16:25 - Aron Wussler, "KEM-combiners" (5 mins)

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 (**AUTH48**): Hashing to Elliptic Curves
 - draft-irtf-cfrg-spake2-26 (**AUTH48**): SPAKE2, a PAKE
 - draft-irtf-cfrg-vrf-15 (**AUTH48-DONE**): Verifiable Random Functions (VRFs)
 - draft-irtf-cfrg-voprf-21 (**EDIT**): Oblivious Pseudorandom Functions (OPRFs) using Prime-Order Groups
 - draft-irtf-cfrg-ristretto255-decaf448-07 (**EDIT**): The ristretto255 and decaf448 Groups
 - draft-irtf-cfrg-rsa-blind-signatures-14 (**EDIT, updated**): RSA Blind Signatures
- In IESG review
 - None
- In IRSG review
 - draft-irtf-cfrg-frost-14 (**updated**) Two-Round Threshold Schnorr Signatures with FROST
- Waiting for IRTF Chair
 - None

Document Status (2/2)

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

AOB